Modicon M580

Manuale di sicurezza

Traduzione delle istruzioni originali

QGH46985.06
06/2024

www.se.com

Informazioni di carattere legale

Le informazioni contenute nel presente documento contengono descrizioni generali, caratteristiche tecniche e/o raccomandazioni relative ai prodotti/soluzioni.

Il presente documento non è inteso come sostituto di uno studio dettagliato o piano schematico o sviluppo specifico del sito e operativo. Non deve essere utilizzato per determinare idoneità o affidabilità dei prodotti/soluzioni per applicazioni specifiche dell'utente. Spetta a ciascun utente eseguire o nominare un esperto professionista di sua scelta (integratore, specialista o simile) per eseguire un'analisi del rischio completa e appropriata, valutazione e test dei prodotti/soluzioni in relazione all'uso o all'applicazione specifica.

Sommario

Informazioni di sicurezza

Informazioni importanti

Leggere attentamente queste istruzioni e osservare l'apparecchiatura per familiarizzare con i suoi componenti prima di procedere ad attività di installazione, uso, assistenza o manutenzione. I seguenti messaggi speciali possono comparire in diverse parti della documentazione oppure sull'apparecchiatura per segnalare rischi o per richiamare l'attenzione su informazioni che chiariscono o semplificano una procedura.

L'aggiunta di questo simbolo a un'etichetta di “Pericolo” o “Avvertimento” indica che esiste un potenziale pericolo da shock elettrico che può causare lesioni personali se non vengono rispettate le istruzioni.

Questo simbolo indica un possibile pericolo. È utilizzato per segnalare all'utente potenziali rischi di lesioni personali. Rispettare i messaggi di sicurezza evidenziati da questo simbolo per evitare da lesioni o rischi all'incolumità personale.

⚠ PERICOLO

PERICOLO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

⚠ AVVERTIMENTO

AVVERTIMENTO indica una situazione di potenziale rischio che, se non evitata, **può provocare** morte o gravi infortuni.

⚠ ATTENZIONE

ATTENZIONE indica una situazione di potenziale rischio che, se non evitata, **può provocare** ferite minori o leggere.

AVVISO

Un ***AVVISO*** è utilizzato per affrontare delle prassi non connesse all'incolumità personale.

Nota

Manutenzione, riparazione, installazione e uso delle apparecchiature elettriche si devono affidare solo a personale qualificato. Schneider Electric non si assume alcuna responsabilità per qualsiasi conseguenza derivante dall'uso di questo materiale.

Il personale qualificato è in possesso di capacità e conoscenze specifiche sulla costruzione, il funzionamento e l'installazione di apparecchiature elettriche ed è addestrato sui criteri di sicurezza da rispettare per poter riconoscere ed evitare le condizioni a rischio.

Prima di iniziare

Non utilizzare questo prodotto su macchinari privi di sorveglianza attiva del punto di funzionamento. La mancanza di un sistema di sorveglianza attivo sul punto di funzionamento può presentare gravi rischi per l'incolumità dell'operatore macchina.

⚠AVVERTIMENTO

APPARECCHIATURA NON PROTETTA

- Non utilizzare questo software e la relativa apparecchiatura di automazione su macchinari privi di protezione per le zone pericolose.
- Non avvicinarsi ai macchinari durante il funzionamento.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Questa apparecchiatura di automazione con il relativo software permette di controllare processi industriali di vario tipo. Il tipo o il modello di apparecchiatura di automazione adatto per ogni applicazione varia in funzione di una serie di fattori, quali la funzione di controllo richiesta, il grado di protezione necessario, i metodi di produzione, eventuali condizioni particolari, la regolamentazione in vigore, ecc. Per alcune applicazioni può essere necessario utilizzare più di un processore, ad esempio nel caso in cui occorra garantire la ridondanza dell'esecuzione del programma.

Solo l'utente, il costruttore della macchina o l'integratore del sistema sono a conoscenza delle condizioni e dei fattori che entrano in gioco durante l'installazione, la configurazione, il funzionamento e la manutenzione della macchina e possono quindi determinare l'apparecchiatura di automazione e i relativi interblocchi e sistemi di sicurezza appropriati. La scelta dell'apparecchiatura di controllo e di automazione e del relativo software per un'applicazione particolare deve essere effettuata dall'utente nel rispetto degli standard locali e nazionali e della regolamentazione vigente. Per informazioni in merito, vedere anche la guida National Safety Council's Accident Prevention Manual (che indica gli standard di riferimento per gli Stati Uniti d'America).

Per alcune applicazioni, ad esempio per le macchine confezionatrici, è necessario prevedere misure di protezione aggiuntive, come un sistema di sorveglianza attivo sul punto di funzionamento. Questa precauzione è necessaria quando le mani e altre parti del corpo dell'operatore possono raggiungere aree con ingranaggi in movimento o altre zone pericolose, con conseguente pericolo di infortuni gravi. I prodotti software da soli non possono proteggere l'operatore dagli infortuni. Per questo motivo, il software non può in alcun modo costituire un'alternativa al sistema di sorveglianza sul punto di funzionamento.

Accertarsi che siano stati installati i sistemi di sicurezza e gli asservimenti elettrici/meccanici opportuni per la protezione delle zone pericolose e verificare il loro corretto funzionamento prima di mettere in funzione l'apparecchiatura. Tutti i dispositivi di blocco e di sicurezza relativi alla sorveglianza del punto di funzionamento devono essere coordinati con l'apparecchiatura di automazione e la programmazione software.

NOTA: Il coordinamento dei dispositivi di sicurezza e degli asservimenti meccanici/elettrici per la protezione delle zone pericolose non rientra nelle funzioni della libreria dei blocchi funzione, del manuale utente o di altre implementazioni indicate in questa documentazione.

Avviamento e verifica

Prima di utilizzare regolarmente l'apparecchiatura elettrica di controllo e automazione dopo l'installazione, l'impianto deve essere sottoposto ad un test di avviamento da parte di personale qualificato per verificare il corretto funzionamento dell'apparecchiatura. È importante programmare e organizzare questo tipo di controllo, dedicando ad esso il tempo necessario per eseguire un test completo e soddisfacente.

⚠ AVVERTIMENTO

RISCHI RELATIVI AL FUNZIONAMENTO DELL'APPARECCHIATURA

- Verificare che tutte le procedure di installazione e di configurazione siano state completate.
- Prima di effettuare test sul funzionamento, rimuovere tutti i blocchi o altri mezzi di fissaggio dei dispositivi utilizzati per il trasporto.
- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Eseguire tutti i test di avviamento raccomandati sulla documentazione dell'apparecchiatura. Conservare con cura la documentazione dell'apparecchiatura per riferimenti futuri.

Il software deve essere testato sia in ambiente simulato che in ambiente di funzionamento reale..

Verificare che il sistema completamente montato e configurato sia esente da cortocircuiti e punti a massa, ad eccezione dei punti di messa a terra previsti dalle normative locali (ad esempio, in conformità al National Electrical Code per gli USA). Nel caso in cui sia necessario effettuare un test sull'alta tensione, seguire le raccomandazioni contenute nella documentazione dell'apparecchiatura al fine di evitare danni accidentali all'apparecchiatura stessa.

Prima di mettere sotto tensione l'apparecchiatura:

- Rimuovere gli attrezzi, i misuratori e i depositi dall'apparecchiatura.
- Chiudere lo sportello del cabinet dell'apparecchiatura.
- Rimuovere tutte le messa a terra temporanee dalle linee di alimentazione in arrivo.
- Eseguire tutti i test di avviamento raccomandati dal costruttore.

Funzionamento e regolazioni

Le precauzioni seguenti sono contenute nelle norme NEMA Standards Publication ICS 7.1-1995:

(In caso di divergenza o contraddizione tra una traduzione e l'originale inglese, prevale il testo originale in lingua inglese).

- Indipendentemente dalla qualità e della precisione del progetto nonché della costruzione dell'apparecchiatura o del tipo e della qualità dei componenti scelti, possono sussistere dei rischi se l'apparecchiatura non viene utilizzata correttamente.
- Eventuali regolazioni involontarie possono provocare il funzionamento non soddisfacente o non sicuro dell'apparecchiatura. Per effettuare le regolazioni funzionali, attenersi sempre alle istruzioni contenute nel manuale fornito dal costruttore. Il personale incaricato di queste regolazioni deve avere esperienza con le istruzioni fornite dal costruttore delle apparecchiature e con i macchinari utilizzati con l'apparecchiatura elettrica.
- All'operatore devono essere accessibili solo le regolazioni funzionali richieste dall'operatore stesso. L'accesso agli altri organi di controllo deve essere riservato, al fine di impedire modifiche non autorizzate ai valori che definiscono le caratteristiche di funzionamento delle apparecchiature.

Informazioni sul manuale

Scopo del documento

La presente documentazione è dedicata a personale qualificato con conoscenze dei sistemi di sicurezza funzionale e Control Expert Safety. Messa in servizio e funzionamento del sistema M580 Safety possono essere eseguiti solo da personale adeguatamente formato autorizzato a mettere in servizio e a utilizzare i sistemi in conformità con gli standard di sicurezza funzionale.

NOTA:

- La versione originale del presente manuale è la versione inglese.
- In caso di richiesta di sostituzione o di problemi di qualità relativi all'offerta M580 Safety, rivolgersi al Centro assistenza clienti locale per assistenza tecnica. Ulteriori informazioni sono disponibili nella sezione *Supporto / I nostri contatti* del sito Web di Schneider Electric al seguente indirizzo:

  www.se.com/b2b/en/support/

Nota di validità

Questo documento è valido per EcoStruxure™ Control Expert 16.0 con ControlExpert_V160_HF001 M580 Safety o successiva.

Per informazioni circa le norme ambientali e la conformità dei prodotti (RoHS, REACH, PEP, EOLI, e così via), visitare www.se.com/ww/en/work/support/green-premium/.

Documenti correlati

Titolo della documentazione	Codice di riferimento
M580 Sicurezza, Condizioni di applicazione relative alla sicurezza — Piano di verifica	EIO0000004540 (ENG) EIO0000004741 (FRE) EIO0000004742 (GER) EIO0000004744 (ITA) EIO0000004743 (SPA) EIO0000004745 (CHS)
Modicon M580, Guida alla pianificazione del sistema di sicurezza	QGH60283 (Inglese), QGH60284 (Francese), QGH60285 (Tedesco), QGH60286 (Spagnolo), QGH60287 (Italiano), QGH60288 (Cinese)

Titolo della documentazione	Codice di riferimento
EcoStruxure™ Control Expert, Safety, Block Library	QGH60275 (Inglese), QGH60278 (Francese), QGH60279 (Tedesco), QGH60280 (Italiano), QGH60281 (Spagnolo), QGH60282 (Cinese)
Piattaforma controller Modicon - Sicurezza informatica, Manuale di riferimento	EIO0000001999 (Inglese), EIO0000002001 (Francese), EIO0000002000 (Tedesco), EIO0000002002 (Italiano), EIO0000002003 (Spagnolo), EIO0000002004 (Cinese)
Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente	NHA58880 (Inglese), NHA58881 (Francese), NHA58882 (Tedesco), NHA58883 (Italiano), NHA58884 (Spagnolo), NHA58885 (Cinese)
Modicon M580, Hardware, Manuale di riferimento	EIO0000001578 (Inglese), EIO0000001579 (Francese), EIO0000001580 (Tedesco), EIO0000001582 (Italiano), EIO0000001581 (Spagnolo), EIO0000001583 (Cinese)
Modicon M580 Standalone, Guida di pianificazione del sistema per architetture di utilizzo frequente	HRB62666 (Inglese), HRB65318 (Francese), HRB65319 (Tedesco), HRB65320 (Italiano), HRB65321 (Spagnolo), HRB65322 (Cinese)
Modicon M580, Guida di pianificazione del sistema per le topologie complesse	NHA58892 (Inglese), NHA58893 (Francese), NHA58894 (Tedesco), NHA58895 (Italiano), NHA58896 (Spagnolo), NHA58897 (Cinese)
EcoStruxure™ Automation Device Maintenance, Guida utente	EIO0000004033 (Inglese), EIO0000004048 (Francese), EIO0000004046 (Tedesco), EIO0000004049 (Italiano), EIO0000004047 (Spagnolo), EIO0000004050 (Cinese)
Unity Loader, Guida utente	33003805 (Inglese), 33003806 (Francese), 33003807 (Tedesco), 33003809 (Italiano), 33003808 (Spagnolo), 33003810 (Cinese)
EcoStruxure™ Control Expert, Modalità di funzionamento	33003101 (Inglese), 33003102 (Francese), 33003103 (Tedesco), 33003104 (Spagnolo), 33003696 (Italiano), 33003697 (Cinese)
EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento	EIO0000002135 (Inglese), EIO0000002136 (Francese), EIO0000002137 (Tedesco), EIO0000002138 (Italiano), EIO0000002139 (Spagnolo), EIO0000002140 (Cinese)

Per trovare i documenti online, visitare il centro download Schneider Electric (www.se.com/ww/en/download/).

Informazioni relative al prodotto

⚠⚠ PERICOLO

PERICOLO DI SCOSSE ELETTRICHE, ESPLOSIONE O ARCO ELETTRICO

- Mettere fuori tensione tutte le apparecchiature, inclusi i dispositivi collegati, prima di rimuovere coperchi o sportelli o prima di installare/disinstallare accessori, hardware, cavi o fili, tranne che nelle condizioni specificate nell'apposita guida hardware per questa apparecchiatura.
- Per verificare che l'alimentazione sia isolata quando e dove indicato, usare sempre un rilevatore di tensione correttamente tarato.
- Prima di riapplicare tensione a questa apparecchiatura, reinstallare e fissare bene tutti i coperchi, accessori, componenti hardware, cavi e fili, e assicurarsi della presenza di una messa a terra appropriata.
- Utilizzare l'apparecchiatura e tutti i prodotti associati solo alla tensione specificata.

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

⚠AVVERTIMENTO

PERDITA DI CONTROLLO

- Eseguire un'analisi FMEA (Failure Mode and Effects Analysis) o un'analisi dei rischi equivalente dell'applicazione e applicare controlli preventivi e di rilevazione prima dell'implementazione.
- Fornire uno stato di posizionamento di sicurezza per sequenze o eventi di controllo indesiderati.
- Fornire percorsi di controllo separati o ridondanti qualora richiesto.
- fornire i parametri appropriati, in particolare per i limiti.
- Esaminare le implicazioni dei ritardi di trasmissione e stabilire azioni di mitigazione.
- Esaminare le implicazioni delle interruzioni del collegamento di comunicazione e stabilire azioni di mitigazione.
- Fornire percorsi indipendenti per le funzioni di controllo (ad esempio, arresto di emergenza, condizioni di superamento limiti e condizioni di guasto) in base alla valutazione dei rischi effettuata e alle normative e regolamentazioni applicabili.
- Applicare le direttive locali per la prevenzione degli infortuni e le linee guida e regolamentazioni sulla sicurezza.[1]
- Testare ogni implementazione di un sistema per il funzionamento adeguato prima di metterlo in servizio.

.

Il mancato rispetto di queste istruzioni può provocare rischio di morte, gravi ferite o danni alle apparecchiature.

[1] Per ulteriori informazioni, fare riferimento a NEMA ICS 1.1 (ultima edizione), Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control e a NEMA ICS 7.1 (ultima edizione), Safety Standards for Construction and Guide for selection, Installation and Operation of Adjustable-Speed Drive Systems o alla pubblicazione equivalente valida nel proprio paese.

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Con questa apparecchiatura utilizzare esclusivamente il software approvato da Schneider Electric.
- Aggiornare il programma applicativo ogni volta che si cambia la configurazione dell'hardware fisico.

Il mancato rispetto di queste istruzioni può provocare rischio di morte, gravi ferite o danni alle apparecchiature.

Informazioni sulla terminologia non inclusiva o non sensibile

In qualità di azienda responsabile e inclusiva, Schneider Electric aggiorna costantemente le sue comunicazioni e i suoi prodotti che contengono una terminologia non inclusiva o indelicata. Tuttavia, nonostante questi sforzi, i nostri contenuti possono ancora contenere termini ritenuti inappropriati da alcuni clienti.

Terminologia derivata dagli standard

I termini tecnici, la terminologia, i simboli e le descrizioni corrispondenti nelle informazioni contenute nel presente documento, o che compaiono nei o sui prodotti stessi, derivano generalmente dai termini o dalle definizioni delle norme internazionali.

Nell'ambito dei sistemi di sicurezza funzionale, degli azionamenti e dell'automazione generale, tali espressioni possono includere, tra l'altro, termini quali *sicurezza*, *funzione di sicurezza*, *stato sicuro*, *guasto*, *reset guasto*, *malfunzionamento*, *errore*, *reset errore*, *messaggio di errore*, *pericoloso* e così via.

Queste norme comprendono, tra le altre:

Norma	Descrizione
IEC 61131-2:2007	Controller programmabili, parte 2: Requisiti per apparecchiature e test.
ISO 13849-1:2023	Sicurezza dei macchinari: Parti di sicurezza dei sistemi di controllo. Principi generali per la progettazione.
EN 61496-1:2020	Sicurezza dei macchinari: Electro-Sensitive Protective Equipment, dispositivo elettrosensibile di protezione. Parte 1: Requisiti generali e test
ISO 12100:2010	Sicurezza dei macchinari - Principi generali di progettazione - Valutazione e riduzione dei rischi
EN 60204-1:2006	Sicurezza dei macchinari - Equipaggiamento elettrico delle macchine - Parte 1: Requisiti generali
ISO 14119:2013	Sicurezza dei macchinari - Dispositivi di interblocco associati alle protezioni - Principi di progettazione e selezione
ISO 13850:2015	Sicurezza dei macchinari - Arresto di emergenza - Principi di progettazione
IEC 62061:2021	Sicurezza dei macchinari - Sicurezza funzionale dei sistemi di controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza
IEC 61508-1:2010	Sicurezza funzionale di sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti generali.

Norma	Descrizione
IEC 61508-2:2010	Sicurezza funzionale dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili.
IEC 61508-3:2010	Sicurezza funzionale dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti software.
IEC 61784-3:2021	Reti di comunicazione industriale - Profili - Parte 3: Bus di campo di sicurezza funzionale - Regole generali e definizioni dei profili.
2006/42/EC	Direttiva macchine
2014/30/EU	Direttiva compatibilità elettromagnetica
2014/35/EU	Direttiva bassa tensione

I termini utilizzati nel presente documento possono inoltre essere utilizzati indirettamente, in quanto provenienti da altri standard, quali:

Standard	Descrizione
Serie IEC 60034	Macchine elettriche rotative
Serie IEC 61800	Variatori di velocità elettrici regolabili
Serie IEC 61158	Comunicazioni dati digitali per misurazioni e controlli – Bus di campo per l'uso con i sistemi di controllo industriali

Infine, l'espressione *area di funzionamento* può essere utilizzata nel contesto di specifiche condizioni di pericolo e in questo caso ha lo stesso significato dei termini *area pericolosa* o *zona di pericolo* espressi nella *Direttiva macchine* (*2006/42/EC*) e *ISO 12100:2010*.

NOTA: Gli standard indicati in precedenza possono applicarsi o meno ai prodotti specifici citati nella presente documentazione. Per ulteriori informazioni relative ai singoli standard applicabili ai prodotti qui descritti, vedere le tabelle delle caratteristiche per tali codici di prodotti.

Funzione di sicurezza M580

Introduzione

Questo capitolo introduce la funzione di sicurezza M580 per il sistema di sicurezza M580 e per ogni modulo di sicurezza.

Funzione di sicurezza M580

Presentazione della funzione di sicurezza M580

Tramite Control Expert con Safety, è possibile programmare, configurare e gestire un'applicazione di sicurezza. Durante la progettazione e la programmazione di un'applicazione di sicurezza, applicare le funzioni di sicurezza solo a componenti di un loop di sicurezza.

NOTA: In un loop di sicurezza si devono includere solo moduli di sicurezza, le relative impostazioni di configurazione e i relativi dati.

Dopo la messa in servizio, mentre il sistema di sicurezza M580 funziona in modalità di sicurezza, il sistema di sicurezza legge periodicamente gli ingressi di sicurezza, elabora la logica di sicurezza del programma applicativo, esegue la diagnostica e applica i risultati logici alle uscite di sicurezza.

Se il controller o la diagnostica I/O rileva un errore, il sistema di sicurezza imposta la parte interessata nello stato sicuro definito. In base alla natura dell'errore rilevato, l'ambito della risposta può porre un singolo canale di I/O, un modulo di I/O o l'intero sistema nello stato sicuro definito.

Lo stato sicuro definito è lo stato non alimentato. Ad esempio:

- Il modulo di ingresso analogico BMXSAI0410 o il modulo di ingresso digitale BMXSDI1602, se rileva un errore irreversibile, imposta il valore dei suoi ingressi nel controller a 0 (stato non alimentato), che rimangono in tale stato fino a quando la condizione sottostante è stata risolta.
- Il modulo di uscita digitale BMXSDO0802 o il modulo di uscita relè digitale BMXSRA0405, se rileva un errore irreversibile, imposta le uscite allo stato non alimentato, che permane fino a quando la condizione sottostante non viene risolta e il modulo riavviato.
- Il modulo di uscita digitale BMXSDO0802 o il modulo di uscita relè digitale BMXSRA0405, se rileva un errore di comunicazione su un collegamento black channel al controller, imposta le proprie uscite allo stato di posizionamento di sicurezza.

  NOTA: È possibile utilizzare Control Expert Safety per configurare lo stato di posizionamento di sicurezza (alimentato, non alimentato o mantenimento dell'ultimo valore) nel caso in cui la comunicazione black channel tra il controller e il modulo di uscita si interrompa.
- Un BMEP58•040S standalone o un controller BMEH58•040S Hot Standby, se rileva un errore di comunicazione su un collegamento black channel a un modulo di ingresso di sicurezza, imposta lo stato degli ingressi interessati a "0" (stato non alimentato) finché il black channel non ritorna operativo e il controller può nuovamente leggere i valori di ingresso effettivi.

Loop di sicurezza

Un loop di sicurezza è l'insieme di apparecchiature e logica che esegue un processo di sicurezza. Un progetto di sicurezza può comprendere più loop di sicurezza. Per ogni loop di sicurezza occorre verificare quanto segue:

- Il tempo di sicurezza del processo, pagina 157 deve essere maggiore del tempo di reazione del sistema, pagina 157.
- La somma dei valori PFD o PFH, pagina 149 per tutti i componenti del loop di sicurezza non deve superare il valore massimo consentito per:
  - livello di integrità della sicurezza (1, 2, 3 o 4)
  - modo di funzionamento (bassa domanda o alta domanda)
  - intervallo del test di prova

In un loop di sicurezza si devono includere solo moduli di sicurezza. Sebbene nel progetto di sicurezza sia possibile includere dei moduli non interferenti, pagina 33, questi vanno utilizzati soltanto per i task non di sicurezza (MAST, FAST, AUX0 o AUX1).

⚠AVVERTIMENTO

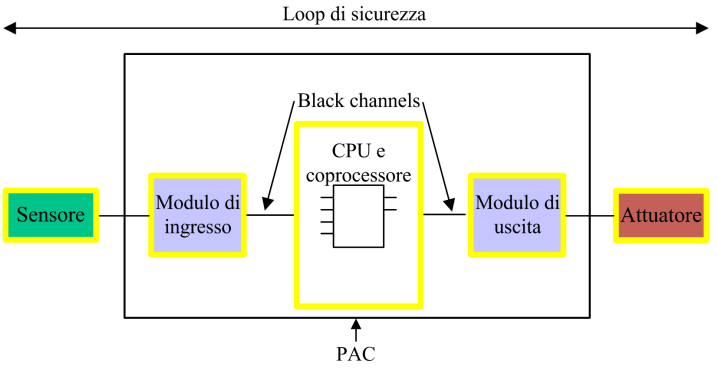
IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

- Per eseguire le funzioni di sicurezza, utilizzare esclusivamente moduli di sicurezza.
- Non utilizzare ingressi o uscite di moduli non interferenti per le funzioni non di sicurezza.
- Non utilizzare le variabili dell'Area globale per le funzioni relative alla sicurezza.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Vedere la sezione *Separazione dei dati in un progetto di sicurezza M580*, pagina 174 per una descrizione delle variabili dell'area globale.

Loop di sicurezza:



L'apparecchiatura di sicurezza include i seguenti moduli di sicurezza Schneider Electric M580:

- Controller BME•58•040S e copro BMEP58CPROS3:

  Il controller e il coprocessore insieme eseguono i task di lettura degli ingressi di sicurezza, elaborano la logica di sicurezza, eseguono la diagnostica e applicano i risultati alle uscite. Tutti questi task fanno parte del loop di sicurezza. Anche le porte utilizzate per le comunicazioni sul black channel fanno parte del loop di sicurezza. Tuttavia, altri componenti del controller, ad esempio la porta USB, la scheda di memoria SD e l'area della memoria statica ad accesso casuale non volatile (nvSRAM), non fanno parte del loop di sicurezza.

  NOTA: all'avvio a freddo e a caldo del sistema, il controller e il coprocessore non caricano i dati memorizzati nella nvSRAM nel task di sicurezza (i dati nvSRAM sono utilizzati solo nei task MAST, FAST e AUX non di sicurezza). Il controller e il coprocessore, invece, applicano inizialmente le impostazioni di configurazione predefinite dalla scheda di memoria SD, quindi applicano i valori ricevuti direttamente dagli ingressi durante il funzionamento.

- I/O di sicurezza (BMXSAI0410, BMXSDI1602, BMXSDO0802 e BMXSRA0405):

  Le funzioni di invio dei segnali di ingresso, di ricezione dei segnali di uscita e dell'esecuzione della diagnostica fanno parte del loop di sicurezza.

- Alimentatori BMXCPS4002S, BMXCPS4022S e BMXCPS3522S:

  Questi alimentatori di sicurezza forniscono il rilevamento della sovratensione e questo fa parte del loop di sicurezza. Dato che l'affidabilità di ogni alimentatore (ossia il tasso di errore pericoloso) è oltre 100 volte superiore alla soglia dello standard SIL3, questi alimentatori di sicurezza non vengono inclusi nei calcoli del livello di integrità relativi al loop di sicurezza.

Il loop di sicurezza include anche le seguenti apparecchiature di sicurezza:

- Sensori, attuatori e relativo cablaggio con i moduli di I/O. Gli I/O di sicurezza eseguono la diagnostica del cablaggio dei sensori e degli attuatori per contribuire alla gestione del loop di sicurezza.

  NOTA: Quando si progetta l'applicazione di sicurezza, occorre identificare le caratteristiche dei sensori e degli attuatori (in particolare i valori PFD/PFH).

Standard e certificazioni

Introduzione

Questo capitolo descrive gli standard e le certificazioni validi per il sistema di sicurezza M580 e i moduli che lo compongono.

Certificazioni

Standard di certificazione PAC M580 Safety

Il PAC M580 Safety è certificato da TÜV Rheinland Group per l'uso in applicazioni fino a:

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50126 (IEC 62278), EN 50128 (IEC 62279), EN 50129 (IEC 62245)
- SIL CL3 / IEC 62061
- PLe, Cat. 4 / ISO 13849-1

Per informazioni più dettagliate sulla classificazione SIL, vedere Descrizione della classificazione SIL, pagina 402.

Specifiche del controller programmabile

- IEC 61131-2: controller programmabili- Parte 2: Requisiti per apparecchiature e test.
- IEC/EN 61010-2-201, UL 61010-2-201, CSA -C22.2 N. 61010-2-201: Requisiti di sicurezza per le apparecchiature elettriche - Parte 2-201: requisiti particolari per le apparecchiature di controllo.

Specifiche ambientali

Consultare Standard e certificazioni M580, pagina 29 per i livelli dei test ambientali.

Specifiche per aree Ex

Per USA e Canada: località a rischio di classe I, divisione 2, gruppi A, B, C e D

- CSA 22.2 No213, ANSI/ISA12.12.01 e FM3611

Per gli altri paesi: CE ATEX (direttiva 2014/34/UE) o IECEx in atmosfera definita Zona 2 (gas) e/o Zona 22 (polvere)

- CEI/EN 60079-0; CEI/EN 60079-7; CEI/EN 60079-15

Specifiche per i sistemi di automazione delle centrali elettriche

- IEC/EN 61000-6-5: Compatibilità elettromagnetica - Parte 6-5: Standard generici - Immunità per ambienti di sottostazioni e centrali elettriche.
- IEC/EN 61850-3: Reti di comunicazione e sistemi per l'automazione delle centrali elettriche - Parte 3: Requisiti generali

Consultare M580 Standard e certificazioni, pagina 29 per le limitazioni dell'installazione.

Specifiche ferroviarie

- EN 45545–2 / IEC 60332–3–24: applicazioni ferroviarie - Prove di resistenza al fuoco dei cavi per treni.
- EN 50126 / IEC 62278: Applicazioni ferroviarie: specifica e dimostrazione di affidabilità, disponibilità, mantenibilità e sicurezza (RAMS).
- EN 50128 / IEC 62279: Applicazioni ferroviarie - Sistemi di comunicazione, segnalazione ed elaborazione - Software per sistemi di controllo e protezione per il settore ferroviario.
- EN 50129 / IEC 62245: Applicazioni ferroviarie - Sistemi di comunicazione, segnalazione ed elaborazione - Sistemi elettronici di segnalazione legati alla sicurezza.
- EN 50155 / IEC 60571: Applicazioni ferroviarie - Materiale rotabile - Apparecchiature elettroniche.
- EN 50121-3-2 / IEC 62236-3-2: Applicazioni ferroviarie - Compatibilità elettromagnetica - Parte 3-2: Materiale rotabile - Apparecchiatura.
- EN 50121-4 / IEC 62236-4: Applicazioni ferroviarie - Compatibilità elettromagnetica - Parte 4: Emissioni e immunità degli apparati di segnalazione e telecomunicazioni.
- EN 50121-5 / IEC 62236-5: Applicazioni ferroviarie - Compatibilità elettromagnetica - Parte 5: Emissione e immunità degli apparati e degli impianti di alimentazione fissi.
- EN 50125-1: Ferrovie - Condizioni ambientali per le apparecchiature - Parte 1: Materiale rotabile e apparecchiatura a bordo.
- EN 50125-3: Ferrovie - Condizioni ambientali per le apparecchiature - Parte 3: Apparecchiature per la segnalazione e le telecomunicazioni.
- EN 50124-1: Ferrovie - Coordinamento dell'isolamento - Parte 1: Requisiti di base: distanze di isolamento in aria e dispersione per tutte le apparecchiature elettriche ed elettroniche.

Consultare M580 Standard e certificazioni, pagina 29 per le limitazioni dell'installazione.

Specifiche di sicurezza funzionale

- IEC/EN 61000-6-7: Compatibilità elettromagnetica - Parte 6-7: Standard generici - Requisiti di immunità per apparecchiature destinate all'esecuzione di funzioni in un sistema legato alla sicurezza (sicurezza funzionale) in ubicazioni industriali.
- IEC 61326-3-1: Apparecchiature elettriche per la misura, il controllo e l'uso in laboratorio - Parte 3-1: Requisiti di immunità per sistemi di sicurezza e per apparecchiature destinate all'esecuzione di funzioni di sicurezza - Applicazione industriale generale.
- IEC 61508: Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili correlati alla sicurezza - Parte 1-7, edizione 2.0.
- IEC 61511-1: Sicurezza funzionale. Sistemi strumentali di sicurezza per il settore dell'industria di processo - Parte 1: Struttura, definizioni, requisiti hardware e software.
- IEC 61511-2: Sicurezza funzionale. Sistemi strumentali di sicurezza per il settore dell'industria di processo - Parte 2: Direttive per l'applicazione della norma IEC 61511-1.
- IEC 61511-3: Sicurezza funzionale. Sistemi strumentali di sicurezza per il settore dell'industria di processo - Parte 3: Guida per la determinazione dei livelli di integrità di sicurezza richiesti.

Specifiche dei macchinari di sicurezza

- IEC/EN 62061: Sicurezza dei macchinari - Sicurezza funzionale dei sistemi di controllo elettrici/elettronici/elettronici programmabili correlati alla sicurezza.
- ISO EN 13849-1: Sicurezza dei macchinari - Componenti di sicurezza dei sistemi di controllo - Parte 1: Principi generali per la progettazione.

Sicurezza funzionale nelle specifiche di sistema

- EN 54-2: Sistemi di rilevamento e allarme antincendio Parte 2: Apparecchiature di controllo e segnalazione.
- EN 50156-1: Apparecchiature elettriche per forni e apparecchiature ausiliarie - Parte 1: Requisiti per la progettazione e l'installazione dell'applicazione.
- EN 50130-4: Sistemi di allarme - Parte 4: Compatibilità elettromagnetica. Famiglia di prodotti standard: Requisiti di immunità per componenti di impianti antincendio, antintrusione, arresto, TVCC, controllo accessi e sistemi di allarme sociale.
- EN 298: Sistemi automatici di comando per bruciatori e sistemi di apparecchi a gas o a combustibile liquido.
- NFPA 85: Boiler and Combustion Systems Hazards Code.

- NFPA 86: Standard for Ovens and Furnaces.
- NFPA 72: National Fire Alarm and Signaling Code.

Note

Per l'elenco completo delle norme (con relative revisioni e date) certificate da TÜV, fare riferimento al certificato TÜV sul sito Web:

www.certipedia.com o https://fs-products.tuvasi.com/certificates.

Standard e certificazioni

Download

Fare clic sul collegamento corrispondente alla lingua preferita per scaricare gli standard e le certificazioni (formato PDF) validi per i moduli in questa linea di prodotti:

Titolo	Lingue
Piattaforme Modicon M580, M340 e X80 I/O, standard e certificazioni	• Inglese: EIO0000002726 • Francese: EIO0000002727 • Tedesco: EIO0000002728 • Italiano: EIO0000002730 • Spagnolo: EIO0000002729 • Cinese: EIO0000002731

Moduli supportati del sistema di sicurezza M580

Introduzione

Un progetto di sicurezza M580 può includere moduli di sicurezza e non di sicurezza. È possibile utilizzare:

- Moduli di sicurezza nel task SAFE.
- Moduli non di sicurezza solo per task non di sicurezza (MAST, FAST, AUX0 e AUX1).

> **NOTA:** È possibile aggiungere a un progetto di sicurezza solo i moduli non di sicurezza che non interferiscono con la funzione di sicurezza.

Utilizzare solo il software di programmazione Control Expert di Schneider Electric per programmare, mettere in servizio e utilizzare l'applicazione di sicurezza M580.

- Control Expert L Safety offre tutte le funzionalità di Control Expert L e può essere utilizzato con controller di sicurezza BMEP582040S e BMEH582040S.
- Control Expert XL Safety offre tutte le funzionalità di Control Expert XL e può essere utilizzato per l'intera gamma di controller di sicurezza BMEP58•040S e BMEH58•040S.

Questo capitolo elenca i moduli di sicurezza e non di sicurezza supportati dal sistema di sicurezza M580.

Moduli certificati del sistema di sicurezza M580

Moduli certificati

Il PAC di sicurezza M580 è un sistema di sicurezza certificato da TÜV Rheinland Group, in base a:

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50126 (IEC 62278), EN 50128 (IEC 62279), EN 50129 (IEC 62245)
- SIL CL3 / IEC 62061
- PLe, Cat. 4 / ISO 13849-1
- CIP Safety IEC 61784-3

Solo le versioni del prodotto Safety e del software Control Expert menzionate nell'elenco di revisione del certificato TÜV sono conformi per l'uso Safety.

Le informazioni più recenti sulle versioni certificate di prodotto, firmware e software sono disponibili sul sito Web di TÜV Rheinland Group: https://www.certipedia.com/ o https://fs-products.tuvasi.com/.

Si basa sulla famiglia M580 di controller logici programmabili (PAC). Sono certificati i seguenti moduli di sicurezza Schneider Electric M580:

- Controller standalone BMEP582040S
- Controller standalone BMEP584040S
- Controller standalone BMEP586040S
- Controller BMEH582040S Hot Standby
- Controller BMEH584040S Hot Standby
- Controller BMEH586040S Hot Standby
- Coprocessore BMEP58CPROS3
- Modulo di ingresso analogico BMXSAI0410
- Modulo di ingresso digitale BMXSDI1602
- Modulo di uscita digitale BMXSDO0802
- Modulo di uscita relè digitale BMXSRA0405
- Alimentatore BMXCPS4002S
- Alimentatore BMXCPS4022S
- Alimentatore BMXCPS3522S

NOTA: Oltre ai moduli di sicurezza elencati sopra, è possibile includere nel progetto moduli non interferenti, non di sicurezza, pagina 33.

NOTA: L'offerta Modicon Safety è fino a SIL3 (reg. IEC 61508) e PLe (reg. ISO 13849), ossia compatibile anche con SIL1/SIL2 e PLa, b,c,d.

NOTA:

- Ogni volta che nel documento viene menzionato SIL2 o SIL3 senza un riferimento standard, si applica la norma IEC 61508 / IEC 61511.
- Ogni volta che viene indicato SIL2, si intende anche SIL3 per quanto riguarda EN 50126 / EN 50128 / EN 50129.
- Ogni volta che viene indicato SIL3, si intende anche SIL4 per quanto riguarda EN 50126 / EN 50128 / EN 50129.

Sostituzione di un controller

È possibile sostituire un controller BME•58•040S con un altro BME•58•040S. La sostituzione, tuttavia, non può avvenire se vengono superate le seguenti limitazioni:

- numero di I/O
- numero di derivazioni di I/O
- numero di variabili
- dimensione memoria applicazione

Consultare gli argomenti:

- *Compatibilità della configurazione* in *Modicon M580 Guida alla pianificazione del sistema Hot Standby per architetture di utilizzo frequente* per una descrizione delle applicazioni Control Expert compatibili con i controller di sicurezza e Hot Standby.
- *Caratteristiche prestazionali del controller e del coprocessore M580* in *Modicon M580 Safety Guida alla pianificazione del sistema* per una descrizione delle limitazioni del controller.

Moduli non interferenti

Introduzione

Un progetto di sicurezza M580 può includere moduli di sicurezza e non di sicurezza. È possibile utilizzare moduli non di sicurezza solo per task non di sicurezza. È possibile aggiungere a un progetto di sicurezza solo i moduli non di sicurezza che non interferiscono con la funzione di sicurezza.

Definizione di un modulo non interferente

NOTA: Confermare che non vengono utilizzati dati di ingresso né dati di uscita dai moduli non interferenti per controllare le uscite correlate alla sicurezza. I moduli non di sicurezza possono elaborare solo dati non di sicurezza.

Un modulo non interferente è un modulo che non può interferire con la funzione di sicurezza. Per moduli M580 backplane (BMEx, BMXx, PMXx e PMEx), vi sono due tipi di moduli non interferenti:

- **Tipo 1:** è possibile installare un modulo di tipo 1 nello stesso backplane dei moduli di sicurezza (ovunque si posizioni il modulo di sicurezza, nel backplane principale o di estensione).
- **Tipo 2:** non è possibile installare un modulo non interferente di tipo 2 nello stesso backplane principale dei moduli di sicurezza (ovunque si posizioni il modulo di sicurezza, nel backplane principale o di estensione).

NOTA: i moduli di tipo 1 e tipo 2 sono elencati sul sito Web TÜV Rheinland all'indirizzo www.certipedia.com/certificates e https://fs-products.tuvasi.com/certificates.

Per i moduli Mx80 non in-backplane, tutte le apparecchiature Ethernet (DIO o DRS) possono essere considerate come non interferenti e quindi possono essere utilizzate come parte di un sistema di sicurezza M580.

Moduli non interferenti di tipo 1 per applicazioni SIL3

I seguenti moduli non di sicurezza possono essere definiti non interferenti di tipo 1 in un sistema di sicurezza M580.

NOTA: L'elenco di moduli non di sicurezza non interferenti di tipo 1 può cambiare di volta in volta. Per l'elenco corrente, visitare il sito Web TÜV Rheinland all'indirizzo https://fs-products.tuvasi.com/certificates.

Tipo di modulo	Codice prodotto modulo
Backplane a 4 slot	BMEXBP0400
Backplane a 8 slot	BMEXBP0800
Backplane a 12 slot	BMEXBP1200
Backplane a 16 slot	BMEXBP1600
Backplane a 4 slot	BMXXBP0400
Backplane a 6 slot	BMXXBP0600
Backplane a 8 slot	BMXXBP0800
Backplane a 12 slot	BMXXBP1200
Backplane a 16 slot	BMXXBP1600
Backplane a 6 slot con doppio slot per alimentatori ridondanti	BMEXBP0602
Backplane a 10 slot con doppio slot per alimentatori ridondanti	BMEXBP1002
Backplane a 14 slot con doppio slot per alimentatori ridondanti	BMEXBP1402
Comunicazione: adattatore derivazione Ethernet Performance X80 1 CH	BMXCRA31210
Comunicazione: adattatore derivazione Ethernet Performance X80 1 CH	BMECRA31210
Comunicazione: modulo Ethernet con servizi Web standard	BMENOC0301
Comunicazione: modulo Ethernet con inoltro IP	BMENOC0321
Comunicazione: modulo Ethernet con servizi Web FactoryCast	BMENOC0311
Comunicazione: modulo di estensione backplane	BMXXBE1000
Comunicazione: AS-Interface	BMXEIA0100
Comunicazione: Dati globali	BMXNGD0100
Comunicazione: convertitore fibra MM/LC 2CH 100 Mb	BMXNRP0200
Comunicazione: convertitore fibra SM/LC 2CH 100 Mb	BMXNRP0201
Comunicazione: modulo di comunicazione M580 IEC 61850	BMENOP0300
Comunicazione: server OPC UA integrato	BMENUA0100
Conteggio: modulo SSI 3 CH	BMXEAE0300
Conteggio: contatore alta velocità 2 CH	BMXEHC0200
Conteggio: contatore alta velocità 8 CH	BMXEHC0800

Tipo di modulo	Codice prodotto modulo
Movimento: uscita treno di impulsi 2 canali indipendenti	BMXMSP0200
analogico: modulo HART 8 ingressi di corrente analogica isolati	BMEAHI0812
Analogico: modulo HART a 4 uscite di corrente analogica isolate	BMEAHO0412
analogico: 4 ingressi U/I isolati analogici ad alta velocità	BMXAMI0410
analogico: 4 U/I Ingressi analogici non isolati ad alta velocità	BMXAMI0800
analogico: 8 ingressi U/I isolati analogici ad alta velocità	BMXAMI0810
analogico: 4 ingressi analogici U/I 4 uscite U/I	BMXAMM0600
analogico: 2 uscite analogiche U/I isolate	BMXAMO0210
analogico: 4 uscite analogiche U/I isolate	BMXAMO0410
analogico: 8 uscite analogiche di corrente non isolate	BMXAMO0802
analogico: 4 TC/RTD ingressi analogici isolati	BMXART0414.2
analogico: 8 TC/RTD ingressi analogici isolati	BMXART0814.2
Digitale: 8 ingressi digitali 220 Vca	BMXDAI0805
Digitale: 8 ingressi digitali da 100 a 120 Vca isolati	BMXDAI0814
Digitale: 16 ingressi digitali 24Vca/24Vcc Source	BMXDAI1602
Digitale: 16 ingressi digitali 48 Vca	BMXDAI1603
Digitale: 16 ingressi digitali da 100 a 120 Vca 20 pin	BMXDAI1604
Digitale: 16 canali di ingresso supervisionati dig da 100 a 120 Vca 40 pin	BMXDAI1614
Digitale: 16 canali di ingresso supervisionati dig da 200 a 240 Vca 40 pin	BMXDAI1615
Digitale: 16 uscite triac dig da 100 a 240 Vca 20 pin	BMXDAO1605
Digitale: 16 uscite triac dig da 24 a 240 Vca 40 pin	BMXDAO1615
Digitale: 16 In digitali 24Vcc Sink	BMXDDI1602
Digitale: 16 In digitali 48Vcc Sink	BMXDDI1603
Digitale: 16 In digitali 125Vcc Sink	BMXDDI1604T
Digitale: 32 In digitali 24Vcc Sink	BMXDDI3202K
Digitale: 64 In digitali 24Vcc Sink	BMXDDI6402K
Digitale: 8 ingressi digitali 24Vcc 8Q Tr Source	BMXDDM16022
Digitale: Relè 8 In digitali 24Vcc 8Q	BMXDDM16025
Digitale: 16 ingressi digitali 24Vcc 16Q Tr Source	BMXDDM3202K

Tipo di modulo	Codice prodotto modulo
Digitale: Dig 16Q Trans Source 0,5A	BMXDDO1602
Digitale: Dig 16 O Trans Sink	BMXDDO1612
Digitale: Dig 32Q Trans Source 0,5A	BMXDDO3202
	BMXDDO3202H
Digitale: 32 uscite digitali Trans source 0,1A	BMXDDO3202K
Digitale: 64 uscite digitali Trans source 0,1A	BMXDDO6402K
Digitale: Dig 8Q 125Vcc	BMXDRA0804T
Digitale: relé isolati 8Q dig 24 Vcc o da 24 a 240 Vca	BMXDRA0805
Digitale: 16 canali di uscita relè non isolati dig da 5 a 125 Vcc o da 25 a 240 Vca	BMXDRA0815
Digitale: 16 uscite digitali relè	BMXDRA1605
Digitale: relè uscita NC dig da 5 a 125 Vcc o da 24 a 240 Vca	BMXDRC0805
Digitale: TSTAMP 16In digitali 24/125Vcc	BMXERT1604
Switch opzionale di rete Mx80	BMENOS0300
Ingresso frequenza turbomacchina 2 CH	BMXETM0200
Il modulo Master Profibus DP/DPV1 supporta	PMEPXM0100
Modulo RTU avanzato Mx80	BMENOR2200H

Moduli non interferenti di tipo 2 per applicazioni SIL2/3

I seguenti moduli non di sicurezza in-backplane possono essere considerati moduli non interferenti di tipo 2 in un sistema di sicurezza M580.

NOTA: L'elenco di moduli non di sicurezza non interferenti di tipo 2 può cambiare di volta in volta. Per l'elenco corrente, visitare il sito Web TÜV Rheinland all'indirizzo https://fs-products.tuvasi.com/certificates.

Tipo di modulo	Codice prodotto modulo
Comunicazione: Adattatore derivazione Ethernet X80 standard 1 CH	BMXCRA31200
Alimentazione CA standard	BMXCPS2000
Alimentazione CC isolata standard	BMXCPS2010
Alimentazione da 24 a 48 VCC isolata di alta potenza	BMXCPS3020
Alimentazione standard ridondante 125 VCC	BMXCPS3522

Tipo di modulo	Codice prodotto modulo
Alimentazione standard ridondante 24/48 VCC	BMXCPS4022
Alimentazione CA standard ridondante	BMXCPS4002
Alimentazione CA alta potenza	BMXCPS3500
Alimentazione CC alta potenza	BMXCPS3540T
Comunicazione: Modulo bus 2 porte RS485/232	BMXNOM0200
Digitale: 32 ingressi digitali 12/24Vcc Sink o Source	BMXDDI3232
Digitale: 32 In digitali 48Vcc Sink	BMXDDI3203
Master CANopen X80	BMECXM0100
Modulo peso	PMESWT0100
Modulo diagnostico partner	PMXCDA0400
Modulo di comunicazione universale Ethernet TCP Open	PMEUCM0302

NOTA: Tutte le apparecchiature autorizzate di un sistema M580 collegate a moduli di sicurezza tramite Ethernet sono considerate come non interferenti. Di conseguenza, tutti i moduli delle gamme Quantum e STB Advantys (non collegabili nello stesso backplane dei moduli M580 Safety) sono moduli non interferenti di Tipo 2.

Cybersicurezza per il sistema di sicurezza M580

Introduzione

Questo capitolo elenca la documentazione disponibile per sviluppare un approccio alla sicurezza informatica per il PAC di sicurezza M580.

Sicurezza informatica per il sistema M580 Safety

Riferimenti relativi alla sicurezza informatica

Lo scopo delle misure di cybersicurezza è di ridurre al massimo la vulnerabilità del sistema di protezione implementato nei confronti dei cyberattacchi. Per informazioni sullo sviluppo di misure di sicurezza informatica per il sistema di sicurezza M580, vedere *Manuale di riferimento sulla sicurezza informatica della piattaforma controller Modicon* (Codice EIO0000001999 (EN).

Ciclo di vita dell'applicazione

Introduzione

Ciclo di vita dell'applicazione

Introduzione

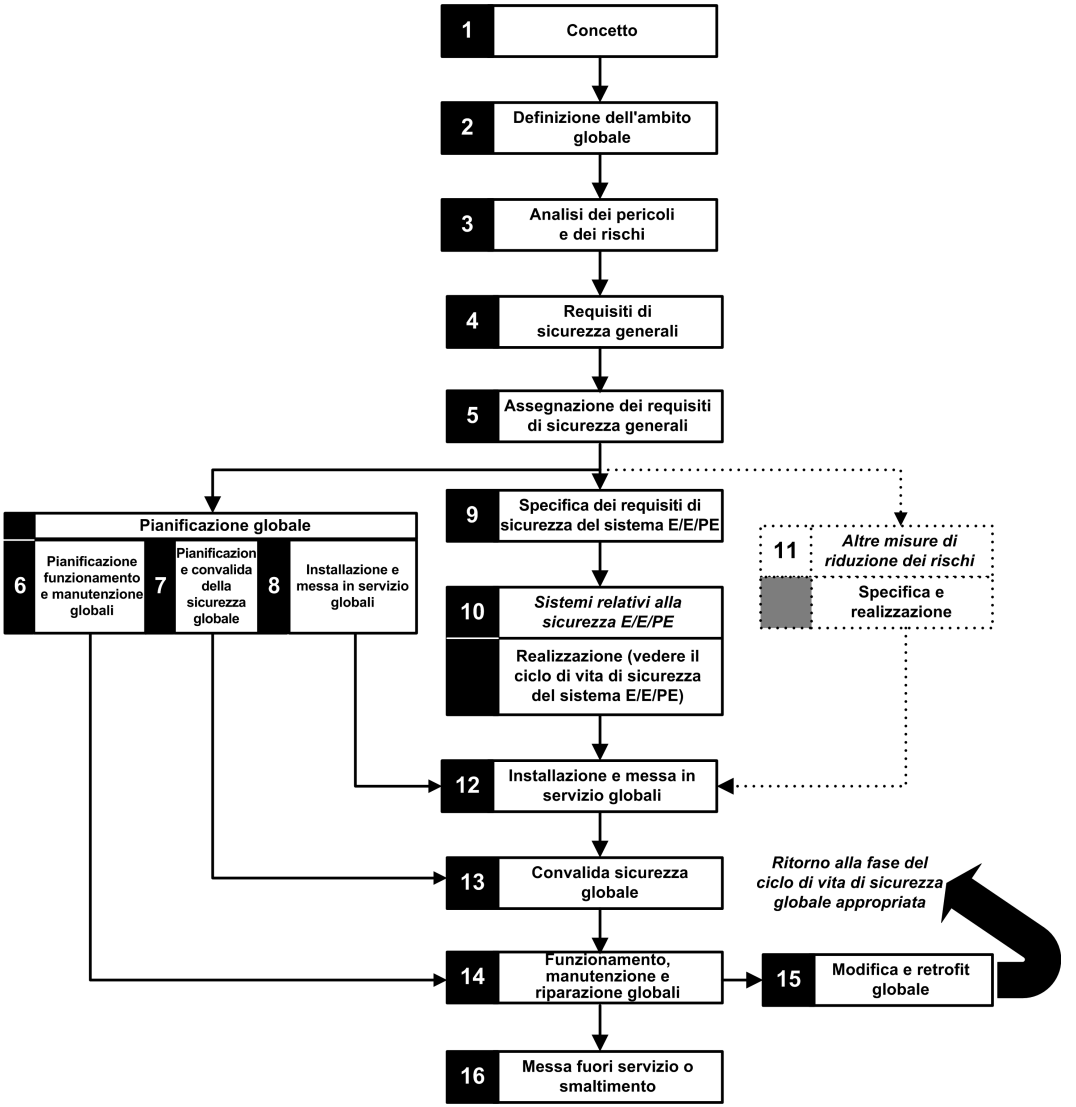
Quando si progetta un'applicazione di sicurezza, seguire le linee guida di una delle norme di sicurezza che si applicano al proprio settore di applicazione. La maggior parte delle norme di applicazione deriva o è collegata alla norma generica IEC 61508 che comprende, ad esempio, la norma sull'industria di processo (IEC 61511), le norme sui macchinari (IEC 62061 e ISO 13489), la norma sull'industria nucleare (IEC 61513), le norme per applicazioni ferroviarie (EN 5012x) e così via.

La norma IEC 61508 definisce il ciclo di vita di un'applicazione con una sequenza di passi. Ogni passo ha un ruolo definito, richiede documenti in ingresso e produce documenti di uscita. La decisione di utilizzare un sistema integrato di sicurezza (Safety Integrated System, SIS) viene presa al termine del passo Allocazione dei requisiti di sicurezza (passo 5).

Questa sezione definisce le verifiche relative all'uso di un sistema di sicurezza M580 che occorre effettuare nei passi seguenti:

9.	Specifica dei requisiti di sicurezza del sistema E/E/PE
10.	Realizzazione dei sistemi di sicurezza E/E/PE
12.	Installazione e messa in servizio globali
13.	Convalida sicurezza globale
14.	Funzionamento, manutenzione e riparazione globali
15.	Modifica e retrofit globale

Lo schema seguente presenta il ciclo di vita di sicurezza generale:



Passaggio 9: Specifica dei requisiti di sicurezza del sistema E/E/PE

Questa fase ha luogo una volta che l'analisi dei rischi è conclusa e ha fornito, tra l'altro, le seguenti informazioni:

- Definizione delle funzioni di sicurezza integrate
- Prestazioni richieste (durata, riduzione dei rischi, SIL...)
- Modalità di guasto delle funzioni

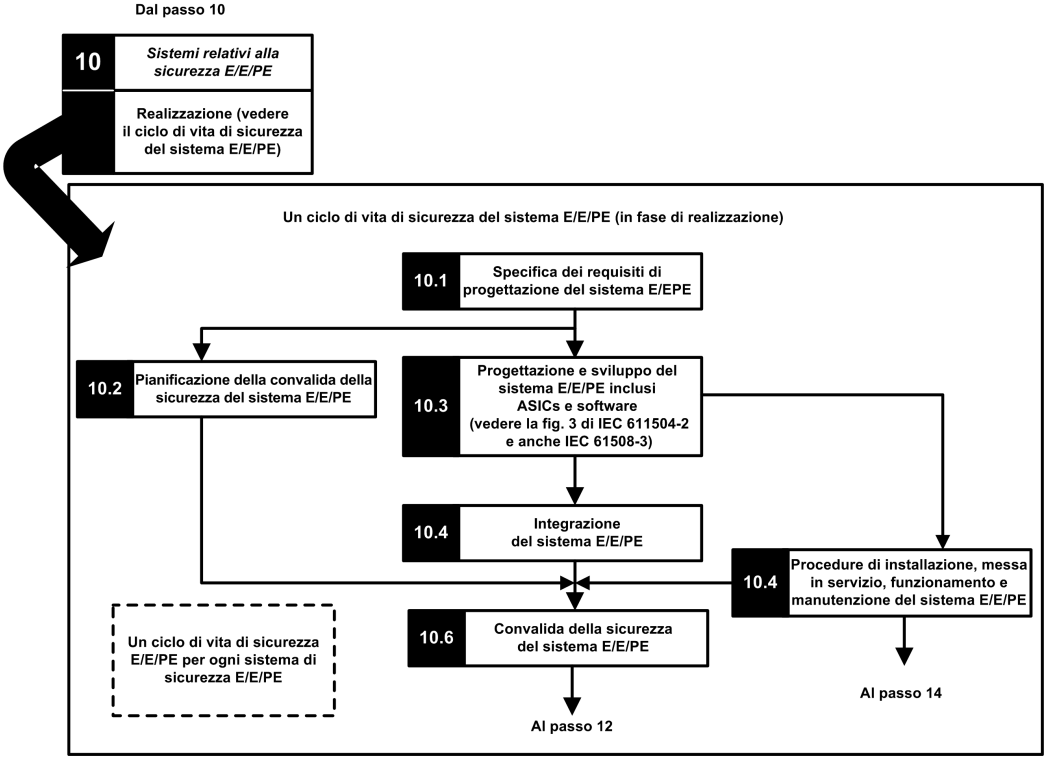
In questo passo dovrebbero essere generate le specifiche dei requisiti di sicurezza che includono, come minimo, le seguenti informazioni necessarie per progettare un'applicazione sicura con un PAC di sicurezza di qualsiasi tipo.

- Stato sicuro definito delle funzioni integrate di sicurezza
- Analisi delle modalità operative del SIS (incluso il comportamento in Run, Stop, sequenza di accensione, manutenzione, riparazione...)
- Intervallo di test delle SIF
- MTTR (tempo medio di riparazione) del SIS
- Scelta della SIF, in stato alimentato o non alimentato
- Prestazioni del logic solver (tempo di reazione, precisione ...)
- Requisiti di prestazioni
  - Tolleranza guasti
  - integrità
  - Frequenza max. di intervento spurio (STR)
  - Frequenza max. di guasti pericolosi
- Specifiche ambientali (dati EMC, meccanici, chimici, relativi al clima...)

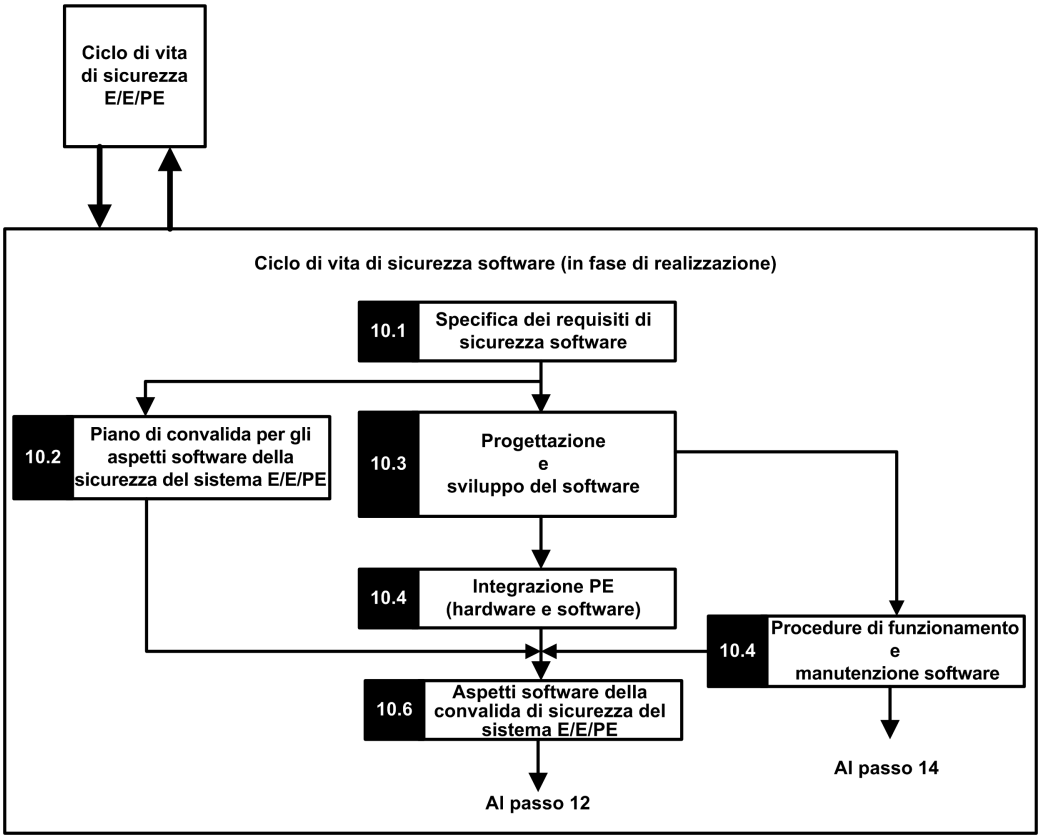
Passaggio 10: Realizzazione dei sistemi di sicurezza E/E/PE

La norma IEC 61508 divide questo passo in 2 sottocicli di vita, uno per la realizzazione del sistema e l'altro per la realizzazione del software.

Realizzazione del sistema:



Realizzazione del software:



L'obiettivo del primo sottopasso (10.1) è quello di convertire i requisiti di sicurezza del SIS in specifiche per la progettazione hardware, test dell'hardware, progettazione software, test del software e test di integrazione. In questa fase si devono fornire come minimo le informazioni necessarie per progettare un'applicazione sicura utilizzando un M580 di sicurezza:

- Architettura hardware che tiene conto dei seguenti fattori:
  - Rispetto delle regole M580 sulla combinazione di moduli non di sicurezza e di sicurezza: tutti i moduli di sicurezza (moduli I/O di sicurezza e controller/ coprocessori di sicurezza) sono posizionati in backplane dove il backplane principale e il backplane esteso sono alimentati da alimentatori dedicati e contengono solo moduli di sicurezza o moduli non interferenti di tipo 1.
  - assorbimento per backplane
  - regole di declassamento.

- Architettura di alimentazione:
  - solo alimentatori SELV/PELV
- Architettura software:
  - incluso l'uso delle variabili globali M580; una variabile globale non deve impedire l'attivazione di un'azione correlata alla sicurezza a meno che non venga utilizzato un *protocollo di applicazione sicuro*.
- Integrazione hardware (cablaggio, cabinet, ecc.):
  - Protezione fusibili
  - Accessori per la diagnostica del cablaggio.
- Interfacce uomo-macchina:
  - incluso l'uso di variabili globali M580; una variabile globale non deve impedire l'attivazione di un'azione correlata alla sicurezza a meno che non venga utilizzato un "protocollo di applicazione sicuro".
- Interfacce elettriche/numeriche:
  - stato sicuro definito
  - sensore e attuatore
- Algoritmo
- Prestazioni (inclusa definizione di periodo task, watchdog e timeout) e previsione di un comportamento corretto tramite la formula:

$$\Sigma_{tutti\ i\ task} \frac{Exe_{task}}{Periodo_{task}} < 80\%$$

NOTA: la formula è applicabile solo quando il task MAST non è in modalità ciclica.

- Comportamento in caso di:
  - sblocco configurazione
  - modalità di manutenzione
  - ingresso manutenzione
  - canale non valido
  - interruzione del cablaggio
  - stato del canale
  - stato del modulo
- Gestione dell'UID dei moduli I/O di sicurezza (definire quando un UID deve essere modificato)

- Server NTP:
  - Scelta del PAC come server NTP o server NTP esterno (in base all'uso di orodatazione degli I/O nell'applicazione di processo)
  - ridondanza server
  - perdita del server

Con i successivi passi secondari le specifiche vengono precisate in una specifica tecnica dettagliata, viene eseguita la progettazione stessa, si effettuano tutti i testi pianificati e si redigono i rapporti.

Passaggio 12: Installazione e messa in servizio globali

Lo scopo di questo passo è definire i requisiti per l'installazione, la pianificazione dei task, l'attrezzaggio, la procedura di messa in servizio, passando quindi a costruire il sistema e a verificarne la regolarità.

- Per applicazioni Hot Standby, verificare che il timeout di posizionamento di sicurezza, pagina 160 del moduli di uscita di sicurezza sia adatto alle condizioni definite per le operazioni di scambio, pagina 161 e switchover, pagina 163 e verificare il tempo di mantenimento CRA.
- Verificare che il timeout di posizionamento di sicurezza (S_TO) per i moduli di uscita di sicurezza sia maggiore almeno del più grande tra 40 ms o (2,5 * T_{SAFE}), dove T_{SAFE} è pari al periodo del task SAFE configurato.
- Cancellare ogni applicazione pre-esistente nel PLC, oppure utilizzare un'applicazione configurata senza dispositivi di sicurezza CIP prima di installare il dispositivo di sicurezza in una rete Ethernet di sicurezza (con dispositivi di sicurezza CIP).

In un sistema di sicurezza M580 la procedura di messa in servizio dovrebbe comprendere i seguenti punti:

- Verificare l'integrità di Control Expert: eseguire la funzionalità di test automatico.
- Verificare la versione di Control Expert notificata nell'elenco di revisione del certificato TÜV.
- Correttezza delle versioni firmware di controller e coprocessore tramite controllo delle parole di sistema %SW14 (versione firmware del processore PLC) e %SW142 (versione firmware del coprocessore).
- Correttezza degli indirizzi di ogni modulo (posizione nel backplane, interruttori CRA).
- Correttezza del cablaggio:
  - verifica punto a punto: dalla variabile interna al modulo di I/O e all'attuatore/sensore
  - fusibili
  - apparecchiatura per diagnostica cablaggio

- Al termine della procedura, i moduli di sicurezza sono in modalità di blocco. Includere la verifica dell'applicazione relativa alla sicurezza.
- Correttezza della configurazione di ogni modulo (inclusi i timeout)
  - Leggere la configurazione sulla schermata di Control Expert e confrontarla con la specifica.
- Tutte le applicazioni di sicurezza sono state ricompilate utilizzando l'opzione **Ricrea tutto il progetto** e quindi scaricate su ogni PLC, con il relativo SAId salvato insieme all'archivio dell'applicazione.
- Il periodo del task e il watchdog del task sono corretti.
- Codici prodotto e versione dei moduli.
- Uso esclusivo di alimentazione SELV/PELV.
- Se i dispositivi CIP Safety vengono utilizzati nell'applicazione di sicurezza:
  - La firma ID di configurazione di sicurezza (SCID) può essere verificata (opzione abilitata nel DTM di CIP Safety in Control Expert) e la configurazione di destinazione bloccata in seguito alla verifica utente.
  - Per confermare che la configurazione di origine creata dall'utente con lo strumento software Control Expert è stata inviata e salvata correttamente nell'origine CIP Safety M580, confrontare visivamente tutti i valori dei parametri di configurazione di destinazione CIP Safety visualizzati nei DDDT di destinazione (in modalità connesso con PAC, utilizzando una tabella di animazione) con i valori dei parametri visualizzati e configurati nella Scheda di verifica di configurazione, pagina 367 del DTM di destinazione. Tutti i valori devono essere uguali.
  - Verificare tutte le configurazioni di connessione di sicurezza dopo la loro applicazione nell'origine CIP Safety M580 per confermare che ciascuna connessione di destinazione stia funzionando nel modo previsto.
  - Prima di installare i dispositivi CIP Safety su una rete di sicurezza, effettuare la messa in servizio di tutti i dispositivi di sicurezza con MacId e Velocità di trasmissione se necessario.
- La verifica utente è lo strumento per mezzo del quale convalidare tutti i download di applicazioni

Passaggio 13: Convalida sicurezza globale

Lo scopo di questo passo è quello di dimostrare che il sistema integrato di sicurezza (SIS) soddisfa i requisiti. Vengono eseguiti tutti i test e prodotti i rapporti definiti nel passo 7 del "ciclo di vita di sicurezza". Dovrebbe comprendere:

- Verificare l'assenza di condizioni di overrun durante gli stati del sistema (verifica del bit di sistema %S19 nei task MAST, FAST, AUX0 e che il tempo di esecuzione massimo e corrente del task SAFE (%SW42 e %SW43) sia inferiore al periodo del task SAFE.

- Verificare la formula di carico del controller: $\Sigma_{tutti\ i\ task} \frac{Exe_{task}}{Periodo_{task}} < 80\%$

  NOTA: È possibile utilizzare le parole di sistema da %SW110 a %SW115, pagina 409 per eseguire una valutazione in tempo reale del carico medio dei task del controller (se tutti i task sono periodici, %SW116 deve essere inferiore a 80).
- Verificare che il tempo di esecuzione del task FAST (se configurato) sia il più breve possibile. Non deve essere maggiore della metà del periodo configurato del task SAFE.
- Verificare le modalità di funzionamento speciali (sblocco modulo, ingresso di manutenzione, canale non valido, interruzione del cablaggio).
- Per applicazioni Hot Standby, verificare che tutti i task siano correttamente sincronizzati attraverso il collegamento Hot Standby controllando e utilizzando i bit MAST_SYNCHRONIZED, FAST_SYNCHRONIZED e SAFE-SYNCHRONIZED in T_M_ECPU_HSBY DDT. Vedere *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente* per una descrizione del DTT_M_ECPU_HSBY.

Passaggio 14: Funzionamento, manutenzione e riparazione globali

- Esecuzione dei test di prova nel periodo appropriato.
- Monitoraggio del codice SAId vedere la nota.

  NOTA: Se SAId non è cambiato, significa che la porzione di sicurezza dell'applicazione non è stata modificata. Per informazioni dettagliate sul comportamento del codice SAId, vedere il blocco funzione S_SYST_STAT_MX.
- Monitoraggio dello stato di blocco configurazione su ogni modulo di sicurezza.
- Registrazione delle operazioni di riparazione.
- Se un modulo viene sostituito, il dispositivo di sostituzione deve essere configurato adeguatamente e l'utente deve verificarne il funzionamento. Eseguire (come minimo) le operazioni di messa in servizio relative a questo modulo.
- Registrazione degli scostamenti.

Passaggio 15: Modifica e retrofit globale

Qualsiasi modifica deve essere considerata come un nuovo progetto. Può essere utile un'analisi dell'impatto per definire la parte del sistema di sicurezza precedente che può essere mantenuta e la parte che deve essere riprogettata.

NOTA: Se la modifica di un'applicazione non riguarda l'applicazione SAFE, è possibile utilizzare la firma di origini SAFE per verificare che nessuna modifica indesiderata sia stata inserita nel codice SAFE. La firma di origini SAFE verifica *a priori* che l'applicazione non sia stata modificata. La firma di origini SAFE non sostituisce SAId, che è l'unico strumento in grado di confermare in modo affidabile che un PAC stia eseguendo la stessa applicazione SAFE convalidata.

Moduli I/O M580 Safety

Introduzione

Questo capitolo descrive i moduli I/O M580 Safety.

Funzioni condivise dei moduli di I/O di sicurezza M580

Introduzione

Questa sezione descrive le funzioni condivise o comuni dei moduli di I/O di sicurezza M580.

Presentazione dei moduli I/O M580 Safety

Introduzione

I seguenti quattro moduli di I/O di sicurezza M580 sono certificati per l'uso nelle applicazioni di sicurezza:

- BMXSAI0410 (ingresso analogico)
- BMXSDI1602 (ingresso digitale)
- BMXSDO0802 (uscita digitale)
- BMXSRA0405 (uscita relè digitale)

I quattro moduli di I/O di sicurezza permettono di collegare il PAC di sicurezza ai sensori e agli attuatori che fanno parte del loop di sicurezza. Ogni modulo di I/O di sicurezza include un processore di sicurezza dedicato. Questi moduli di I/O possono essere installati nel backplane locale o nelle derivazioni RIO.

Requisiti per l'installazione e per la custodia

Installare l'apparecchiatura di sicurezza M580 in modo che soddisfi i seguenti requisiti:

- Il grado di inquinamento 2 secondo IEC 60950 per la sicurezza delle apparecchiature per la tecnologia dell'informazione; e
- lo standard IEC 60529 per la protezione degli ingressi IP54, in modo tale che:
  - la presenza di polvere non interferisca con il funzionamento dell'apparecchiatura e
  - gli spruzzi d'acqua non possano danneggiare l'apparecchiatura o il funzionamento.

In genere questi standard vengono rispettati collocando l'apparecchiatura di sicurezza in un involucro di sicurezza, ad esempio un cabinet.

Altitudine di funzionamento massima

L'altitudine operativa massima per i moduli di I/O di sicurezza M580 è 2000 m sul livello del mare.

Comunicazione tra PAC e I/O

Il coprocessore e il controller di sicurezza M580 controllano insieme tutti gli scambi sul backplane, mentre gli I/O di sicurezza rispondono ai comandi del controller e del coprocessore. I moduli I/O di sicurezza possono essere installati in un backplane X Bus BMXXBP•••• o un backplane Ethernet BMEXBP••••.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza nel backplane principale locale avvengono tramite il backplane.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza installati in una derivazione RIO avvengono attraverso un modulo adattatore installato nella derivazione RIO:

- un adattatore BMECRA31210 per un backplane Ethernet, oppure
- un adattatore BMXCRA31210 per un backplane X Bus.

  NOTA: con il firmware del controller 3.20 o successivo, la comunicazione con il PAC e gli I/O di sicurezza richiede un BM•CRA31210 con firmware 2.60 o successivo.

  NOTA: un adattatore BMXCRA31200 non può essere utilizzato per collegare i moduli di I/O di sicurezza al PAC di sicurezza M580.

Opzionalmente, si possono utilizzare i moduli ripetitori a fibre ottiche BMXNRP0200 oppure BMXNRP0201 per estendere il collegamento fisico tra il controller e il coprocessore nel backplane locale e l'adattatore nella derivazione RIO. I moduli ripetitori a fibre ottiche migliorano l'immunità ai disturbi della rete RIO e garantiscono al contempo il mantenimento della massima disponibilità dinamica della rete e il livello di integrità di sicurezza.

Il protocollo di comunicazione tra gli I/O di sicurezza e il PAC consente gli scambi sulla rete. Questo protocollo permette ad entrambi i dispositivi di verificare l'accuratezza dei dati ricevuti, di rilevare eventuali dati corrotti e di determinare se il modulo di trasmissione diventa non operativo. Pertanto, un loop di sicurezza può includere qualsiasi adattatore RIO e backplane non interferente, pagina 33.

Alimentazione esterna utilizzata con gli I/O di sicurezza digitali

I moduli digitali BMXSDI1602 e BMXSDO0802 richiedono un alimentatore esterno a tensione ultra bassa protetta 24 Vcc (SELV/PELV) per fornire alimentazione ai sensori e agli attuatori. I moduli di I/O di sicurezza supervisionano l'alimentatore di processo non di sicurezza per rilevare eventuali condizioni di sovratensione e sottotensione.

⚠⚠PERICOLO

RICHIESTO ALIMENTATORE SELV/PELV CATEGORIA DI SOVRATENSIONE II

Per alimentare i sensori e gli attuatori, utilizzare solo un alimentatore di tipo SELV/PELV di categoria di sovratensione II con uscita max. 60 Vcc.

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

AVVISO

NON CONFORMITÀ DEL CIRCUITO ELETTRICO

Non collegare 0 V di un alimentatore SELV a terra.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Panoramica della diagnostica per moduli I/O M580 Safety

Introduzione

Ogni modulo di I/O di sicurezza M580 dispone delle seguenti funzioni di diagnostica:

- Autotest all'avvio del modulo
- Autotest continuo al runtime integrato
- LED di diagnostica del modulo e del canale

Inoltre, i moduli di I/O di sicurezza digitali eseguono anche la diagnostica del cablaggio.

Autotest all'accensione

All'accensione, i moduli di I/O eseguono un'ampia serie di autotest. Se i risultati di questi test sono:

- Positivi: i moduli sono considerati funzionanti e funzionanti.
- Negativi: i moduli non sono considerati funzionanti e non sono operativi. In questo caso, gli ingressi vengono impostati a 0 e le uscite vengono disattivate.

  NOTA: Se a un modulo di ingresso digitale o un modulo di uscita digitale non è collegata l'alimentazione 24 Vdc esterna, gli autotest all'accensione non vengono eseguiti e il modulo non si avvia.

Autotest continuo al runtime integrato

Durante il runtime, i moduli di I/O eseguono continuamente una serie di autotest. I moduli di ingresso verificano di potere leggere i dati provenienti dai sensori in tutto il campo. I moduli di uscita verificano che lo stato attuale dell'uscita corrisponda allo stato richiesto.

LED

Ogni modulo I/O di sicurezza dispone di una serie di LED di diagnostica del modulo e del canale sul lato anteriore del modulo:

- I quattro LED superiori (**Run**, **Err**, **I/O** e **Lck**) descrivono insieme lo stato del modulo.
- Le due o quattro (a seconda del modulo) file inferiori di LED, insieme alle quattro file di LED superiori, descrivono lo stato di ogni canale di ingresso o di uscita.

Per maggiori informazioni sulla lettura dei LED del modulo, vedere la sezione relativa alla diagnostica mediante LED dei seguenti moduli di I/O di sicurezza:

- BMXSAI0410 - modulo di ingresso analogico di sicurezza, pagina 235
- BMXSDI1602 - modulo di ingresso digitale di sicurezza, pagina 240
- BMXSDO0802 - modulo di uscita digitale di sicurezza, pagina 246
- BMXSRA0405 - modulo di uscita relè digitale di sicurezza, pagina 251

Diagnostica del cablaggio dei moduli digitali

Sia il modulo di ingresso digitale di sicurezza che il modulo di uscita digitale di sicurezza possono rilevare le seguenti condizioni di diagnostica del cablaggio del canale:

- Conduttore aperto (o interrotto).
- Cortocircuito a 0 V verso terra.
- Cortocircuito a 24 Vcc.
- Circuiti incrociati tra due canali.

  NOTA: La disponibilità di queste funzioni di diagnostica dipende dalla struttura di cablaggio specifica del modulo con i rispettivi dispositivi di campo. Per maggiori informazioni, vedere gli esempi di cablaggio dell'applicazione per i seguenti moduli di I/O digitali di sicurezza:

  - BMXSDI1602 - modulo di ingresso digitale di sicurezza, pagina 76
  - BMXSDO0802 - modulo di uscita digitale di sicurezza, pagina 104

Modulo di ingresso analogico BMXSAI0410

Introduzione

Questa sezione descrive il modulo di ingresso analogico di sicurezza BMXSAI0410.

Modulo di ingresso analogico di sicurezza BMXSAI0410

Introduzione

Il modulo di ingresso analogico di sicurezza BMXSAI0410 presenta le seguenti caratteristiche:

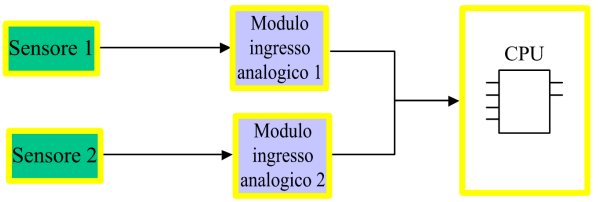
- 4 canali di ingresso di corrente analogici isolati da 4...20 mA.
- 12500 conteggi risoluzione, nel campo dati 0...25 mA.
- Rilevamento di corrente fuori campo per valori di corrente inferiori a 3,75 mA o maggiori di 20,75 mA.
- Supporta i seguenti standard SIL3 (IEC61508):
  - Il modulo è in grado di raggiungere fino a Categoria 2 (Cat2) / Performance Level d (PLd) utilizzando 1 canale di ingresso (valutazione uno su uno (1oo1)). È quindi possibile ottenere Cat1 e Cat2 / PL a, b, c, d utilizzando 1 canale di ingresso.
  - Il modulo è in grado di raggiungere fino a Categoria 4 (Cat4) / Performance Level e (PLe) utilizzando 2 canali di ingresso (valutazione uno su due (1oo2)). È quindi possibile ottenere Cat3 e Cat4 / PL d, e utilizzando 2 canali di ingresso.
- Visualizzazione diagnostica mediante LED, pagina 235 fornita per il modulo e per ogni canale di ingresso.
- Sostituzione a caldo del modulo al runtime.
- CCOTF del modulo in modalità di manutenzione, pagina 261. (La funzione CCOTF non è supportata in modalità di sicurezza, pagina 260).

Alta disponibilità

È possibile configurare l'applicazione di sicurezza con vari livelli di prestazioni e disponibilità, utilizzando canali e moduli di ingresso singoli o ridondanti, nel seguente modo:

Progettazione:	Livelli della funzione di sicurezza:			
Canali di ingresso => Moduli	**SIL**	**Cat**	**PL**	**Alta disponibilità?**
Da canale di ingresso singolo a modulo di ingresso singolo, pagina 60	SIL3	Cat 2	PLd	–
Da canale di ingresso singolo a moduli di ingresso ridondanti, pagina 61	SIL3	Cat 2	PLd	✓
Da canali di ingresso ridondanti a modulo di ingresso singolo, pagina 62	SIL3	Cat 4	PLe	–
Da canali di ingresso ridondanti a moduli di ingresso ridondanti, pagina 63	SIL3	Cat 4	PLe	✓
✓: Fornito – : Non fornito				

La seguente figura illustra la configurazione degli ingressi analogici ridondanti:



Il valore della corrente di ingresso analogica dal sensore 1 e dal sensore 2 viene inviato dal modulo di ingresso 1 e dal modulo di ingresso 2, rispettivamente, a un controller di sicurezza attraverso un black channel. Il controller esegue un blocco funzione dedicato, (`S_AIHA`, in ciascuno dei due programmi logici compilati separati per gestire e selezionare i dati dai due moduli di ingresso. Questo blocco funzione opera nel seguente modo:

- Se lo stato dei dati di ingresso provenienti dal modulo 1 è corretto, i dati di ingresso provenienti da questo modulo vengono utilizzati nella funzione di sicurezza.
- Se lo stato dei dati di ingresso provenienti dal modulo 1 non è corretto, ma lo stato dei dati di ingresso provenienti dal modulo 2 è corretto, vengono utilizzati i dati di ingresso del modulo 2.
- Se lo stato dei dati di ingresso provenienti dal modulo 1 e dal modulo 2 non è corretto, il sistema attiva la funzione di sicurezza.

Connettore di cablaggio BMXSAI0410

Introduzione

Il modulo di ingresso analogico BMXSAI0410 comprende 4 ingressi analogici. Il modulo dispone di due coppie di contatti per ogni ingresso: due contatti di canale (Ch) positivi e due contatti comuni (Com) negativi.

Per ogni ingresso:

- i due contatti del canale (Ch*n*) sono collegati internamente e
- anche i due contatti comuni (Com*n*) sono collegati internamente.

Per collegare un sensore analogico a un ingresso, è possibile utilizzare un contatto del canale o un contatto comune per tale ingresso.

Morsettiere

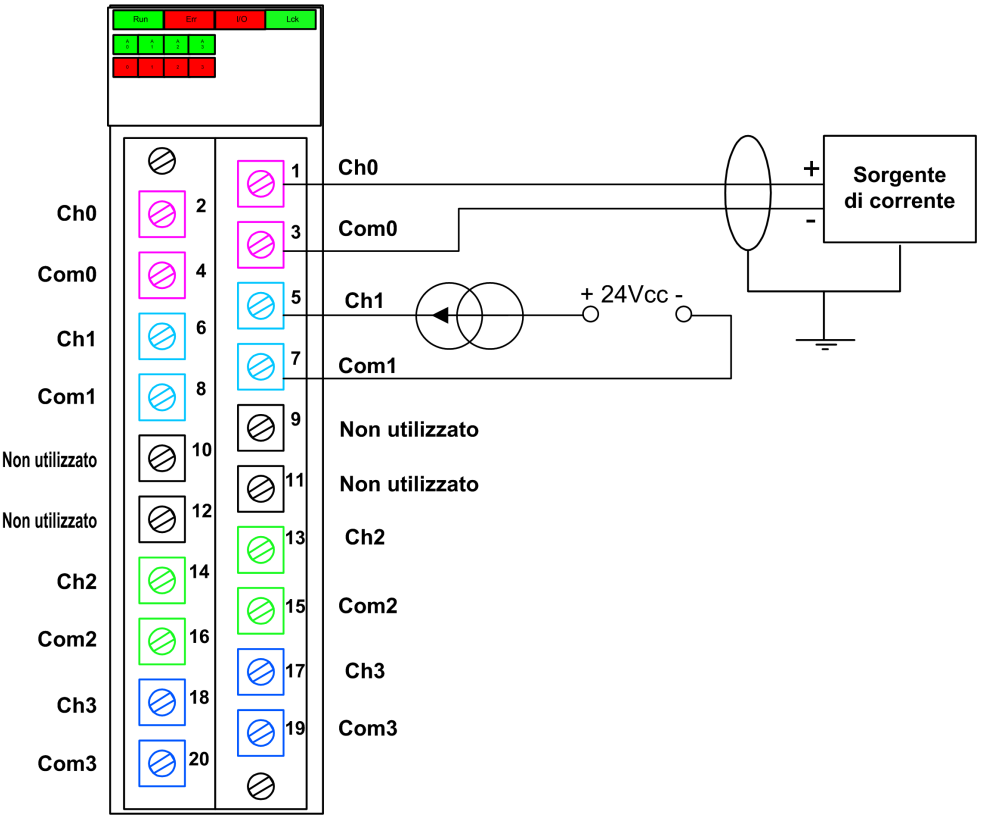
Per inserire il connettore a 20 contatti nel lato anteriore del modulo si possono utilizzare le seguenti morsettiere Schneider Electric a 20 contatti:

- morsettiera con morsetti a vite BMXFTB2010
- morsettiera con morsetti a gabbia BMXFTB2000
- morsettiera con morsetti a molla BMXFTB2020

NOTA: Le morsettiere possono essere rimosse soltanto quando il modulo è disinserito.

Connettore di cablaggio

L'esempio seguente presenta uno schema di cablaggio generico per ingressi sul modulo:



NOTA: Il modulo rileva una condizione di filo interrotto e la segnala come condizione di corrente fuori campo (inferiore a 3,75 mA) impostando l'elemento `OOR` della struttura `T_U_ANA_SIS_CH_IN`, `pagina 67` a "1".

Mappatura degli ingressi ai contatti del connettore

La seguente sezione fornisce una descrizione di ogni contatto del modulo di ingresso analogico BMXSAI0410:

Descrizione del contatto	Numero del contatto sulla morsettiera		Descrizione del contatto
Ingresso (+) del canale 0	2	1	Ingresso (+) del canale 0
Ingresso (–) del canale 0	4	3	Ingresso (–) del canale 0

Descrizione del contatto	Numero del contatto sulla morsettiera		Descrizione del contatto
Ingresso (+) del canale 1	6	5	Ingresso (+) del canale 1
Ingresso (–) del canale 1	8	7	Ingresso (–) del canale 1
Non usato	10	9	Non usato
Non usato	12	11	Non usato
Ingresso (+) del canale 2	14	13	Ingresso (+) del canale 2
Ingresso (–) del canale 2	16	15	Ingresso (–) del canale 2
Ingresso (+) del canale 3	18	17	Ingresso (+) del canale 3
Ingresso (–) del canale 3	20	19	Ingresso (–) del canale 3

NOTA: Dato che i due contatti positivi di ogni ingresso sono collegati internamente, si deve usare solo un contatto positivo per un canale di ingresso. Analogamente, dato che i due contatti negativi di ogni ingresso sono collegati internamente, si deve usare solo un contatto negativo per ogni canale di ingresso.

Ad esempio, per collegare un sensore analogico al canale di ingresso 0, si può collegare:

- il conduttore positivo del sensore al contatto 1 o 2.
- il conduttore negativo del sensore al contatto 3 o 4.

BMXSAI0410 Esempi di cablaggio dell'applicazione di ingresso

Introduzione

È possibile cablare il modulo di ingresso analogico di sicurezza BMXSAI0410 a sensori analogici per raggiungere la conformità SIL3 in diversi modi, a seconda dei seguenti fattori:

- lo standard richiesto di Category (Cat2 o Cat4) e Performance Level (PLd o PLe)
- i requisiti di alta disponibilità dell'applicazione.

Il livello di integrità di sicurezza (SIL) massimo è determinato dall'affidabilità del sensore e dalla lunghezza dell'intervallo del test di prova per IEC 61508.

⚠AVVERTIMENTO

PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Cablare i sensori, che non soddisfano l'affidabilità degli standard SIL previsti, in modo ridondante a due canali.

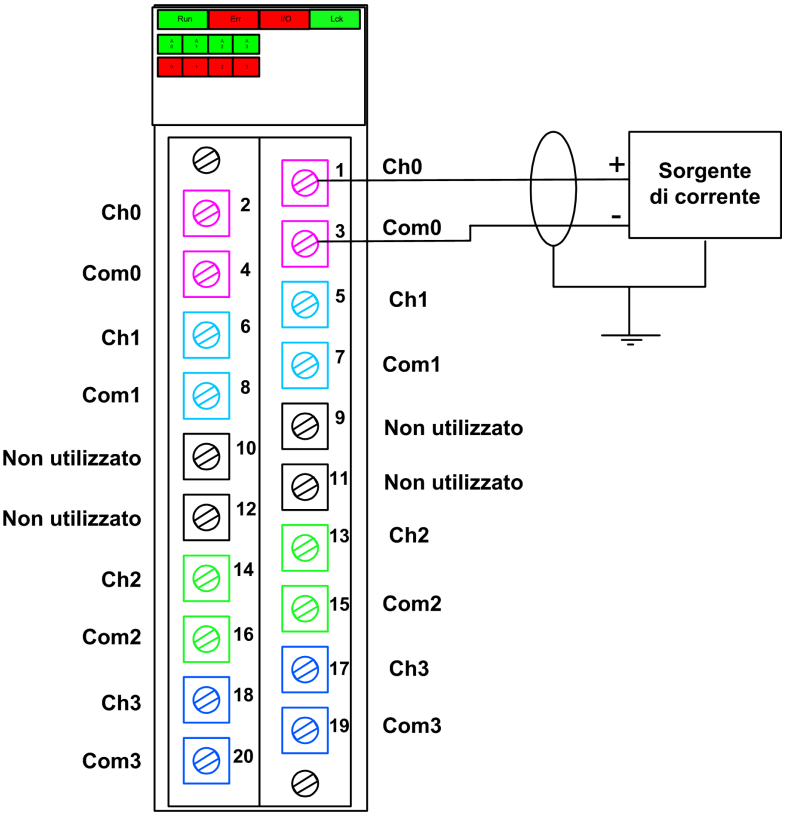
Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Di seguito sono descritti i seguenti esempi di cablaggio dell'applicazione di ingresso digitale SIL3:

- Cat2/PLd:
  - un solo sensore collegato a un ingresso.
- Cat2/PLd con alta disponibilità:
  - due sensori cablati a due punti di ingresso su moduli di ingresso diversi.
- Cat4/PLe:
  - due sensori, ognuno dei quali cablato a un punto di ingresso diverso sullo stesso modulo di ingresso.
- Cat4/PLe con alta disponibilità:
  - due coppie di sensori (per un totale di quattro sensori): i sensori della prima coppia sono singolarmente cablati a un punto di ingresso diverso su un modulo e i sensori della seconda coppia sono singolarmente cablati a un punto di ingresso diverso su un secondo modulo.

SIL3 Cat2/PLd

L'esempio seguente presenta un solo sensore collegato a un punto di ingresso su un singolo modulo di ingresso. Il controller esegue la valutazione 1oo1D sul singolo valore monitorato:



⚠AVVERTIMENTO

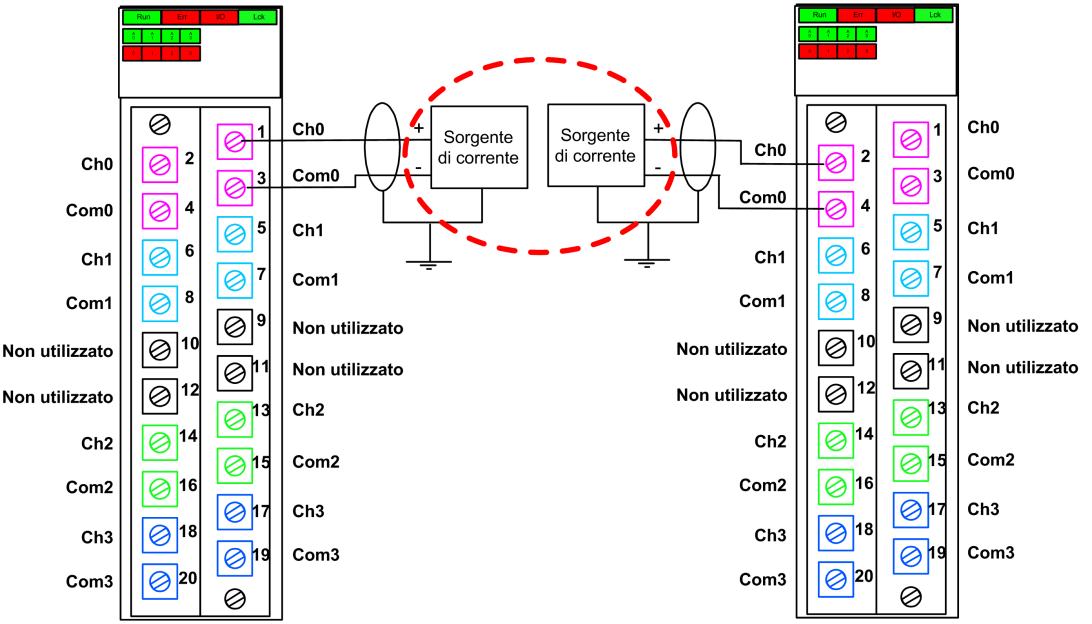
PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Utilizzare un sensore qualificato e idoneo per raggiungere il livello SIL3 secondo IEC61508 e Category 2/Performance Level d secondo ISO13849 tramite questa configurazione di cablaggio.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

SIL3 Cat2/PLd con alta disponibilità

L'esempio seguente presenta due sensori che monitorano la stessa variabile di processo. Ogni sensore è collegato a un solo punto di ingresso su vari moduli di ingresso. Il controller esegue la valutazione 1oo1D del singolo valore monitorato:



NOTA: In questa configurazione, utilizzare il blocco funzione `S_AIHA` nel task SAFE per gestire i due valori delle variabili di processo forniti dai due sensori.

⚠AVVERTIMENTO

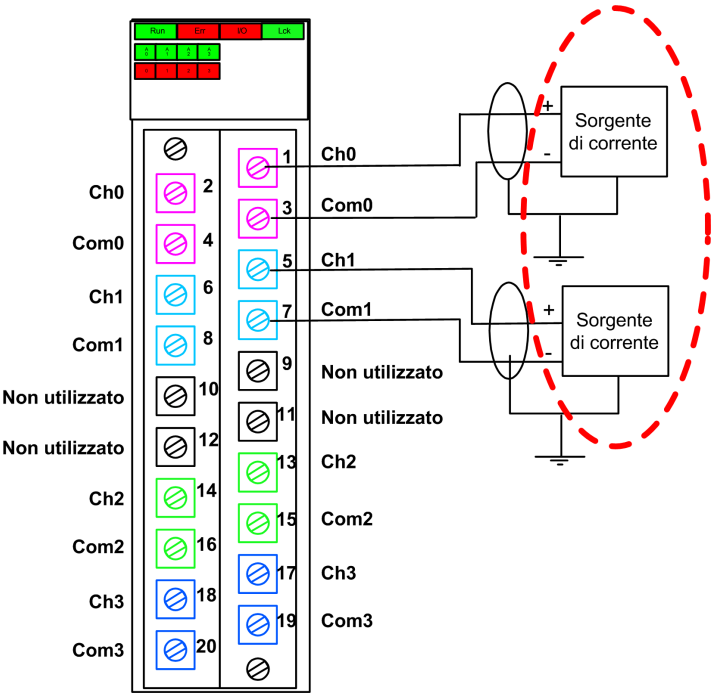
PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Utilizzare un sensore qualificato e idoneo per raggiungere il livello SIL3 secondo IEC61508 e Category 2/Performance Level d secondo ISO13849 tramite questa configurazione di cablaggio.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

SIL3 Cat4/PLe

L'esempio seguente presenta due sensori che monitorano la stessa variabile di processo. Ogni sensore è collegato a un solo punto di ingresso sullo stesso modulo di ingresso. Il controller esegue una valutazione 1oo2D dei valori concorrenti forniti dai due sensori per la stessa variabile di processo:



NOTA: In questa configurazione, utilizzare il blocco funzione `S_AI_COMP` nel task SAFE per eseguire una valutazione 1oo2D dei valori concorrenti provenienti dai due sensori.

⚠AVVERTIMENTO

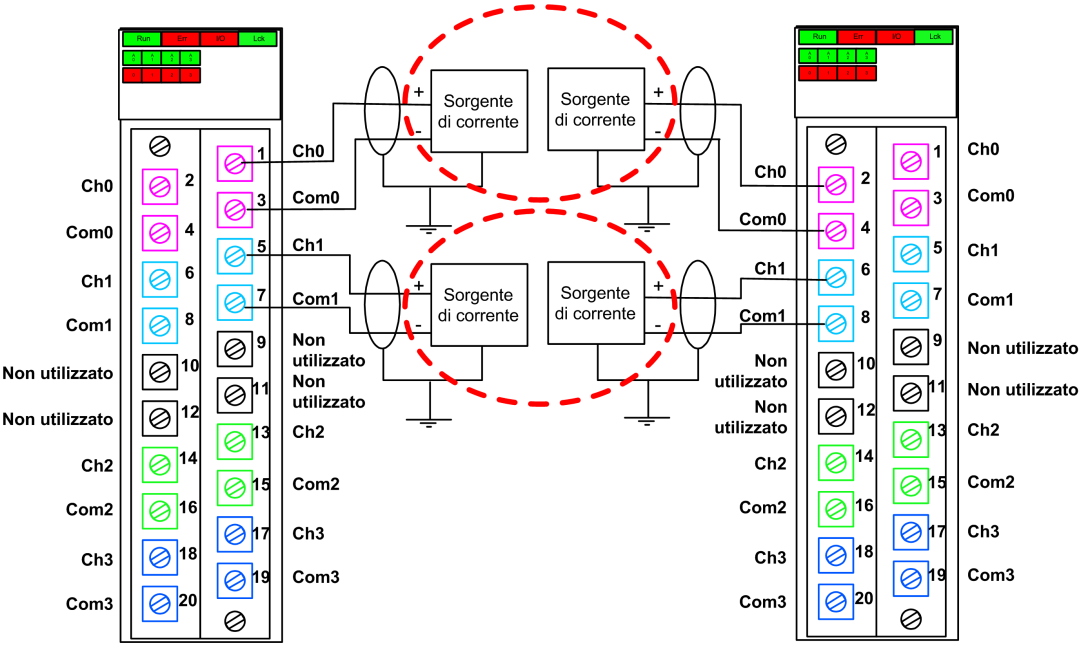
PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Utilizzare un sensore qualificato e idoneo per raggiungere il livello SIL3 secondo IEC 61508 e Category 4/Performance Level e secondo ISO13849 tramite questa configurazione di cablaggio.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

SIL3 Cat4/PLe con alta disponibilità

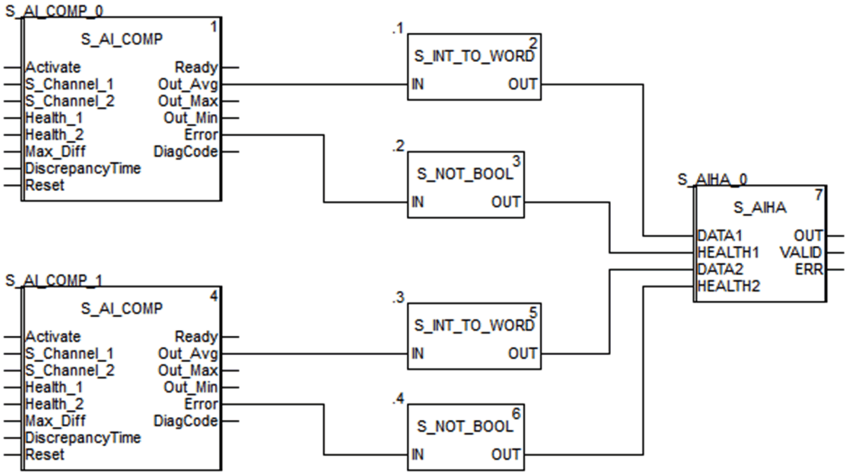
L'esempio seguente presenta due coppie sensori ridondanti che monitorano la stessa variabile di processo. Ogni sensore è collegato a un solo punto di ingresso su due diversi moduli di ingresso (due ingressi in ogni modulo). Questa configurazione consente al controller di eseguire una valutazione 1oo2D:



NOTA: In questa configurazione, è necessario utilizzare i blocchi funzione `S_AI_COMP` e `S_AIHA` all'interno del task SAFE per gestire i quattro segnali di ingresso:

- `S_AI_COMP` per eseguire la valutazione 1oo2 di due coppie di valori provenienti da entrambi i sensori collegati allo stesso modulo.
- `S_AIHA` per gestire la funzione di alta disponibilità.

Il seguente diagramma dei blocchi funzione illustra la configurazione del segmento di codice indicato sopra:



⚠AVVERTIMENTO

PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Utilizzare un sensore qualificato e idoneo per raggiungere il livello SIL3 secondo IEC 61508 e Category 4/Performance Level e secondo ISO13849 tramite questa configurazione di cablaggio.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Struttura dei dati BMXSAI0410

Introduzione

Il tipo di dati derivati del dispositivo (DDDT) `T_U_ANA_SIS_IN_4` è l'interfaccia tra il modulo di ingresso analogico BMXSAI0410 e l'applicazione eseguita nel controller. Il DDDT `T_U_ANA_SIS_IN_4` incorpora i tipi di dati `T_SAFE_COM_DBG_IN` e `T_U_ANA_SIS_CH_IN`.

Tutte queste strutture sono descritte più avanti.

Struttura DDDT `T_U_ANA_SIS_IN_4`

La struttura DDDT `T_U_ANA_SIS_IN_4` include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
MOD_HEALTH[1]	BOOL	• 1: Il modulo funziona correttamente. • 0: Il modulo non funziona correttamente.	RO
SAFE_COM_STS[1]	BOOL	• 1: Comunicazione modulo valida. • 0: Comunicazione modulo non valida.	RO
S_COM_DBG	T_SAFE_COM_DBG_IN	Struttura di debug comunicazione sicura.	RO
CONF_LOCKED	BOOL	• 1: Configurazione del modulo bloccata. • 0: Configurazione del modulo non bloccata.	RO
CH_IN	ARRAY[0...3] di T_U_ANA_SIS_CH_IN	Array di struttura del canale.	–
MUID[2]	ARRAY[0...3] di DWORD	ID univoco del modulo (assegnato automaticamente da Control Expert)	RO
RISERVATO	ARRAY[0...9] di INT	–	–

1. Quando il task SAFE sul controller non è in modalità di esecuzione, i dati scambiati tra il controller e il modulo non vengono aggiornati e MOD_HEALTH e SAFE_COM_STS vengono impostati a 0.

2. Questo valore autogenerato può essere modificato eseguendo il comando **Crea > Rinnova ID e Ricrea tutto** nel menu principale di Control Expert.

Struttura `T_SAFE_COM_DBG_IN`

La struttura `T_SAFE_COM_DBG_IN` include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso[1]
S_COM_EST	BOOL	• 1: Comunicazione con il modulo stabilita. • 0: Comunicazione con il modulo non stabilita o danneggiata.	RO
M_NTP_SYNC	BOOL	Con firmware del controller 3.10 o precedente: • 1: Il modulo è sincronizzato con il server NTP. • 0: Il modulo non è sincronizzato con il server NTP. **NOTA:** con firmware del controller 3.20 o successivo, il valore è sempre 1.	RO
CPU_NTP_SYNC	BOOL	Con firmware del controller 3.10 o precedente: • 1: Il controller è sincronizzato con il server NTP. • 0: Il controller non è sincronizzato con il server NTP. **NOTA:** con firmware del controller 3.20 o successivo, il valore è sempre 1.	RO
CHECKSUM	BYTE	Checksum del frame di comunicazione.	RO
COM_DELAY	UINT	Ritardo di comunicazione tra due valori ricevuti dal modulo: • 1 ... 65534: Il tempo, in ms, trascorso dalla ricezione da parte del controller dell'ultima comunicazione del modulo. • 65535: Il controller non ha ricevuto una comunicazione dal modulo.	RO
COM_TO	UINT	Valore di timeout di comunicazione proveniente dal modulo. **NOTA:** Può essere utili modificare questo valore di lettura/scrittura per renderlo equivalente o maggiore del tempo di comunicazione effettivo per il modulo (ad es. in una derivazione RIO remota).	L/S
STS_MS_IN	UINT	Valore di timestamp sicuro per la frazione di secondo, arrotondato al millisecondo più vicino, dei dati ricevuti dal modulo.	RO
S_NTP_MS	UINT	Valore di tempo sicuro per la frazione di secondo, arrotondato al secondo, per il ciclo corrente.	RO

Elemento	Tipo di dati	Descrizione	Accesso[1]
STS_S_IN	UDINT	Valore di timestamp sicuro in secondi dei dati ricevuti dal modulo.	RO
S_NTP_S	UDINT	Valore di tempo sicuro in secondi per il ciclo corrente.	RO
CRC_IN	UDINT	Valore CRC per i dati ricevuti dal modulo.	RO

Struttura T_U_ANA_SIS_CH_IN

La struttura T_U_ANA_SIS_CH_IN include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
FCT_TYPE	WORD	• 1: Il canale è attivato. • 0: Il canale non è attivato.	RO
CH_HEALTH[1]	BOOL	• 1: Il canale è operativo. • 0: È stato rilevato un errore sul canale, che non è operativo. **Formula**: CH_HEALTH = non (OOR o IC) e SAFE_COM_STS	RO
VALUE	INT	Valore di ingresso analogico. **Formula**: VALUE = se (SAFE_COM_STS e non(IC)) allora READ_VALUE diverso da 0	RO
OOR	BOOL	• 1: Il valore della corrente di ingresso del canale è fuori intervallo: ◦ <3,75 mA ◦ >20,75 mA • 0: Il valore della corrente di ingresso del canale non è fuori intervallo.	RO
IC	BOOL	• 1: Canale non valido rilevato dal modulo. • 0: Il canale è dichiarato internamente operativo dal modulo.	RO
1. Quando il task SAFE sul controller non è in modalità di esecuzione, i dati scambiati tra il controller e il modulo non vengono aggiornati e CH_HEALTH è impostato a 0.			

Modulo di ingresso digitale BMXSDI1602

Introduzione

Questa sezione descrive il modulo di ingresso digitale di sicurezza BMXSDI1602.

Modulo di ingresso digitale di sicurezza BMXSDI1602

Introduzione

Il modulo di ingresso di sicurezza BMXSDI1602 presenta le seguenti caratteristiche:

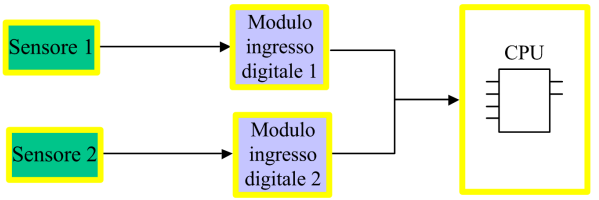
- 16 ingressi del tipo 3 (IEC61131-2), in due gruppi elettricamente non isolati di 8 ingressi.
- Tensione di ingresso nominale 24 Vcc.
- Si ottiene quanto segue:
  - SIL3 IEC61508, SILCL3 IEC62061.
  - SIL4 EN5012x.
  - Categoria 2 (Cat2) / Performance Level d (PLd) ISO13849 ottenuta con 1 canale di ingresso (valutazione uno su uno (1oo1D)).
  - Categoria 4 (Cat4) / Performance Level e (PLe) ISO13849 ottenuta con 2 canali di ingresso (valutazione uno su due (1oo2D)).
- Compatibile con sensori di prossimità a 2 o 3 fili.
- Fornisce in opzione due uscite 24 Vcc (VS1 e VS2) per la supervisione di cortocircuito 24 Vcc:
  - VS1 per monitorare il cortocircuito sugli ingressi 0...3 (rank A e B).
  - VS2 per monitorare il cortocircuito sugli ingressi 4...7 (rank A e B).
- Monitoraggio della tensione di alimentazione esterna 24 Vcc.
- Visualizzazione diagnostica mediante LED, pagina 240 fornita per il modulo e per ogni canale di ingresso.

- Diagnostica del cablaggio del canale configurabile (attiva/disattiva), pagina 77 in grado di rilevare le seguenti condizioni:
  - Conduttore aperto (o interrotto).
  - Cortocircuito a 0 V verso terra.
  - Cortocircuito a 24 Vcc (se l'alimentazione al sensore è fornita internamente).
  - Circuiti incrociati tra i due canali (se l'alimentazione al sensore è fornita internamente).
- Sostituzione a caldo del modulo al runtime.
- CCOTF del modulo in modalità di manutenzione, pagina 261. (La funzione CCOTF non è supportata in modalità di sicurezza, pagina 260).

Alta disponibilità

È possibile usare due sensori collegati a due canali di ingresso diversi situati su moduli di ingresso diversi per monitorare lo stesso valore fisico, aumentando così la disponibilità del sistema.

La figura seguente illustra le configurazioni di ingressi digitali ridondanti:



Il valore dello stato di ingresso dal sensore 1 e dal sensore 2 viene inviato dal modulo di ingresso 1 e dal modulo di ingresso 2, rispettivamente, a un controller di sicurezza tramite un black channel. Il controller esegue un blocco funzione dedicato, S_DIHA, per gestire e selezionare i dati dai due moduli di ingresso. Questo blocco funzione opera nel seguente modo:

- Se lo stato dei dati di ingresso provenienti dal modulo 1 è corretto, i dati di ingresso provenienti da questo modulo vengono utilizzati nella funzione di sicurezza.
- Se lo stato dei dati di ingresso provenienti dal modulo 1 non è corretto, ma lo stato dei dati di ingresso provenienti dal modulo 2 è corretto, vengono utilizzati i dati di ingresso del modulo 2.
- Se lo stato dei dati di ingresso provenienti dal modulo 1 e dal modulo 2 non è corretto, lo stato dell'ingresso viene impostato allo stato sicuro definito ("0") per attivare la funzione di sicurezza.

Per maggiori dettagli su come cablare il modulo per l'alta disponibilità, vedere la descrizione degli esempi di cablaggio dell'applicazione di ingresso, pagina 76.

Connettore di cablaggio BMXSDI1602

Introduzione

Il modulo di ingresso BMXSDI1602 digitale presenta 16 ingressi in due gruppi di 8 ingressi. Il primo gruppo è composto dagli ingressi 0...3 (rank A e B) e il secondo gruppo è composto dagli ingressi 4...7 (rank A e B). Questi due gruppi non sono isolati tra di loro.

L'alimentazione può essere fornita ai sensori sia direttamente da un alimentatore esterno, sia internamente tramite gli alimentatori VS1 e VS2. Le due strutture sono presentate più avanti.

Morsettiere

Per inserire il connettore a 20 contatti nel lato anteriore del modulo si possono utilizzare le seguenti morsettiere Schneider Electric a 20 contatti:

- morsettiera con morsetti a vite BMXFTB2010
- morsettiera con morsetti a gabbia BMXFTB2000
- morsettiera con morsetti a molla BMXFTB2020

NOTA: Le morsettiere possono essere rimosse soltanto quando il modulo è disinserito.

Alimentatore di processo

È necessario un alimentatore di processo a tensione ultra bassa protetta (SELV/PELV) di categoria di sovratensione II da 24 Vcc. Utilizzare un alimentatore che non ripristini automaticamente l'alimentazione dopo un'interruzione dell'alimentazione.

Il livello di integrità di sicurezza (SIL) massimo è determinato dall'affidabilità del sensore e dalla lunghezza dell'intervallo del test di prova per IEC 61508.

⚠PERICOLO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Utilizzare solo un modulo alimentatore di processo di tipo SELV/PELV con un'uscita massima di 60 V.

Il mancato rispetto di queste istruzioni provocherà morte o gravi infortuni.

AVVISO
NON CONFORMITÀ DEL CIRCUITO ELETTRICO Non collegare 0 V di un alimentatore SELV a terra. **Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.**

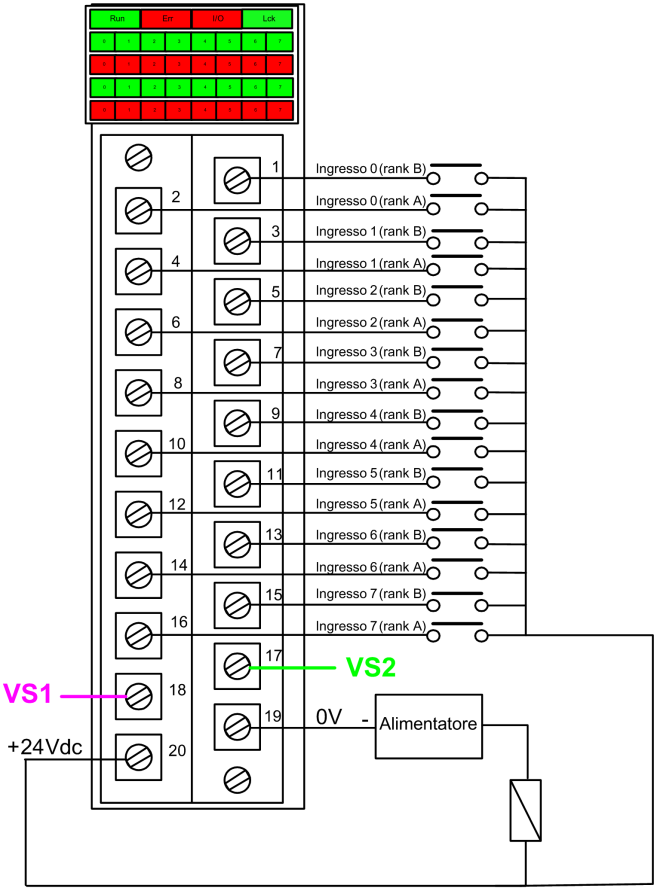
Fusibile

Per proteggere l'alimentatore esterno dai cortocircuiti e da eventuali condizioni di sovratensione, è necessario un fusibile rapido.

AVVISO
SCELTA ERRATA DEL FUSIBILE Utilizzare fusibili rapidi per proteggere i componenti elettronici del modulo di ingresso digitale da una condizione di sovracorrente. **Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.**

Connettore di cablaggio: sensori con alimentazione esterna

Nella seguente struttura, i sensori sono alimentati direttamente da un alimentatore esterno:



alimentazione: 24Vcc

fusibile: fusibile ad azione veloce da 0,5 A

NOTA: L'alimentazione dei sensori dall'esterno limita la diagnostica dei canali che il modulo può effettuare. In questa configurazione di cablaggio, il modulo può rilevare:

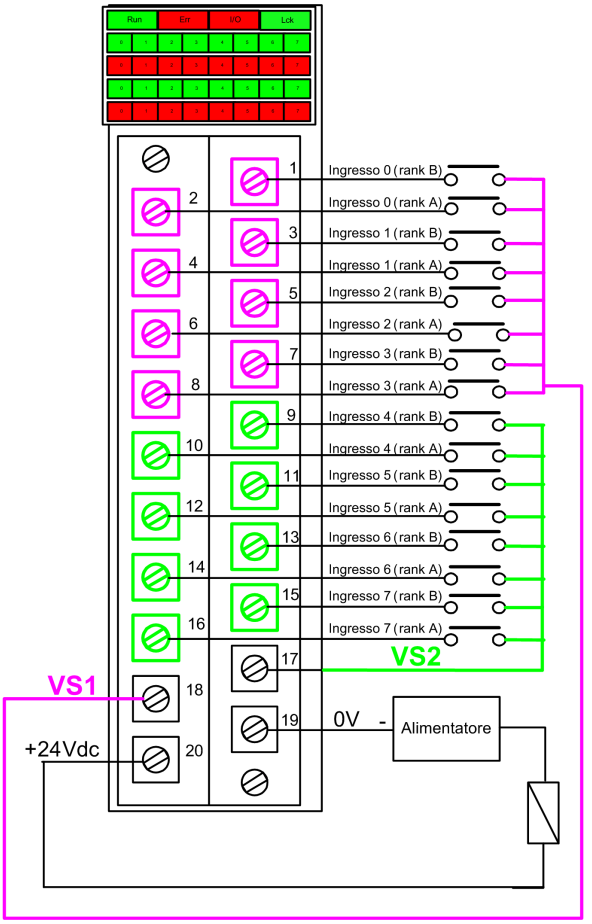
- Una condizione di conduttore interrotto (o aperto), se attivato per il canale in Control Expert.
- Una condizione di cortocircuito verso terra.

Tuttavia, in questa configurazione il modulo non è in grado di rilevare:

- Una condizione di cortocircuito a 24 Vcc.
- Una condizione di circuito incrociato con un altro ingresso di cablaggio.

Connettore di cablaggio: sensori con alimentazione interna VS

Nella seguente configurazione, i sensori per i canali 0...3 sono alimentati dall'alimentatore VS1 monitorato e i sensori per i canali 4...7 sono alimentati dall'alimentatore VS2 monitorato:



Se si usa questa configurazione, applicare l'alimentazione interna ai gruppi di canali nel seguente modo:

- Utilizzare VS1 per alimentare i canali 0...3 (rank A e B).
- Utilizzare VS2 per alimentare i canali 4...7 (rank A e B).

NOTA: In questa configurazione, il modulo può rilevare:

- Una condizione di cortocircuito a 24 Vcc, se attivato per il canale in Control Expert.
- Una condizione di circuito incrociato con un altro ingresso di cablaggio.
- Una condizione di conduttore interrotto (o aperto), se attivato per il canale in Control Expert.
- Una condizione di cortocircuito verso terra.

Mappatura degli ingressi ai contatti del connettore e ai canali Control Expert

Di seguito viene fornita una descrizione di ogni pin sul modulo di ingresso BMXSDI1602 e con assegnazione di ciascun contatto al relativo canale, come indicato nella scheda **Configurazione** del canale per il modulo in Control Expert Safety:

Canale Control Expert	**Descrizione del contatto**	**Numero del contatto sulla morsettiera**		**Descrizione del contatto**	**Canale Control Expert**
0	Ingresso 0 (rank A)	2	1	Ingresso 0 (rank B)	8
1	Ingresso 1 (rank A)	4	3	Ingresso 1 (rank B)	9
2	Ingresso 2 (rank A)	6	5	Ingresso 2 (rank B)	10
3	Ingresso 3 (rank A)	8	7	Ingresso 3 (rank B)	11
4	Ingresso 4 (rank A)	10	9	Ingresso 4 (rank B)	12
5	Ingresso 5 (rank A)	12	11	Ingresso 5 (rank B)	13
6	Ingresso 6 (rank A)	14	13	Ingresso 6 (rank B)	14
7	Ingresso 7 (rank A)	16	15	Ingresso 7 (rank B)	15
–	Alimentatore VS1	18	17	Alimentatore VS2	–
–	Alimentazione di processo 24 Vcc	20	19	Alimentazione di processo 24 Vcc	–

BMXSDI1602 Esempi di cablaggio dell'applicazione di ingresso

Introduzione

È possibile cablare il modulo di ingresso digitale di sicurezza BMXSDI1602 a sensori per raggiungere la conformità SIL3 in diversi modi, a seconda dei seguenti fattori:

- lo standard richiesto di Category (Cat2 o Cat4) e Performance Level (PLd o PLe)
- i requisiti di alta disponibilità dell'applicazione.

Il livello di integrità di sicurezza (SIL) massimo è determinato dall'affidabilità del sensore e dalla lunghezza dell'intervallo del test di prova per IEC 61508.

⚠AVVERTIMENTO

PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Cablare i sensori, che non soddisfano l'affidabilità degli standard SIL previsti, in modo ridondante a due canali.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Di seguito sono descritti i seguenti esempi di cablaggio dell'applicazione di ingresso digitale SIL3:

- Cat2/PLd:
  - un sensore singolo collegato a un ingresso
- Cat2/PLd con alta disponibilità:
  - un sensore singolo collegato a due punti di ingresso su moduli di ingresso diversi
  - due sensori cablati a due punti di ingresso su moduli di ingresso diversi
- Cat4/PLe:
  - un sensore singolo collegato a due punti di ingresso sullo stesso modulo di ingresso
  - due sensori, ognuno dei quali cablato a un punto di ingresso diverso sullo stesso modulo di ingresso
- Cat4/PLe con alta disponibilità:
  - due sensori, ognuno dei quali cablato a due punti di ingresso diversi su moduli di ingresso diversi

Diagnostica di cablaggio configurabile in Control Expert

Per il modulo di ingresso digitale di sicurezza BMXSDI1602, utilizzare la pagina **Configurazione** in Control Expert per:

- Attivare **Rilevamento cortocircuito a 24V** per ogni canale alimentato. Questo test esegue le seguenti operazioni di diagnostica del cablaggio degli attuatori per un canale:
  - Rilevamento cortocircuito a 24V.
  - Rilevamento circuiti incrociati tra due canali di uscita.

  Il principio è quello fornire l'alimentazione ai sensori, per gruppi di 8 canali (con VS1 per i canali da 0 a 3 (rank A e B) e VS2 per i canali da 4 a 7 (rank A e B)). Un impulso di OFF viene applicato periodicamente a queste uscite di alimentazione con un periodo inferiore a 1 secondo e una durata inferiore a 1 ms. Durante questo impulso, se la corrente immessa nell'ingresso non è pari a 0, il modulo considera che l'ingresso è in cortocircuito.
- Attivare **Rilevamento filo aperto** per ognuno degli otto canali, che esegue la seguente diagnostica di cablaggio per quel canale:
  - Rilevamento di conduttore aperto (o interrotto) (ovvero il canale di ingresso non è collegato al sensore)
  - Rilevamento di cortocircuito a 0 Vcc verso terra.

  L'obiettivo è creare artificialmente e quindi misurare una corrente di dispersione (dispersione) sulla linea (con un resistore in parallelo al sensore) quando il sensore è aperto. Se la corrente di dispersione (0,4 mA <dispersione < 1,3 mA) non può essere misurata sulla linea di ingresso dal modulo, la linea esterna viene considerata interrotta (o in una condizione di cortocircuito verso terra). La diagnostica viene eseguita con un periodo inferiore a 10 ms.
  - Per un sensore con contatto a secco, impostare in parallelo con il sensore una resistenza da 33 kΩ.
  - Con DDP a 2 o 3 fili la corrente di dispersione deve scendere entro i limiti definiti sopra. Occorre definire il valore della resistenza da impostare in parallelo al sensore, considerando la corrente di dispersione naturale del sensore e la resistenza interna dell'ingresso (7,5 kΩ).

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

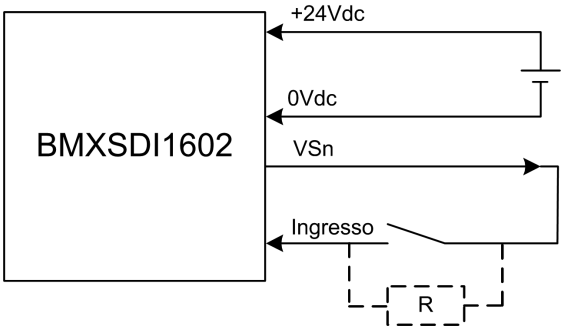
Attivare la diagnostica disponibile fornita in Control Expert per rilevare o escludere le condizioni elencate sopra.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Se un test di diagnostica non è attivato o non è disponibile in Control Expert, applicare misure di sicurezza alternative per rilevare o escludere tali condizioni.

SIL3 Cat2/PLd

Sensore singolo collegato a un ingresso, alimentato da VS interno:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

Dato che il sensore è alimentato internamente tramite un contatto VS, si applica la seguente diagnostica di cablaggio del canale:

Condizione	**Rilevabile?**	**Tempo di rilevamento tipico**
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc[1]	Sì	< 1 s
Circuiti incrociati tra due canali[1]	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di un **sensore singolo collegato con un ingresso, alimentato da VS interno**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di circuiti incrociati tra canali nello stesso gruppo.

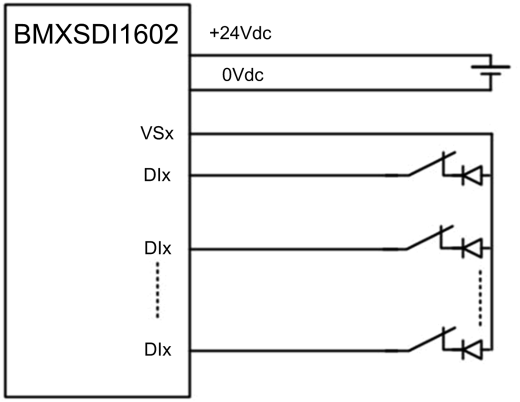
⚠AVVERTIMENTO

CIRCUITI INCROCIATI TRA CANALI NELLO STESSO GRUPPO

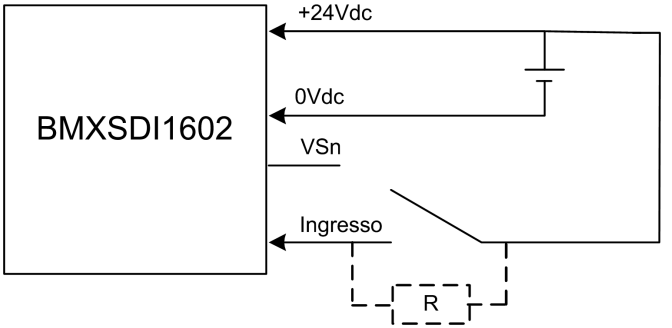
Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali nello stesso gruppo VS del canale.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

NOTA: Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito a 24 Vcc su un canale possa causare la stessa condizione su un canale contiguo.



Sensore singolo collegato con un ingresso alimentato da alimentatore esterno:



Poiché il sensore è alimentato esternamente, si applica la seguente diagnostica di cablaggio del canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc	No	–
Circuiti incrociati tra due canali	No	

1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.

Nel caso di un **sensore singolo collegato con un ingresso, alimentato esternamente**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di un cortocircuito a 24 Vcc e/o circuito incrociato tra due canali.

⚠AVVERTIMENTO

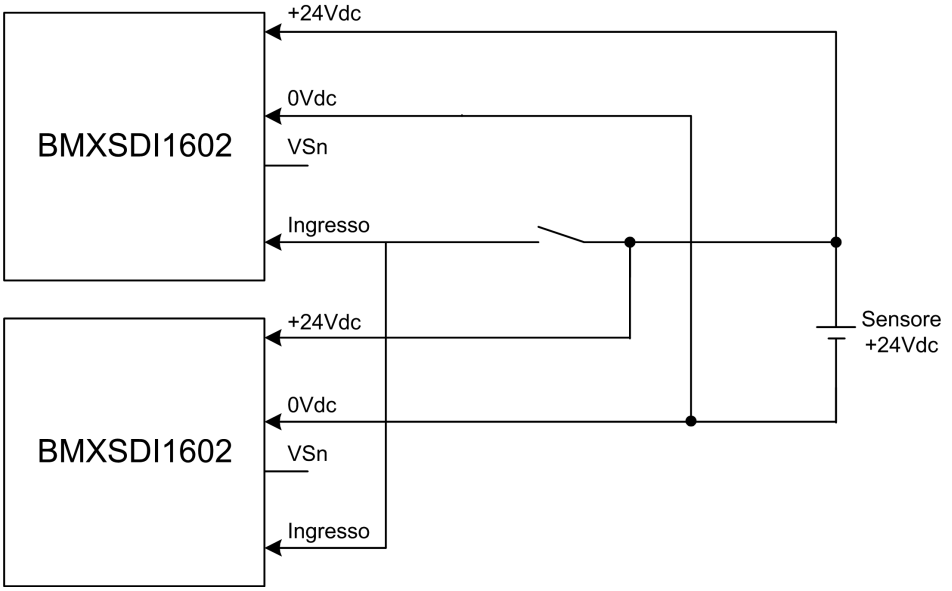
CIRCUITI INCROCIATI TRA CANALI O CORTOCIRCUITO A 24 VCC

Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali o un cortocircuito a 24 VCC.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

SIL3 Cat2/PLd con alta disponibilità

Sensore singolo collegato su due ingressi alimentati esternamente:



Poiché il sensore singolo è alimentato esternamente, si applica la seguente diagnostica di cablaggio del canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	No	–
Cortocircuito a 0 V verso terra	No	
Cortocircuito a 24 Vcc[1]	No	
Circuiti incrociati tra due canali	No	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di un **sensore singolo collegato con due ingressi, con alimentazione esterna**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di un cortocircuito a 24 Vcc e/o circuito incrociato tra due canali.

⚠AVVERTIMENTO

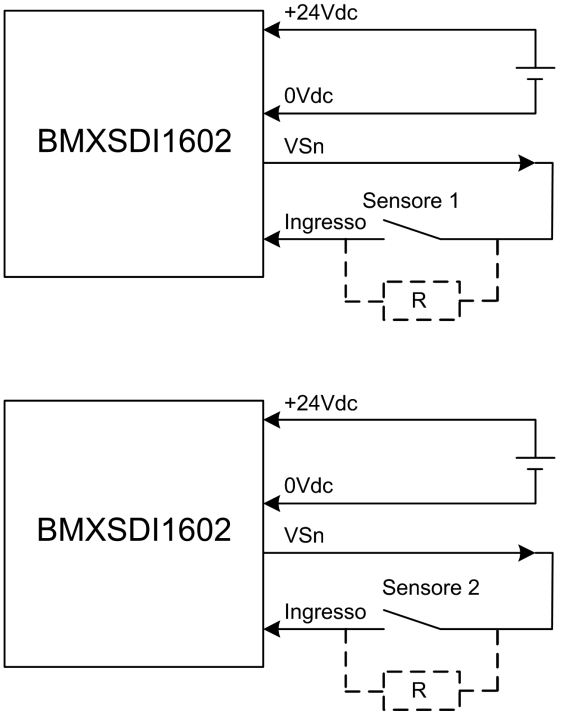
CIRCUITI INCROCIATI TRA CANALI O CORTOCIRCUITO A 24 VCC

Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali o un cortocircuito a 24 VCC.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Due sensori ridondanti collegati su ingressi singoli di due moduli che utilizzano VS:

L'esempio seguente presenta due sensori ridondanti (che possono essere accoppiati meccanicamente o meno) che vengono utilizzati per acquisire la stessa variabile di processo. Ogni sensore è cablato a un singolo punto di ingresso su un modulo di ingresso diverso, con alimentazione fornita dall'alimentatore VS monitorato:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione si può utilizzare il blocco funzione `S_DIHA` per gestire i due segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito a 24 Vcc su un canale possa causare la stessa condizione su un canale contiguo.

Dato che il sensore è alimentato internamente tramite un contatto VS, si applica la seguente diagnostica di cablaggio del canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc[1]	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di **due sensori ridondanti collegati su ingressi singoli di due moduli che usano VS**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di circuiti incrociati tra canali nello stesso gruppo.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI TRA CANALI NELLO STESSO GRUPPO

Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali nello stesso gruppo VS del canale.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Due sensori ridondanti collegati su ingressi singoli di due moduli con alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vcc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Dato che il sensore è alimentato internamente tramite un contatto VS, si applica la seguente diagnostica di cablaggio del canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc	No	–
Circuiti incrociati tra due canali	No	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

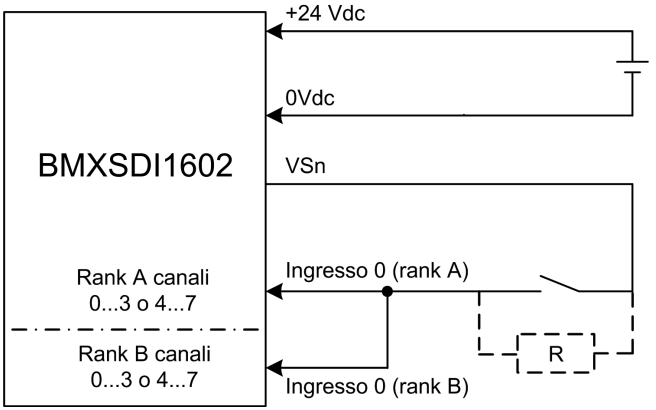
Nel caso di **due sensori ridondanti collegati su ingressi singoli di due moduli con alimentazione esterna**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di un cortocircuito a 24 Vcc e/o circuito incrociato tra due canali.

⚠AVVERTIMENTO
CIRCUITI INCROCIATI TRA CANALI O CORTOCIRCUITO A 24 VCC Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali o un cortocircuito a 24 VCC. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Cat4/PLe

Sensore singolo collegato su due ingressi dello stesso modulo con Vs:

L'esempio seguente presenta un sensore singolo cablato a due punti di ingresso sullo stesso modulo di ingresso, con alimentazione fornita dall'alimentatore VS monitorato:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione si può utilizzare il blocco funzione `S_EQUIVALENT` per gestire i due segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito a 24 Vcc su un canale possa causare la stessa condizione su un canale contiguo.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione dal pin VS:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc[1]	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di un **sensore singolo collegato su due ingressi dello stesso modulo con Vs**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di circuiti incrociati tra canali nello stesso gruppo.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI TRA CANALI NELLO STESSO GRUPPO

Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali nello stesso gruppo VS del canale.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Sensore singolo collegato su due ingressi dello stesso modulo con alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vcc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione esterna:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc[1]	No	–
Circuiti incrociati tra due canali	No	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di un **sensore singolo collegato su due ingressi dello stesso modulo con alimentazione esterna**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di un cortocircuito a 24 Vcc e/o circuito incrociato tra due canali.

⚠AVVERTIMENTO

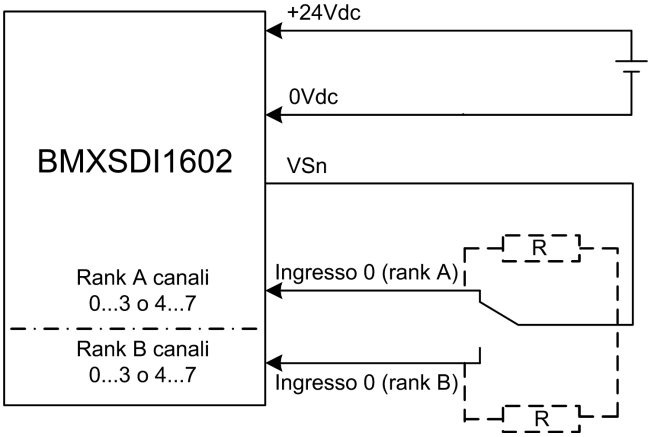
CIRCUITI INCROCIATI TRA CANALI O CORTOCIRCUITO A 24 VCC

Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali o un cortocircuito a 24 VCC.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Sensore non equivalente collegato su due ingressi non equivalenti dello stesso modulo con Vs:

L'esempio seguente presenta un sensore singolo non equivalente cablato a due punti di ingresso sullo stesso modulo di ingresso, con alimentazione fornita da un alimentatore VS monitorato. Il modulo esegue una valutazione 1oo2D:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione si può utilizzare il blocco funzione `S_ANTIIVALENT` per gestire i due segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito a 24 Vcc su un canale possa causare la stessa condizione su un canale contiguo.

Diagnostica di cablaggio con sensori singoli non equivalenti collegati su due ingressi e alimentazione dal pin VS:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc[1]	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Sensore non equivalente collegato su due ingressi non equivalenti dello stesso modulo con alimentazione esterna:

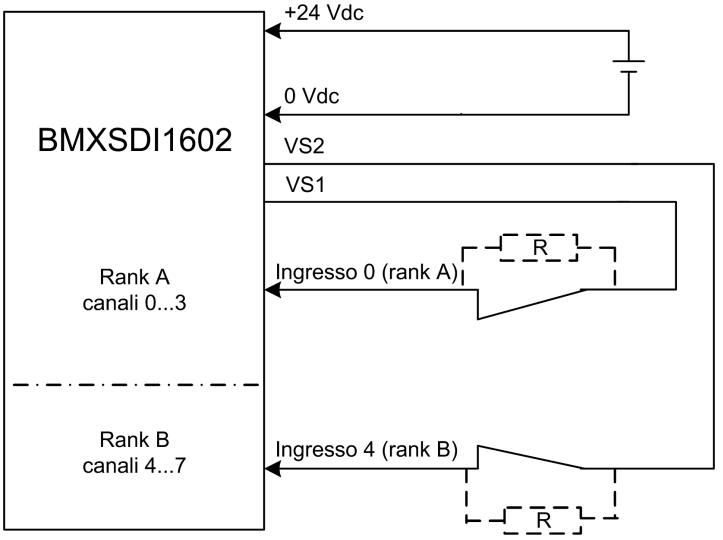
NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vcc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Diagnostica di cablaggio con sensori singoli non equivalenti collegati su due ingressi e alimentazione esterna:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc[1]	No	–
Circuiti incrociati tra due canali	No	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Acquisizione della stessa variabile di processo tramite due sensori separati (accoppiati meccanicamente o meno) con VS:

L'esempio seguente presenta due sensori ridondanti (che possono essere accoppiati meccanicamente o meno) che vengono utilizzati per acquisire la stessa variabile di processo. Ogni sensore è cablato a un singolo punto di ingresso sullo stesso modulo di ingresso, con alimentazione fornita dall'alimentatore VS monitorato:



NOTA:

- Gli ingressi 0...3 dal rank A vengono utilizzati con gli ingressi 4...7 dal rank B.
- Gli ingressi 0...3 dal rank B vengono utilizzati con gli ingressi 4...7 dal rank A.

⚠AVVERTIMENTO

PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Utilizzare sensori idonei e qualificati per raggiungere il livello SIL3 secondo IEC 61508 e Category 4/Performance Level e secondo ISO13849 tramite questa configurazione di cablaggio.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione si può utilizzare il blocco funzione `S_EQUIVALENT` per gestire i due segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito a 24 Vcc su un canale possa causare la stessa condizione su un canale contiguo.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione dal pin VS:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc[1]	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di **Acquisizione della stessa variabile di processo tramite due sensori separati (accoppiati meccanicamente o meno) con VS**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di circuiti incrociati tra canali nello stesso gruppo.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI TRA CANALI NELLO STESSO GRUPPO

Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali nello stesso gruppo VS del canale.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Acquisizione della stessa variabile di processo tramite due sensori separati (accoppiati meccanicamente o meno) con alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vcc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione esterna:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc[1]	No	–
Circuiti incrociati tra due canali	No	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di **Acquisizione della stessa variabile di processo tramite due sensori separati (accoppiati meccanicamente o meno) con alimentazione esterna**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di un cortocircuito a 24 Vcc e/o circuito incrociato tra due canali.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI TRA CANALI O CORTOCIRCUITO A 24 VCC

Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali o un cortocircuito a 24 VCC.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠AVVERTIMENTO

PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

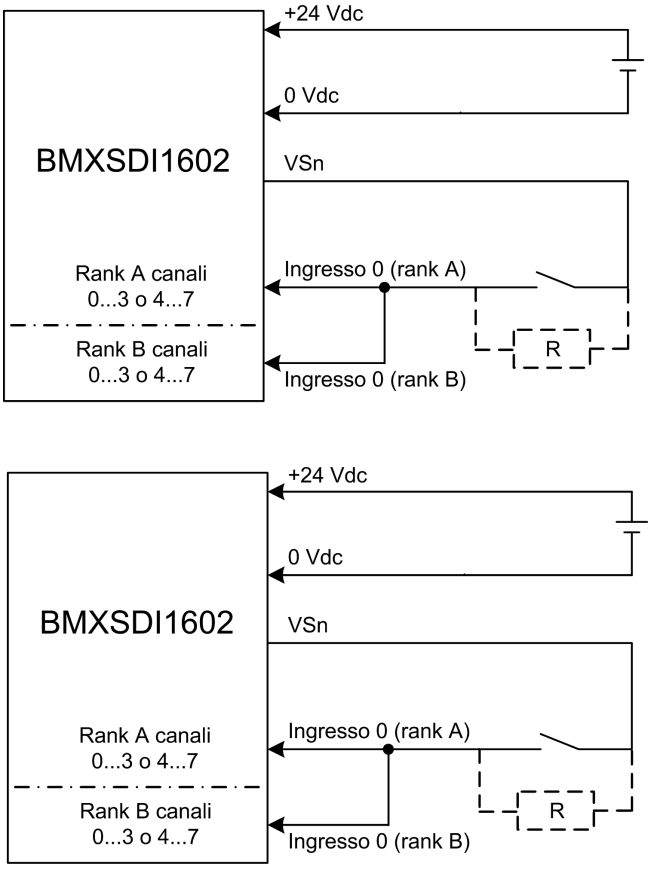
Utilizzare un sensore idoneo per raggiungere il livello SIL3/Cat4/PLe utilizzando questo cablaggio.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Cat4/PLe con alta disponibilità

Schema di cablaggio con collegamento a canale singolo di due sensori a canale singolo ridondanti con uso del modulo Vs:

L'esempio seguente presenta due sensori a canale singolo ridondanti (che possono essere accoppiati meccanicamente o meno), ognuno dei quali è cablato a due punti di ingresso su due moduli di ingresso diversi, con alimentazione fornita dall'alimentatore VS monitorato:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione, è possibile utilizzare i blocchi funzione `S_EQUIVALENT` e `S_DIHA` per gestire i quattro segnali di ingresso.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito a 24 Vcc su un canale possa causare la stessa condizione su un canale contiguo.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione dal pin VS:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vcc[1]	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di un **collegamento a canale singolo di due sensori a canale singolo ridondanti con Vs**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di circuiti incrociati tra canali nello stesso gruppo.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI TRA CANALI NELLO STESSO GRUPPO

Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali nello stesso gruppo VS del canale.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Schema di cablaggio con collegamento a canale singolo di due sensori a canale singolo ridondanti con uso di alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno. In questo caso una condizione di cortocircuito 24 Vcc e una condizione di circuiti incrociati tra due canali non sarebbero rilevabili.

Diagnostica di cablaggio con sensore singolo collegato su due ingressi e alimentazione esterna:

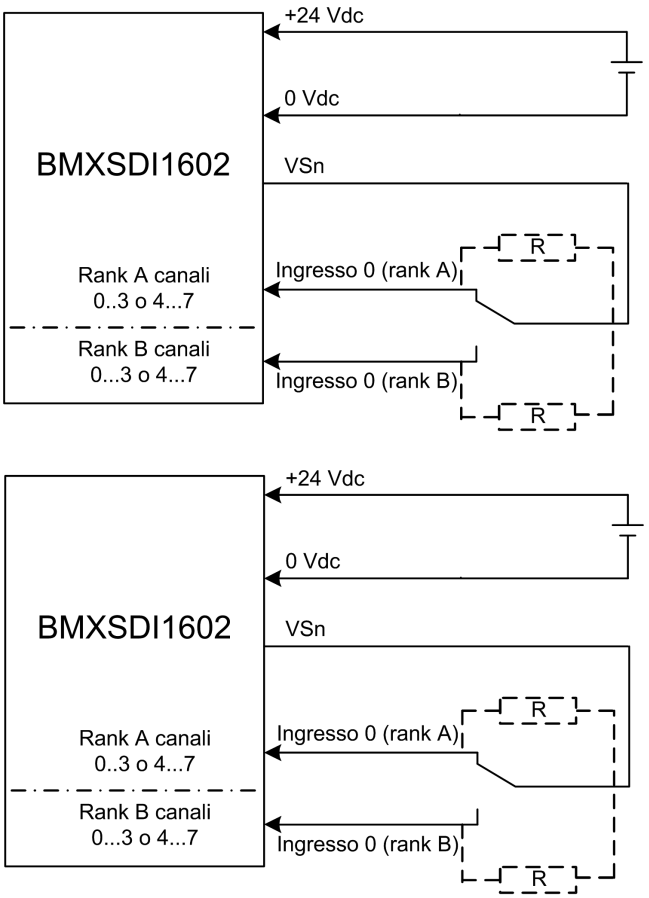
Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc[1]	No	–
Circuiti incrociati tra due canali	No	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di un **collegamento a canale singolo di due sensori a canale singolo ridondanti con alimentazione esterna**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di un cortocircuito a 24 Vcc e/o circuito incrociato tra due canali.

⚠ AVVERTIMENTO
CIRCUITI INCROCIATI TRA CANALI O CORTOCIRCUITO A 24 VCC Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali o un cortocircuito a 24 VCC. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Sensore non equivalente (accoppiato meccanicamente o meno) collegato su due ingressi non equivalenti di due moduli diversi con uso del modulo Vs:

L'esempio seguente presenta due coppie di sensori non equivalenti ridondanti (che possono essere accoppiati meccanicamente o meno), ognuno dei quali è cablato a un singolo punto di ingresso su due moduli di ingresso diversi (due su ciascun modulo), con alimentazione fornita dall'alimentatore VS monitorato:



In questo esempio, se l'alimentazione interna è fornita da:

- VS1, utilizza i canali 0...3 rank A e B.
- VS2, utilizza i canali 4...7 rank A e B.

NOTA:

- In questa configurazione, è necessario utilizzare i blocchi funzione `S_ANTIVALENT` e `S_DIHA` per gestire i quattro segnali di ingresso.
  - `S_ANTIVALENT` per eseguire la valutazione 1oo2 di due coppie di valori provenienti da entrambi i sensori collegati allo stesso modulo.
  - `S_DIHA` per gestire la funzionalità di alta disponibilità.
- Prendere in considerazione la possibilità di aggiungere un diodo Shottky al loop di ingresso, tra il sensore e il punto di ingresso, per ridurre la probabilità che una condizione di cortocircuito a 24 Vcc su un canale possa causare la stessa condizione su un canale contiguo.

Dato che il sensore è alimentato internamente tramite un contatto VS, si applica la seguente diagnostica di cablaggio del canale:

Condizione	Rilevabile?	Tempo di rilevamento tipico
Conduttore aperto (o interrotto)[1]	Sì	< 10 ms
Cortocircuito a 0 V verso terra	Sì	
Cortocircuito a 24 Vdc[1]	Sì	< 1 s
Circuiti incrociati tra due canali	Sì	
1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.		

Nel caso di un **sensore non equivalente (accoppiato meccanicamente o meno) collegato su due ingressi non equivalenti di due moduli diversi con Vs**, applicare misure di sicurezza alternative per rilevare o escludere la possibilità di circuiti incrociati tra canali nello stesso gruppo.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI TRA CANALI NELLO STESSO GRUPPO

Applicare misure di sicurezza alternative per il modulo per rilevare i circuiti incrociati tra due canali nello stesso gruppo VS del canale.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Sensore non equivalente (accoppiato meccanicamente o meno) collegato su due ingressi non equivalenti di due moduli diversi con alimentazione esterna:

NOTA: In alternativa, l'alimentazione può essere fornita ai sensori da un alimentatore esterno (nel caso di un sensore non equivalente collegato su due ingressi non equivalenti di due moduli diversi con alimentazione esterna). In questo caso una condizione di circuiti incrociati tra due canali non sarebbe rilevabile.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI TRA CANALI

Applicare misure di sicurezza alternative per il modulo per rilevare circuiti incrociati tra due canali.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠AVVERTIMENTO

PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Utilizzare sensori idonei e qualificati per raggiungere il livello SIL3 secondo IEC 61508 e Category 4/Performance Level e secondo ISO13849 tramite questa configurazione di cablaggio.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Struttura dei dati BMXSDI1602

Introduzione

Il tipo di dati derivati del dispositivo (DDDT) `T_U_DIS_SIS_IN_16` il è l'interfaccia tra il modulo di ingresso digitale BMXSDI1602 e l'applicazione eseguita nel controller. Il DDDT `T_U_DIS_SIS_IN_16` incorpora i tipi di dati `T_SAFE_COM_DBG_IN` e `T_U_DIS_SIS_CH_IN`.

Tutte queste strutture sono descritte più avanti.

Struttura DDDT `T_U_DIS_SIS_IN_16`

La struttura DDDT `T_U_DIS_SIS_IN_16` include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
MOD_HEALTH[1]	BOOL	• 1: Il modulo funziona correttamente. • 0: Il modulo non funziona correttamente.	RO
SAFE_COM_STS[1]	BOOL	• 1: Comunicazione modulo valida.	RO

Elemento	Tipo di dati	Descrizione	Accesso
		• 0: Comunicazione modulo non valida.	
PP_STS	BOOL	• 1: L'alimentazione di processo è funzionante. • 0: L'alimentazione di processo non è funzionante.	RO
CONF_LOCKED	BOOL	• 1: Configurazione del modulo bloccata. • 0: Configurazione del modulo non bloccata.	RO
S_COM_DBG	T_SAFE_COM_DBG_IN	Struttura di debug comunicazione sicura.	RO
CH_IN_A	ARRAY[0...7] di T_U_DIS_SIS_CH_IN	Array di struttura del canale dal rank A.	–
CH_IN_B	ARRAY[0...7] di T_U_DIS_SIS_CH_IN	Array di struttura del canale dal rank B.	–
MUID[2]	ARRAY[0...3] di DWORD	ID univoco del modulo (assegnato automaticamente da Control Expert)	RO
RISERVATO	ARRAY[0...9] di INT	–	–

1. Quando il task SAFE sul controller non è in modalità di esecuzione, i dati scambiati tra il controller e il modulo non vengono aggiornati e MOD_HEALTH e SAFE_COM_STS vengono impostati a 0.

2. Questo valore autogenerato può essere modificato eseguendo il comando **Crea > Rinnova ID e Ricrea tutto** nel menu principale di Control Expert.

Struttura `T_SAFE_COM_DBG_IN`

La struttura `T_SAFE_COM_DBG_IN` include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
S_COM_EST	BOOL	• 1: Comunicazione con il modulo stabilita. • 0: Comunicazione con il modulo non stabilita o danneggiata.	RO
M_NTP_SYNC	BOOL	Con firmware del controller 3.10 o precedente: • 1: Il modulo è sincronizzato con il server NTP. • 0: Il modulo non è sincronizzato con il server NTP.	RO

Elemento	Tipo di dati	Descrizione	Acces-so
		NOTA: con firmware del controller 3.20 o successivo, il valore è sempre 1.	
CPU_NTP_SYNC	BOOL	Con firmware del controller 3.10 o precedente: • 1: Il controller è sincronizzato con il server NTP. • 0: Il controller non è sincronizzato con il server NTP. **NOTA:** con firmware del controller 3.20 o successivo, il valore è sempre 1.	RO
CHECKSUM	BYTE	Checksum del frame di comunicazione.	RO
COM_DELAY	UINT	Ritardo di comunicazione tra due valori ricevuti dal modulo: • 1 ... 65534: Il tempo, in ms, trascorso dalla ricezione da parte del controller dell'ultima comunicazione del modulo. • 65535: Il controller non ha ricevuto una comunicazione dal modulo.	RO
COM_TO	UINT	Valore di timeout di comunicazione proveniente dal modulo.	L/S
STS_MS_IN	UINT	Valore di timestamp sicuro per la frazione di secondo, arrotondato al millisecondo più vicino, dei dati ricevuti dal modulo.	RO
S_NTP_MS	UINT	Valore di tempo sicuro per la frazione di secondo, arrotondato al secondo, per il ciclo corrente.	RO
STS_S_IN	UDINT	Valore di timestamp sicuro in secondi dei dati ricevuti dal modulo.	RO
S_NTP_S	UDINT	Valore di tempo sicuro in secondi per il ciclo corrente.	RO
CRC_IN	UDINT	Valore CRC per i dati ricevuti dal modulo.	RO

Struttura `T_U_DIS_SIS_CH_IN`

La struttura `T_U_DIS_SIS_CH_IN` include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
CH_HEALTH[1]	BOOL	• 1: Il canale è operativo. • 0: È stato rilevato un errore sul canale, che non è operativo. **Formula:** CH_HEALTH = non (OC o IC o SC) e SAFE_COM_STS	RO
VALUE[2]	EBOOL	• 1: L'ingresso è alimentato. • 0: L'ingresso non è alimentato. **Formula:** VALUE = se (SAFE_COM_STS e non(IC)) allora READ_VALUE diverso da 0	RO
OC	BOOL	• 1: Il canale è aperto o cortocircuitato verso terra. • 0: Il canale è collegato e non cortocircuitato verso terra.	RO
SC	BOOL	• 1: Il canale è cortocircuitato con una sorgente 24 V oppure i due canali sono incrociati. • 0: Il canale non è cortocircuitato con una sorgente 24 V oppure i due canali sono incrociati.	RO
IC	BOOL	• 1: Canale non valido rilevato dal modulo. • 0: Il canale è dichiarato internamente operativo dal modulo.	RO
V_OC	BOOL	Stato di configurazione del test circuito aperto o cortocircuito verso terra: • 1: Abilitato. • 0: Disabilitato.	RO
V_SC	BOOL	Stato di configurazione del test cortocircuito a 24 V: • 1: Abilitato. • 0: Disabilitato.	RO

1. Quando il task SAFE sul controller non è in modalità di esecuzione, i dati scambiati tra il controller e il modulo non vengono aggiornati e CH_HEALTH è impostato a 0.

2. L'elemento VALUE può avere un'indicazione oraria fornita da BMX CRA o BME CRA.

Modulo di uscita digitale BMXSDO0802

Introduzione

Questa sezione descrive il modulo di uscita digitale di sicurezza BMXSDO0802.

Modulo di uscita digitale di sicurezza BMXSDO0802

Introduzione

Il modulo di uscita digitale di sicurezza BMXSDO0802 presenta le seguenti caratteristiche:

- 8 uscite da 0,5 A non elettricamente isolate.
- Tensione di uscita nominale 24 Vcc.
- Si ottiene quanto segue:
  - SIL3 IEC61508, SILCL3 IEC62061.
  - SIL4 EN5012x.
  - Categoria 4 (Cat4) / Performance Level e (PLe) ISO13849.
- Monitoraggio dell'alimentazione esterna dei preattuatori.
- Visualizzazione diagnostica mediante LED, pagina 246 fornita per il modulo e per ogni canale di uscita.
- Diagnostica del cablaggio del canale fornita automaticamente, in grado di rilevare le seguenti condizioni quando l'uscita è *alimentata*:
  - Corrente di sovraccarico
  - Cortocircuito a 0 Vcc verso terra
- Diagnostica del cablaggio del canale configurabile (attiva/disattiva), pagina 105 in grado di rilevare le seguenti condizioni:
  - Conduttore aperto (o interrotto).
- Diagnostica del cablaggio del canale configurabile (attiva/disattiva) in grado di rilevare le seguenti condizioni quando l'uscita *non è alimentata*:
  - Cortocircuito a 0 V verso terra.
- Diagnostica del cablaggio del canale configurabile (attiva/disattiva) in grado di rilevare le seguenti condizioni quando l'uscita è*alimentata* o *non alimentata*:
  - Cortocircuito a 24 Vcc.
  - Circuiti incrociati tra i due canali (se l'alimentazione al sensore è fornita internamente).

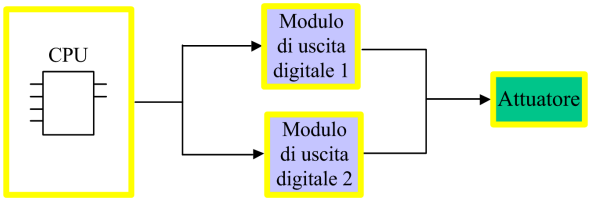
- Impostazioni configurabili del posizionamento di sicurezza per ogni canale che vengono applicate se viene persa la comunicazione tra il controller e il modulo di uscita.
- Sostituzione a caldo del modulo al runtime.
- CCOTF del modulo in modalità di manutenzione, pagina 261. (La funzione CCOTF non è supportata in modalità di sicurezza, pagina 260).

  NOTA: Viene avviato un autotest su ciascuna uscita per verificarne la capacità di essere non alimentata e di raggiungere lo stato sicuro definito senza alcun impatto sul carico (impulso di spegnimento < 1ms). L'autotest viene eseguito alternativamente, un'uscita per volta, su ciascuna uscita alimentata per meno di 1 secondo. Se l'uscita viene collegata ad un ingresso statico di un prodotto, l'ingresso statico collegato può individuare questo impulso. Per evitare un potenziale impatto dell'impulso sull'ingresso, potrebbe essere utile l'impiego di un filtro.

Alta disponibilità

È possibile collegare il controller a due moduli di uscita tramite un black channel, quindi collegare ciascun modulo di uscita a un singolo attuatore. Non sono necessari blocchi funzione, poiché il segnale del controller è collegato a entrambi i canali di uscita.

La seguente figura illustra la configurazione dell'uscita digitale ridondante per l'alta disponibilità:



Lo stato di ogni modulo di uscita può essere letto dagli elementi della rispettiva struttura DDDT `T_U_DIS_SIS_OUT_8`, pagina 111 DDDT. Questi dati possono essere utilizzati per determinare se è necessario sostituire un modulo. Se un modulo non è più operativo e deve essere sostituito, il sistema continua a funzionare con una configurazione conforme a SIL3 mentre avviene la sostituzione del modulo.

Per maggiori dettagli su questa struttura, vedere esempio di cablaggio delle uscite ad alta disponibilità, pagina 108.

Connettore di cablaggio BMXSDO0802

Introduzione

Il modulo di uscita digitale BMXSDO0802 dispone di un singolo gruppo di 8 uscite.

- Entrambi i contatti di alimentazione a +24 Vcc (18 e 20) sono collegati internamente.
- Tutti i contatti comuni a 0 V (1, 3, 5, 7, 9, 11, 13, 15, 17 e 19) sono collegati internamente.

Morsettiere

Per inserire il connettore a 20 contatti nel lato anteriore del modulo si possono utilizzare le seguenti morsettiere Schneider Electric a 20 contatti:

- morsettiera con morsetti a vite BMXFTB2010
- morsettiera con morsetti a gabbia BMXFTB2000
- morsettiera con morsetti a molla BMXFTB2020

NOTA: Le morsettiere possono essere rimosse soltanto quando il modulo è disinserito.

Alimentatore di processo

È necessario un alimentatore di processo a tensione ultra bassa protetta (SELV/PELV) di categoria di sovratensione II da 24 Vcc. Utilizzare un alimentatore che non ripristini automaticamente l'alimentazione dopo un'interruzione dell'alimentazione.

AVVISO
NON CONFORMITÀ DEL CIRCUITO ELETTRICO Non collegare 0 V di un alimentatore SELV a terra. **Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.**

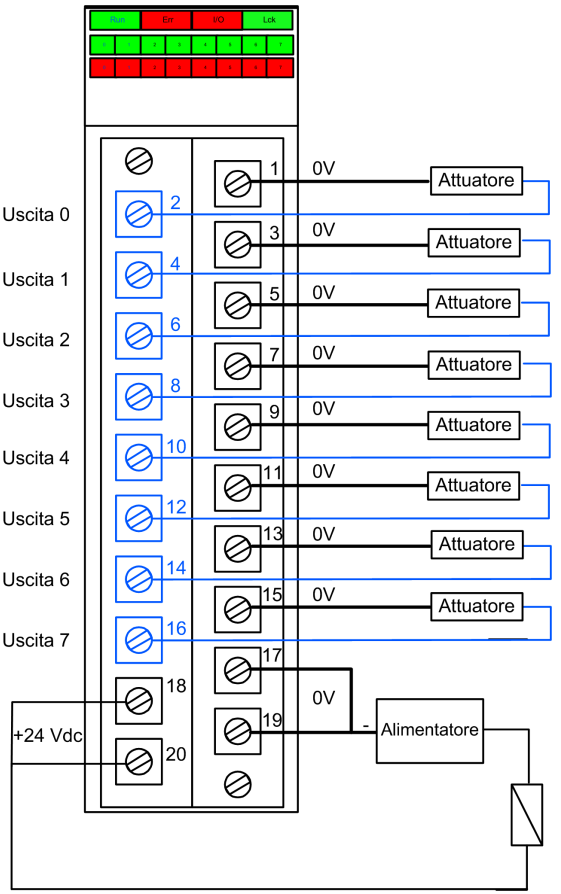
Fusibile

Per proteggere l'alimentatore esterno dai cortocircuiti e da eventuali condizioni di sovratensione, è necessario un fusibile rapido, max. 6 A.

AVVISO
SCELTA ERRATA DEL FUSIBILE Utilizzare fusibili rapidi per proteggere i componenti elettronici del modulo di uscita digitale da una condizione di sovracorrente. **Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.**

Contatti del connettore di cablaggio

Il seguente schema di cablaggio presenta un singolo modulo di uscita collegato a 8 attuatori:



Mappatura delle uscite ai contatti del connettore

La seguente tabella fornisce una descrizione di ogni contatto del modulo di uscita BMXSDO0802:

Descrizione del contatto	Numero del contatto sulla morsettiera		Descrizione del contatto
Uscita 0	2	1	Comune 0 V
Uscita 1	4	3	Comune 0 V
Uscita 2	6	5	Comune 0 V
Uscita 3	8	7	Comune 0 V
Uscita 4	10	9	Comune 0 V
Uscita 5	12	11	Comune 0 V
Uscita 6	14	13	Comune 0 V
Uscita 7	16	15	Comune 0 V
Alimentazione di processo 24 Vdc	18	17	Comune 0 V
Alimentazione di processo 24 Vcc	20	19	Comune 0 V

BMXSDO0802 Esempi di cablaggio dell'applicazione di uscita

Introduzione

È possibile cablare il modulo di uscita digitale di sicurezza BMXSDO0802 agli attuatori per raggiungere la conformità SIL3 Category 4 (Cat4) / Performance Level e (PLe) in diversi modi, a seconda dei requisiti di alta disponibilità.

Il livello di integrità di sicurezza (SIL) massimo è determinato dall'affidabilità dell'attuatore e dalla lunghezza dell'intervallo del test di prova per IEC 61508.

⚠AVVERTIMENTO

PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Cablare gli attuatori, che non soddisfano l'affidabilità degli standard SIL previsti, in modo ridondante su due canali.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Di seguito sono descritti i seguenti esempi di cablaggio dell'applicazione di uscita digitale SIL3 Cat4/PLe:

- Cat4/PLe:
  - un unico canale del modulo di uscita che comanda una variabile di processo. Questa struttura utilizza un singolo attuatore.
- Cat4/PLe con alta disponibilità:
  - due moduli di uscita ridondanti, ognuno con un canale collegato a un attuatore separato, ma che comandano la stessa variabile di processo.

Quando l'apparecchiatura è utilizzata in un'applicazione con gas e fiamma o quando lo stato dell'uscita deve essere sotto tensione, seguire queste istruzioni.

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- La procedura di test deve comprendere un test specifico che attesti l'efficacia del rilevamento di cavo interrotto mediante rimozione della morsettiera e verifica che i corrispondenti bit di errore siano impostati.
- Verificare l'efficacia del rilevamento di cortocircuito verso terra attivando la funzione di diagnostica **Test impulso con alimentazione** nella scheda **Configurazione** del modulo o adottando un'altra procedura (ad esempio impostando l'uscita a 1 e verificando la diagnostica, ecc.).

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Non utilizzare attuatori a spia in quanto la loro impedenza è molto bassa quando sono accesi, il che può comportare il rischio di rilevamento di una falsa condizione di cortocircuito o sovraccarico.

Diagnostica di cablaggio configurabile in Control Expert

Per il modulo di uscita digitale di sicurezza BMXSDO0802, utilizzare la pagina **Configurazione** in Control Expert per:

- Attivare **Rilevamento cortocircuito a 24V** per ogni canale alimentato. Questo test esegue le seguenti operazioni di diagnostica del cablaggio degli attuatori per un canale:
  - Rilevamento cortocircuito a 24V
  - Rilevamento circuiti incrociati tra due canali di uscita

- Attivare **Rilevamento filo aperto** per ognuno degli otto canali, che esegue la seguente diagnostica di cablaggio per quel canale:
  - Rilevamento di conduttore aperto (o interrotto) (ovvero il canale di uscita non è collegato all'attuatore)
  - Rilevamento cortocircuito a 0 V verso terra
- Attivare il **Test impulso con alimentazione** per ogni canale di uscita. Questo test viene eseguito periodicamente quando l'uscita è nello stato non alimentato e applica un impulso (della durata inferiore a 1 ms) all'uscita per determinare se può passare allo stato alimentato. Se la corrente supera una soglia di 0,7 A, l'uscita viene considerata come in condizione di cortocircuito verso terra a 0 Vcc. Il periodo di test è inferiore a 1 s.

⚠ AVVERTIMENTO

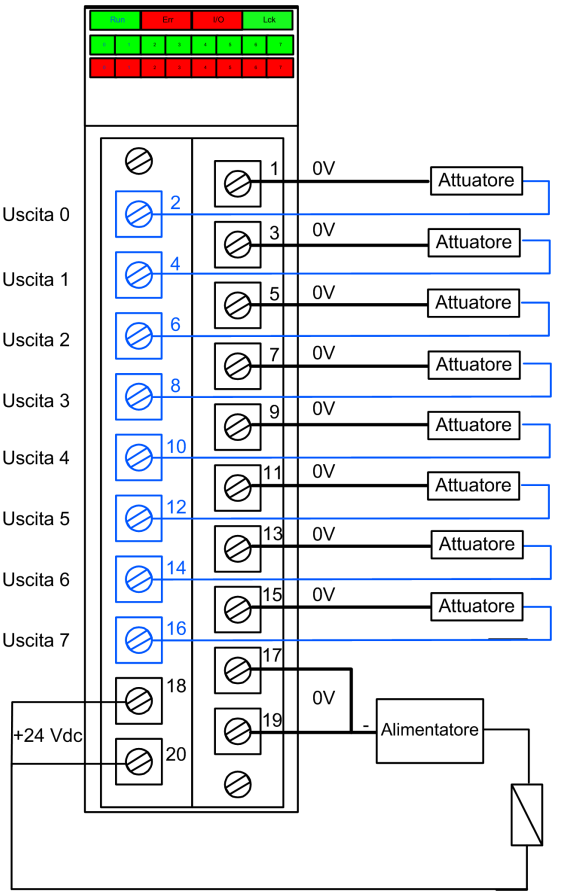
FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Attivare la diagnostica disponibile fornita in Control Expert per rilevare o rispondere alle condizioni elencate sopra.
- Applicare misure di sicurezza alternative per rilevare o escludere queste condizioni se un test di diagnostica non è abilitato o non è disponibile in Control Expert.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

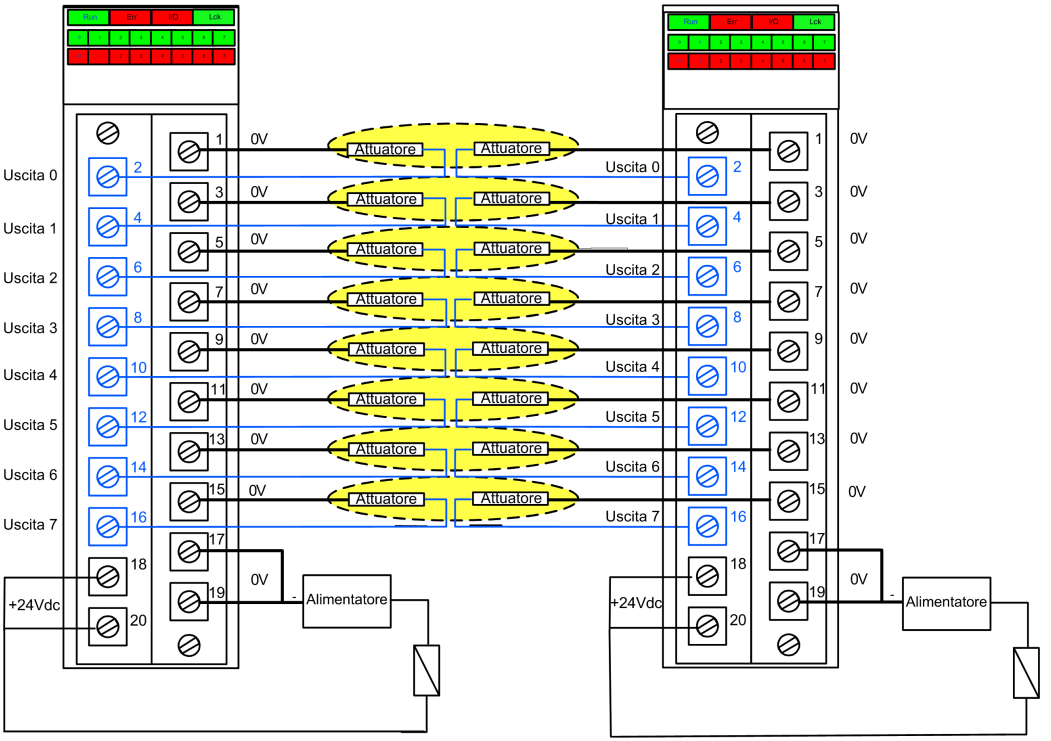
SIL 3 Cat4/PLe - Esempio di modulo di uscita digitale singolo

L'esempio seguente presenta un attuatore esclusivo cablato a ogni uscita su un singolo modulo di uscita. Ogni loop è SIL 3 Cat4/PLe:



Esempio SIL 3 Cat4/PLe - Alta disponibilità:

Nel seguente schema di cablaggio, due uscite ridondanti comandano la stessa variabile di processo. Come illustrato di seguito, ogni uscita è collegata ad attuatori separati, per cui ogni attuatore esegue lo stesso comando inviato su canali diversi. In alternativa, si possono collegare tra di loro le due uscite ridondanti per comandare lo stesso attuatore.



Riepilogo della diagnostica del cablaggio delle uscite

Le due strutture forniscono le seguenti diagnostiche di cablaggio:

Condizione	**Diagnostica fornita nello stato di uscita?**	
	Alimentato	**Non alimentato**
Conduttore aperto (o interrotto)[1]	Sì. Diagnostica per ogni ciclo.	Sì. Diagnostica per ogni ciclo.
Uscita in sovraccarico[2]	Sì. Diagnostica per ogni ciclo.	No.
Cortocircuito a 0 V verso terra	Sì. Diagnostica per ogni ciclo.	Sì. Periodo di diagnostica < 1 s.
Cortocircuito a 24 Vdc[1]	Sì. Periodo di diagnostica < 1 s.	Sì. Diagnostica per ogni ciclo.

Condizione	Diagnostica fornita nello stato di uscita?	
	Alimentato	**Non alimentato**
Circuiti incrociati tra due canali	Sì. Periodo di diagnostica < 1 s.	Sì. Diagnostica per ogni ciclo.

1. Questa funzione di diagnostica viene eseguita se abilitata nella scheda **Configurazione** del modulo in Control Expert.

2. Dopo che la condizione è risolta, riarmare l'uscita interrompendo l'alimentazione elettrica.

⚠AVVERTIMENTO

CORTOCIRCUITO VERSO TERRA 0 VCC

- Attivare l'opzione **Rilevamento filo aperto** nella scheda **Configurazione** del modulo per la condizione di cortocircuito verso terra a 0 V con lo stato di uscita non alimentato.
- In alternativa, applicare altre misure di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠AVVERTIMENTO

CORTOCIRCUITO A 24 VCC

- Attivare l'opzione **Rilevamento cortocircuito a 24V** nella scheda **Configurazione** del modulo per la condizione di cortocircuito a 24 Vcc con lo stato di uscita alimentato o non alimentato.
- In alternativa, applicare altre misure di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI

Applicare misure di sicurezza alternative quando il modulo non è in grado di rilevare la condizione di circuiti incrociati tra due canali con lo stato di uscita non alimentato e l'altro canale non alimentato; questa ulteriore misura di sicurezza rileva o esclude questa condizione se si verifica quando lo stato dell'uscita passa ad alimentato.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI

- Attivare l'opzione **Rilevamento cortocircuito a 24V** nella scheda **Configurazione** del modulo per la condizione di circuiti incrociati tra due canali con lo stato di uscita non alimentato e l'altro canale alimentato.
- In alternativa, applicare altre misure di sicurezza per rilevare o escludere questa condizione quando lo stato dell'uscita diventa alimentato.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI

Applicare misure di sicurezza alternative quando il modulo non è in grado di rilevare la condizione di circuiti incrociati tra canali con lo stato di uscita alimentato e l'altro canale non alimentato; questa ulteriore misura di sicurezza rileva o esclude questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

⚠AVVERTIMENTO

CIRCUITI INCROCIATI

- Attivare l'opzione **Rilevamento cortocircuito a 24V** nella scheda **Configurazione** del modulo per la condizione di circuiti incrociati tra due canali con lo stato di uscita alimentato e l'altro canale alimentato.
- In alternativa, applicare altre misure di sicurezza per rilevare o escludere questa condizione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Struttura dei dati BMXSDO0802

Introduzione

Il tipo di dati derivati del dispositivo (DDDT) `T_U_DIS_SIS_OUT_8` il è l'interfaccia tra il modulo di uscita digitale BMXSDO0802 e l'applicazione eseguita nel controller. Il DDDT `T_`

`U_DIS_SIS_OUT_8` incorpora i tipi di dati `T_SAFE_COM_DBG_OUT` e `T_U_DIS_SIS_CH_OUT`.

Tutte queste strutture sono descritte più avanti.

Struttura DDDT `T_U_DIS_SIS_OUT_8`

La struttura DDDT `T_U_DIS_SIS_OUT_8` include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
MOD_HEALTH[1]	BOOL	• 1: Il modulo funziona correttamente. • 0: Il modulo non funziona correttamente.	RO
SAFE_COM_STS[1]	BOOL	• 1: Comunicazione modulo valida. • 0: Comunicazione modulo non valida.	RO
PP_STS	BOOL	• 1: L'alimentazione di processo è funzionante. • 0: L'alimentazione di processo non è funzionante.	RO
CONF_LOCKED	BOOL	• 1: Configurazione del modulo bloccata. • 0: Configurazione del modulo non bloccata.	RO
S_COM_DBG	T_SAFE_COM_DBG_OUT	Struttura di debug comunicazione sicura.	RO
CH_OUT	ARRAY[0...7] di T_U_DIS_SIS_CH_OUT	Array di struttura del canale.	RO
S_TO	UINT	Timeout di sicurezza prima che il modulo entri nello stato di posizionamento di sicurezza.	RO
MUID[2]	ARRAY[0...3] di DWORD	ID univoco del modulo (assegnato automaticamente da Control Expert)	RO
RESERVED_1	ARRAY[0...8] di INT	–	–
RESERVED_2	ARRAY[0...6] di INT	–	–

1. Quando il task SAFE sul controller non è in modalità di esecuzione, i dati scambiati tra il controller e il modulo non vengono aggiornati e MOD_HEALTH e SAFE_COM_STS vengono impostati a 0.

2. Questo valore autogenerato può essere modificato eseguendo il comando **Crea > Rinnova ID e Ricrea tutto** nel menu principale di Control Expert.

Struttura T_SAFE_COM_DBG_OUT

La struttura T_SAFE_COM_DBG_OUT include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Acces-so
S_COM_EST	BOOL	• 1: Comunicazione con il modulo stabilita. • 0: Comunicazione con il modulo non stabilita o danneggiata.	RO
M_NTP_SYNC	BOOL	Con firmware del controller 3.10 o precedente: • 1: Il modulo è sincronizzato con il server NTP. • 0: Il modulo non è sincronizzato con il server NTP. **NOTA:** con firmware del controller 3.20 o successivo, il valore è sempre 1.	RO
CPU_NTP_SYNC	BOOL	Con firmware del controller 3.10 o precedente: • 1: Il controller è sincronizzato con il server NTP. • 0: Il controller non è sincronizzato con il server NTP. **NOTA:** con firmware del controller 3.20 o successivo, il valore è sempre 1.	RO
CHECKSUM	BYTE	Checksum del frame di comunicazione.	RO
COM_DELAY	UINT	Ritardo di comunicazione tra due valori ricevuti dal modulo: • 1 ... 65534: Il tempo, in ms, trascorso dalla ricezione da parte del controller dell'ultima comunicazione del modulo. • 65535: Il controller non ha ricevuto una comunicazione dal modulo.	RO
COM_TO	UINT	Valore di timeout di comunicazione proveniente dal modulo.	L/S
STS_MS_IN	UINT	Valore di timestamp sicuro per la frazione di secondo, arrotondato al millisecondo più vicino, dei dati ricevuti dal modulo.	RO
S_NTP_MS	UINT	Valore di tempo sicuro per la frazione di secondo, arrotondato al secondo, per il ciclo corrente.	RO
STS_S_IN	UDINT	Valore di timestamp sicuro in secondi dei dati ricevuti dal modulo.	RO

Elemento	Tipo di dati	Descrizione	Accesso
S_NTP_S	UDINT	Valore di tempo sicuro in secondi per il ciclo corrente.	RO
CRC_IN	UDINT	Valore CRC per i dati ricevuti dal modulo.	RO
STS_MS_OUT	UINT	Valore di timestamp sicuro della frazione di secondo, arrotondato al millisecondo più vicino, dei dati da inviare al modulo.	RO
STS_S_OUT	UDINT	Valore di timestamp sicuro in secondi dei dati da inviare al modulo.	RO
CRC_OUT	UDINT	Valore CRC per i dati da inviare al modulo.	RO

Struttura `T_U_DIS_SIS_CH_OUT`

La struttura `T_U_DIS_SIS_CH_OUT` include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
CH_HEALTH[1]	BOOL	• 1: Il canale è operativo. • 0: È stato rilevato un errore sul canale, che non è operativo. **Formula:** CH_HEALTH = non (SC o OL o C o OC) e SAFE_COM_STS e non (modulo in stato di posizionamento di sicurezza)	RO
VALUE	EBOOL	Comando del canale di uscita: • 1: Comanda la chiusura dell'uscita (alimentata). • 0: Comanda l'apertura dell'uscita (non alimentata).	L/S
TRUE_VALUE[2]	BOOL	Valore di restituzione del canale di uscita relè: • 1: L'uscita è chiusa (alimentata). • 0: L'uscita è aperta (non alimentata).	RO
OC	BOOL	• 1: Il canale è aperto o cortocircuitato verso terra. • 0: Il canale è collegato e non cortocircuitato verso terra.	RO
SC	BOOL	• 1: Il canale è cortocircuitato con una sorgente 24 V oppure incrociato con un altro canale.	RO

Elemento	Tipo di dati	Descrizione	Accesso
		• 0: Il canale non è cortocircuitato con una sorgente 24 V oppure è incrociato.	
OL	BOOL	• 1: Il canale è sovraccarico o cortocircuitato a 0 V. • 0: Il canale non è sovraccarico o cortocircuitato a 0 V.	RO
IC	BOOL	• 1: Canale non valido rilevato dal modulo. • 0: Il canale è dichiarato internamente operativo dal modulo.	RO
V_OC	BOOL	Stato configurazione del test circuito aperto: • 1: Abilitato. • 0: Disabilitato	RO
V_SC	BOOL	Stato di configurazione del test cortocircuito a 24 V: • 1: Abilitato. • 0: Disabilitato	RO
V_PULSE_ON	BOOL	Stato di configurazione del test impulsi sotto tensione: • 1: Abilitato. • 0: Disabilitato	RO
CH_FBC	BOOL	Configurazione dell'impostazione di posizionamento di sicurezza del canale: • 1: Valore definito dall'utente. • 0: Mantieni ultimo valore.	RO
CH_FBST	BOOL	Configurazione dello stato di posizionamento di sicurezza del canale quando è selezionato definito da utente: • 1: Alimentato. • 0: Non alimentato.	RO

1. Quando il task SAFE sul controller non è in modalità di esecuzione, i dati scambiati tra il controller e il modulo non vengono aggiornati e CH_HEALTH è impostato a 0.

2. L'elemento TRUE_VALUE può avere un'indicazione oraria fornita da BMX CRA o BME CRA.

Modulo di uscita relè digitale BMXSRA0405

Introduzione

Questa sezione descrive il modulo di uscita relè digitale di sicurezza BMXSRA0405.

Modulo di uscita relè digitale di sicurezza BMXSRA0405

Introduzione

Il modulo di uscita relè digitale di sicurezza BMXSRA0405 presenta la seguenti caratteristiche:

- 4 uscite relè con corrente 5 A.
- Tensione di uscita nominale di 24 Vcc e 24...230 Vca (categoria di sovratensione II).
- Conformità fino a SIL4 (EN5012x) / SIL3 (IEC61508) Categoria 4 (Cat4) / Performance Level e (PLe).
- Supporta 8 opzioni di configurazione di cablaggio dell'applicazione predefinite.
- Monitoraggio mediante autotest automatico configurabile della capacità del relè di eseguire lo stato comandato delle uscite (a seconda della configurazione di cablaggio dell'applicazione selezionata).
- Impostazioni del modulo configurabili per la modalità di posizionamento di sicurezza e il timeout di posizionamento di sicurezza (in ms).
- Visualizzazione diagnostica mediante LED, pagina 251 fornita per il modulo e per ogni canale di uscita.
- Sostituzione a caldo del modulo al runtime.
- CCOTF del modulo in modalità di manutenzione, pagina 261. (La funzione CCOTF non è supportata in modalità di sicurezza, pagina 260).

Connettore di cablaggio BMXSRA0405

Introduzione

Il modulo di uscita relè digitale BMXSRA0405 include 4 relè e supporta fino a 4 uscite. Il modulo dispone di una coppia di contatti *a* e *b* per ogni relè. Notare che per ogni relè:

- i due contatti *a* sono collegati internamente e

- anche i due contatti *b* sono collegati internamente.

Morsettiere

Per inserire il connettore a 20 contatti nel lato anteriore del modulo si possono utilizzare le seguenti morsettiere Schneider Electric a 20 contatti:

- morsettiera con morsetti a vite BMXFTB2010
- morsettiera con morsetti a gabbia BMXFTB2000
- morsettiera con morsetti a molla BMXFTB2020

NOTA: Le morsettiere possono essere rimosse soltanto quando il modulo è disinserito.

Alimentatore di processo

È necessario installare l'alimentatore di processo a 24 Vcc o 24 Vca ... 230 Vca.

Fusibile

È necessario un fusibile rapido, max. 6 A, adatto per l'applicazione selezionata e la struttura relè selezionata.

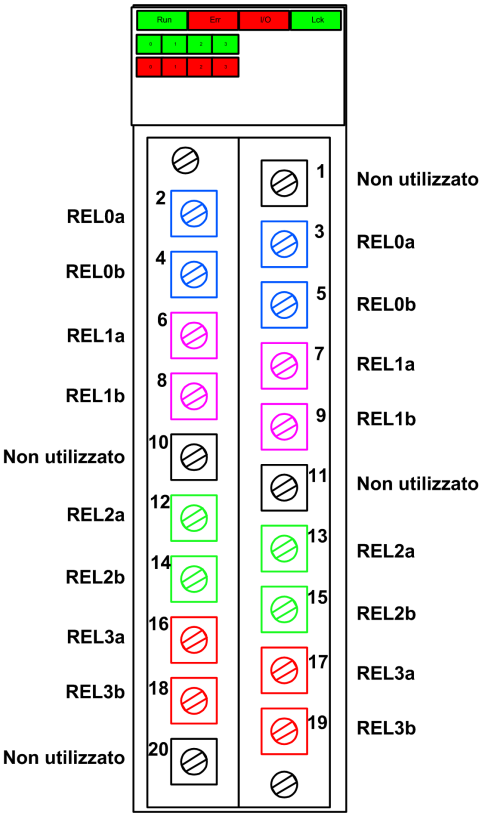
AVVISO
SCELTA ERRATA DEL FUSIBILE Utilizzare fusibili rapidi per proteggere i componenti elettronici del modulo di uscita digitale da una condizione di sovracorrente. **Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.**

Installare un fusibile esterno in serie con l'alimentatore esterno, il relè e il carico.

⚠AVVERTIMENTO
FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA Implementare la diagnostica di cablaggio appropriata per rilevare e prevenire gli errori sul cablaggio esterno. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Connettore di cablaggio

Il seguente esempio illustra i contatti del modulo relè:



Mappatura degli ingressi ai contatti del connettore

La seguente tabella fornisce una descrizione di ogni contatto del modulo di uscita relè digitale BMXSRA0405:

Descrizione del contatto	Numero del contatto sulla morsettiera		Descrizione del contatto
Contatto NO, relè 0a	2	1	Non usato
Contatto NO, relè 0b	4	3	Contatto NO, relè 0a
Contatto NO, relè 1a	6	5	Contatto NO, relè 0b
Contatto NO, relè 1b	8	7	Contatto NO, relè 1a
Non usato	10	9	Contatto NO, relè 1b

Descrizione del contatto	Numero del contatto sulla morsettiera		Descrizione del contatto
Contatto NO, relè 2a	12	11	Non usato
Contatto NO, relè 2b	14	13	Contatto NO, relè 2a
Contatto NO, relè 3a	16	15	Contatto NO, relè 2b
Contatto NO, relè 3b	18	17	Contatto NO, relè 3a
Non usato	20	19	Contatto NO, relè 3b

NOTA: Dato che i due contatti *a* per ogni relè sono collegati internamente, si deve usare solo un contatto *a* per ogni relè. Analogamente, dato che i due contatti *b* per ogni relè sono collegati internamente, si deve usare solo un contatto *b* per ogni relè.

BMXSRA0405 Esempi di cablaggio dell'applicazione di uscita

Introduzione

È possibile configurare il modulo relè di uscita digitale di sicurezza BMXSRA0405 per raggiungere la conformità SIL2 Category 2 (Cat2) / Performance Level c (PLc) o SIL3 Cat4 / PLe in modi diversi, a seconda dei fattori seguenti:

- il numero di uscite che il modulo supporterà e
- il modo in cui si intende verificare la capacità del modulo di commutare l'attuatore nello stato di domanda previsto, ovvero:
  - automaticamente da parte del modulo (in questo caso non vi è alcuna transizione di stato per l'attuatore) oppure
  - tramite una procedura che effettua e verifica una transizione giornaliera del segnale dal modulo all'attuatore (in questo caso la transizione influenza lo stato dell'attuatore).

Realizzare questa configurazione selezionando un numero di applicazione (descritto nelle tabelle seguenti) nell'elenco **Funzione** della scheda **Configurazione** del modulo in Control Expert.

Applicazioni della configurazione di cablaggio SIL2 Cat2 / PLc:

Funzione	Stato richiesto	Relè	Uscite	Test del segnale?		Schema di cablaggio (vedere di seguito)
				Test automatico del segnale?[1]	Transizione di segnale giornaliera?	
Applicazione_1	Non alimentato	1	4	No	Sì	A
Applicazione_2	Non alimentato	2	2	Sì	No	B
Applicazione_3	Alimentato	1	4	No	Sì	A
Applicazione_4	Alimentato	2	2	Sì	No	C
1. Il test automatico del segnale non influenza lo stato dell'attuatore.						

Applicazioni della configurazione di cablaggio SIL3 Cat4 / PLe:

Funzione	Stato richiesto	Relè	Uscite	Test del segnale?		Schema di cablaggio (vedere di seguito)
				Test automatico del segnale?[1]	Transizione di segnale giornaliera?	
Applicazione_5	Non alimentato	2	2	No	Sì	C
Applicazione_6	Non alimentato	4	1	Sì	No	D
Applicazione_7	Alimentato	2	2	No	Sì	C
Applicazione_8	Alimentato	2	2	Sì	No	C
1. Il test automatico del segnale non influenza lo stato dell'attuatore.						

Ognuna di queste otto applicazioni è descritta negli esempi di cablaggio seguenti.

Applicazione_1: 4 uscite, SIL2 / Cat2 / PLc, stato non alimentato, nessun test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è non alimentato. Se il modulo rileva un errore interno per un'uscita, interrompe l'alimentazione per quell'uscita.

⚠AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Per raggiungere il livello SIL2 secondo IEC61508 e Category 2 / Performance Level c secondo ISO 13849 tramite questa configurazione di cablaggio, eseguire almeno una transizione del segnale giornaliera dallo stato alimentato a quello non alimentato.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Per una raffigurazione della configurazione di cablaggio per Applicazione_1, vedere lo schema di cablaggio A, pagina 124 di seguito.

Applicazione_2: 2 uscite, SIL2 / Cat2 / PLc, stato non alimentato, test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è non alimentato. Il modulo, se rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

Il modulo effettua in sequenza un test degli impulsi periodici automatico su ogni relè. La durata del test è inferiore a 50 ms. Data la configurazione dei due relè utilizzati (in parallelo), il test non ha alcuna influenza sul carico di uscita (normalmente *alimentato*). È possibile configurare la frequenza del test impostando il **Periodo di monitoraggio** nella scheda **Configurazione** del modulo. I valori di frequenza del test validi sono compresi tra 1 e 1440 minuti.

Per una raffigurazione della configurazione di cablaggio per Applicazione_2, vedere lo schema di cablaggio B, pagina 125 di seguito.

Applicazione_3: 4 uscite, SIL2 / Cat2 / PLc, stato alimentato, nessun test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è alimentato. Il modulo, se rileva un errore interno per un'uscita, interrompe l'alimentazione per quell'uscita ovvero lo stato sicuro definito.

⚠ AVVERTIMENTO
IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA Per raggiungere il livello SIL2 secondo IEC61508 e Category 2 / Performance Level c secondo ISO 13849 tramite questa configurazione di cablaggio, eseguire almeno una transizione del segnale giornaliera dallo stato non alimentato a quello alimentato. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Per una raffigurazione della configurazione di cablaggio per Applicazione_3, vedere lo schema di cablaggio A, pagina 124 di seguito.

Applicazione_4: 2 uscite, SIL2 / Cat2 / PLc, stato alimentato, test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è alimentato. Il modulo, se rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

Il modulo effettua in sequenza un test degli impulsi periodici su ogni relè. La durata del test è inferiore a 50 ms. Data la configurazione dei due relè utilizzati (in parallelo), il test non ha alcuna influenza sul carico di uscita (normalmente *alimentato*). È possibile configurare la frequenza del test impostando il **Periodo di monitoraggio** nella scheda **Configurazione** del modulo. I valori di frequenza del test validi sono compresi tra 1 e 1440 minuti.

Per una raffigurazione della configurazione di cablaggio per Applicazione_4, vedere lo schema di cablaggio C, pagina 126 di seguito.

Applicazione_5: 2 uscite, SIL3 / Cat4 / PLe, stato non alimentato, nessun test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è non alimentato. Il modulo, se rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

⚠ AVVERTIMENTO
IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA Per raggiungere il livello SIL3 secondo IEC61508 e Category 4 / Performance Level e secondo ISO 13849 tramite questa configurazione di cablaggio, eseguire almeno una transizione del segnale giornaliera dallo stato alimentato a quello non alimentato. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Per una raffigurazione della configurazione di cablaggio per Applicazione_5, vedere lo schema di cablaggio C, pagina 126 di seguito.

Applicazione_6: 1 uscita, SIL3 / Cat4 / PLe, stato non alimentato, test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è non alimentato. Il modulo, se rileva un errore dell'uscita interno su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di tutti i relè (relè 0, relè 1, relè 2 e relè 3) per il modulo.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

Il modulo effettua in sequenza un test degli impulsi periodici su ogni relè. La durata del test è inferiore a 50 ms. Data la configurazione dei quattro relè utilizzati (2 coppie di relè in serie impostati in parallelo), il test non ha alcuna influenza sul carico di uscita (normalmente *alimentato*). È possibile configurare la frequenza del test impostando il **Periodo di monitoraggio** nella scheda **Configurazione** del modulo. I valori di frequenza del test validi sono compresi tra 1 e 1440 minuti.

Per una raffigurazione della configurazione di cablaggio per Applicazione_6, vedere lo schema di cablaggio D, pagina 127 di seguito.

Applicazione_7: 2 uscite, SIL3 / Cat4 / PLe, stato alimentato, nessun test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è alimentato. Il modulo, se rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

⚠ AVVERTIMENTO
IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA Per raggiungere il livello SIL3 secondo IEC61508 e Category 4 / Performance Level e secondo ISO 13849 tramite questa configurazione di cablaggio, eseguire almeno una transizione del segnale giornaliera dallo stato non alimentato a quello alimentato. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Per una raffigurazione della configurazione di cablaggio per Applicazione_7, vedere lo schema di cablaggio C, pagina 126 di seguito.

Applicazione_8 2 uscite, SIL3 Cat4 / PLe, stato alimentato, test automatico del segnale

Lo stato richiesto per questa configurazione dell'applicazione è alimentato. Il modulo, se rileva un errore interno dell'uscita su uno dei relè utilizzati per un'uscita, interrompe l'alimentazione di entrambi i relè (relè 0 e relè 1 o relè 2 e relè 3) per quell'uscita.

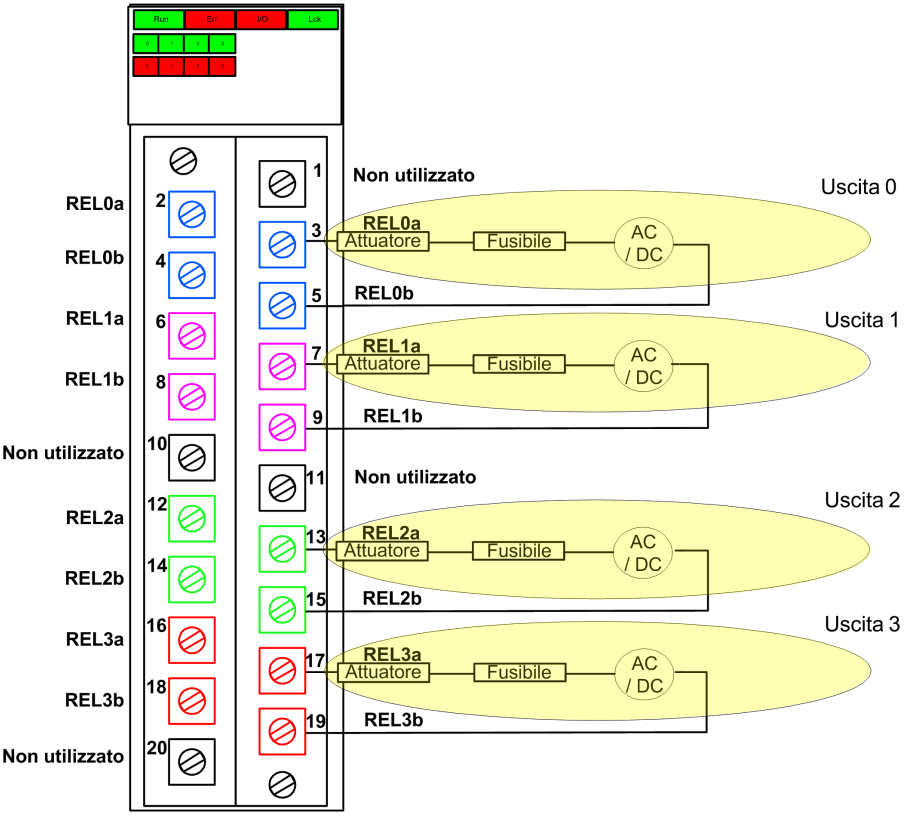
Il programma applicativo deve comandare lo stesso stato di uscita a tutti i relè che attivano lo stesso attuatore.

Il modulo effettua in sequenza un test degli impulsi periodici su ogni relè. La durata del test è inferiore a 50 ms. Data la configurazione dei due relè utilizzati (in serie), il test non ha alcuna influenza sul carico di uscita (normalmente *non alimentato*). È possibile configurare la frequenza del test impostando il **Periodo di monitoraggio** nella scheda **Configurazione** del modulo. I valori di frequenza del test validi sono compresi tra 1 e 1440 minuti.

Per una raffigurazione della configurazione di cablaggio per Applicazione_8, vedere lo schema di cablaggio C, pagina 126 di seguito.

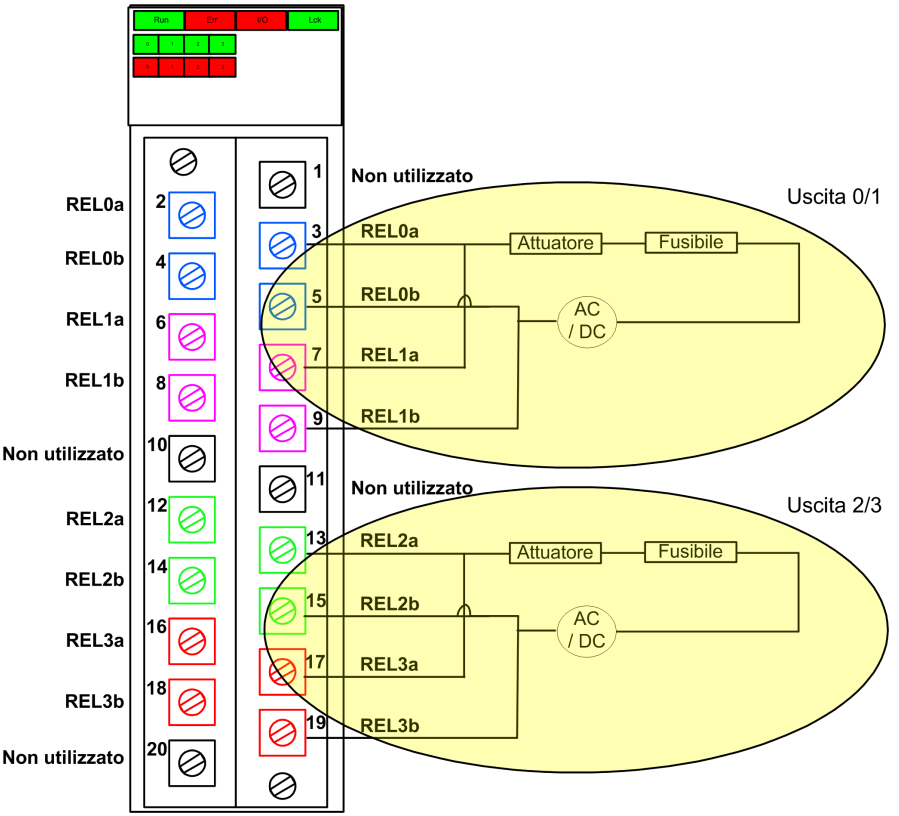
Schema di cablaggio A

Questo schema di cablaggio si applica a Applicazione_1 e Applicazione_3:



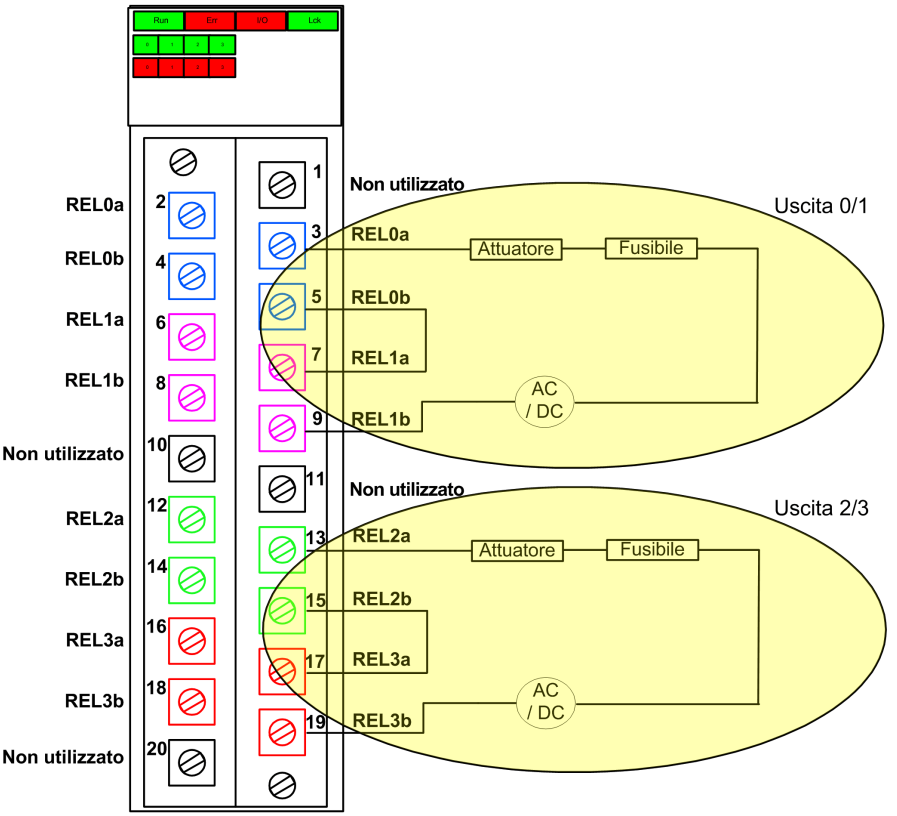
Schema di cablaggio B

Questo schema di cablaggio si applica a Applicazione_2:



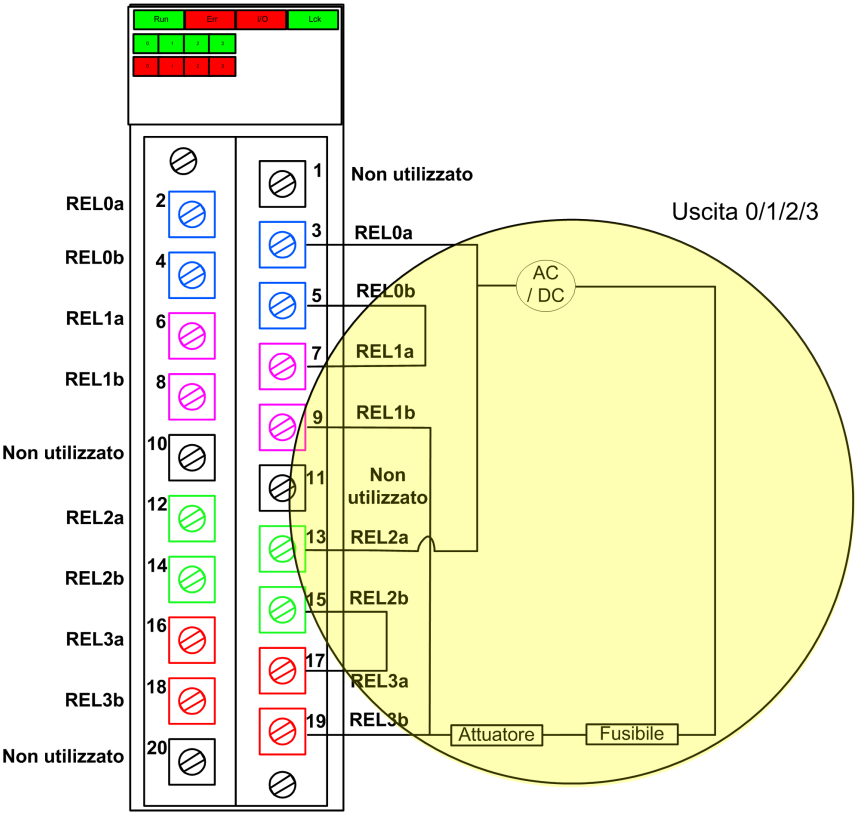
Schema di cablaggio C

Questo schema di cablaggio si applica a Applicazione_4, Applicazione_5, Applicazione_7 e Applicazione_8:



Schema di cablaggio D

Questo schema di cablaggio si applica a Applicazione_6:



Struttura dei dati BMXSRA0405

Introduzione

Il tipo di dati derivati del dispositivo (DDDT) `T_U_DIS_SIS_OUT_4` è l'interfaccia tra il modulo di uscita relè BMXSRA0405 e l'applicazione eseguita nella CPU. Il DDDT `T_U_DIS_SIS_OUT_4` incorpora i tipi di dati `T_SAFE_COM_DBG_OUT` e `T_U_DIS_SIS_CH_ROUT`.

Tutte queste strutture sono descritte più avanti.

Struttura DDDT T_U_DIS_SIS_OUT_4

La struttura DDDT T_U_DIS_SIS_OUT_4 include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
MOD_HEALTH[1]	BOOL	• 1: Il modulo funziona correttamente. • 0: Il modulo non funziona correttamente.	RO
SAFE_COM_STS[1]	BOOL	• 1: Comunicazione modulo valida. • 0: Comunicazione modulo non valida.	RO
CONF_LOCKED	BOOL	• 1: Configurazione del modulo bloccata. • 0: Configurazione del modulo non bloccata.	RO
APPLI	UINT	Configurazione applicazione relè: 1, 2, 3, 4, 5, 6 o 7.	RO
TIME_PERIOD	UINT	Periodo di tempo per il monitoraggio automatico dei relè (in minuti).	RO
S_COM_DBG	T_SAFE_COM_DBG_OUT	Struttura di debug comunicazione sicura.	RO
CH_OUT	ARRAY[0...3] di T_U_DIS_SIS_CH_ROUT	Array di struttura del canale.	–
S_TO	UINT	Timeout di sicurezza prima che il modulo entri nello stato di posizionamento di sicurezza.	RO
MUID[2]	ARRAY[0...3] di DWORD	ID univoco del modulo (assegnato automaticamente da Control Expert)	RO
RESERVED_1	ARRAY[0...7] di INT	–	–
RESERVED_2	ARRAY[0...6] di INT	–	–

1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e MOD_HEALTH e SAFE_COM_STS vengono impostati a 0.

2. Questo valore autogenerato può essere modificato eseguendo il comando **Crea > Rinnova ID e Ricrea tutto** nel menu principale di Control Expert.

Struttura T_SAFE_COM_DBG_OUT

La struttura T_SAFE_COM_DBG_OUT include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Acces-so
S_COM_EST	BOOL	• 1: Comunicazione con il modulo stabilita. • 0: Comunicazione con il modulo non stabilita o danneggiata.	RO
M_NTP_SYNC	BOOL	Con firmware della CPU 3.10 o precedente: • 1: Il modulo è sincronizzato con il server NTP. • 0: Il modulo non è sincronizzato con il server NTP. **NOTA:** Con firmware della CPU 3.20 o successivo, il valore è sempre 1.	RO
CPU_NTP_SYNC	BOOL	Con firmware della CPU 3.10 o precedente: • 1: La CPU è sincronizzata con il server NTP. • 0: La CPU non è sincronizzata con il server NTP. **NOTA:** Con firmware della CPU 3.20 o successivo, il valore è sempre 1.	RO
CHECKSUM	BYTE	Checksum del frame di comunicazione.	RO
COM_DELAY	UINT	Ritardo di comunicazione tra due valori ricevuti dal modulo: • 1 ... 65534: Il tempo, in ms, trascorso dalla ricezione da parte della CPU dell'ultima comunicazione dal modulo. • 65535: La CPU non ha ricevuto una comunicazione dal modulo.	RO
COM_TO	UINT	Valore di timeout di comunicazione proveniente dal modulo.	L/S
STS_MS_IN	UINT	Valore di timestamp sicuro per la frazione di secondo, arrotondato al millisecondo più vicino, dei dati ricevuti dal modulo.	RO
S_NTP_MS	UINT	Valore di tempo sicuro per la frazione di secondo, arrotondato al secondo, per il ciclo corrente.	RO
STS_S_IN	UDINT	Valore di timestamp sicuro in secondi dei dati ricevuti dal modulo.	RO
S_NTP_S	UDINT	Valore di tempo sicuro in secondi per il ciclo corrente.	RO
CRC_IN	UDINT	Valore CRC per i dati ricevuti dal modulo.	RO
STS_MS_OUT	UINT	Valore di timestamp sicuro della frazione di secondo, arrotondato al millisecondo più vicino, dei dati da inviare al modulo.	RO

Elemento	Tipo di dati	Descrizione	Accesso
STS_S_OUT	UDINT	Valore di timestamp sicuro in secondi dei dati da inviare al modulo.	RO
CRC_OUT	UDINT	Valore CRC per i dati da inviare al modulo.	RO

Struttura T_U_DIS_SIS_CH_ROUT

La struttura T_U_DIS_SIS_CH_ROUT include i seguenti elementi:

Elemento	Tipo di dati	Descrizione	Accesso
CH_HEALTH[1]	BOOL	• 1: Il canale è operativo. • 0: È stato rilevato un errore sul canale, che non è operativo. **Formula:** CH_HEALTH = non (IC) e SAFE_COM_STS e non (modulo in stato di posizionamento di sicurezza)	RO
VALUE	EBOOL	Comando del canale di uscita: • 1: Comanda la chiusura dell'uscita (alimentata). • 0: Comanda l'apertura dell'uscita (non alimentata).	L/S
TRUE_VALUE[2]	BOOL	Valore di restituzione del canale di uscita relè: • 1: L'uscita è chiusa (alimentata). • 0: L'uscita è aperta (non alimentata).	RO
IC	BOOL	• 1: Canale non valido rilevato dal modulo. • 0: Il canale è dichiarato internamente operativo dal modulo.	RO
CH_FBC	BOOL	Configurazione dell'impostazione di posizionamento di sicurezza del canale: • 1: Valore definito dall'utente. • 0: Mantieni ultimo valore.	RO

Elemento	Tipo di dati	Descrizione	Acces-so
CH_FBST	BOOL	Configurazione dello stato di posizionamento di sicurezza del canale quando è selezionato definito da utente: • 1: Alimentato. • 0: Non alimentato.	RO
1. Quando il task SAFE sulla CPU non è in modalità di esecuzione, i dati scambiati tra la CPU e il modulo non vengono aggiornati e CH_HEALTH è impostato a 0. 2. L'elemento TRUE_VALUE può avere un'indicazione oraria fornita da BMX CRA o BME CRA.			

Alimentatori di sicurezza M580

Introduzione

Questo capitolo descrive i moduli alimentatore di sicurezza M580.

Alimentatori di sicurezza M580

Introduzione

Con il PAC di sicurezza M580 possono essere usati i seguenti alimentatori:

- Alimentatore di sicurezza 100-240 Vca ridondante BMXCPS4002S
- alimentatore di sicurezza ad alta potenza 24/48 Vcc ridondante BMXCPS4022S
- alimentatore di sicurezza ad alta potenza 125 Vcc ridondante BMXCPS3522S

⚠ AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Utilizzare solo un modulo di alimentazione BMXCPS4002S, BMXCPS4022S o BMXCPS3522S in qualsiasi backplane contenente un modulo di sicurezza M580.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Verificare l'installazione fisica e il progetto in Control Expert per confermare che vengano utilizzati solo moduli di alimentazione di sicurezza M580.

Funzionalità degli alimentatori

Ogni modulo di alimentazione M580 Safety converte l'energia Vcc o Vca in due tensioni di uscita, 24 Vcc e 3,3 Vcc, come descritto di seguito:

Caratteristiche	**Alimentazione**		
	BMXCPS4002S	**BMXCPS4022S**	**BMXCPS3522S**
Rete di alimentazione di ingresso principale	100...240 Vca, 50...60 Hz	24...48 Vcc	100...150 Vcc
Uscita limite di potenza verso backplane	40 Vcc	40 Vcc	40 Vcc

Caratteristiche	Alimentazione		
	BMXCPS4002S	**BMXCPS4022S**	**BMXCPS3522S**
Temperatura ambiente per limite di potenza	-25° C...+60° C	-25° C...+60° C	-25° C...+60° C
Cablaggio con	• rete AC con neutro cablato a terra OPPURE • rete AC con neutro isolato e impedente verso terra, con neutro AC protetto tramite fusibile dall'utente.	Una rete DC 24...48 Vcc	Una rete DC 125 Vcc

Ogni alimentatore rileva le condizioni di sovratensione, sovraccarico e cortocircuito su entrambe le linee del backplane, 3,3 Vcc e 24 Vcc.

Se viene rilevata la soglia superiore 40 Vcc, il modulo esegue le seguenti azioni di risposta:

- Viene eseguito un reset, che causa la reinizializzazione dei moduli alimentati dall'alimentatore.
- Se la soglia di tensione superiore è stata rilevata sulla linea:
  - 24 Vcc del backplane: il PAC viene spento.
  - 3,3 Vcc del backplane: il PAC smette di funzionare, ma continua a ricevere alimentazione.

Per maggiori informazioni su come reagire a queste condizioni vedere la sezione *Diagnostica per le tensioni del backplane 24 Vcc e 3,3 Vcc*, pagina 136.

Moduli di alimentazione ridondanti

I moduli BMXCPS4002S, BMXCPS4022S e BMXCPS3522S sono moduli di alimentazione ridondanti. Due di questi moduli di alimentazione possono essere installati (uno come primario e uno come secondario) in un backplane Ethernet ridondante. Le configurazioni possibili sono le seguenti:

Configurazione	Caratteristiche		
	Gestione della ridondanza (controllo alimentazione e segnali LED)	**Fornire i dati all'applicazione**	**Monitorare e salvare i dati di alimentazione**
due alimentatori nel backplane principale	✓	✓	✓
due alimentatori nel backplane esteso	✓	X	✓

Configurazione	Caratteristiche		
	Gestione della ridondanza (controllo alimentazione e segnali LED)	**Fornire i dati all'applicazione**	**Monitorare e salvare i dati di alimentazione**
un alimentatore in un backplane esistente	X	X	✓
✓ = supportato. X = non supportato.			

Per ulteriori informazioni sugli alimentatori ridondanti, vedere *Descrizione dei moduli di alimentazione Modicon X80* (vedere *Modicon X80, Backplane e alimentatori, Manuale di riferimento hardware*).

Diagnostica del modulo di alimentazione M580 Safety

Diagnostica per le tensioni del backplane 24 Vcc e 3,3 Vcc

Gli alimentatori di sicurezza BMXCPS4002S, BMXCPS4022S e BMXCPS3522S forniscono automaticamente il rilevamento di una condizione di sovratensione, sovraccarico o cortocircuito che può verificarsi rispetto alle tensioni del backplane 24 VCC e 3,3 VCC.

Se l'alimentatore rileva una delle seguenti condizioni sulla tensione 24 Vcc, si verifica quanto segue:

- La funzione di conversione dell'alimentazione viene disattivata per l'intero backplane.
- Viene emesso un comando RESET per tutti i moduli nel backplane.
- Il **OK** OK dell'alimentatore è spento.
- L'intero PAC è disinserito.

Se l'alimentatore rileva una di queste condizioni sulla tensione 3,3 Vcc, si verifica quanto segue:

- La funzione di conversione dell'alimentazione viene disinserita per la tensione del backplane 3,3 Vcc.
- Viene emesso un comando RESET per tutti i moduli nel backplane.
- Il **OK** OK dell'alimentatore è spento.
- Il funzionamento dell'intero programma PAC viene interrotto, sebbene alcuni circuiti PAC possano continuare a ricevere energia.

In ogni caso, per correggere queste condizioni procedere nel seguente modo:

1. Disinserire la linea di alimentazione principale.
2. Verificare la compatibilità tra l'assorbimento di potenza stimato del PAC rispetto alla capacità del modulo di alimentazione di sicurezza sulle linee del backplane 24 Vcc e 3,3 Vcc.
3. Eliminare la causa della condizione esistente.
4. Attendere un minuto dopo lo spegnimento.
5. Alimentare la linea principale per riavviare il modulo di alimentazione di sicurezza .

Diagnostica dei contatti relè di allarme

Gli alimentatori di sicurezza BMXCPS4002S, BMXCPS4022S e BMXCPS3522S presentano un contatto relè di allarme a due pin che permette di ottenere le seguenti informazioni:

- Se il relè è attivato (ossia chiuso):
  - Le tensioni del backplane 24 Vcc e 3,3 Vcc sono corrette.
  - RESET non è attivo.
  - Se l'alimentatore è posizionato nel backplane locale principale:

    - il controller è operativo.

    - il controller è in modalità RUN.
- Se il relè è disattivato (ossia aperto), può verificarsi uno dei seguenti eventi:
  - Una o entrambe le tensioni del backplane 24 Vcc e 3,3 Vcc non sono OK.
  - RESET è attivo.
  - Se l'alimentatore è posizionato nel backplane locale principale:

    - il controller non è operativo.

    - il controller è in modalità STOP.

DDT di sicurezza M580

Introduzione

I moduli di alimentazione di sicurezza M580 presentano due set di tipi di dati derivati (DDT):

- PWS_DIAG_DDT_V2 per diagnostica
- PWS_CMD_DDT per i comandi

PWS_DIAG_DDT_V2

Offset byte	Nome	Tipo	Commento
0	Riservato	BYTE	–
1	Riservato	BYTE	–
2	PwsMajorVersion	BYTE	Versione firmware maggiore alimentatore
3	PwsMinorVersion	BYTE	Versione firmware minore alimentatore
4	Modello	BYTE	Identificativo modello Identificativo modello: • BMXCPS4002S = 01 • BMXCPS4022S = 02 • BMXCPS3522S = 03
5	Stato	BYTE	Stato alimentatore
6	I33BacPos	UINT	Misura corrente sulla linea backplane 3,3V nel ruolo nominale (produttore)
8	V33Buck	UINT	Misura tensione 3,3V Buck
10	I24Bac	UINT	Misura corrente della linea backplane 24V
12	V24Int	UINT	Misura tensione 24V Int
14	Temperatura	INT	Misura della temperatura ambiente
16	OperTimeMasterSincePO	UDINT	Tempo operativo come master dall'ultima accensione
20	OperTimeSlaveSincePO	UDINT	Tempo operativo come slave dall'ultima accensione
24	OperTimeMaster	UDINT	Tempo operativo come master dal momento della produzione
28	OperTimeSlave	UDINT	Tempo operativo come slave dal momento della produzione

Offset byte	Nome	Tipo	Commento
32	Work	UDINT	Lavoro fornito dal momento della produzione
36	RemainingLTPC	UINT	Durata di vita residua in percentuale
38	NbPowerOn	UINT	Numero di accensioni dal momento della produzione
40	NbVoltageLowFail	UINT	Numero di errori rilevati sulla tensione del primario dalla soglia bassa
42	NbVoltageHighFail	UINT	Numero di errori rilevati sulla tensione del primario dalla soglia alta
44	Riservato	UDINT	–
48	Riservato	UDINT	–
52	RemainingLTMO	UINT	Durata di vita residua in mesi
54	Riservato	BYTE	–
63	Riservato	BYTE	–

PWS_CMD_DDT

Offset byte	Nome	Tipo	Commento
0	Riservato	BYTE	–
1	Codice	BYTE	Codice di comando: • 1 = scambia • 3 = azzera
2	PwsTarget	BYTE	Alimentatore di destinazione: 1 per sinistro, 2 per destro, 3 per entrambi Alimentatore di destinazione: • 1 = sinistro • 2 = destro
3	Riservato	BYTE	–
15	Riservato	BYTE	–

Convalida di un sistema di sicurezza M580

Introduzione

Questo capitolo spiega come eseguire i calcoli per la convalida del sistema di sicurezza M580 utilizzato.

Architetture del modulo di sicurezza M580

Introduzione

Questa sezione descrive le architetture interne dei moduli di sicurezza.

Architettura di sicurezza della CPU e del coprocessore di sicurezza M580

Introduzione

Le CPU BME•58•040S e il coprocessore BMEP58CPROS3 (Copro), con funzionalità di coppia di processori, sono certificati da TÜV Rheinland Group per l'uso in soluzioni di sicurezza conformi a Safety Integrity Level 3 (SIL3) M580.

Lavorando insieme, la CPU e il coprocessore forniscono le seguenti funzioni di sicurezza SIL3:

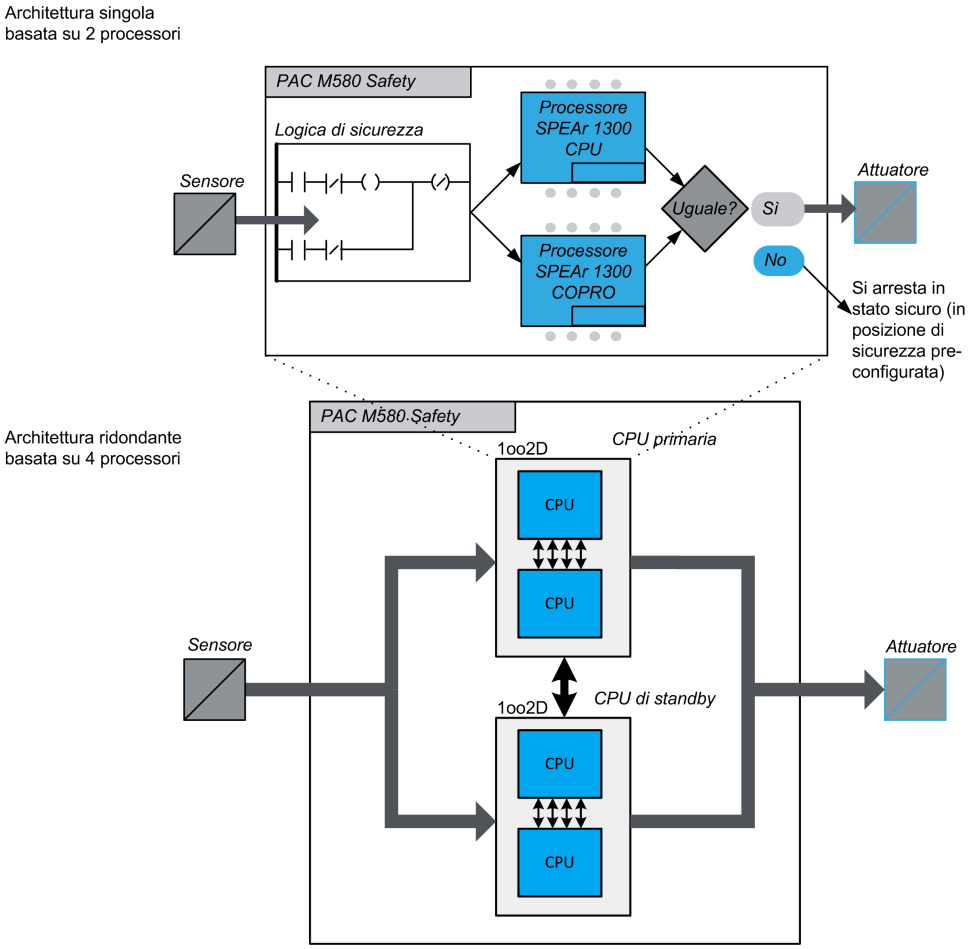
- Doppia esecuzione indipendente del codice del task di sicurezza.
- Confronto dei risultati della doppia esecuzione del codice.
- Autotest periodici.
- Supporto per un'architettura 1oo2D ("uno su due") con diagnostica.

NOTA: Oltre alla funzionalità di sicurezza, le CPU BMEP58•040S forniscono funzionalità comparabili alle CPU M580 standalone non di sicurezza equivalenti e le CPU BMEH58•040S forniscono funzionalità comparabili alle CPU Hot Standby M580 non di sicurezza equivalenti. Per informazioni sulle funzionalità non di sicurezza di queste CPU di sicurezza, consultare *Modicon M580, Hardware, Manuale di riferimento* e *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente*.

Descrizione dell'architettura interna della CPU e del coprocessore

La CPU di sicurezza e il Copro M580 contengono un processore SPEAr 1300 ciascuno. Ogni processore esegue la logica di sicurezza nella propria area di memoria e confronta i risultati dell'esecuzione alla fine del task di sicurezza.

La illustrazioni seguenti mostrano l'architettura interna della CPU M580 Safety in configurazioni singola e ridondante:



Generazione ed esecuzione del doppio codice

I due processori presenti all'interno del PAC di sicurezza M580 provvedono alla generazione e all'esecuzione del doppio codice. La presenza di due processori diversi consente i seguenti vantaggi nel rilevamento degli errori:

- Vengono generati in modo indipendente due codici di programma eseguibili. Viene facilitato il rilevamento degli errori di sistema durante la generazione del codice grazie all'uso di due compilatori indipendenti.

- I due codici di programma generati vengono eseguiti da due processori separati. In questo modo, la CPU può rilevare sia gli errori di sistema nell'esecuzione del codice e gli errori casuali nel PAC.
- Ogni processore utilizza la propria area di memoria indipendente. Gli errori casuali nella RAM possono quindi essere rilevati dal PAC, per cui non è necessario eseguire un test della RAM completo ad ogni scansione.

Architettura 1oo2D

L'architettura 1oo2D ("uno su due con Diagnostica") significa che due canali indipendenti eseguono la logica di sicurezza e, se viene rilevato un errore su uno dei canali, il sistema passa allo stato sicuro definito.

Architettura singola

L'architettura PAC M580 Safety singola si basa su 1oo2D composta da processori doppi che garantiscono la compatibilità a SIL3 (safety integrated level) anche in un'architettura non ridondante.

Architettura ridondante

Il PAC M580 Safety nell'architettura ridondante fornisce la massima disponibilità del sistema e attività del processo tramite aggiunta di piena ridondanza (Quadrupla struttura, ad esempio quattro CPU) su controllo, alimentazione e comunicazione.

Una delle CPU (coppia di processori) funge da Primario, esegue l'applicazione tramite esecuzione della logica di programma e attuazione degli IO. La CPU primaria (coppia di processori) aggiorna la CPU secondaria (coppia di processori) in modo che sia pronta per assumere il controllo degli IO.

Il sistema esegue continuamente l'automonitoraggio. In caso di errore irreversibile nel controller primario, il sistema passa il controllo al controller secondario. In questa modalità degradata, il sistema rimane SIL3. Se si verificano errori irreversibili nel controller primario e secondario, il sistema passa allo stato sicuro definito.

Il PAC M580 Safety ridondante, basato su architettura quadrupla (4 processori) consente di aumentare la disponibilità del sistema e garantisce compatibilità SIL3 (safety integrated level).

Watchdog

Un watchdog hardware e un watchdog firmware controllano l'attività del PAC e il tempo necessario per eseguire la logica del programma di sicurezza.

NOTA: Configurare il watchdog software (nella finestra di dialogo **Proprietà di SAFE**) per consentire:

- il tempo di esecuzione dell'applicazione
- il filtraggio degli errori di comunicazione degli I/O rilevati
- il tempo di sicurezza del processo.

Per maggiori informazioni, vedere la sezione *Tempo di sicurezza del processo*, pagina 157.

Controllo della memoria

L'integrità del contenuto della memoria statica viene testata mediante il controllo ciclico della ridondanza (CRC) e l'esecuzione del doppio codice. L'integrità del contenuto della memoria dinamica viene testata mediante l'esecuzione del doppio codice e l'uso di un sistema di codice correzione errore (ECC) che individua e corregge le istanze più comuni di dati interni corrotti. Durante l'avvio a freddo, questi test vengono reinizializzati ed eseguiti completamente prima che la CPU passi in modalità Stop o Run.

Monitoraggio della sovratensione

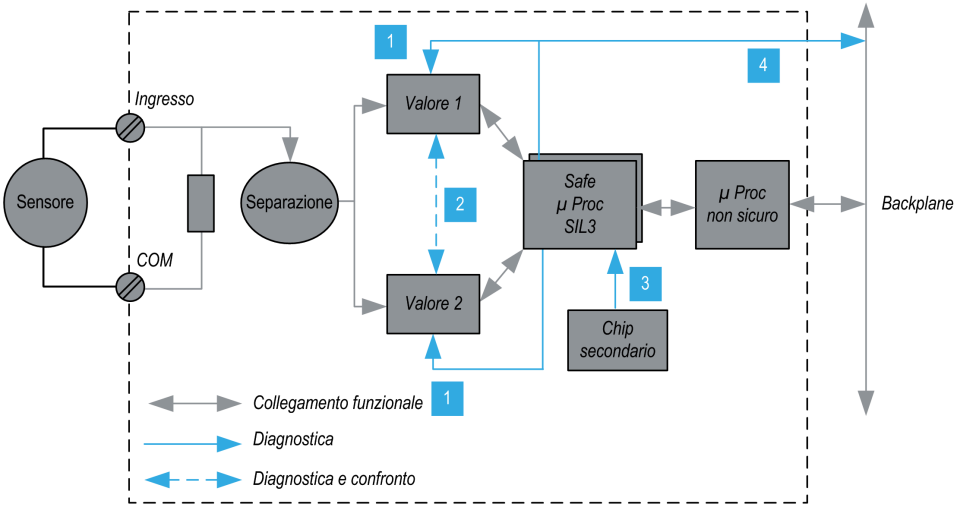
La CPU riceve l'alimentazione dal modulo di alimentazione di sicurezza dedicato M580 sulla linea del backplane. Il modulo di alimentazione di sicurezza fornisce 24V regolati con una tensione max. assoluta compresa nel campo 0...36V.

La CPU contiene una funzione integrata che controlla gli alimentatori interni. Se viene rilevata una condizione di sovratensione o sottotensione, il PAC si spegne.

Architettura di sicurezza del modulo di ingresso analogico BMXSAI0410

Architettura della funzione di sicurezza

L'architettura interna del modulo BMXSAI0410 esegue la funzione di sicurezza nel seguente modo:



1 Viene costantemente monitorata la capacità dei dispositivi di misura di misurare, senza errori rilevati, 10 valori analogici compresi tra 4 e 20 mA. Contemporaneamente viene misurata la linearità delle fasi della misura.

2 Ogni valore di ingresso è acquisito da 2 circuiti identici. I valori misurati vengono confrontati dal processore di sicurezza. Se i valori sono diversi, il canale viene dichiarato non valido. Tra i due valori è tollerata una discrepanza massima pari allo 0,35% della scala completa fino a 20 mA.

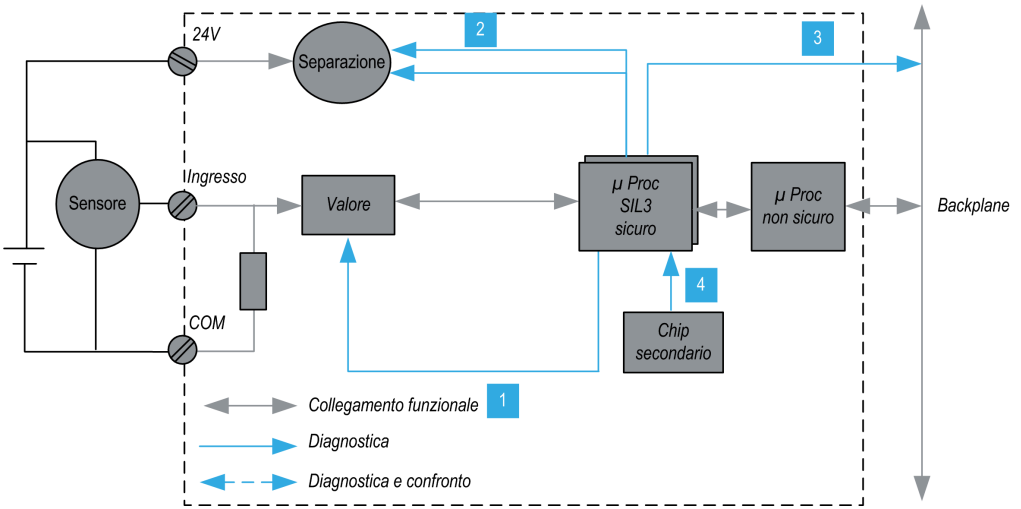
3 Il chip secondario alimenta il processore di sicurezza, effettua la diagnostica continua del processore di sicurezza e sorveglia la tensione del backplane.

4 La tensione di alimentazione dal backplane viene monitorata per rilevare un'eventuale condizione di sovratensione o di sottotensione.

Architettura di sicurezza del modulo di ingresso digitale BMXSDI1602

Architettura della funzione di sicurezza

L'architettura interna del modulo BMXSDI1602 esegue la funzione di sicurezza nel seguente modo:



1 Viene costantemente monitorata la capacità dei dispositivi di misura di misurare un valore "1" e un valore "0".

2 L'alimentazione esterna 24 Vdc è monitorata costantemente dal processore di sicurezza. Ogni valore di ingresso è acquisito da due circuiti identici. I valori acquisiti vengono confrontati dal processore di sicurezza. Se i valori sono diversi, il canale viene dichiarato non valido.

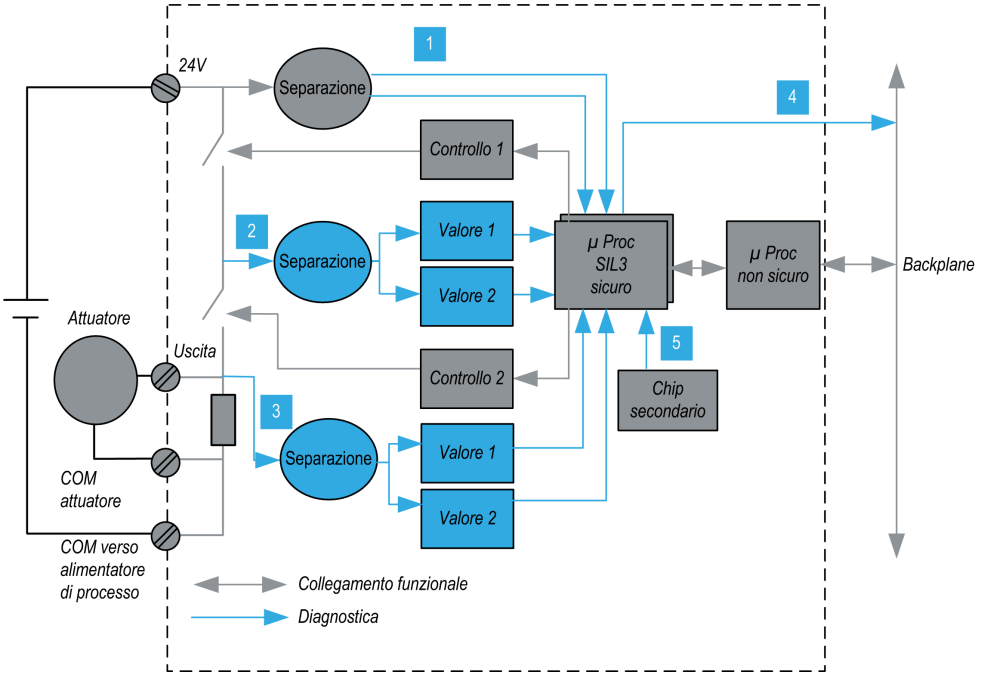
3 La tensione di alimentazione dal backplane viene monitorata per rilevare un'eventuale condizione di sovratensione o di sottotensione.

4 Il chip secondario alimenta il processore di sicurezza, effettua la diagnostica continua del processore di sicurezza e sorveglia la tensione del backplane.

Architettura di sicurezza del modulo di uscita digitale BMXSDO0802

Architettura della funzione di sicurezza

L'architettura interna del modulo BMXSDO0802 esegue la funzione di sicurezza nel seguente modo:



1 L'alimentazione esterna 24 Vdc è monitorata costantemente dal processore di sicurezza.

2 Ogni uscita consiste di 2 interruttori in serie tra l'alimentazione esterna +24 Vdc e la terra. Il valore del punto medio (2) viene letto in modo ridondante e inviato al processore di sicurezza. I valori misurati dei punti medi vengono confrontati dal processore di sicurezza. Se i valori non corrispondono a quelli previsti, il canale viene dichiarato non valido.

3 Anche il valore del punto inferiore (3) viene monitorato per la diagnostica del cablaggio estgerno.

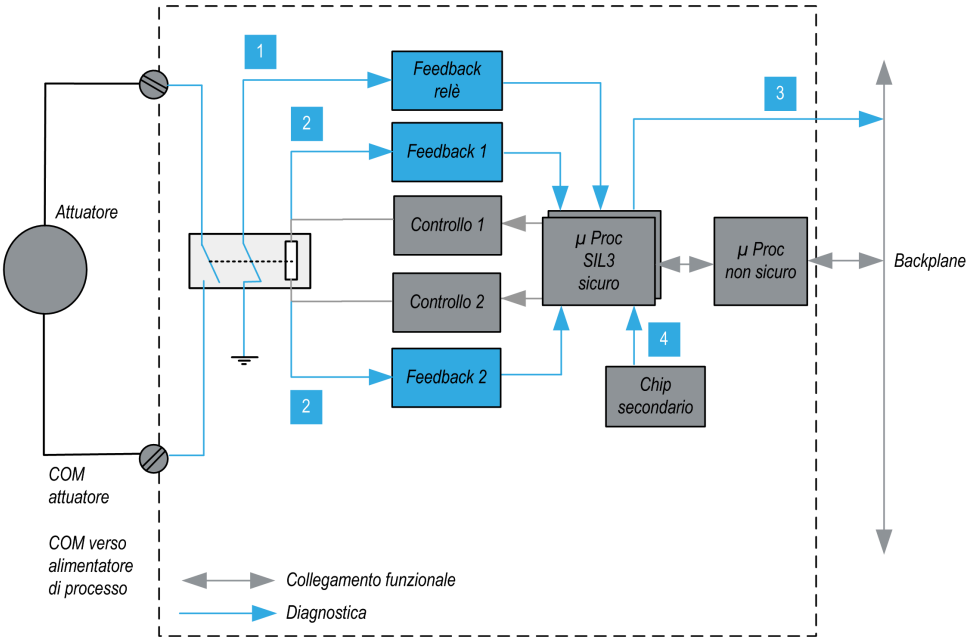
4 La tensione di alimentazione dal backplane viene monitorata per determinare se sussiste una condizione di sovratensione o di sottotensione.

5 Il chip secondario alimenta il processore di sicurezza, effettua la diagnostica continua del processore di sicurezza e sorveglia la tensione del backplane.

Architettura di sicurezza del modulo di uscita relè digitale BMXSRA0405

Architettura della funzione di sicurezza

L'architettura interna del modulo BMXSRA0405 esegue la funzione di sicurezza nel seguente modo:



1 Lo stato del relè è monitorato costantemente dal processore di sicurezza, che legge lo stato di un contatto NC collegato meccanicamente al contatto NO, a sua volta collegato all'attuatore.

2 Lo stato del comando relè è monitorato costantemente. Ogni valore di ingresso è acquisito da 2 circuiti identici. I valori misurati vengono confrontati dal processore di sicurezza. Se i valori sono diversi, il canale viene dichiarato non valido.

3 La tensione di alimentazione dal backplane viene monitorata per determinare se sussiste una condizione di sovratensione o di sottotensione.

4 Il chip secondario alimenta il processore di sicurezza, effettua la diagnostica continua del processore di sicurezza e sorveglia la tensione del backplane.

Valori SIL e MTTF del modulo di sicurezza M580

Introduzione

Questa sezione descrive i valori SIL e MTTF che si possono utilizzare per i calcoli relativi al modulo di sicurezza M580.

Calcoli del livello di integrità della sicurezza

Classificazione dei prodotti Schneider Electric

Il PAC di sicurezza M580 può comprendere:

- Moduli di sicurezza, che possono eseguire funzioni di sicurezza, tra cui:
  - CPU e coprocessore
  - moduli di I/O
  - alimentazione
- Moduli non interferenti, pagina 33, che non eseguono funzioni di sicurezza, ma consentono di aggiungere elementi non di sicurezza al progetto di sicurezza.

  NOTA:

  - Dato che i moduli non interferenti non fanno parte del loop di sicurezza, non rientrano nei calcoli del livello di integrità della sicurezza.
  - Un errore rilevato in un modulo non interferente non influisce negativamente sull'esecuzione delle funzioni di sicurezza.
  - Gli alimentatori BMXCPS4002S, BMXCPS4022S e BMXCPS3522S sono certificati. Dato che presenta un tasso di errore pericoloso trascurabile (<1% del SIL3 desiderato), l'alimentatore non è incluso nei calcoli del livello di integrità di sicurezza per il loop di sicurezza. Di conseguenza, per i moduli di alimentazione non vengono forniti né PFH né PFD.

Valori PFD/PFH per moduli di sicurezza M580

Schneider Electric propone i seguenti moduli di sicurezza certificati per l'uso in applicazioni di sicurezza. I moduli di sicurezza sono elencati con i valori corrispondenti di probabilità di errore, pagina 153 (PFD/PFH) per diversiintervalli dei test di prova, pagina 156 (PTI). Le probabilità PFD/PFH sono espresse come valori che contribuiscono alla probabilità PFD/PFH totale dell'intero loop di sicurezza, pagina 21.

Le tabelle che seguono elencano i moduli di sicurezza e i rispettivi valori PFD/PFH per le applicazioni SIL2 e SIL3, laddove applicabili:

Tipo prodotto	**Codice prodotto**	**SIL**	**PTI = 1 anno**	
			PFD_G	**PFH_G**
CPU con coprocessore	BME•58•040S & BMEP58CPROS3	SIL3[1]	4.41E-07	1.01E-10
Ingresso analogico	BMXSAI0410	SIL3[2]	5.76E-06	1.31E-09
Ingresso digitale	BMXSDI1602	SIL3[2]	6.81E-06	1.56E-09
Uscita digitale	BMXSDO0802	SIL3[1]	5.75E-06	1.31E-09
Uscita relè digitale	BMXSRA0405	SIL2 [3]	5.85E-06	1.68E-09
		SIL3[4]	5.84E-06	1.34E-09
		SIL3[5]	–	1.35E-09
Alimentazione	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL3	–	–

1. 1 uscita a 80° C
2. 1 ingresso a 80° C
3. 1 relè per uscita a 80° C
4. 2 relè per uscita a 80° C
5. 4 relè per uscita a 80° C

Tipo prodotto	**Codice prodotto**	**SIL**	**PTI = 5 anni**	
			PFD_G	**PFH_G**
CPU e coprocessore	BME•58•040S & BMEP58CPROS3	SIL3 [1]	2.22E-06	1.02E-10
Ingresso analogico	BMXSAI0410	SIL3[2]	2.88E-05	1.31E-09
Ingresso digitale	BMXSDI1602	SIL3[2]	3.41E-05	1.56E-09
Uscita digitale	BMXSDO0802	SIL3[1]	2.88E-05	1.31E-09
Uscita relè digitale	BMXSRA0405	SIL2 [3]	2.92E-05	1.68E-09
		SIL3[4]	2.92E-05	1.34E-09
		SIL3[5]	–	1.35E-09

Tipo prodotto	Codice prodotto	SIL	PTI = 5 anni	
			PFD_G	PFH_G
Alimentazione	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL3	–	–
1. 1 uscita a 80° C 2. 1 ingresso a 80° C 3. 1 relè per uscita a 80° C 4. 2 relè per uscita a 80° C 5. 4 relè per uscita a 80° C				

Tipo prodotto	Codice prodotto	SIL	PTI = 10 anni	
			PFD_G	PFH_G
CPU e coprocessore	BME•58•040S & BMEP58CPROS3	SIL3[1]	4.47E-06	1.03E-10
Ingresso analogico	BMXSAI0410	SIL3[2]	5.76E-05	1.31E-09
Ingresso digitale	BMXSDI1602	SIL3[2]	6.81E-05	1.56E-09
Uscita digitale	BMXSDO0802	SIL3[1]	5.75E-05	1.31E-09
Uscita relè digitale	BMXSRA0405	SIL2 [3]	5.84E-05	1.68E-09
		SIL3[4]	5.84E-05	1.34E-09
		SIL3[5]	–	1.35E-09
Alimentazione	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL3	–	–
1. 1 uscita a 80° C 2. 1 ingresso a 80° C 3. 1 relè per uscita a 80° C 4. 2 relè per uscita a 80° C 5. 4 relè per uscita a 80° C				

Tipo prodotto	Codice prodotto	SIL	PTI = 20 anni	
			PFD_G	PFH_G
CPU e coprocessore	BME•58•040S & BMEP58CPROS3	SIL3[1]	9.06E-06	1.05E-10
Ingresso analogico	BMXSAI0410	SIL3[2]	1.15E-04	1.31E-09
Ingresso digitale	BMXSDI1602	SIL3[2]	1.36E-04	1.56E-09
Uscita digitale	BMXSDO0802	SIL3[1]	1.15E-04	1.31E-09

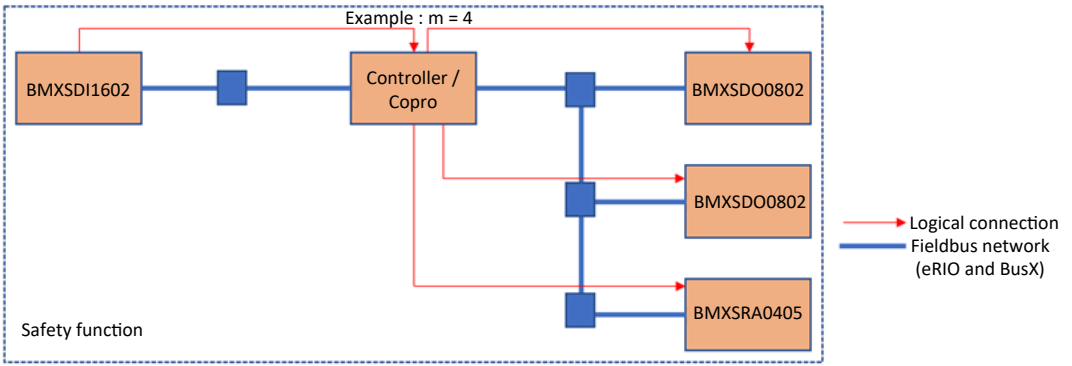
Tipo prodotto	Codice prodotto	SIL	PTI = 20 anni	
			PFD_G	PFH_G
Uscita relè digitale	BMXSRA0405	SIL2 [3]	1.17E-04	1.68E-09
		SIL3[4]	1.17E-04	1.34E-09
		SIL3[5]	–	1.35E-09
Alimentazione	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL3	–	–

1. 1 uscita a 80° C
2. 1 ingresso a 80° C
3. 1 relè per uscita a 80° C
4. 2 relè per uscita a 80° C
5. 4 relè per uscita a 80° C

Valori PFH per la comunicazione di sicurezza tra controller e moduli I/O Mx80 Safety

Per applicazioni ad alta richiesta, occorre considerare l'errore residuo legato alla comunicazione di sicurezza (black channel) tra il controller e i moduli I/O di sicurezza BMX. Per ogni comunicazione logica tra il controller e un modulo di I/O di sicurezza BMX coinvolto nella funzione di sicurezza, nel calcolo del PFH deve essere conteggiato un tasso di errore residuo di 1,5E-10.

Se "m" è il numero di moduli di I/O di sicurezza (SDI, SDO, SAI o SRA) utilizzati nella funzione di sicurezza, il PFH collegato alle comunicazioni di sicurezza uguale a "m * 1.5E-10" deve essere aggiunto al valore PFH globale:



Probabilità di guasto per applicazioni SIL3

Per le applicazioni SIL3, IEC 61508 definisce le seguenti probabilità di guasto su richiesta (PFD) e probabilità di guasto all'ora (PFH) per ogni loop di sicurezza, in base alla modalità di funzionamento:

- PFD ≥ 10^{-4} - < 10^{-3} per modalità di domanda di funzionamento bassa
- PFH ≥ 10^{-8} - < 10^{-7} per modalità di domanda di funzionamento alta

Il PAC di sicurezza M580 è certificato per un utilizzo in sistemi a bassa domanda e ad alta domanda di funzionamento.

Esempio di calcolo del livello di integrità della sicurezza

Questo esempio di calcolo mostra come determinare:

- Il contributo di rischio dei moduli di sicurezza Schneider Electric all'applicazione di sicurezza.
- Per applicazioni ad alta richiesta, il contributo delle comunicazioni di sicurezza tra il controller e i moduli I/O Mx80 Safety.
- Il restante contributo di rischio che altri dispositivi nel loop di sicurezza (ad esempio, sensori e attuatori) possono aggiungere all'applicazione di sicurezza per un determinato livello di integrità della sicurezza e un modo di funzionamento.

  NOTA: Quando si calcola il contributo di rischio di sensori e attuatori all'applicazione di sicurezza, contattare i costruttori di questi dispositivi per ottenere i valori PFD/PFH per l'intervallo del test di prova appropriato.

Questo esempio comprende i seguenti moduli di sicurezza Schneider Electric:

- 1: BMEP584040S CPU
- 1: BMEP58CPROS3 Copro
- 1: BMXSAI0410 Ingresso analogico
- 1: BMXSDO0802 Uscita digitale
- 1: BMXCPS4002S Alimentatore

Il calcolo seguente utilizza i valori PFH_G per una modalità di funzionamento ad alta domanda per un loop di sicurezza SIL3 con un PTI di 20 anni. Il valore PFH massimo consentito per questa applicazione di sicurezza è 10^{-7} (o 1.0E-7):

Modulo Safety	Contributo (notazione scientifica)	Contributo residuo per sensori e attuatori
CPU con coprocessore	7.01E-10	–
Ingresso analogico	1.31E-09	
Uscita digitale	1.31E-09	

Modulo Safety		Contributo (notazione scientifica)	Contributo residuo per sensori e attuatori
Alimentatore		–	
Comunicazioni I/O di sicurezza (m=2)		2 * 1.5E-10	
Totale	numerico	**3.62E-09**	**96.38E-09**
	% max	**3.62%**	**96,38%**
Nota 1: l'uscita relè utilizza quattro relè per supportare un'uscita.			

Valori per moduli di sicurezza M580 per macchinari

Schneider Electric propone i seguenti moduli di sicurezza certificati per l'uso in applicazioni di sicurezza per macchinari secondo la norma ISO13849-1. La tabella che segue elenca i moduli di sicurezza e i rispettivi valori, la categoria e il livello, laddove applicabili:

Tipo prodotto	Codice prodotto	Configurazione	Categoria	Performance Level	MTTF (anni)	DCav
CPU con coprocessore	BME•58•040S & BMEP58CPROS3	ND	4	e	235	Alto (>99%)
Ingresso analogico	BMXSAI0410	uso di 1 canale	2	d	255	99,66%
		uso di 2 canali	4	e	255	99,66%
Ingresso digitale	BMXSDI1602	uso di 1 canale	2	d	231	99,69%
		uso di 2 canali	4	e	231	99,69%
Uscita digitale	BMXSDO0802	ND	4	e	253	99,63%
Uscita relè digitale	BMXSRA0405	uso di 1 canale	2	c	156	99,77%
		uso di 2 canali	4	e	156	99,77%

Valori per i moduli M580 Safety per il settore ferroviario

Schneider Electric offre i seguenti moduli di sicurezza certificati per il settore ferroviario in base alle norme Cenelec EN50126, EN50128, EN50129. Nella tabella seguente sono elencati i moduli di sicurezza e i relativi valori di affidabilità:

Tipo prodotto	Codice prodotto	SIL	TFFR (PTI = 20 anni)
CPU e coprocessore	BME•58•040S & BMEP58CPROS3	SIL4	1.04E-10
Ingresso analogico	BMXSAI0410	SIL4	1.31E-09
Ingresso digitale	BMXSDI1602	SIL4	1.56E-09
Uscita digitale	BMXSDO0802	SIL4	1.31E-09
Uscita relè digitale	BMXSRA0405	SIL3 [1]	1.68E-09
		SIL4[2]	1.34E-09
		SIL4[3]	1.35E-09
Alimentazione	BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S	SIL4	–

NOTA: I valori SIL sono a 80° C

1. 1 relè per uscita a 80° C
2. 2 relè per uscita a 80° C
3. 4 relè per uscita a 80° C

La somma di TFFR di un modulo di ingresso, della CPU e del coprocessore, dell'alimentatore e di un modulo di uscita è sempre inferiore a 3.5E-09/h, che è inferiore al budget allocato massimo del 40%, visto come tasso di guasto residuo massimo per una funzione di sicurezza SIL4 che consente di integrare altri prodotti nel loop di sicurezza.

TFFR all'ora e per funzione	Attributo SIL
$10^{-9} \leq TFFR \leq 10^{-8}$	4
$10^{-8} \leq TFFR \leq 10^{-7}$	3
$10^{-7} \leq TFFR \leq 10^{-6}$	2
$10^{-60} \leq TFFR \leq 10^{-5}$	1

Descrizione dei tempi di sicurezza

Il PAC di sicurezza M580 dispone di un tempo di ciclo minimo del PAC di 10 ms, necessario per elaborare il segnale dai moduli di I/O, eseguire la logica utente e impostare le uscite. Per calcolare il tempo di reazione massimo del PAC, occorre conoscere il tempo di reazione massimo dei sensori e attuatori utilizzati. Inoltre, il tempo di reazione massimo del PAC dipende dal tempo di sicurezza del processo (PST), pagina 157 richiesto dal processo specifico.

Intervallo del test di prova

Il test di prova è un test periodico che occorre eseguire per rilevare errori in un sistema di sicurezza in modo che, se necessario, il sistema possa essere ripristinato a una nuova condizione o a quella più vicina possibile a questa condizione. Il periodo di tempo tra questi test è chiamato intervallo del test di prova.

L'intervallo del test di tenuta dipende dal livello di integrità di sicurezza mirato, dai sensori, dagli attuatori e dall'applicazione del controller. Il sistema di sicurezza M580 è adatto per essere utilizzato in un'applicazione SIL3 riguardante IEC 61508 e un intervallo di test di tenuta di 20 anni.

NOTA: Un test di tenuta può essere eseguito e considerato positivo se il controller funziona correttamente dopo un ciclo di spegnimento-accensione della configurazione di sicurezza completa che include CPU e I/O. In questo caso, non è necessario ricreare l'applicazione.

Calcolo delle prestazioni e dei tempi per il sistema di sicurezza M580

Introduzione

Questa sezione spiega come calcolare il tempo di reazione PAC, il tempo di reazione del sistema e il tempo di sicurezza del processo per il proprio sistema di sicurezza M580.

Tempo di sicurezza del processo

Descrizione del tempo di sicurezza del processo

Il tempo di sicurezza del processo (process safety time, PST) è una misura essenziale di un processo eseguito da un loop di sicurezza. Viene definito come il periodo di tempo che intercorre tra il verificarsi di un errore rilevato nell'apparecchiatura sotto controllo (EUC, Equipment Under Control) e il verificarsi di un evento pericoloso se la funzione di sicurezza non viene eseguita (ovvero se lo stato sicuro definito non viene raggiunto).

NOTA: Il tempo di sicurezza del processo è determinato dal processo di sicurezza specifico. È necessario verificare che il sistema relativo alla sicurezza possa eseguire le funzioni di sicurezza entro il tempo di sicurezza del sistema.

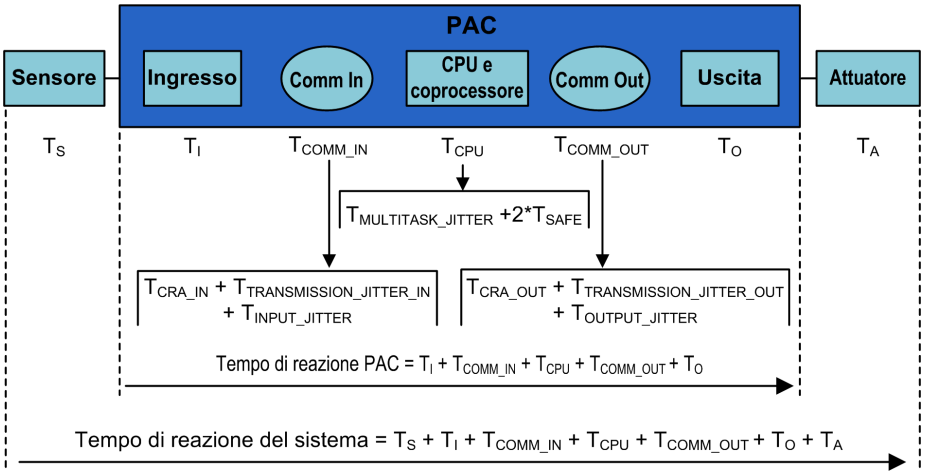
Descrizione del tempo di reazione del sistema

Il tempo di reazione del sistema è la somma del tempo di reazione del PAC più i tempi di reazione per il sensore selezionato (T_S) e l'attuatore selezionato (T_A).

NOTA: T_S e T_A sono specifici del dispositivo.

Per ogni loop di sicurezza verificare che il tempo di reazione del sistema sia minore del tempo di sicurezza del processo.

Il tempo di reazione del sistema è illustrato di seguito:



I componenti del tempo di reazione del sistema possono includere:

Componente	Descrizione	Valore worst case stimato
T_S	Tempo di reazione richiesto dal sensore selezionato per reagire a un evento di processo.	Specifico del dispositivo.
T_I	Tempo massimo richiesto dal modulo di ingresso per campionare e confermare un evento di sensore. Comprende: • Un periodo di campionamento del modulo di ingresso. • Periodi di campionamento multipli del modulo di ingresso per filtraggio.	6 ms
T_{COMM_IN}	Ritardo di comunicazione ingressi. I componenti sono descritti nell'argomento *Tempo di risposta dell'applicazione* in *Modicon M580 Guida alla pianificazione del sistema standalone per architetture di utilizzo frequente* e comprendono quanto indicato di seguito (i numeri si riferiscono al calcolo ART nell'argomento di riferimento): • T_{CRA_IN}: CRA_Drop_Process (2) + CRA Input RPI (3) • T_{JITTER_IN}: Network_In_Time (4) + Network_In_Jitter (5) + CPU_In_Jitter (6)	–
T_{CPU}	Il tempo di reazione di CPU e coprocessore, pari alla somma del ritardo causato dai task in sospeso di maggiore priorità (il task FAST) più due tempi di scansione del task SAFE – dove il primo è una scansione mancata e il secondo una scansione riuscita: $T_{MULTITASK\_JITTER}$ +2* T_{SAFE}.	
$T_{MULTITASK\_JITTER}$	Il ritardo massimo provocato dall'esecuzione di task in sospeso con priorità più alta. In questo caso, il task FAST. $T_{MULTITASK\_JITTER}$ = T_{FAST}.	–

Componente	Descrizione	Valore worst case stimato
T_{SAFE}	Periodo del task SAFE configurato.	–
T_{FAST}	Questo valore viene incluso perché l'esecuzione del task FAST è prioritaria rispetto al task SAFE. **NOTA:** Per semplificare la formula, si presume che nessun task del sistema si trovi in condizione di overrun. Pertanto questo valore equivale al periodo del task FAST configurato, o a 0 se il task FAST non è configurato.	–
T_{COMM_OUT}	Ritardo di comunicazione uscite. I componenti sono descritti nell'argomento *Tempo di risposta dell'applicazione* in *Modicon M580 Guida alla pianificazione del sistema standalone per architetture di utilizzo frequente* e comprendono quanto indicato di seguito (i numeri si riferiscono al calcolo ART nell'argomento di riferimento): • T_{CRA_OUT}: CRA_Drop_Process (12) • T_{JITTER_IN}: CPU_Out_Jitter (9) + Network_Out_Time (10) + Network_Out_Jitter (11)	–
T_O	Equivale alla somma dei seguenti tempi: • Tempo di ritardo tra la lettura e l'applicazione del valore di uscita della CPU (0...3 ms). • Tempo richiesto dal modulo di uscita di sicurezza per modificare l'uscita fisica, ossia per propagare lo scambio dalla RAM X all'uscita fisica (tra 0...3 ms).	6 ms
T_A	Tempo di reazione dell'attuatore selezionato.	Specifico del dispositivo.

Descrizione del tempo di reazione del PAC

Per gli I/O posizionati nel rack principale locale (con la CPU), il tempo di reazione del PAC è la somma dei tempi di reazione correlati per il modulo di ingresso selezionato (T_I) e il modulo di uscita selezionato (T_O), più il tempo di reazione della CPU e del coprocessore (T_{CPU}):

Tempo di reazione PAC (locale) = T_{CPU} + $T_{COMM\_IN + TI}$ + TCOMM_OUT +T_O

Se gli I/O si trovano in un rack remoto, il tempo di reazione del PAC include anche il tempo di ritardo di comunicazione ingressi (T_{COMM_IN}) e ritardo di comunicazione uscite (T_{COMM_OUT}):

Tempo di reazione PAC (remoto) = T_{CPU} + T_{COMM_IN} + T_I + T_{COMM_OUT} +T_O

Descrizione del tempo di reazione della CPU e del coprocessore

Il tempo di reazione della CPU e del coprocessore è influenzato direttamente dal periodo del task SAFE e dal periodo del task FAST. Verificare che la logica di sicurezza sarà eseguita entro il periodo del task SAFE.

Poiché può comparire un segnale all'inizio del ciclo di esecuzione quando i segnali sono già stati elaborati, possono essere necessari due cicli del task SAFE per reagire al segnale.

Poiché il task FAST ha la priorità sul task SAFE, quando si stima il tempo di reazione di CPU e coprocessore occorre anche considerare il tempo necessario per l'esecuzione del task FAST quando si valuta il jitter.

Ne consegue la seguente equazione per il tempo di reazione massimo (caso peggiore):

Tempo di reazione della CPU e del coprocessore = 2 x T_{SAFE} + T_{FAST}

NOTA: Se si usa la comunicazione peer-to-peer sicura, pagina 186 per eseguire la funzione di sicurezza, la stima del tempo di reazione della CPU è diversa.

Descrizione del tempo per moduli di ingresso

I tempi massimi (caso peggiore) per il modulo di ingresso digitale di sicurezza e per il modulo di ingresso analogico di sicurezza T_I sono 6 ms.

Descrizione del tempo per moduli di uscita

Il tempo massimo T_O per il modulo di uscita digitale di sicurezza è stimato a 6 ms.

Occorre configurare un timeout di posizionamento di sicurezza S_TO per il modulo di uscita digitale, pagina 111 e il modulo di uscita relé digitale, pagina 128. In base al periodo del task SAFE configurato (T_{SAFE}), il valore per S_TO deve essere configurato come indicato di seguito:

- Se (2,5 * T_{SAFE}) ≤ 40 ms, impostare S_TO a un minimo di 40 ms.
- Se (2,5 * T_{SAFE}) > 40 ms, impostare S_TO a un minimo di (2,5 * T_{SAFE}) ms.

AVVISO
DANNI ALL'APPARECCHIATURA Impostare il timeout di posizionamento di sicurezza (S_TO) per un modulo di uscita di sicurezza ad almeno un valore maggiore del più grande tra 40 ms o (2,5 * T_{SAFE}), dove T_{SAFE} è uguale al periodo del task SAFE configurato. **Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.**

Per applicazioni Hot Standby, considerare l'impatto sul parametro del timeout del posizionamento di sicurezza (S_TO) di tempo aggiuntivo (T_{SWAP}) richiesto da uno scambio, pagina 161 e di un tempo aggiuntivo T_{SWITCH} richiesto da uno switchover, pagina 163.

Calcolo del tempo di reazione del sistema

Conoscendo il tempo di sicurezza del processo (PST) e il tempo di reazione massimo di sensori e attuatori, si può calcolare il tempo di reazione del sistema (SRT) massimo ammissibile nel processo.

Il tempo di reazione max. (worst case) del sistema può essere calcolato come segue:

Per sistemi con I/O in derivazioni remote:

Max SRT = $T_S + T_I + 2 \times T_{CRA} + T_{RPI} + 2 \times T_{SAFE} + T_{FAST} + T_O + T_A$.

oppure

Max SRT = 16 ms + $T_S + 2{,}5 \times T_{SAFE} + T_{FAST} + T_A$.

Per sistemi con I/O locali:

Max SRT = $T_S + T_I + 2{,}5 \times T_{SAFE} + T_{FAST} + T_O + T_A$.

oppure

Max SRT = 15 ms + $T_S + 2{,}5 \times T_{SAFE} + T_{FAST} + T_A$.

NOTA: Per i PAC Hot Standby, per il calcolo del tempo di reazione di sicurezza massimo, prendere in considerazione i componenti aggiuntivi ai calcoli precedenti:

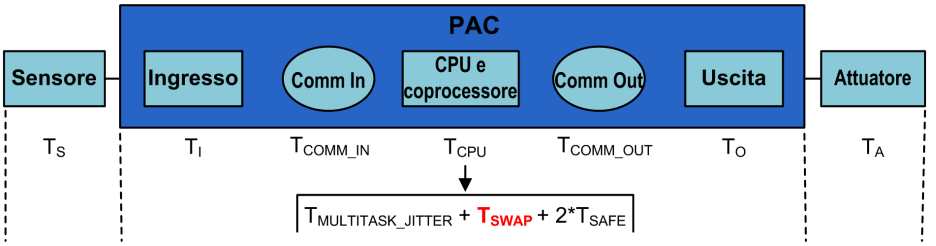
- Durante uno switchover, il tempo di reazione di sicurezza massimo potrebbe aumentare aggiungendo il componente, pagina 163 T_{SWITCH} ai calcoli precedenti.
- Mentre l'operatore del sistema esegue uno scambio, il tempo di reazione massimo potrebbe aumentare con un componente aggiuntivo, pagina 161 T_{SWAP} ai calcoli precedenti.

Tempo di reazione del sistema durante uno scambio

Uno scambio è l'azione avviata dall'operatore su un sistema Hot Standby, che provoca lo scambio di ruoli tra i controller primario e di standby. Lo scambio consuma tempo aggiuntivo, perché durante lo scambio non si possono perdere informazioni e tutte le uscite del sistema devono aver timeout sicuri.

Il componente di tempo dello scambio viene aggiunto al tempo T_{CPU} che segue il normale componente T_{JITTER}, come indicato di seguito:

Il componente di tempo T_{SWAP} viene aggiunto al tempo T_{CPU} che segue il normale componente T_{JITTER}. La sequenza è mostrata di seguito. Tranne per l'inclusione del componente di scambio, la descrizione del tempo di reazione del sistema è uguale a quella descritta in precedenza, pagina 157:



Il componente del tempo T_{SWAP} è la somma di:

$T_{ADDITIONAL\_JITTER} + T_{TRANSFER}$

I componenti specifici dello scambio sono descritti di seguito:

Componente	Descrizione	Valore worst case stimato
$T_{ADDITIONAL\_JITTER}$	Jitter introdotto dal sistema multi-task per riavviare il task sul nuovo PAC. Quindi, $T_{ADDITIONAL\_JITTER} = T_{SAFE}$.	–
$T_{TRANSFER}$	Durante la diagnostica del task MAST, il PAC accetta il comando di scambio e inizia il trasferimento di tutti i dati più recenti per ogni task.	Vedere la formula seguente.

$T_{TRANSFER}$ può essere calcolato come indicato di seguito:

$K3 \times (MAST_{KB} + 2 \times SAFE_{KB} + FAST_{KB}) + K4 \times (MAST_{DFB} + 2 \times SAFE_{DFB} + FAST_{DFB}) / 1000$

dove:

- $TASK_{KB}$ = Dimensione dei dati (in KB) scambiati per il TASK tra il PAC primario e il PAC di standby.
- $MAST_{DFB}$ = numero di DFB dichiarati nel TASK.
- K3 e K4 sono costanti, con i valori determinati dal modulo CPU specifico utilizzato nell'applicazione:

Coefficiente	BMEH582040S	BMEH584040S oppure BMEH586040S
K3	46,4 µs/kB	14,8 µs/kB
K4	34,5 µs/istanza DFB	11,0 µs/istanza DFB

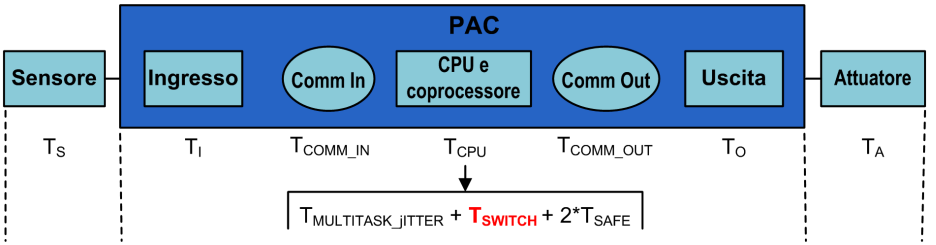
Se l'operatore di sistema vuole eseguire uno scambio senza uscite del modulo di sicurezza che vanno in stato di posizionamento di sicurezza, impostare il parametro di timeout di

posizionamento di sicurezza dei moduli di uscita di sicurezza (S_TO) ad almeno un valore maggiore di: $T_{JITTER\_MULTITASK} + T_{SWAP} + T_{SAFE}$.

Tempo di reazione del sistema durante uno switchover

Uno switchover si verifica quando il controller di standby in un sistema Hot Standby diventa il controller primario, ad esempio quando l'hardware nel controller primario diventa improvvisamente non operativo. Lo scopo dello switchover è, per il nuovo PAC primario, di sostituire senza interruzioni quello vecchio e iniziare le operazioni dal punto in cui il precedente PAC primario ha cessato di funzionare. Tuttavia, l'ultimo ciclo potrebbe dover essere rieseguito. Lo scopo del sistema è raggiungere il ripristino più rapido possibile.

Il componente di tempo T_{SWITCH} viene aggiunto al tempo T_{CPU} che segue il normale componente T_{JITTER}. La sequenza è mostrata di seguito. Tranne per l'inclusione del componente di switchover, la descrizione del tempo di reazione del sistema è uguale a quella descritta in precedenza, pagina 157:



Il componente del tempo T_{SWITCH} è la somma di:

$T_{DETECT} + T_{ADDITIONAL\_JITTER}$

I componenti specifici dello switchover sono descritti di seguito:

Componente	Descrizione	Valore worst case stimato
T_{DETECT}	Tempo impiegato dal PAC di standby per rilevare e confermare che il PAC primario è diventato non operativo.	15 ms
$T_{ADDITIONAL\_JITTER}$	Jitter introdotto dal sistema multi-task per riavviare il task sul nuovo PAC. Quindi, $T_{ADDITIONAL\_JITTER} = T_{SAFE}$.	–

A differenza dallo scambio, non è necessario tempo aggiuntivo per eseguire un trasferimento di dati.

Per consentire al sistema di rispondere a un errore rilevato ed eseguire uno switchover senza uscite del modulo di sicurezza che vanno in stato di posizionamento di sicurezza, impostare il parametro di timeout di posizionamento di sicurezza dei moduli di uscita di sicurezza (S_TO) ad almeno un valore maggiore di: $T_{JITTER} + T_{SWITCH} + T_{SAFE}$.

Configurazione del periodi massimi dei task SAFE e FAST della CPU

Il PAC di sicurezza M580 può effettuare soltanto l'esecuzione periodica dei task SAFE e FAST (l'esecuzione ciclica non è supportata per questi task).

Le impostazioni del **Periodo** del task SAFE e del **Watchdog** massimo consentito della CPU sono configurate nella scheda **Generale** della finestra di dialogo **Proprietà di SAFE**. Le impostazioni di **Timeout posizionamento di sicurezza** dell'uscita digitale di sicurezza sono configurate nella scheda **Configurazione** del modulo di uscita, pagina 105.

Analogamente, le impostzioni di **Periodo** del task FAST e **Watchdog** massimo consentito della CPU sono configurate nella scheda **Generale** della finestra di dialogo **Proprietà di FAST**.

NOTA:

- L'intervallo di valori di impostazione ammessi per il periodo del task SAFE è 10...255 ms, con un valore predefinito di 20 ms.
- L'intervallo di valori di impostazione ammessi per il periodo del task FAST è 1...255 ms, con un valore predefinito di 5 ms.
- L'intervallo di valori di impostazione ammessi per il watchdog è 10...500 ms, con un valore predefinito di 250 ms.
- L'intervallo delle impostazioni ammesse per il timeout di posizionamento di sicurezza delle uscite digitali è 0...65535 ms, con un valore predefinito di 500 ms.

Verificare che l'impostazione del watchdog sia maggiore del periodo del task SAFE.

Verificare l'impostazione del periodo del task SAFE della CPU al momento della messa in servizio del progetto. Attualmente, Control Expert Safety fornisce i valori in tempo reale dal PAC.

Queste informazioni sono disponibili in Control Expert Safety nella scheda **Task** tramite la voce di menu **Strumenti > Schermata PLC**.

Il periodo del task SAFE del controller deve essere inferiore al tempo di sicurezza del processo del progetto.

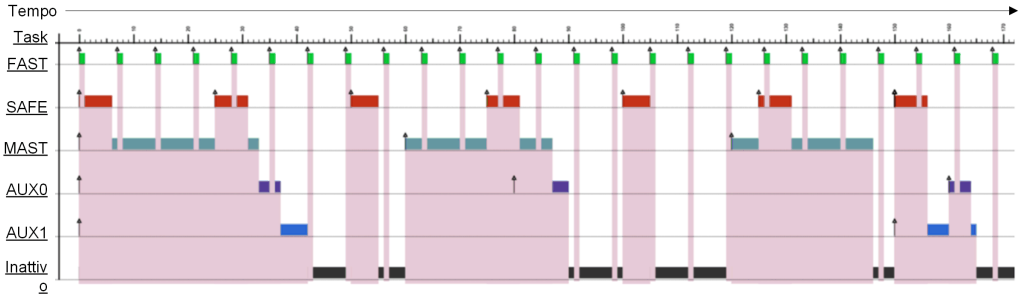
⚠AVVERTIMENTO

SUPERAMENTO DEL TEMPO DI SICUREZZA DEL PROCESSO

Impostare il periodo massimo del task SAFE del controller tenendo in considerazione il tempo di sicurezza del processo.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

L'illustrazione seguente mostra l'esecuzione di ogni task in un sistema multi-task e mostra la priorità delle risorse della CPU in base alla priorità dei task:



FAST			SAFE			MAST			AUX0			AUX1			IDLE
Periodo 7 ms	Exe 1 ms	Ampiezza banda 14%	Periodo 25 ms	Exe 5 ms	Ampiezza banda 20%	Periodo 60 ms	Exe 18 ms	Ampiezza banda 30%	Periodo 80 ms	Exe 3 ms	Ampiezza banda 4%	Periodo 150 ms	Exe 5 ms	Ampiezza banda 3%	Ampiezza di banda libera 29%

NOTA: quando il task MAST è in modalità periodica e per prestazioni ottimali della CPU, la percentuale totale di larghezza di banda della CPU utilizzata da un'applicazione non deve superare l'80%.

Calcolo dell'impatto dei periodi di esecuzione dei task sulla larghezza di banda della CPU

Ogni task configurato utilizza una parte del tempo di elaborazione, o larghezza di banda, della CPU. Il valore stimato della percentuale di larghezza di banda della CPU utilizzata da un task è il risultato (o quoziente) del valore stimato del tempo di esecuzione richiesto da un task (E_{TASK}) diviso per il periodo di esecuzione configurato per tale task (T_{TASK}) e può essere descritto come segue:

Larghezza di banda del task = $E_{TASK:}$ / $T_{TASK:}$.

Pertanto, il valore percentuale totale della larghezza di banda della CPU utilizzata da un'applicazione è la somma dei valori percentuali delle larghezze di banda della CPU utilizzate per tutti i task.

NOTA: quando il task MAST è in modalità periodica e per prestazioni ottimali della CPU, la percentuale totale di larghezza di banda della CPU utilizzata da un'applicazione non deve superare l'80%.

La tabella seguente presenta due applicazioni e indica l'impatto di task ad alta priorità (FAST e SAFE) sull'uso della larghezza di banda totale della CPU.

#	FAST			SAFE			MAST			AUX0			To-tale
	Per	Exe	BW %	Per	Exe	BW%	Per	Exe	BW%	Per	Exe	BW%	
1	5 ms	1 ms	20%	20 ms	5 ms	25%	50 ms	18 ms	35%	200 ms	30 ms	15%	96%
2	7 ms	1 ms	14%	25 ms	5 ms	20%	60 ms	18 ms	30%	200 ms	30 ms	15%	79%

Per = Periodo task (T_{TASK})

Exe = Tempo di esecuzione richiesto per il task (E_{TASK})

BW% = larghezza di banda del task.

Impatto delle comunicazioni CIP Safety sul tempo di reazione del sistema di sicurezza

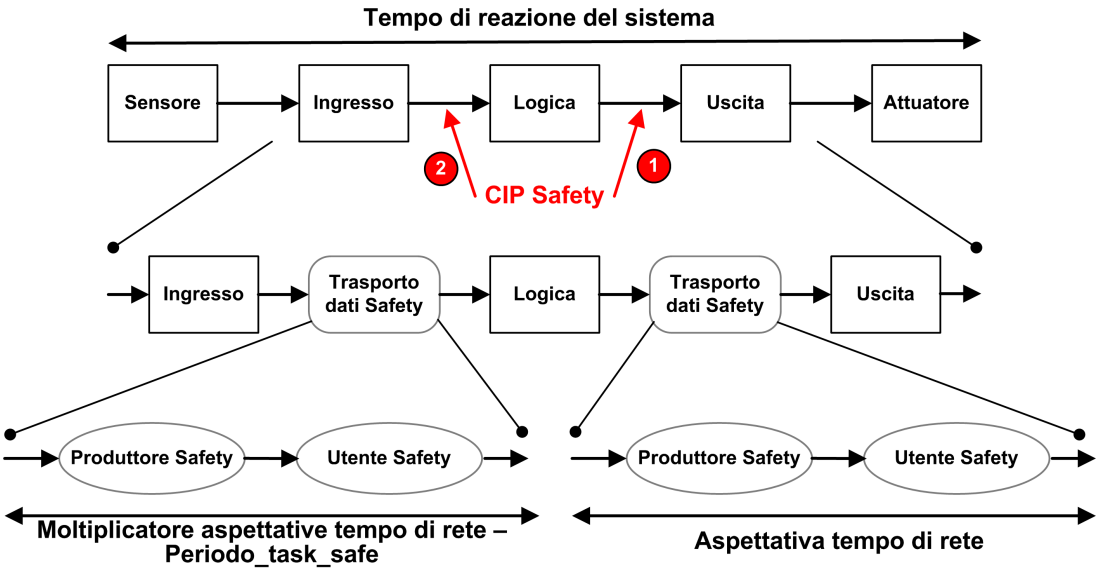
Introduzione

Il tempo impiegato dalla comunicazione CIP Safety, chiamato *aspettativa tempo di rete*, viene aggiunto al e fa parte del *tempo di reazione del sistema*, pagina 157. L'aspettativa tempo di rete rappresenta il periodo di tempo massimo, o caso peggiore, a partire dal momento in cui i dati vengono catturati dal produttore di dati di sicurezza fino a quando l'applicazione di utilizzo riconosce lo stato di sicurezza. Ciò comprende anche errori durante la produzione e l'utilizzo.

Se la comunicazione CIP Safety è compresa tra ingresso e logica, sostituire la variabile termine TCOMM_IN nel calcolo del tempo di sicurezza processo, pagina 157 con *Aspettativa tempo di rete – Periodo_task_safe* Se la comunicazione CIP Safety è compresa tra logica e uscita, sostituire la variabile termine TCOMM_OUT nel calcolo del tempo di sicurezza processo con *Aspettativa tempo di rete*.

Le misure predefinite dell'Aspettativa tempo di rete possono variare, in base al ruolo della CPU di sicurezza M580 come produttore o utilizzatore.

Gli elementi dell'aspettativa tempo di rete e il posizionamento di quest'ultima nel contesto del tempo di reazione del sistema sono indicati nel seguente diagramma:



1 CPU CIP Safety come produttore

2 CPU CIP Safety come utilizzatore

Calcolo dell'Aspettativa tempo di rete

L'aspettativa tempo di rete può essere calcolata con la formula seguente:

Aspettativa tempo di rete = Moltiplicatore_Aspettativa_tempo_di_rete * 128 µSec > (EPI * Moltiplicatore_Timeout+ Ora_Messaggio_sicurezza(max) + Ora_Messaggio_Coord_Tempo (max) + Costante_Correzione_Connessione*128 µSec)

Dove:

- **Ora_Messaggio_sicurezza(max)** è il tempo effettivo intercorso tra il momento in cui i dati vengono catturati dal produttore dati di sicurezza e il momento in cui i dati di sicurezza vengono passati all'applicazione consumatrice per l'utilizzo.
- **Ora_Messaggio_Coord_Tempo(max)** è il tempo massimo necessario per l'invio dell'informazione di coordinamento di tempo dall'utilizzatore al produttore.
- **Moltiplicatore_Timeout** è un parametro utilizzato dall'elaboratore del protocollo CIP Safety, che determina il numero di messaggi che potrebbero andare persi prima di dichiarare un errore di connessione. Un Moltiplicatore_Timeout pari a 1 indica che nessun messaggio viene perso.

- **Costante_Correzione_Connessione** è un valore a incrementi di 128 µSec che viene sottratto dal time stamp per rappresentare il peggiore errore possibile causato da una deviazione di tempo, dalla natura asincrona degli orologi del produttore e utilizzatore e dal tempo minimo necessario al Messaggio di Coordinamento di tempo per passare dall'utilizzatore al produttore.
- **EPI** è l'intervallo di pacchetto atteso ed è basato su un periodo task SAFE configurato.
- **Moltiplicatore_Aspettativa_tempo_di_rete** e **Moltiplicatore_Timeout** sono parametri di comunicazione CIP configurati per il frame di connessione SafetyOpen di tipo 2, pagina 376.

Valori predefiniti dell'Aspettativa tempo di rete

Il calcolo predefinito del valore dell'aspettativa tempo di rete dipende dal ruolo della CPU CIP Safety come utilizzatore (caso 2 del diagramma precedente) o produttore (caso 1).

CPU come utilizzatore (caso 2):

- Moltiplicatore_Timeout = 2
- EPI = periodo task SAFE / 2
- Ora_Messaggio_di_sicurezza(max) = Periodo task Safe + 20 ms (caso peggiore)
- Ora_Messaggio_Coord_Tempo(max) = Periodo task Safe + 20 ms (caso peggiore)
- Costante_Correzione_Connessione = 0 ms

Aspettativa tempo di rete = 1,5 * Aspettativa_tempo_di_rete minima = 1,5 * (3 * Periodo task safe + 40 ms) = 4,5 * Periodo task safe + 60 ms

CPU come produttore (caso 1):

- Moltiplicatore_Timeout = 2
- EPI = periodo task SAFE
- Ora_Messaggio_di_sicurezza(max) = Periodo task Safe + 20 ms (caso peggiore)
- Ora_Messaggio_Coord_Tempo(max) = Periodo task Safe + 20 ms (caso peggiore)
- Costante_Correzione_Connessione = 0 ms

Aspettativa tempo di rete = 1,5 * Aspettativa_tempo_di_rete minima = 1,5 * (4 * Periodo task safe + 40 ms) = 6 * Periodo task safe + 60 ms

Libreria di sicurezza

Libreria di sicurezza

Presentazione della libreria di sicurezza

Quando si installa Control Expert Safety, vengono automaticamente inclusi una libreria di sicurezza di funzioni elementari (EF), blocchi funzione elementari (EFB) e blocchi funzione derivati (DFB). Questi EF, EFB e DFB sono identificati dal prefisso "S_" e sono riservati all'uso in sezioni di codice gestite dal task SAFE.

NOTA: Inoltre viene installata una raccolta aggiuntiva di EF, EFB e DFB. Si tratta della stessa raccolta di oggetti dati usata dai PC M580 non di sicurezza. Questi EF, EFB e DFB possono essere usati solo in sezioni di codice gestite dai task dello spazio dei nomi di processo (MAST, FAST, AUX0 e AUX1).

Per una descrizione dei blocchi inclusi nella libreria M580 di sicurezza, vedere il documento *Control Expert - Libreria dei blocchi di sicurezza*.

Funzioni e blocchi funzione di sicurezza certificati

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

- Non utilizzare la V1.00 del blocco funzione derivata S_GUARD_LOCKING nell'applicazione.
- In Unity Pro 13.0 XLS o successiva, aggiornare il blocco funzione S_GUARD_LOCKING nell'applicazione con V1.01 o successiva, quindi ricompilare l'applicazione.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

NOTA:

Unity Pro è il nome precedente di Control Expert per versione 13.1 o precedenti.

Di seguito sono elencati gli EF e i blocchi funzione che possono essere usati nella logica di sicurezza e che sono forniti nella libreria di sicurezza.

Famiglia	Gruppo o nome	Tipo	Descrizione
Logica	S_AND_*, S_OR_*, S_XOR_*, S_NOT_*, S_SHL_*, S_SHR_*, S_ROR_*, S_ROL_*	EF	Specifico del tipo, ad esempio S_AND con 2 - 32 ingressi (codice inline)
Logica	S_RS, S_SR, S_F_TRIG, S_R_TRIG	EFB	–
Matematica	S_ADD_*, S_MUL_*, S_SUB_*, S_DIV_*, S_ABS_*, S_SIGN_*, S_NEG_*, S_MOVE, S_SQRT_REAL	EF	Gestione errori rilevati specifica del tipo (ad esempio overflòow) da considerare (codice inline)
Confronto	S_GT_*, S_GE_*, S_LT_*, S_LE_*, S_NE_*, S_EQ_*	EF	Specifico del tipo (codice inline)
Statistica	S_LIMIT_*, S_MAX_*, S_MIN_*, S_MUX_*, S_SEL	EF	Specifico del tipo (codice inline)
Tipo a tipo	S_BIT_TO*, S_BOOL_TO_*, S_BYTE_TO_*, S_DINT_TO_*, S_DWORD_TO_*, S_INT_TO_*, S_REAL_TO_*, S_TIME_TO_*, S_UDINT_TO_*, S_UINT_TO_*, S_WORD_TO_*	EF	Specifico del tipo (codice inline)
Temporizzatori e contatori	S_CTU_*, S_CTD_*, S_CTUD_*	EFB	Specifico del tipo
Temporizzatori e contatori	S_TON, S_TOF, S_TP	EFB	–
Peer to peer	S_RD_ETH_MX, S_WR_ETH_MX, S_RD_ETH_MX2, S_WR_ETH_MX2	DFB	Funzioni per eseguire una comunicazione peer-to-peer di sicurezza
Connessione attuatori	S_EDM, S_ENABLE_SWITCH, S_ESPE, S_OUTCONTROL, S_GUARD_LOCKING, S_GUARD_MONITORING, S_MODE_SELECTOR	DFB	Blocchi funzione di sicurezza macchina collegati ad attuatori
Connessione sensori	S_EQUIVALENT, S_ANTIVALENT, S_EMERGENCYSTOP, S_TWO_HAND_CONTROL_TYPE_II, S_TWO_HAND_CONTROL_TYPE_III, S_MUTING_SEQ, S_MUTING_PAR, S_AI_COMP	DFB	Blocchi funzione di sicurezza macchina collegati a sensori
Sistema	S_SYST_STAT_MX, S_SYST_TIME_MX, S_SYST_CLOCK_MX, S_SYST_RESET_TASK_BIT_MX, S_SYST_READ_TASK_BIT_MX	EFB	Blocchi funzione di sistema

Funzioni e blocchi funzione di sicurezza non certificati

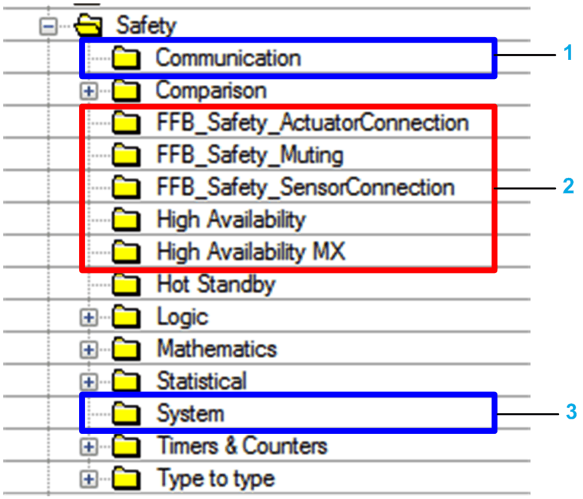
Di seguito è elencato un sottoinsieme di blocchi di funzioni derivate (DFB) che possono essere usati nella logica di sicurezza. Questi blocchi funzione non sono certificati. Lo scopo è fornire blocchi funzione di sicurezza che possono essere riutilizzati e adattati. È possibile

copiare e incollare questi blocchi funzione nella propria applicazione e modificarli per soddisfare i requisiti dell'applicazione.

Famiglia	Gruppo o nome	Tipo	Descrizione
Alta disponibilità MX	S_DIHA, S_AIHA	DFB	Funzione per moduli di ingresso digitali SIL2 o SIL3 ad alta disponibilità (codice inline)
Connessione sensori	AI_COMP	DFB	Blocchi funzione di sicurezza macchina collegati a sensori

Visualizzazione della libreria di sicurezza in Control Expert

Si può accedere alla libreria di sicurezza solo dal task SAFE. Quando si apre la libreria di sicurezza nell'**Editor FBD**, la libreria di sicurezza presenta gruppi di EF, EFB e DFB. Alcuni di questi gruppi comprendono versioni di sicurezza di funzioni e blocchi che si trovano in task non di sicurezza. Altri gruppi, riportati di seguito, contengono funzioni e blocchi specifici del task SAFE:



1 Blocchi per la lettura e la scrittura dei valori dei dati di sicurezza.

2 Blocchi per l'esecuzione di task specifici della sicurezza.

3 Blocchi per la lettura e la scrittura dei valori del sistema di sicurezza.

Per un esempio di come sono implementati i blocchi di sicurezza, vedere l' esempio di configurazione di comunicazione PAC-PAC, pagina 188, che comprende S_RD_ETH_MX e S_WR_ETH_MX.

Per una descrizione di ogni funzione e blocco di sicurezza vedere anche *EcoStruxure™ Control Expert - Libreria dei blocchi di sicurezza*.

Separazione dei dati in un sistema di sicurezza M580

Introduzione

Questo capitolo descrive la separazione dei dati in un sistema di sicurezza M580.

Separazione dei dati in un progetto di sicurezza M580

Separazione dei dati e ambito

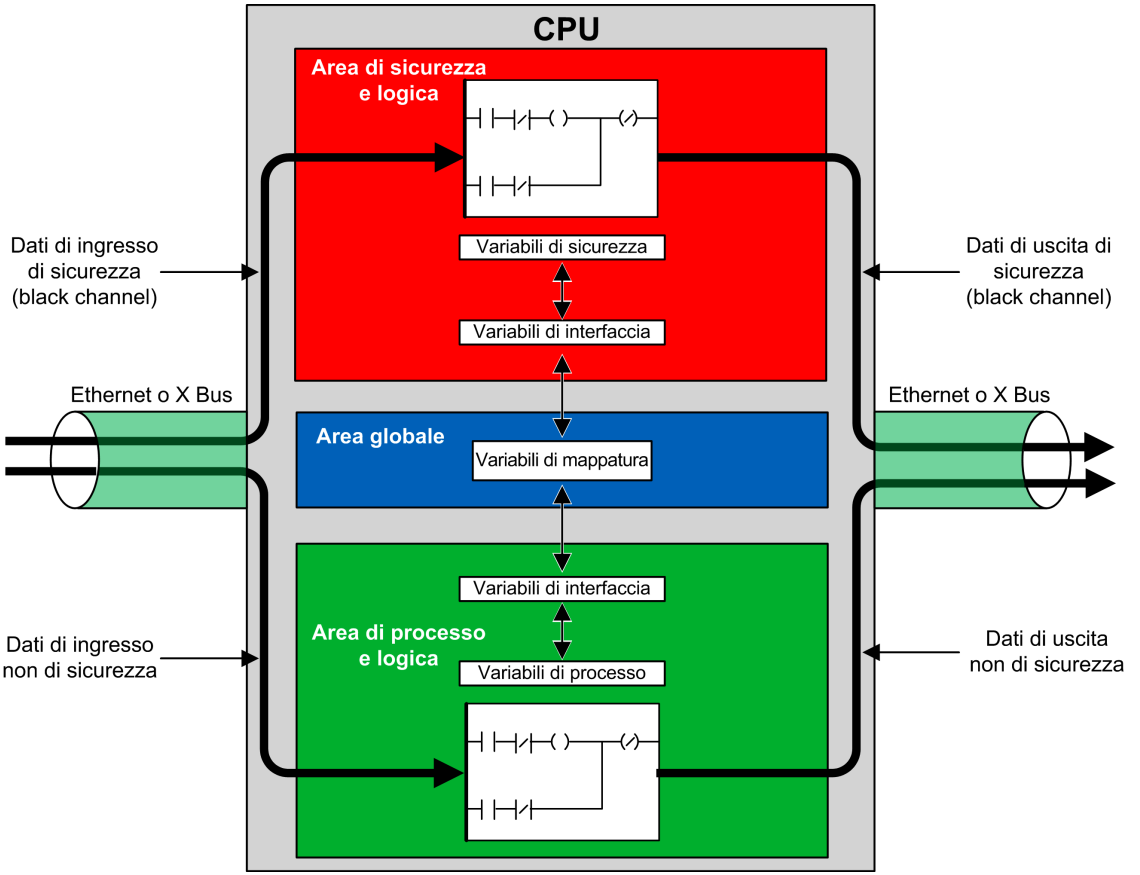
Un progetto di sicurezza M580 include sia un programma di sicurezza sia un programma di processo (non di sicurezza). Control Expert isola la logica e i dati utilizzati dal programma di sicurezza dalla logica e dai dati utilizzati dal programma di processo. Per questo, Control Expert colloca ogni parte del progetto nel proprio spazio dei nomi (detto anche area), *sicuro* o *di processo*.

A seguito di questa configurazione, l'ambito di una variabile di sicurezza è limitato all'area sicura e l'ambito di una variabile di processo è limitato all'area di processo. Questo diventa evidente quando si aggiunge la logica di programma all'applicazione:

- Quando si configura un EF o EFB nel task SAFE, sono visibili solo le variabili create nell'area sicura. Le variabili create nell'area di processo non sono visibili.
- Quando si configura un EF o EFB in un task non sicuro (MAST, FAST, AUX0 o AUX1), sono visibili solo le variabili create nell'area di processo. Le variabili create nell'area sicura non sono visibili.

Per consentire la comunicazione tra l'area sicura e l'area di processo, Control Expert fornisce anche un'area *globale*. L'area globale consente il passaggio nelle trasmissioni dati tra l'area sicura e l'area di processo. Per fare questo si dichiarano le variabili di interfaccia sia nell'area sicura che nell'area di processo, quindi si collegano queste variabili di interfaccia alle variabili di mappatura dichiarate nell'area globale.

Questa separazione dei dati nella CPU di sicurezza e nel coprocessore M580 è descritta graficamente di seguito:



Proprietà delle aree sicura, di processo e globale

Le tre aree dati di un progetto di sicurezza M580 presentano le proprietà seguenti:

Area	Tipi di variabili supportati	Ambito	Accesso esterno
Globale	Solo variabili non identificate. **NOTA:** Le variabili identificate non possono essere usate per la mappatura in una variabile di interfaccia sicura o di processo.	Può accedere a: • variabili di sicurezza, tramite indirizzamento dello spazio dei nomi, • variabili di processo, tramite indirizzamento dello spazio dei nomi, • altre variabili globali.	Alle variabili di queste tre aree possono accedere le applicazioni HMI, SCADA o FactoryCast. (Vedere la nota sotto).
Sicura	Solo variabili non identificate.	Può accedere solo ad altre variabili di sicurezza.	
Di processo	Entrambe: • Variabili identificate • Variabili non identificate	Può accedere solo ad altre variabili di processo.	

Quando un visualizzatore esterno cerca di leggere una variabile di processo, il formato di indirizzamento dipende dal fatto che sia selezionata o meno l'impostazione **Uso dello spazio dei nomi di processo** nell'area **Ambito > comune** della finestra **Strumenti > Impostazioni progetto...**. Se l'impostazione **Uso dello spazio dei nomi di processo** è

- Selezionata: la schermata operatore può leggere le variaibli dell'area di processo solo tramite il formato "PROCESS.<nome variabile>".
- Deselezionata: la schermata operatore può leggere le variabili dell'area di processo solo mediante il formato "<nome variabile>" senza il prefisso PROCESS. In questo caso, verificare che il nome di ogni variabile di processo sia univoco e che non coincida con il nome di una variabile globale.

  NOTA: Se l'impostazione **Uso dello spazio dei nomi di processo** è deselezionata, verificare che il nome di ogni variabile di processo sia univoco e che non coincida con il nome di una variabile globale. Se un nome di variabile è comune alle aree globale e di processo, Control Expert rileverà un errore quando si compila il progetto.

Come trasferire i dati tra le aree dello spazio dei nomi

Introduzione

Il PAC M580 Safety include tre diversi editor di dati:

- un **Editor dati di sicurezza** per gestire i dati utilizzati nello spazio dei nomi sicuro.
- un **Editor dati di processo** per gestire i dati utilizzati nello spazio dei nomi di processo.
- un **Editor dati globali** per gestire le variabili globali e i tipi di dati utilizzati nell'applicazione.

Entrambi gli **Editor dati di sicurezza** ed **Editor dati di processo** includono una scheda **Interfaccia**. Utilizzare la scheda **Interfaccia** per creare variabili non identificate nello spazio dei nomi di processo specifico. La scheda **Interfaccia** presenta due gruppi di variabili non identificate:

- <ingressi>: una variabile creata in questo gruppo può essere collegata a una variabile pass-through valida a livello globale e ricevere dati da essa nell'**Editor dati globali**.
- <uscite>: una variabile di questo gruppo può essere collegata a una variabile pass-through valida a livello globale e inviarvi dati nell'**Editor dati globali**.

  NOTA: Una variabile creata nella scheda **Interfaccia** deve essere una delle seguenti:

  - Deve essere una variabile di categoria EDT o DDT.
  - Deve essere una variabile dello stesso tipo della variabile alla quale è collegata.
  - Non deve essere una variabile collegata a un bit estratto di una variabile identificata (ad esempio, non %MW10.1).

Le variabili non identificate create nei gruppi di schede **Interfaccia** dell'**Editor dati di sicurezza** ed **Editor dati di processo** possono essere collegate come segue:

Una variabile di processo di questo gruppo dell'Editor dati di processo...	**può essere collegata a una variabile di sicurezza di questo gruppo dell'Editor dati di sicurezza...**
<ingressi>	<uscite>
<uscite>	<ingressi>

Mediante questi tre editor dati, è possibile configurare il trasferimento di dati tra lo spazio dei nomi sicuro e lo spazio dei nomi di processo.

Trasferimento dei dati tra gli spazi dei nomi

Il processo per il passaggio dei dati dallo spazio dei nomi sicuro a quello di processo e dallo spazio dei nomi di processo a quello sicuro è l'immagine mirror di ciascuno. L'esempio seguente mostra come passare i dati dal processo all'area sicura:

Passo	Azione
1	Aprire l'**Editor dati di processo**, fare clic sulla scheda **Interfaccia** di programma, quindi creare una nuova variabile nella parte **<uscite>** dell'editor dati.
2	Aprire l'**Editor dati di sicurezza**, fare clic sulla scheda **Interfaccia** di programma, quindi creare una nuova variabile con lo stesso tipo di quella creata al passo 1 nella parte **<ingressi>** dell'editor dati. Quindi, fare doppio clic sul campo **Parametro effettivo**. Si apre **Editor ambito dati: Selezione delle variabili**.
3	Nel menu a discesa in alto a destra nella finestra di dialogo, selezionare lo spazio dei nomi di destinazione **PROCESS**. Vengono visualizzate le variabili nello spazio dei nomi di PROCESSO selezionato nella parte <uscite>.
4	Selezionare la variabile di processo creata al passo 1 da collegare alla variabile SAFE creata al passo 2, quindi selezionare **OK**. La variabile di destinazione selezionata compare nel campo **Parametro effettivo**.
5	**Salvare** le modifiche.

Dopo avere compilato, scaricato ed eseguito il programma applicativo modificato, il valore viene trasferito nel seguente modo:

- I dati provenienti dalla scheda **Interfaccia** creati nelle **<uscite>** vengono pubblicati alla fine dell'esecuzione del task corrispondente.
- I dati provenienti dalla scheda **Interfaccia** creata negli **<ingressi>** sono sottoscritti all'inizio dell'esecuzione del task corrispondente.

Comunicazioni del sistema di sicurezza M580

Introduzione

Questo capitolo descrive le comunicazioni interne al sistema di sicurezza M580.

Sincronizzazione dell'ora

Introduzione

Per PAC con firmware della CPU 3.10 o precedente:	La configurazione del servizio NTP è richiesta per consentire una comunicazione sicura. Mittenti e riceventi devono essere sincronizzati con l'ora mediante i servizi NTP.
Per PAC con firmware della CPU 3.20 o successivo:	La sincronizzazione dell'ora sicura si basa su orologio interno e "monotonico". La comunicazione sicura non richiede la sincronizzazione dell'ora NTP: • Il controller di sicurezza condivide l'ora sicura con tutti gli I/O locali e remoti. • Il modulo di comunicazione di testa di IO remoto BM•CRA31210 richiede un firmware 2.60 o successivo. • Per la comunicazione peer-to-peer, i controller condividono l'ora sicura.

Configurazione della sincronizzazione dell'ora con il firmware del controller 3.10 o precedente

Introduzione

Se si installano moduli di I/O di sicurezza in una derivazione RIO, configurare l'ora per il controller, utilizzando tre configurazioni con firmware del controller 3.10 o precedente:

1. **Progettazione del server NTP remoto con il controller come client NTP**: configurare un dispositivo sulla rete di controllo come server NTP, quindi configurare il controller di sicurezza come client NTP.
2. **Progettazione del server NTP locale**: configurare il controller di sicurezza come server NTP per i dispositivi sulla rete RIO Ethernet.
3. **Progettazione del server NTP remoto con eNOC o eNOP**: nel rack locale principale, configurare un dispositivo nella rete di controllo come server NTP, quindi configurare un modulo (un modulo BMENOP0300, un modulo BMENOC0301 o un modulo BMENOC0311) e attivare la seguente funzionalità opzionale nel DTM corrispondente:

   Aggiornamento ora controller > Aggiorna ora del controller con questo modulo

   Se in una derivazione RIO sono installati dispositivi di sicurezza, configurare il controller di sicurezza come server NTP come descritto nel precedente caso 2.

In entrambe le configurazioni:

- Abilitare il servizio NTP.
- Impostare il periodo di interrogazione NTP a 20 s.

Se il controller di sicurezza non è configurato come server NTP o client NTP, l'impostazione dell'ora dei moduli di I/O di sicurezza remoti e del controller non sarà sincronizzata e la comunicazione del canale non funzionerà correttamente. Gli ingressi e le uscite dei moduli di I/O di sicurezza nelle derivazioni RIO entrano nello stato definito (non alimentato) o di posizionamento di sicurezza definito.

NOTA: se si installano moduli di I/O di sicurezza in una derivazione RIO, configurare l'ora per il controller con versione firmware 3.10 o precedente. Attivare il servizio NTP per il sistema M580 e configurare il controller di sicurezza come server NTP o client NTP.

Configurare due origini NTP, che possano funzionare in modo ridondante, una come server dell'ora primario e l'altra come server dell'ora di standby. Configurare entrambi i server per la sincronizzazione dell'ora. Una regolazione uguale o superiore a 2s in un periodo di interrogazione NTP provoca la desincronizzazione del controller e dei moduli di I/O di sicurezza e la deviazione dal server dell'ora NTP.

Modifica dell'impostazione dell'ora NTP durante il funzionamento

Se si utilizza Control Expert V13.0 o V13.1 o il firmware del controller 2.70 o precedente, la modifica dell'ora durante il funzionamento può causare una perdita di comunicazione e l'arresto del sistema di sicurezza.

AVVISO
APPARECCHIATURA NON FUNZIONANTE Non modificare l'impostazione dell'ora durante il funzionamento (quando si utilizza Control Expert V13.0 o V13.1 o il firmware del controller 2.70 o precedente). **Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.**

La modifica dell'ora durante il funzionamento può provocare una desincronizzazione con l'orologio di riferimento. Si potrebbe inoltre attivare un'interruzione della comunicazione di sicurezza provocando l'ingresso degli I/O nello stato definito o di posizionamento di sicurezza. Monitorare il sistema al fine di individuare un'eventuale desincronizzazione e nel caso si verifichi, ripristinare la sincronizzazione per evitare l'interruzione della comunicazione. Se si verifica tale desincronizzazione, utilizzare la procedura seguente, pagina 182 per risincronizzare il sistema.

Se si utilizza Control Expert V14.0 o successiva e il firmware del controller 2.80, 2.90 o 3.10: è possibile modificare l'impostazione dell'ora nel server NTP o nel controller durante il funzionamento senza impatti negativi. Eseguire questa operazione seguendo la procedura riportata di seguito subito dopo una modifica dell'ora.

Vedere la sezione *Scheda NTP* in *Modicon M580 - Manuale di riferimento hardware* per informazioni su come configurare il servizio NTP per un controller M580.

Procedura per sincronizzare le impostazioni dell'ora NTP

Quando si spegne e riaccende oppure ripristina il controller, quest'ultimo riceve inizialmente un'impostazione dell'ora da un server NTP esterno, utilizzare la procedura seguente per sincronizzare l'ora del controller.

AVVISO

APPARECCHIATURA NON FUNZIONANTE

Sincronizzare l'ora sicura con il server NTP esterno utilizzando %SW128 dal momento in cui il server NTP esterno diventa operativo (quando %SW152 passa da 0 a 1) mentre si utilizza la funzionalità **Aggiorna ora CPU con questo modulo** opzionale in un modulo BMENOP0300, un modulo BMENOC0301 o un modulo BMENOC0311 per aggiornare l'ora del controller.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

La procedura seguente è valida con il task SAFE in stato RUN, con Control Expert V14.0 o versioni successive e firmware del controller 2.80, 2.90 o 3.10:

Passo	Azione
1	Verificare che l'ora del controller o del server NTP esterno sia valida, corretta e stabile.
2	Se la configurazione comprende una o più derivazioni RIO, attendere due periodi di interrogazione NTP per consentire l'invio del nuovo valore dell'ora di riferimento a tutti i moduli CRA. Eseguire questa operazione dopo che il servizio NTP è di nuovo operativo o dopo la modifica dell'ora (che ha portato alla desincronizzazione).
3	Sincronizzare l'ora di sistema in base all'orologio di riferimento tramite la parola di sistema %SW128: • impostare %SW128 a 16#1AE5 per almeno 500 ms, • Impostare %SW128 a #E51A per almeno 500 ms.
4	Verificare che l'ora sia sincronizzata verificando che i valori del parametro per CPU_NTP_SYNC e M_NTP_SYNC nel DDDT IO di sicurezza siano veri (1).

Ripetere questa sequenza di sincronizzazione nel caso in cui non venga eseguita correttamente.

AVVISO

APPARECCHIATURA NON FUNZIONANTE

Eseguire una procedura di sincronizzazione per evitare che gli I/O di sicurezza entrino nello stato sicuro definito o di posizionamento di sicurezza dopo la deviazione dell'orologio per circa un timeout di ritardo di comunicazione.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Se si utilizza Control Expert V14.0 o versioni successive e firmware del controller 2.80 o versioni successive per eseguire una modifica dell'ora del controller, far seguire alla modifica la procedura di sincronizzazione descritta in precedenza.

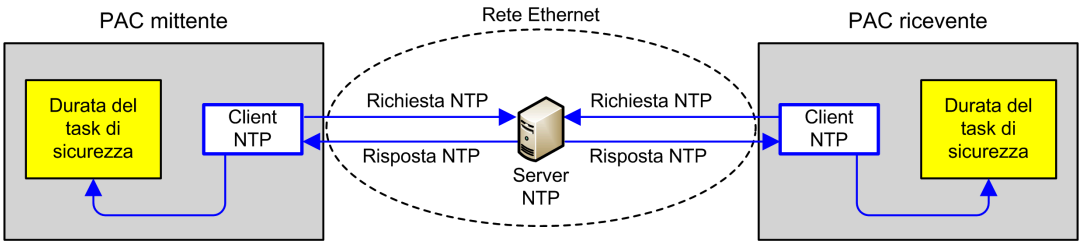
Durante il passo 3 nella procedura di sincronizzazione dell'ora, alcune diagnostiche della comunicazione di sicurezza sono disattivate per una durata di 500 ms. Eseguire un massimo di una modifica e sincronizzazione dell'ora al giorno.

Servizio NTP per comunicazione peer-to-peer

La comunicazione Ethernet controller - controller di sicurezza richiede la sincronizzazione della base tempo dei controller mittente e ricevente.

NOTA: Configurare in ogni controller (il controller di sicurezza, un modulo BMENOP0300, un modulo BMENOC0301 o un modulo BMENOC011) un client NTP e configurare un altro dispositivo di rete come server NTP.

La figura seguente descrive il principio di sincronizzazione della base tempo del controller mittente e ricevente:



In Control Expert, configurare i parametri del servizio NTP per ogni client nel seguente modo:

- Selezionare **Client NTP**.
- Impostare l'**Indirizzo IP del server NTP primario** con l'indirizzo IP del server NTP remoto.
- Impostare il valore **Periodo di interrogazione** a 20 secondi.

Coerenza temporale e bit di sistema del server NTP

Coerenza temporale del server NTP:

- Se l'ora del server NTP corrisponde all'ora del controller interno visualizzata dall'EF `S_SYST_CLOCK` con meno di 2 secondi di differenza, il valore temporale nell'EF `S_SYST_CLOCK` si aggiorna con l'ultima ora del server NTP ricevuta, filtrata con una pendenza di 1ms/s.

- Se l'ora del server NTP ricevuta differisce dall'ora del controller interno visualizzata dall'EF `S_SYST_CLOCK` di oltre 2 secondi:
  - Il controller ignora l'ultima ora del server NTP ricevuta.
  - Il valore di tempo visualizzato dall'EF `S_SYST_CLOCK` viene aggiornato internamente.
  - Il parametro di stato `S_SYST_CLOCK` è impostato a 0.
  - Il parametro di uscita `SYNCHRO_NTP` da `S_RD_ETH_MX` e il DFB `S_WR_ETH_MX` è impostato a 0 per indicare questa condizione.

  In questo caso, ripristinare l'ora interna del controller eseguendo una di queste azioni:
  - Reinizializzare l'applicazione con un avvio a freddo.
  - Scaricare l'applicazione.
  - Riavviare il controller.
  - Seguire le procedura per la modifica delle impostazioni dell'ora NTP, pagina 182.

    NOTA: Se si perde la sincronizzazione NTP su uno dei due controller (parametro `SYNCHRO_NTP` impostato a 0), la base tempo del controller mittente e quella del controller ricevente può essere desincronizzata. In questo caso, la comunicazione peer-to-peer di sicurezza può cessare di essere operativa (il parametro di uscita `health` del DFB `S_RD_ETH_MX` è impostato a 0).

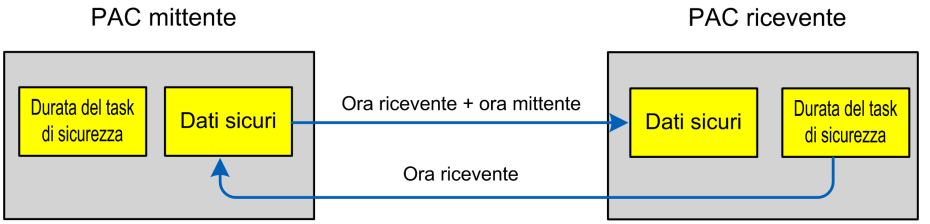
Sincronizzazione dell'ora per firmware della CPU 3.20 o successivo

Sincronizzazione dell'ora per comunicazione peer-to-peer

NOTA: Con firmware del controller 3.20 o successivo, il servizio NTP non viene utilizzato per la sincronizzazione dell'ora.

La comunicazione Ethernet controller-controller di sicurezza richiede che i controller mittente e ricevente condividano un'ora sicura comune.

La figura seguente descrive il principio di condivisione dell'ora del controller mittente e ricevente:



In Control Expert, configurare:

- comunicazione per trasmissione dati da mittente a ricevente
- comunicazione per trasmissione del tempo di sicurezza da ricevitore a mittente

Coerenza dell'ora

Un'ora interna di sicurezza (indipendente da NTP) viene distribuita dal controller ai relativi moduli di I/O di sicurezza locali e remoti.

Comunicazione peer-to-peer

Introduzione

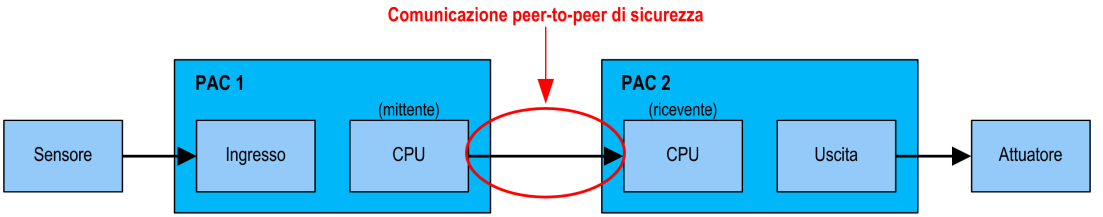
Questa sezione descrive la comunicazione peer-to-peer tra controller di sicurezza M580.

Comunicazione peer-to-peer

Introduzione

È possibile configurare due controller M580 Safety per eseguire comunicazioni di sicurezza peer-to-peer su Ethernet. La configurazione è basata sulla comunicazione dello scanner Modbus TCP, integrato in un canale.

Schema funzionale della comunicazione peer-to-peer sicura:



La comunicazione viene eseguita da due blocchi funzione elementari della libreria dei blocchi di sicurezza M580, che gestisce il loop di sicurezza a un livello SIL3. Il protocollo rileva gli errori di trasmissione, tra cui omissioni, inserimenti, sequenza non ordinata, ritardi, indirizzamento impreciso e bit mascherati, quindi gestisce le ritrasmissioni.

Questa comunicazione peer-to-peer sicura è possibile solo tra:

- due controller M580 Safety con firmware 3.10 o precedente
- due controller M580 Safety con firmware 3.20 o successiva

NOTA: la comunicazione peer-to-peer sicura è inoltre possibile tra un controller di sicurezza Modicon Quantum e un controller M580 Safety con firmware 3.10 o precedente.

NOTA: con firmware del controller successivo alla versione 4.20, la comunicazione peer-to-peer sicura non è possibile se la **Modalità Engineering Link** è impostata su **Rinforzato** sul controller ricevente.

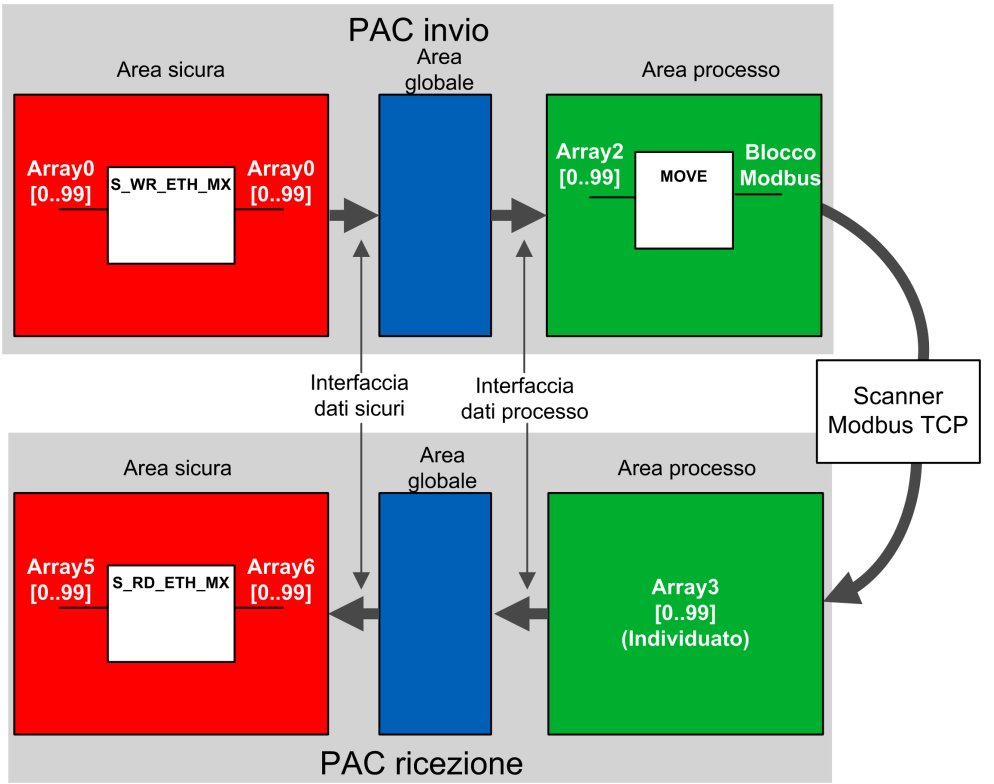
Architettura peer-to-peer con firmware della CPU 3.10 o precedente

Progettazione dell'architettura

Con firmware della CPU 3.10 o precedente, l'architettura della soluzione è basata su:

- Servizio NTP per la sincronizzazione della base tempo.
- Esecuzione di 2 DFB (`S_WR_ETH_MX` e `MOVE` nel PAC mittente e 1 DFB (`S_RD_ETH_MX`) nel PAC ricevente).
- Scanning tramite Modbus TCP per il trasferimento dei dati.

La seguente figura mostra una panoramica del processo richiesto per eseguire la comunicazione peer-to-peer:

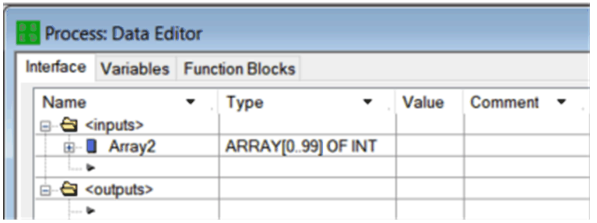
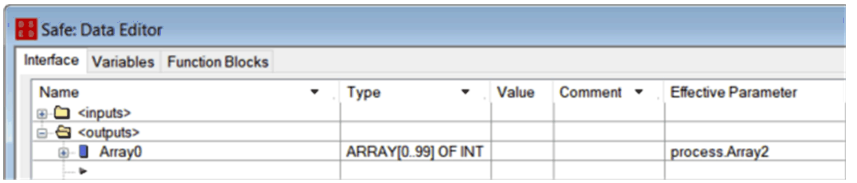


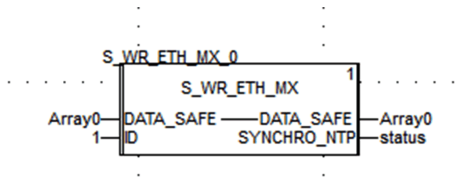
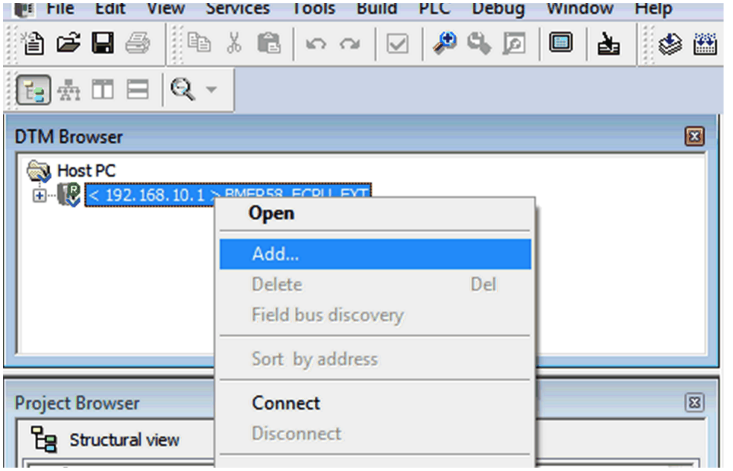
Nella figura precedente, Control Expert crea automaticamente, e nasconde dalla vista esterna, l'Array 1 e l'Array 4 nelle aree Globali dei PAC peer. Da un punto di vista utente, i collegamenti sono effettuati da Array 0 ad Array 2 e da Array 3 ad Array 5.

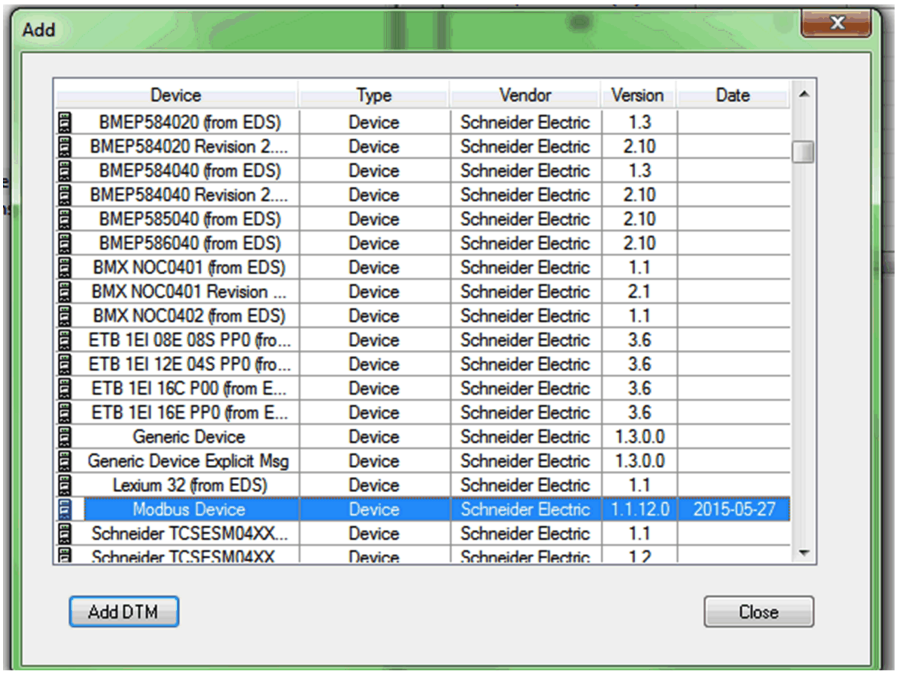
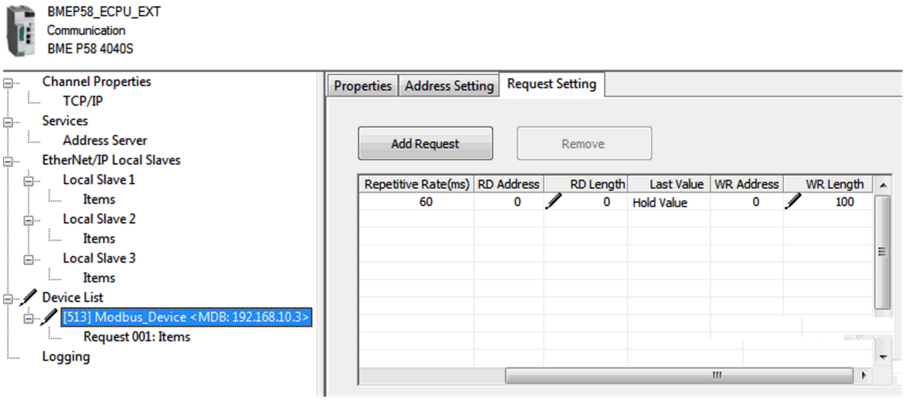
NOTA: Sulla rete Ethernet, si possono mischiare dati di sicurezza e dati non di sicurezza senza alcun impatto sul livello di integrità dei dati di sicurezza. Non vi sono restrizioni sulla rete Ethernet quando si utilizza la comunicazione peer-to-peer sicura.

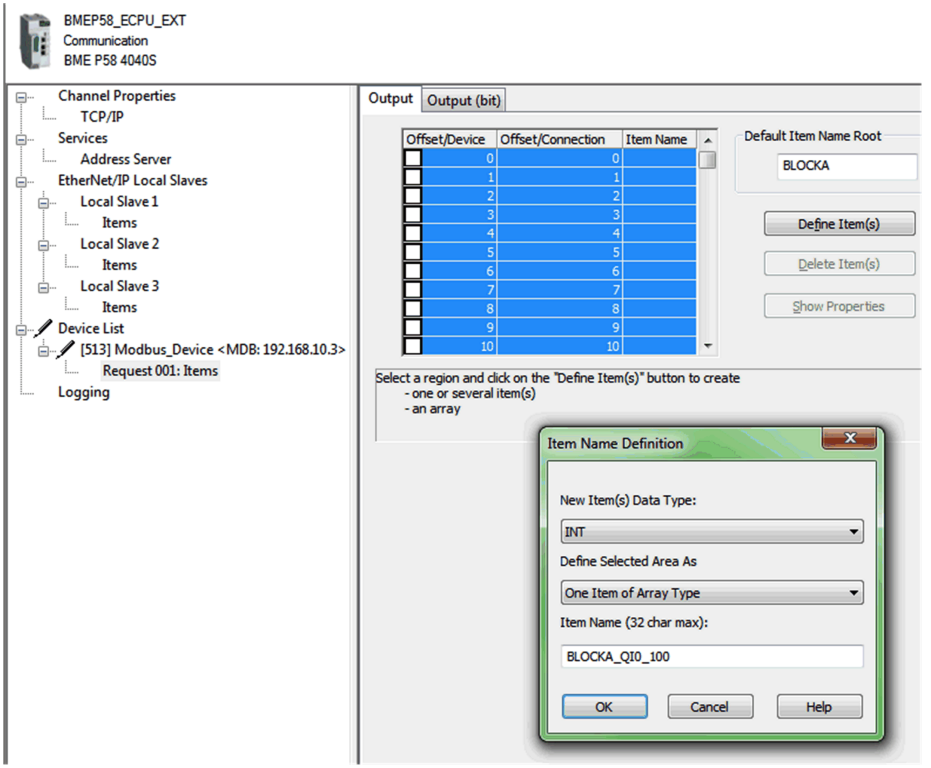
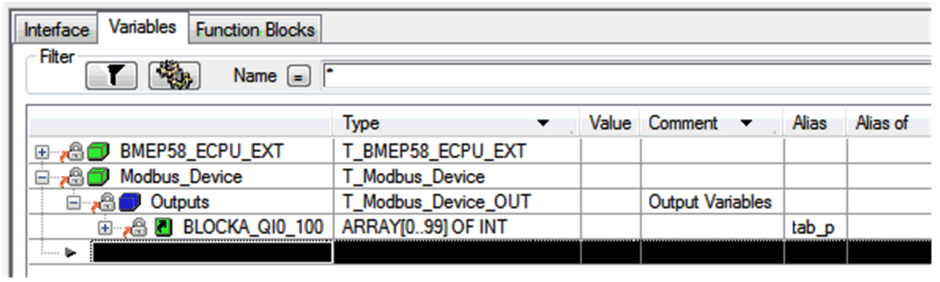
Dettagli della configurazione del trasferimento dati Peer-to-Peer

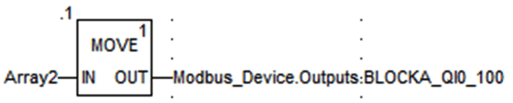
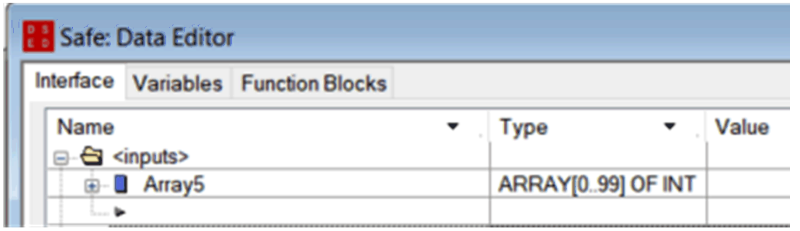
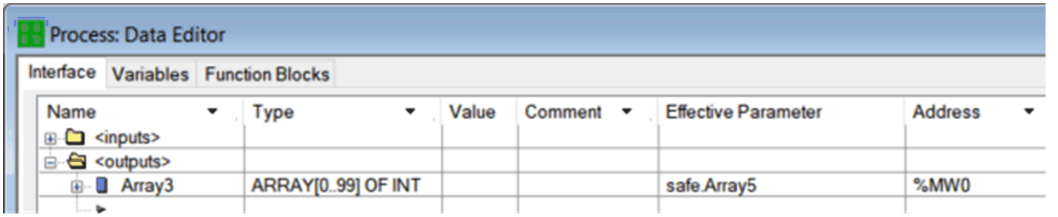
L'esempio che segue mostra come configurare un trasferimento di dati peer-to-peer tra due PAC di sicurezza con firmware della CPU 3.10 o precedente e Control Expert 14.1 o precedente:

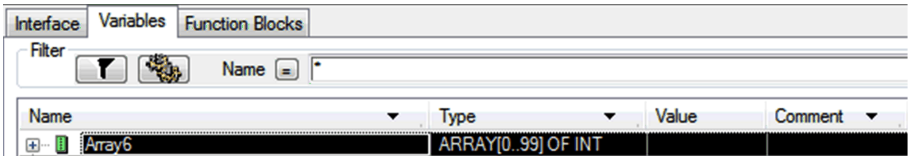
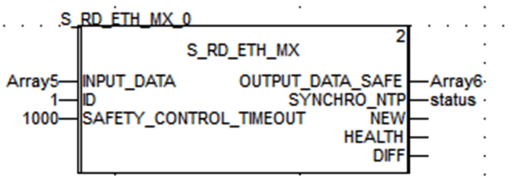
Passo	Azione
1	Sul PAC mittente, utilizzare l'**Editor dati di processo** per creare un array di 100 interi come ingresso nell'area **Interfaccia**. In questo esempio, il nome dell'array è Array2: 
2	Sul PAC mittente, creare un altro array di 100 interi come uscita nella scheda **Interfaccia** dell'**Editor dati di sicurezza** e collegarlo all'array dell'area di processo di ingresso creato al passo 1, sopra, nella colonna **Parametro effettivo**. In questo esempio, il nome dell'array è Array0:  **NOTA:** Le variabili di interi dall'indice 0 a 90 dell'array contengono i valori delle variabili di sicurezza da scambiare con il PAC ricevente. L'area rimanente è riservata per i dati di diagnostica autogenerati, incluso un CRC e un time stamp. Questi dati di diagnostica vengono utilizzati dal PAC ricevente per determinare se i dati trasferiti sono sicuri.

Passo	Azione
3	Sul PAC mittente, configurare il DFB `S_WR_ETH_MX` in una sezione dei task SAFE. Collegare il DFB ad Array0: 
4	Nel **Browser DTM** nel PAC mittente, selezionare la CPU (in questo esempio) o a un modulo di comunicazione NOC (se presente), quindi fare clic su **Aggiungi...** per creare uno scanner Modbus che può inviare i dati tramite Modbus TCP dal PAC mittente al PAC ricevente: 

Passo	Azione
5	Selezionare **Dispositivo Modbus** e fare clic **Aggiungi DTM** per aggiungere lo scanner Modbus: 
6	Aprire il dispositivo Modbus appena aggiunto, aggiungere una richiesta e nella scheda **Impostazione richiesta**: • Impostare la colonna **Lunghezza WR**, ossia la lunghezza dei dati da scrivere, al valore 100, quindi • Impostare la colonna **Indirizzo WR**, che è l'indirizzo in cui la tabella del PAC ricevente scriverà i dati che riceve (in questo esempio: 0, ossia il PAC mittente scriverà nella tabella a partire da %MW0 nel PAC ricevente). 

Passo	Azione
7	Selezionare il nodo **Request 001: Items**, quindi nella scheda **Uscita** definire un tipo di array di INT (ossia ≥100 interi). Questa è la tabella del PAC mittente che verrà scritta nel PAC ricevente: 
8	Dopo aver salvato e compilato la configurazione, il blocco (BLOCKA_QI0_100 in questo esempio) viene creato automaticamente come variabile di processo: 

Passo	Azione
9	Sul PAC mittente, in una sezione del codice di processo, usare un DFB `MOVE` per copiare il contenuto di Array2 nell'array definito sopra nella struttura del dispositivo Modbus: 
10	Sul PAC ricevente, utilizzare l'**Editor dati di sicurezza** per creare un array di 100 interi (Array5) come ingresso nell'area **Interfaccia**: 
11	Sul PAC ricevente, nell'**Editor dati di processo**, creare un array (Array3) di 100 INT nella sezione <uscite> della scheda **Interfaccia**. Collegare questo array all'array dell'area dati (Array5, creato al passo 10) nella colonna **Parametro effettivo**. I dati inviati dal PAC mittente verranno scritti in questo array tramite lo scanner Modbus, a condizione che questa variabile sia localizzata all'indirizzo definito nello scanner del PAC mittente (in questo esempio %MW0): 

Passo	Azione
12	Sul PAC ricevente, utilizzare l'**Editor dati di sicurezza** per creare un array di 100 interi (Array6): 
13	Nel PAC ricevente, in una sezione di codice nel task SAFE, creare un'istanza del DFB `S_RD_ETH_MX` con l'array creato al passo 10 (Array5) quale parametro di ingresso e con l'array creato al passo 12 (Array6) quale parametro di uscita: 

Black channel peer-to-peer

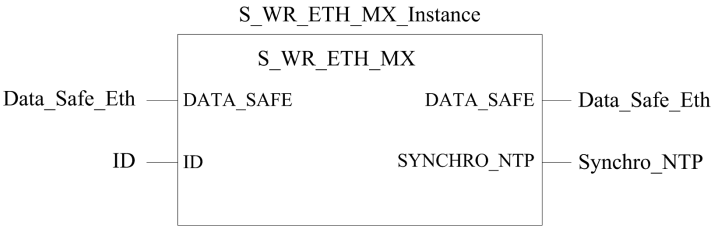
Ogni trasmissione dati peer-to-peer è costituita da *Dati di sicurezza utente*, che trasmettono il contenuto legato all'applicazione, e *Dati riservati*. I *Dati riservati* servono al PAC di sicurezza per testare l'affidabilità della trasmissione, che deve soddisfare i requisiti SIL3. I *Dati riservati* sono formati dai seguenti elementi:

- Un CRC calcolato dal PAC mittente a partire dai dati che devono essere trasmessi. Il PAC ricevente verifica il CRC prima di usare i dati trasmessi.
- Un identificativo di comunicazione, che è incluso nel calcolo del CRC per evitare bit mascherati e cyberattacchi sulla trasmissione dei dati di sicurezza.
- Un'indicazione oraria contenente la durata della trasmissione in ms. Questa indicazione oraria è basata sul valore orario fornito dal servizio NTP e permette di sincronizzare sia il PAC mittente che il PAC ricevente. Il PAC mittente aggiunge un valore temporale ai dati inviati al PAC ricevente. Il PAC ricevente confronta l'indicazione oraria con il proprio valore orario e la usa per:
  - Verificare l'età dei dati.
  - Rifiutare trasmissioni doppie.
  - determinare l'ordine cronologico delle trasmissioni ricevute
  - determinare il tempo trascorso tra la le notifiche di ricezione delle trasmissioni dati.

Configurazione del DFB S_WR_ETH_MX nella logica di programma del controller mittente

Rappresentazione

Rappresentazione DFB:



Per una descrizione estesa di questo DFB, consultare *EcoStruxure™ Control Expert, Safety, Block Library*.

Descrizione

Il DFB S_WR_ETH_MX è per i controller che utilizzano il firmware 3.10 o precedente. Calcola i dati (dati riservati contenenti un CRC e un timestamp) richiesti dal controller ricevente per verificare e gestire gli errori rilevati durante la comunicazione peer-to-peer di sicurezza.

Chiama il blocco funzione DFB S_WR_ETH_MX a ogni ciclo nel controller mittente. Nell'ambito del ciclo, viene eseguito nella logica dopo che sono state eseguite tutte le modifiche richieste sui dati da inviare. Questo significa che i dati da inviare non possono essere modificati nel ciclo dopo l'esecuzione del DFB; altrimenti, le informazioni CRC utilizzate nell'area dati riservati non saranno corrette e la comunicazione peer-to-peer di sicurezza non può avere luogo.

Assegnare al parametro ID un valore univoco che identifica la comunicazione peer-to-peer di sicurezza tra un controller mittente e un controller ricevente.

⚠AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

Il valore del parametro ID deve essere univoco e fisso nella rete per una coppia di controller mittente/ricevente.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Descrizione dell'array DATA_SAFE

Utilizzare le schede **Interfaccia** nell'**Editor dati di sicurezza** ed **Editor dati di processo** in Control Expert per collegare le variabili di processo e le variabili di sicurezza.

Il processo di collegamento e le variabili di sicurezza possono:

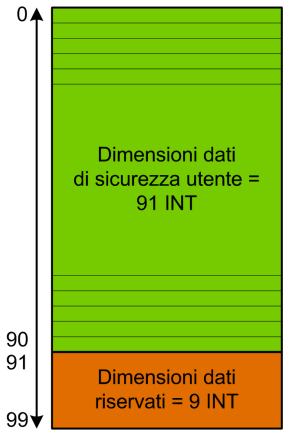
- Trasferire il valore delle variabili di sicurezza alle variabili di processo tramite variabili globali collegate.
- Inviare valori variabili dall'area processo del controller mittente all'area processo del controller ricevente tramite messaggistica esplicita su Modbus TCP.

L'array DATA_SAFE è composto da due aree:

- L'area **Dati sicurezza utente** contiene i dati provenienti dall'area sicura del controller. Quest'area inizia all'indice 0 e finisce all'indice 90.
- L'area **Dati riservati** è riservata per i dati diagnostici generati automaticamente, compresi un CRC e timestamp. Questi dati vengono utilizzati dal controller ricevente per determinare se i dati contenuti nell'area **Dati sicurezza utente** sono sicuri o no. Quest'area inizia all'indice 91 e finisce all'indice 99.

  NOTA: non scrivere nell'area **Dati riservati**. La scrittura in quest'area sovrascrive i dati diagnostici generati automaticamente.

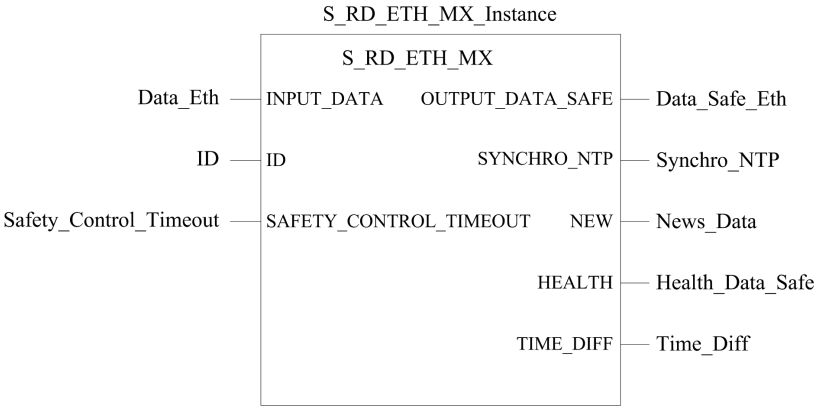
La rappresentazione della struttura dell'array DATA_SAFE (array[0..99] of INT):



Configurazione del DFB S_RD_ETH_MX nella logica di programma del controller ricevente

Rappresentazione

Rappresentazione DFB:



Vedere *EcoStruxure™ Control Expert, Safety, Block Library* per una descrizione estesa di questo DFB.

Descrizione

Il DFB S_RD_ETH_MX è per i controller che utilizzano il firmware 3.10 o precedente. Copia i dati ricevuti nell'area di processo nell'area di sicurezza e convalida l'accuratezza dei dati ricevuti.

⚠AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

- Chiama il blocco funzione DFB S_RD_ETH_MX a ogni ciclo nella logica di programma del controller ricevente prima che vengano utilizzati i dati del ciclo.
- Il valore del parametro ID deve essere univoco e fisso nella rete per una coppia mittente/ricevente.
- Testare il valore del bit HEALTH del DFB S_RD_ETH_MX a ogni ciclo prima di utilizzare dati sicuri per gestire la funzione di sicurezza.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Il blocco funzione S_RD_ETH_MX:

- Copia i dati ricevuti nel registro INPUT_DATA sul registro OUTPUT_DATA_SAFE se supera i seguenti test:
  - Il blocco funzione verifica il CRC dell'ultimo pacchetto dati ricevuto tramite scanner degli I/O su Ethernet (Modbus TCP). Se il CRC non è corretto, i dati sono considerati non sicuri e non vengono scritti nel registro OUTPUT_DATA_SAFE nell'area di sicurezza.
  - Il blocco funzione verifica gli ultimi dati ricevuti per determinare se sono più recenti dei dati già scritti nel registro OUTPUT_DATA_SAFE nell'area di sicurezza (confrontando le indicazioni di data/ora). Se gli ultimi dati ricevuti non sono più recenti, non vengono copiati nel registro OUTPUT_DATA_SAFE nell'area di sicurezza.
- Verifica l'età dei dati nell'area di sicurezza. Se l'età è superiore a un valore massimo configurabile impostato nel registro di ingresso SAFETY_CONTROL_TIMEOUT, i dati sono dichiarati non sicuri e il bit HEALTH è impostato a 0.

  NOTA: l'età dei dati è data dalla differenza tra l'ora in cui i dati sono calcolati nel controller mittente e l'ora in cui i dati vengono verificati nel controller ricevente. Il riferimento in base tempo viene aggiornato periodicamente con l'ora ricevuta da un server NTP.

  Se il bit HEALTH è impostato a 0, i dati disponibili nell'array OUTPUT_DATA_SAFE sono considerati non sicuri. In questo caso, prendere le misure appropriate.

Descrizione degli array INPUT_DATA e OUTPUT_DATA_SAFE

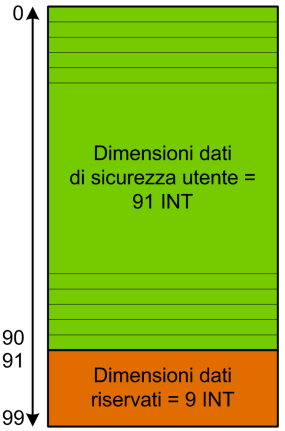
Gli array INPUT_DATA consistono di dati provenienti dall'area di memoria dei dati di processo. Gli array OUTPUT_DATA_SAFE consistono di variabili di sicurezza. Utilizzare le schede **Interfaccia dati di sicurezza** e **Interfaccia dati di processo** in Control Expert per creare il collegamento tra le variabili di processo e le variabili di sicurezza.

Gli array INPUT_DATA e OUTPUT_DATA_SAFE sono composti da due aree:

- L'area **Dati sicurezza utente** contiene i dati dell'utente. Quest'area inizia all'indice 0 e finisce all'indice 90.
- L'area **Dati riservati** è riservata per i dati diagnostici generati automaticamente, compresi un CRC e timestamp. Questi dati vengono utilizzati dal controller ricevente per determinare se i dati contenuti nell'area **Dati sicurezza utente** sono sicuri o no. Quest'area inizia all'indice 91 e finisce all'indice 99.

  NOTA: non scrivere nell'area **Dati riservati**. La scrittura in quest'area sovrascrive i dati diagnostici generati automaticamente.

La rappresentazione della struttura degli array `INPUT_DATA` e `OUTPUT_DATA_SAFE` (array [0..99] of INT):



Calcolo di un valore SAFETY_CONTROL_TIMEOUT

Quando si calcola un valore `SAFETY_CONTROL_TIMEOUT` considerare quanto segue:

- valore minimo: `SAFETY_CONTROL_TIMEOUT` > T1
- valore tipico: `SAFETY_CONTROL_TIMEOUT` > 2 * T1

T1 = tempo di ciclo MAST controller$_{mittente}$ + tempo di ciclo SAFE controller$_{mittente}$ + frequenza_ripetizione + tempo trasmissione di rete + tempo di ciclo MAST controller$_{ricevente}$ +tempo di ciclo SAFE controller$_{ricevente}$

dove:

- *Tempo di ciclo MAST controller$_{mittente}$* è il tempo di ciclo MAST del controller mittente
- *Tempo di ciclo SAFE controller$_{mittente}$* è il tempo di ciclo SAFE del controller mittente
- *Frequenza_ripetizione* è la frequenza di tempo della query di scrittura dello scanner degli I/O dal controller mittente al controller ricevente.
- *Tempo trasmissione di rete* è il tempo impiegato sulla rete Ethernet per la trasmissione dei dati dal controller mittente al controller ricevente.
- *Tempo di ciclo MAST controller$_{ricevente}$* è il tempo di ciclo MAST del controller ricevente
- *Tempo di ciclo SAFE controller$_{ricevente}$* è il tempo di ciclo SAFE del controller ricevente

Tenere presente che il valore definito per il parametro `SAFETY_CONTROL_TIMEOUT` ha un effetto diretto sulla robustezza e sulla disponibilità della comunicazione peer-to-peer sicura. Se il valore del parametro `SAFETY_CONTROL_TIMEOUT` supera T1, la comunicazione tollererà vari ritardi (ad esempio, ritardi di rete) o trasmissioni di dati danneggiate.

Configurare la rete Ethernet in modo che il carico non provochi un ritardo eccessivo sulla rete durante la trasmissione dei dati, che potrebbe provocare la scadenza del timeout. Per proteggere la comunicazione peer-to-peer di sicurezza da eccessivi ritardi dovuti ad altri dati non di sicurezza trasmessi sulla stessa rete, utilizzare una rete Ethernet dedicata per il protocollo peer-to-peer di sicurezza.

Quando si mette in servizio il progetto, valutare le prestazioni della comunicazione peer-to-peer di sicurezza verificando i valori forniti nel parametro di uscita `TIME_DIFF` e valutando il margine utilizzando il valore definito nel parametro `SAFETY_CONTROL_TIMEOUT`.

Note sul bit `HEALTH`

Quando il valore del bit `HEALTH` è uguale a:

- 1: l''integrità dei dati è corretta (CRC) e l'età dei dati è inferiore al valore impostato nel registro di ingresso `SAFTETY_CONTROL_TIMEOUT`.

  NOTA: L'età dei dati è il tempo tra:

  - l'inizio del ciclo dove i dati sono calcolati nel controller mittente
  - l'inizio del ciclo in cui i dati vengono controllati nel controller ricevente
- 0: i nuovi dati validi non vengono ricevuti nell'intervallo di tempo richiesto (il timer scade e il bit `HEALTH` è impostato a 0).

  NOTA: se il bit `HEALTH` è impostato a 0, i dati nell'array di uscita `OUTPUT_DATA_SAFE` sono considerati non sicuri; rispondere in modo adeguato.

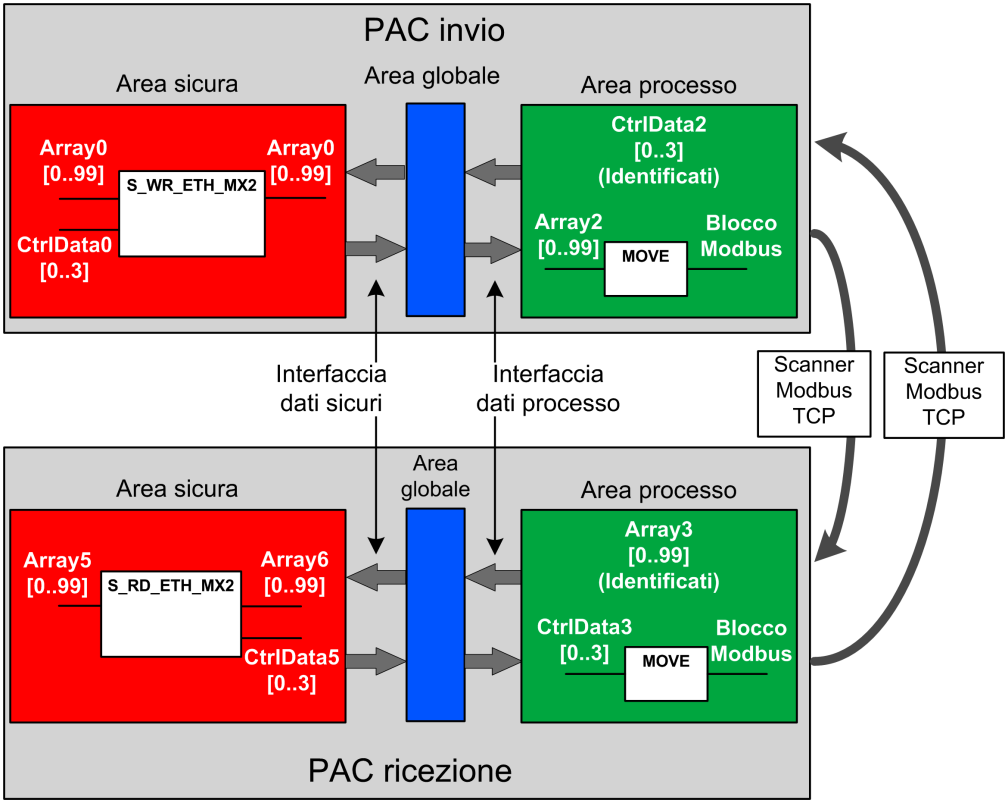
Architettura peer-to-peer con firmware della CPU 3.20 o successivo

Progettazione dell'architettura

Con firmware della CPU 3.20 o successivo, l'architettura della soluzione è basata su:

- Esecuzione di 2 DFB (`S_WR_ETH_MX2` e `MOVE` nel PAC mittente e 2 DFB (`S_RD_ETH_MX2` e `MOVE`) nel PAC ricevente.
- Scansione tramite Modbus TCP, per trasporto dati sicuro da mittente a ricevente.
- Scansione tramite Modbus TCP, per trasporto dati di controllo da ricevente a mittente.

La figura seguente mostra una panoramica del processo richiesto per eseguire la comunicazione sicura peer-to-peer:

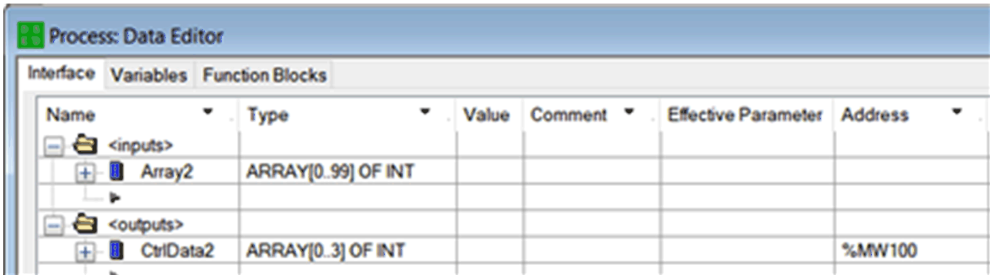
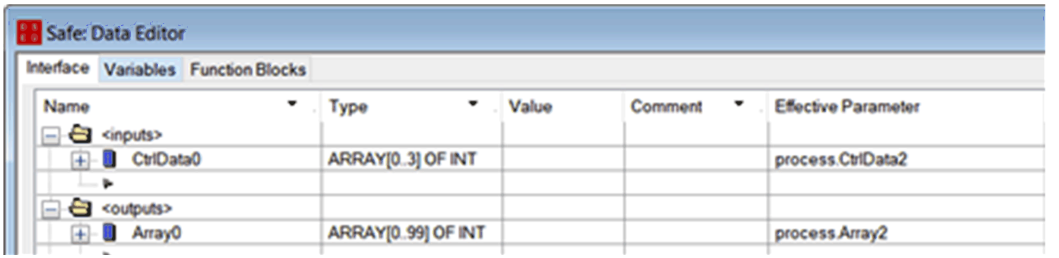
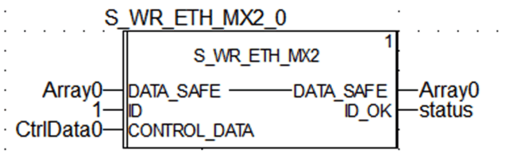


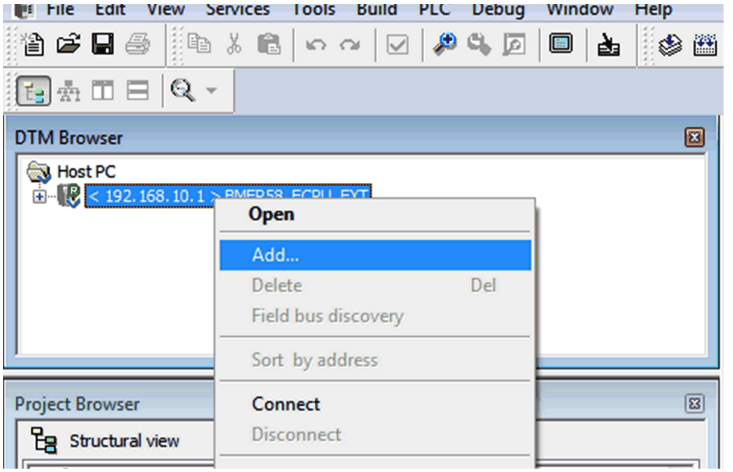
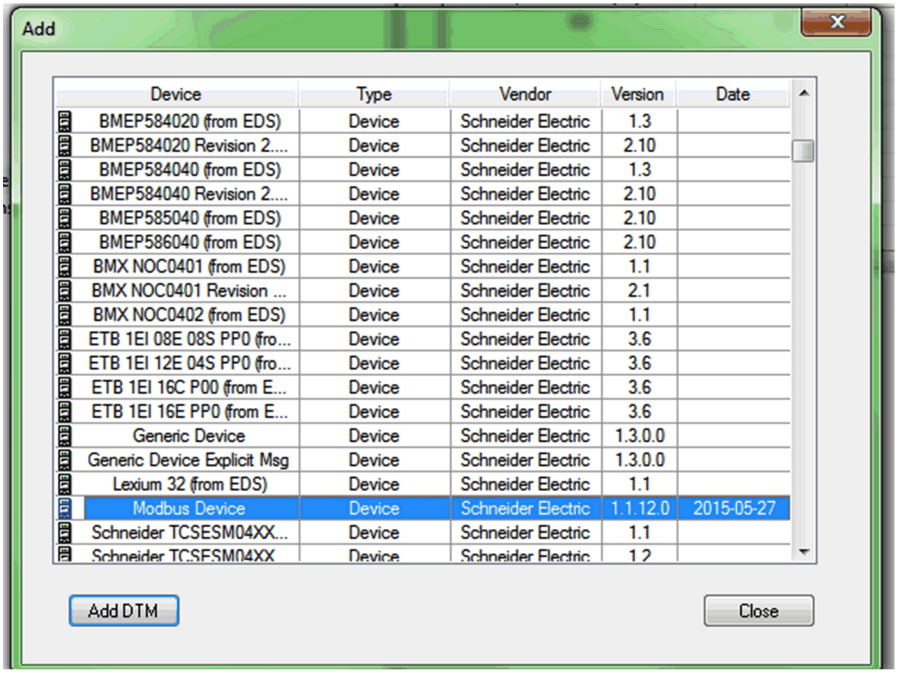
Nella figura precedente, Control Expert crea automaticamente, e nasconde dalla vista esterna, Array1 e Array4 nelle aree Globali dei PAC peer. Da un punto di vista utente, i collegamenti sono effettuati da Array0 ad Array2 e da Array3 ad Array5.

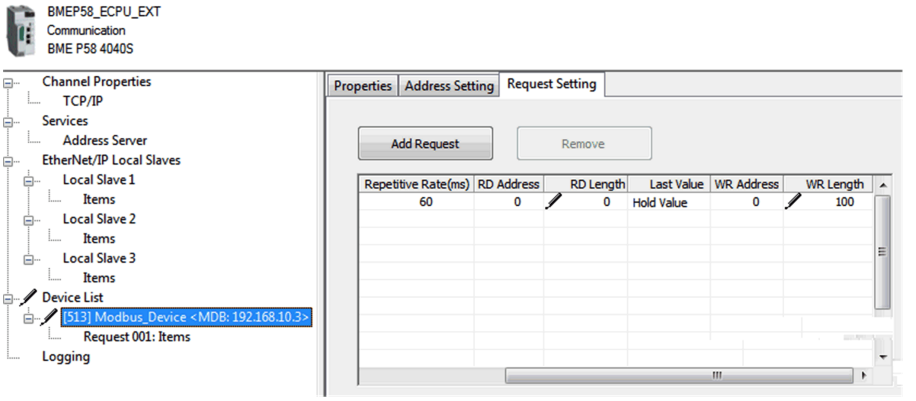
NOTA: Sulla rete Ethernet, si possono mischiare dati di sicurezza e dati non di sicurezza senza alcun impatto sul livello di integrità dei dati di sicurezza. Non vi sono restrizioni sulla rete Ethernet quando si utilizza la comunicazione peer-to-peer sicura.

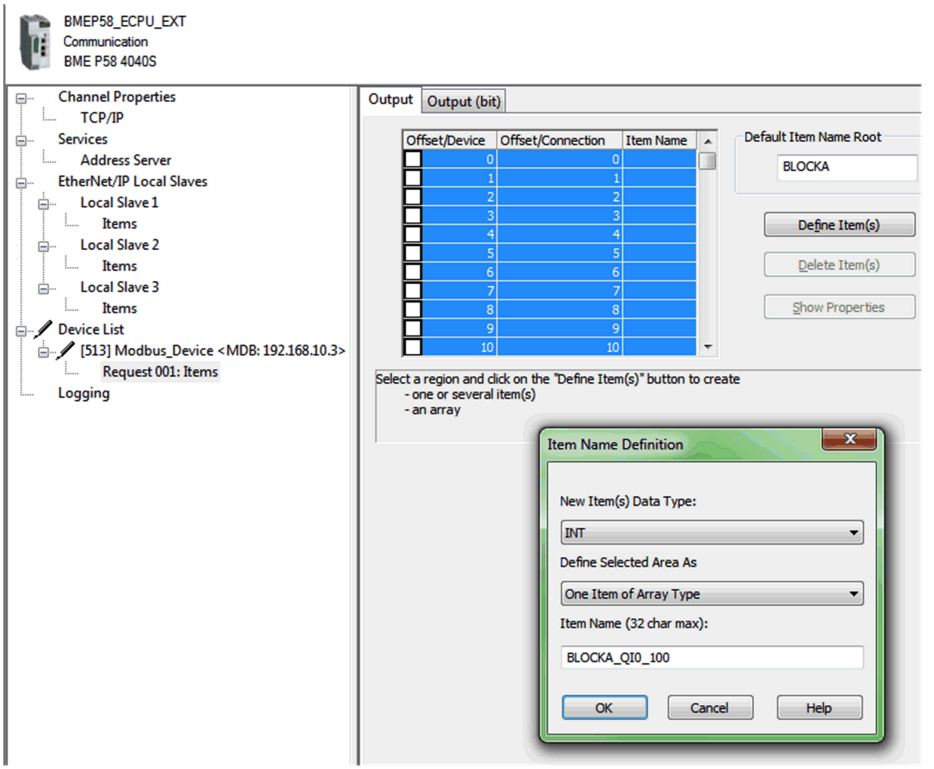
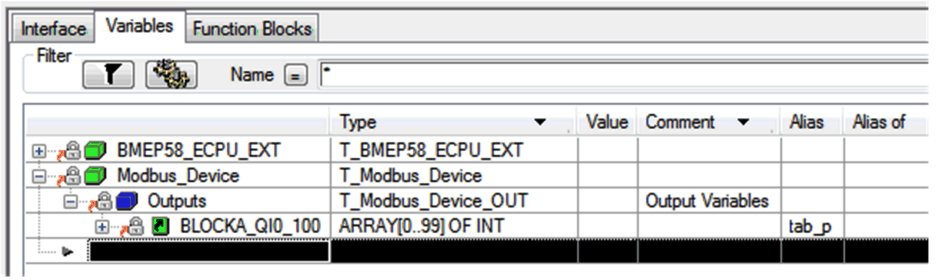
Dettagli della configurazione del trasferimento dati Peer-to-Peer

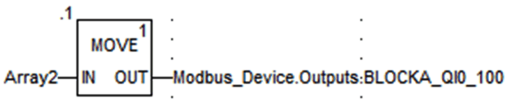
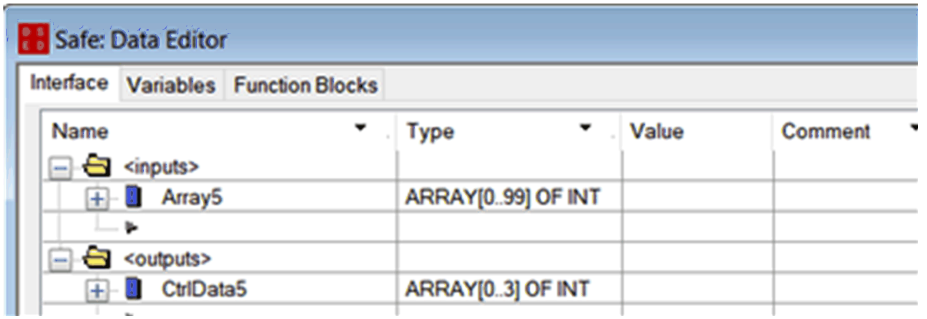
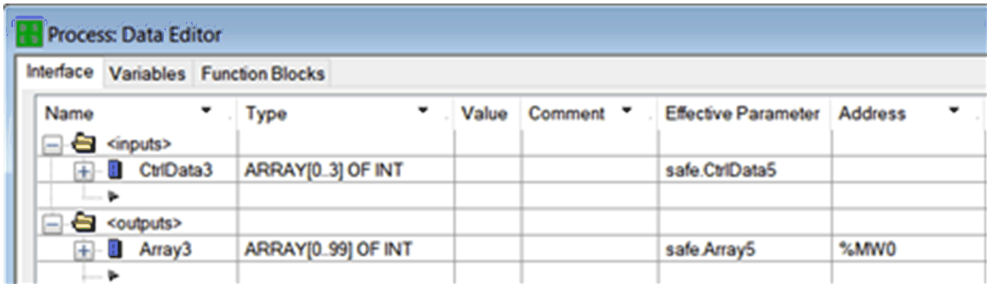
L'esempio che segue mostra come configurare un trasferimento di dati peer-to-peer tra due PAC di sicurezza con firmware della CPU 3.20 o successivo e Control Expert 15.0 o successivo:

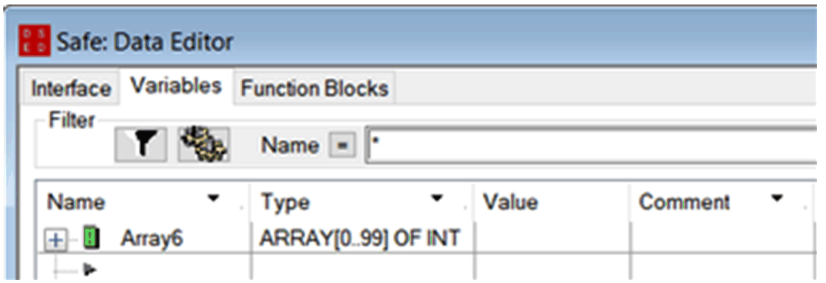
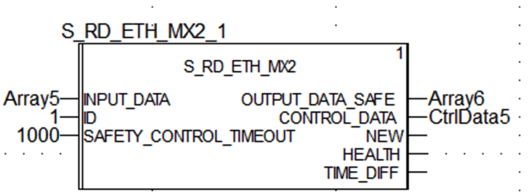
Passo	Azione
1	Sul PAC mittente, usare l'**Editor dati di processo** per creare un array di 100 interi (Array2) come ingresso nell'area Interfaccia: Creare nello stesso **Editor dati di processo** un array di 4 interi (CtrlData2) come uscita nell'area **Interfaccia**. I dati di controllo dal PAC ricevente verranno scritti in questo CtrlData2 tramite lo scanner Modbus, a condizione che CtrlData2 sia localizzato all'indirizzo definito nello scanner del PAC mittente (in questo esempio %MW100, vedere il passo 14): 
2	Sul PAC mittente, utilizzare l'**Editor dati di sicurezza** per creare un altro array di 100 interi (Array0) come uscita nell'area **Interfaccia** e collegarlo ai dati process.Array2 creati al passo 1 precedente, nella colonna **Parametro effettivo**. Creare nello stesso **Editor dati di sicurezza** un array di 4 interi (CtrlData0) come ingresso nell'area di sicurezza **Interfaccia** e collegarlo ai dati process.CtrlData2 creati al passo 1 precedente, nella colonna **Parametro effettivo**.  **NOTA:** Le variabili di interi degli indici 0 ... 90 dell'array contengono i valori delle variabili di sicurezza che si vogliono scambiare con il PAC ricevente. L'area rimanente è riservata per i dati di diagnostica autogenerati, incluso un CRC e un time stamp. Questi dati di diagnostica vengono utilizzati dal PAC ricevente per determinare se i dati trasferiti sono sicuri.
3	Sul PAC mittente, configurare il DFB `S_WR_ETH_MX2` in una sezione dei task SAFE. Collegare il DFB ad Array0 e CtrlData0: 

Passo	Azione
4	Nel **Browser DTM** nel PAC mittente, selezionare la CPU (in questo esempio) o a un modulo di comunicazione NOC (se presente), quindi fare clic su **Aggiungi...** per creare uno scanner Modbus che può inviare i dati tramite Modbus TCP dal PAC mittente al PAC ricevente: 
5	Selezionare **Dispositivo Modbus** e fare clic **Aggiungi DTM** per aggiungere lo scanner Modbus: 

Passo	Azione
6	Aprire il dispositivo Modbus appena aggiunto e nella scheda **Impostazione richiesta**: • Impostare la colonna **Lunghezza WR**, ossia la lunghezza dei dati da scrivere, al valore 100, quindi • Impostare la colonna **Indirizzo WR**, che è l'indirizzo in cui la tabella del PAC ricevente scriverà i dati che riceve (in questo esempio: 0, ossia il PAC mittente scriverà nella tabella a partire da %MW0 nel PAC ricevente). 
7	Selezionare il nodo **Request 001: Items**, quindi nella scheda **Uscita** definire un tipo di array di INT (ossia ≥100 interi). Questa è la tabella del PAC mittente che verrà scritta nel PAC ricevente:

Passo	Azione
	
8	Dopo che la configurazione è stata salvata e compilata, il blocco (BLOCKA_QI0_100 in questo esempio) viene creato automaticamente come variabile di processo: 

Passo	Azione
9	Sul PAC mittente, in una sezione del codice di processo, usare un DFP `MOVE` per copiare il contenuto dell'array "tab_p" nell'array definito sopra nella struttura del dispositivo Modbus: 
10	Sul PAC ricevente, usare l'**Editor dati di sicurezza** per creare un array di 100 interi (Array5) come ingresso nell'area **Interfaccia**: Creare nello stesso **Editor dati di sicurezza** un array di 4 interi (CtrlData5) come uscita nell'area **Interfaccia**. 
11	Sul PAC ricevente, nell'**Editor dati di processo** creare un array di 100 interi (Array3) come uscita dell'area **Interfaccia**. Collegare questo Array3 all'Array5 (creato al passo 10) nella colonna **Parametro effettivo**. I dati inviati dal PAC mittente verranno scritti in questo Array3 tramite lo scanner Modbus, a condizione che questo Array3 sia localizzato all'indirizzo definito nello scanner del PAC mittente (in questo esempio %MW0). Creare nello stesso **Editor dati di processo** un array di 4 interi (CtrlData3) come ingresso nell'area **Interfaccia**. Collegare questo CtrlData3 all'CtrlData5 (creato al passo 10) nella colonna **Parametro effettivo**. 

Passo	Azione
12	Sul PAC ricevente, utilizzare l'**Editor dati di sicurezza** per creare un array di 100 interi (Array6): 
13	Nel PAC ricevente, in una sezione di codice nel task SAFE, creare un'istanza del DFB `S_RD_ETH_MX2` con l'array creato al passo 10 (Array5) quale parametro di ingresso e con gli array creati al passo 10 (CtrlData5) e al passo 12 (Array6) quali parametri di uscita: 
14	Sul PAC ricevente, ripetere i passi da 4 a 9 per configurare una comunicazione a 4 interi per inviare l'array CtrlData2 dal PAC ricevente al PAC mittente. In questo esempio, CtrlData deve essere scritto nel PAC mittente all'indirizzo %MW100.

Black channel peer-to-peer

Ogni trasmissione dati peer-to-peer è costituita da *Dati di sicurezza utente*, che trasmettono il contenuto legato all'applicazione, e *Dati riservati*. I *Dati riservati* servono al PAC di sicurezza per testare l'affidabilità della trasmissione, che deve soddisfare i requisiti SIL3. I *Dati riservati* sono formati dai seguenti elementi:

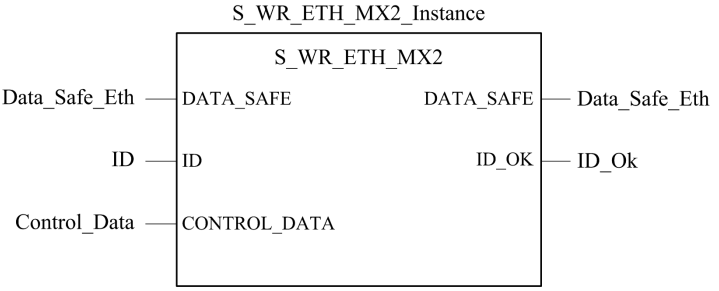
- Un CRC calcolato dal PAC mittente a partire dai dati che devono essere trasmessi. Il PAC ricevente verifica il CRC prima di usare i dati trasmessi.
- Un identificativo di comunicazione, che è incluso nel calcolo del CRC per evitare bit mascherati e cyberattacchi sulla trasmissione dei dati di sicurezza.

- Un'indicazione oraria contenente la durata della trasmissione in ms. Con firmware della CPU 3.20 o successivo, questa indicazione dell'ora è il valore di tempo sicuro fornito dalla CPU ricevente. Il PAC mittente aggiunge un valore temporale ai dati inviati al PAC ricevente. Il PAC ricevente confronta l'indicazione oraria con il proprio valore orario e la usa per:
  - Verificare l'età dei dati.
  - Rifiutare trasmissioni doppie.
  - determinare l'ordine cronologico delle trasmissioni ricevute
  - determinare il tempo trascorso tra la le notifiche di ricezione delle trasmissioni dati.

Configurazione del DFB S_WR_ETH_MX2 nella logica di programma del controller mittente

Rappresentazione

Rappresentazione DFB:



Per una descrizione estesa di questo DFB, consultare *EcoStruxure™ Control Expert, Safety, Block Library*.

Descrizione

Il DFB S_WR_ETH_MX2 è per controller con firmware 3.20 o successivo. Calcola i dati (dati riservati contenenti un CRC e un timestamp) richiesti dal controller ricevente per verificare e gestire gli errori rilevati durante la comunicazione peer-to-peer di sicurezza.

NOTA: Quando si configura la comunicazione di sicurezza tra i controller M580 Safety e i controller Quantum Safety, utilizzare i blocchi funzione S_RD_ETH_MX, pagina 196 e S_WR_ETH_MX, pagina 194 invece dei blocchi funzione S_RD_ETH_MX2 e S_WR_ETH_MX2.

Chiama il blocco funzione DFB `S_WR_ETH_MX2` a ogni ciclo nel controller mittente. Nell'ambito del ciclo, viene eseguito nella logica dopo che sono state eseguite tutte le modifiche richieste sui dati da inviare. Questo significa che i dati da inviare non possono essere modificati nel ciclo dopo l'esecuzione del DFB; altrimenti, le informazioni CRC utilizzate nell'area dati riservati non sono corrette e la comunicazione peer-to-peer di sicurezza non può avere luogo.

Assegnare al parametro `ID` un valore univoco che identifica la comunicazione peer-to-peer di sicurezza tra un controller mittente e un controller ricevente.

⚠ AVVERTIMENTO
IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA Il valore del parametro `ID` deve essere univoco e fisso nella rete per una coppia di controller mittente/ricevente. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Descrizione dell'array `DATA_SAFE`

Utilizzare le schede **Interfaccia** nell'**Editor dati di sicurezza** ed **Editor dati di processo** in Control Expert per collegare le variabili di processo e le variabili di sicurezza.

Il processo di collegamento e le variabili di sicurezza possono:

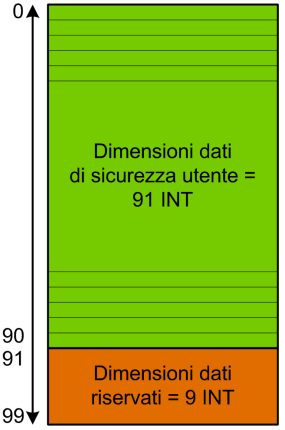
- Trasferire il valore delle variabili di sicurezza alle variabili di processo tramite variabili globali collegate.
- Inviare valori variabili dall'area processo del controller mittente all'area processo del controller ricevente tramite messaggistica esplicita su Modbus TCP.

L'array `DATA_SAFE` è composto da due aree:

- L'area **Dati sicurezza utente** contiene i dati provenienti dall'area sicura del controller. Quest'area inizia all'indice 0 e finisce all'indice 90.
- L'area **Dati riservati** è riservata per i dati diagnostici generati automaticamente, compresi un CRC e timestamp. Questi dati vengono utilizzati dal controller ricevente per determinare se i dati contenuti nell'area **Dati sicurezza utente** sono sicuri o no. Quest'area inizia all'indice 91 e finisce all'indice 99.

  NOTA: Non scrivere nell'area **Dati riservati**. La scrittura in quest'area sovrascrive i dati diagnostici generati automaticamente.

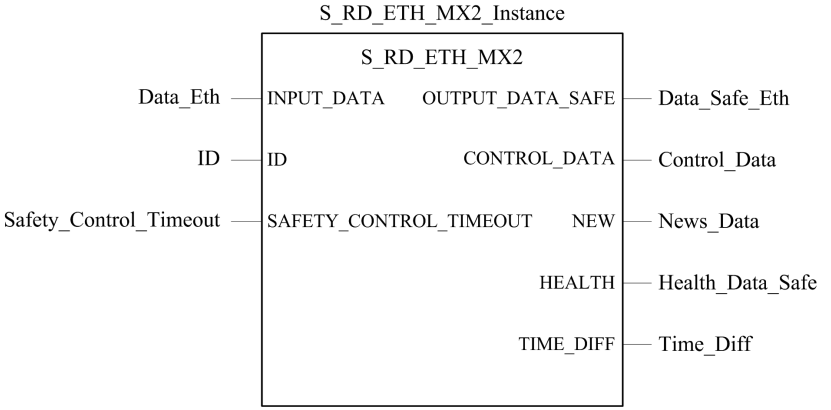
La rappresentazione della struttura dell'array `DATA_SAFE` (array[0..99] of INT):



Configurazione del DFB `S_RD_ETH_MX2` nella logica di programma del PAC ricevente

Rappresentazione

Rappresentazione del DFB:



Vedere *EcoStruxure™ Control Expert, Safety, Block Library* per una descrizione estesa di questo DFB.

Descrizione

Il DFB S_RD_ETH_MX2 è per PAC con firmware della CPU 3.20 o successivo. Copia i dati ricevuti nell'area di processo sull'area di sicurezza e convalida la precisione dei dati ricevuti.

NOTA: Quando si configurano le comunicazioni sicure tra CPU M580 Safety e CPU Quantum Safety, utilizzare i blocchi funzione S_RD_ETH_MX, pagina 196 e S_WR_ETH_MX, pagina 194 invece dei blocchi funzione S_RD_ETH_MX2 e S_WR_ETH_MX2.

⚠AVVERTIMENTO

IMPOSSIBILE ESEGUIRE LE FUNZIONI DI SICUREZZA

- Il blocco funzione DFB S_RD_ETH_MX2 deve essere richiamato a ogni ciclo nella logica di programma del PAC ricevente e deve essere eseguito prima che i dati del ciclo vengano utilizzati.
- Il valore del parametro ID deve essere univoco e fisso nella rete per una coppia mittente/ricevente.
- Testare il valore del bit HEALTH del DFB S_RD_ETH_MX2 a ogni ciclo prima di utilizzare dati sicuri per gestire la funzione di sicurezza.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Il blocco funzione S_RD_ETH_MX2:

- Copia i dati ricevuti nel registro INPUT_DATA sul registro OUTPUT_DATA_SAFE se supera i seguenti test:
  - Il blocco funzione verifica il CRC dell'ultimo pacchetto dati ricevuto, tramite scanner degli I/O su Ethernet (Modbus TCP). Se il CRC non è corretto, i dati sono considerati non sicuri e non vengono scritti nel registro OUTPUT_DATA_SAFE nell'area di sicurezza.
  - Il blocco funzione controlla gli ultimi dati ricevuti per determinare se sono più recenti di quelli già scritti nel registro OUTPUT_DATA_SAFE nell'area di sicurezza (confrontando i timestamp). Se gli ultimi dati ricevuti non sono più recenti, non vengono copiati nel registro OUTPUT_DATA_SAFE nell'area di sicurezza.
- Verifica l'età dei dati presenti nell'area di sicurezza. Se l'età è superiore a un valore massimo configurabile impostato nel registro di ingresso SAFETY_CONTROL_TIMEOUT, i dati sono dichiarati non sicuri e il bit HEALTH è impostato a 0.

  NOTA: L'età dei dati è data dalla differenza tra l'ora in cui i dati sono calcolati nel PAC di invio e l'ora in cui vengono verificati nel PAC di ricezione.

  Se il bit HEALTH è impostato a 0, i dati disponibili nell'array OUTPUT_DATA_SAFE sono considerati non sicuri. In questo caso, prendere le appropriate misure.

Descrizione degli array INPUT_DATA e OUTPUT_DATA_SAFE

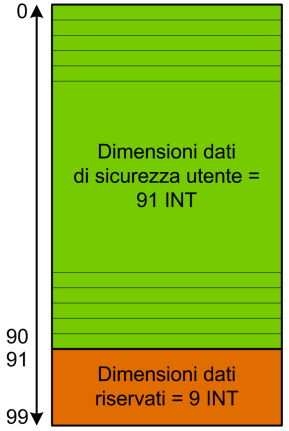
Gli array INPUT_DATA consistono di dati provenienti dall'area di memoria dei dati di processo. Gli array OUTPUT_DATA_SAFE consistono di variabili di sicurezza. Utilizzare le schede **Interfaccia dati di sicurezza** e **Interfaccia dati di processo** in Control Expert per creare il collegamento tra le variabili di processo e le variabili di sicurezza.

Gli array INPUT_DATA e OUTPUT_DATA_SAFE sono composti da due aree:

- L'area **Dati sicurezza utente** contiene i dati dell'utente. Quest'area inizia all'indice 0 e finisce all'indice 90.
- L'area **Dati riservati** è riservata per i dati diagnostici generati automaticamente, compresi un CRC e timestamp. Tali dati sono utilizzati dal PAC ricevente per determinare se i dati contenuti nell'area **Dati sicurezza utente** sono sicuri o meno. Quest'area inizia all'indice 91 e finisce all'indice 99.

  NOTA: Non scrivere nell'area **Dati riservati**. La scrittura in quest'area sovrascrive i dati diagnostici generati automaticamente.

La rappresentazione della struttura degli array INPUT_DATA e OUTPUT_DATA_SAFE (array [0..99] of INT):



Descrizione dell'array CONTROL_DATA

L'array CONTROL_DATA deve essere collegato con variabili nell'area “Globale” (definita tramite “Interfaccia dati di sicurezza”) quindi, le variabili “Globali” devono essere collegate a variabili identificate nell'area “Processo” (definita tramite “Interfaccia dati di processo”) per poter inviare i dati dallo IO Scanner al mittente corrispondente.

Calcolo di un valore SAFETY_CONTROL_TIMEOUT

Quando si calcola un valore `SAFETY_CONTROL_TIMEOUT` considerare quanto segue:

- Valore minimo: `SAFETY_CONTROL_TIMEOUT` > 2 * T1
- Valore tipico: `SAFETY_CONTROL_TIMEOUT` > 3 * T1

T1 = tempo ciclo MAST $CPU_{mittente}$ + tempo ciclo SAFE $CPU_{mittente}$ SAFE + Frequenza_ ripetizione + Tempo trasmissione di rete + tempo ciclo MAST $CPU_{ricevente}$ + tempo ciclo SAFE $CPU_{ricevente}$

dove:

- *Tempo ciclo $CPU_{mittente}$ MAST* è il tempo di ciclo MAST del PAC mittente.
- *Tempo ciclo $CPU_{mittente}$ SAFE* è il tempo di ciclo SAFE del PAC mittente.
- *Frequenza_ripetizione* è la frequenza di tempo della query di scrittura dello scanner degli I/O dal PAC mittente al PAC ricevente.
- *Tempo trasmissione di rete* è il tempo impiegato sulla rete Ethernet per la trasmissione dei dati dal PAC mittente al PAC ricevente.
- *Tempo ciclo $CPU_{ricevente}$ MAST* è il tempo di ciclo MAST del PAC ricevente.
- *Tempo ciclo $CPU_{ricevente}$ SAFE* è il tempo di ciclo SAFE del PAC ricevente.

Tenere presente che il valore definito per il parametro `SAFETY_CONTROL_TIMEOUT` ha un effetto diretto sulla robustezza e sulla disponibilità della comunicazione peer-to-peer sicura. Se il valore del parametro `SAFETY_CONTROL_TIMEOUT` supera T1, la comunicazione tollererà vari ritardi (ad esempio, ritardi di rete) o trasmissioni di dati danneggiate.

Configurare la rete Ethernet in modo che il carico non provochi un ritardo eccessivo sulla rete durante la trasmissione dei dati, che potrebbe provocare la scadenza del timeout. Per consentire una comunicazione peer-to-peer sicura senza eccessivi ritardi dovuti ad altri dati non sicuri trasmessi sulla stessa rete, utilizzare una rete Ethernet dedicata per il protocollo peer-to-peer sicuro.

Quando si mette in servizio il progetto, valutare le prestazioni della comunicazione peer-to-peer sicura controllando i valori forniti nel parametro di uscita `TIME_DIFF` e valutando il margine utilizzando il valore definito nel parametro `SAFETY_CONTROL_TIMEOUT`.

Note sul bit `HEALTH`

Quando il bit `HEALTH` è uguale a:

- 1: l''integrità dei dati è corretta (CRC) e l'età dei dati è inferiore al valore impostato nel registro di ingresso `SAFTETY_CONTROL_TIMEOUT`.

  NOTA: L'età dei dati considerati è il tempo tra:

  - l'inizio del ciclo dove i dati sono danneggiati nel PAC mittente.
  - l'inizio del ciclo dove i dati sono controllati nel PAC mittente.

- 0: i nuovi dati validi non vengono ricevuti nell'intervallo di tempo richiesto (il timer scade e il bit `HEALTH` è impostato a 0).

  NOTA: se il bit `HEALTH` è impostato a 0, i dati nell'array di uscita `OUTPUT_DATA_SAFE` sono considerati non sicuri; rispondere in modo adeguato.

Comunicazioni black channel M580

Black channel

Black channel è il sistema utilizzato per crittografare e convalidare i dati di sicurezza trasmessi:

- Solo le apparecchiature di sicurezza Schneider Electric possono crittografare e convalidare i dati inviati tramite il black channel in un sistema di sicurezza M580.
- Lo stato di ogni trasmissione dei dati di sicurezza viene testato dai moduli di sicurezza mittente e ricevente per ogni messaggio trasmesso.

Grazie all'uso del black channel è possibile trasmettere dati di sicurezza tramite apparecchiature intermedie non sicure, come backplane, cablaggio Ethernet, adattatori di comunicazione, ecc. Dato che le trasmissioni black channel sono crittografate, l'apparecchiatura intermedia non può leggere o modificare il contenuto dei dati di sicurezza trasmessi senza essere rilevata.

Le trasmissioni black channel avvengono in modo indipendente dal protocollo di comunicazione utilizzato per la trasmissione:

- X Bus è la portante delle trasmissioni backplane tra dispositivi di sicurezza sullo stesso backplane (ad esempio dal controller ai moduli di I/O locali o da un modulo adattatore di comunicazione remoto (CRA) ai moduli di I/O locali).
- EtherNet/IP è la portante per le trasmissioni di dati tra backplane (ad esempio dal controller a un modulo adattatore CRA).

I moduli di I/O di sicurezza M580 e il controller possono inviare e ricevere comunicazioni black channel. Per ogni trasmissione, il dispositivo trasmettitore (controller o modulo I/O) aggiunge le seguenti informazioni al messaggio:

- un tag CRC per attivare la verifica del contenuto del messaggio
- un time stamp per attivare la verifica del puntualità del messaggio
- altre informazioni, tra cui la versione dell'applicazione e la configurazione del modulo di I/O utilizzato, che identificano il modulo di I/O nella trasmissione

Con firmware del controller 3.10 o precedente e moduli di I/O di sicurezza su un backplane remoto, configurare il controller come client NTP o server NTP.

Se una di queste configurazioni non è implementata, le impostazioni dell'ora dei moduli di I/O di sicurezza e del controller non sono sincronizzate e la comunicazione black channel non

funziona correttamente. Gli ingressi e le uscite dei moduli di I/O di sicurezza nelle derivazioni RIO entrano nello stato sicuro definito (non alimentato) o di posizionamento di sicurezza.

NOTA: Se si installano moduli di I/O di sicurezza in una derivazione RIO, configurare l'ora per il controller con versione firmware 3.10 o precedente. Attivare il servizio NTP per il sistema M580 e configurare il controller di sicurezza come server NTP o client NTP.

Il dispositivo ricevente (modulo I/O o controller) decrittografa il messaggio e verifica la precisione del suo contenuto. Possono essere rilevate le seguenti condizioni:

Condizione	Descrizione
Errori di trasmissione	Errore rilevato nell'indirizzo del messaggio o nel routing.
Ripetizioni	Messaggio inviato più volte.
Dati eliminati	Manca una parte del messaggio o il messaggio è andato perduto.
Dati inseriti	Sono stati inseriti dati supplementari al messaggio.
Dati fuori sequenza	L'ordine dei messaggi è cambiato.
Dati danneggiati	Sono stati rilevati uno o più errori di bit nel messaggio.
Ritardi	Il tempo di consegna dei messaggi è eccessivamente lungo.
Mascherato	La sorgente del messaggio non è autorizzata a trasmettere dati.

Quando vengono rilevati questi errori, il canale viene considerato danneggiato e viene eseguita la funzione di sicurezza appropriata:

- Il controller, se rileva che una trasmissione da un modulo di ingresso è danneggiata, imposta i valori di ingresso da tale modulo nello stato sicuro definito (non alimentato o di posizionamento di sicurezza).
- Un modulo di uscita, se rileva che una trasmissione dal controller è danneggiata, porta le uscite nel loro stato di posizionamento di sicurezza preconfigurato.

Le uscite entrano automaticamente nello stato comandato dal controller dopo che la comunicazione tra il controller e il modulo di uscita è stata ristabilita correttamente.

AVVISO

MODIFICA IMPREVISTA DELLO STATO DELL'USCITA AL RIPRISTINO DELLA COMUNICAZIONE

Monitorare lo stato dei canali di uscita e attivare la funzione di sicurezza di conseguenza, impostando i comandi di uscita allo stato sicuro definito.

Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.

Comunicazione tra la CPU M580 e gli I/O di sicurezza

Introduzione

Questa sezione descrive la comunicazione tra la CPU di sicurezza M580 e i moduli di I/O di sicurezza.

Comunicazioni tra PAC M580 Safety e I/O

Comunicazione tra PAC e I/O

La CPU e il coprocessore di sicurezza M580 insieme controllano tutti gli scambi sul backplane, mentre gli I/O di sicurezza rispondono ai comandi di CPU e coprocessore. I moduli di I/O di sicurezza possono essere installati in un rack X Bus BMXXBP•••• o in un rack Ethernet BMEXBP••••.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza nel rack principale locale avvengono tramite il backplane.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza installati in una derivazione RIO avvengono attraverso un modulo adattatore installato nella derivazione RIO:

- un adattatore BMECRA31210 per un rack Ethernet, oppure
- un adattatore BMXCRA31210 per un rack X Bus.

  NOTA: Con firmware della CPU 3.20 o successivo, il modulo adattatore BM•CRA31210 richiede un firmware 2.60 o successivo.

  NOTA: Un adattatore BMXCRA31200 non può essere utilizzato per collegare i moduli di I/O di sicurezza al PAC di sicurezza M580.

Le comunicazioni tra il PAC di sicurezza e i moduli di I/O di sicurezza, sia nel rack principale locale che in una derivazione RIO, avvengono tramite il avvengono tramite il black channel, pagina 213.

Il modo per sincronizzare le impostazioni dell'ora della CPU e dei moduli di I/O di sicurezza dipende dalla versione del firmware della CPU:

- Per PAC con firmware della CPU 3.10 o precedente, è richiesta la configurazione del servizio NTP.

  NOTA: Se si installano i moduli di I/O di sicurezza in un rack locale (o in un'estensione del rack locale) non è necessario attivare il servizio NTP.

- Per PAC con firmware della CPU 3.20 o successivo, la sincronizzazione dell'ora sicura si basa su un orologio interno e "monotonico".

Per ulteriori informazioni, consultare il capitolo *Sincronizzazione dell'ora*, pagina 180.

Opzionalmente, si possono utilizzare i moduli ripetitori a fibre ottiche BMXNRP0200 oppure BMXNRP0201 per estendere il collegamento fisico tra la CPU e il coprocessore nel rack locale e l'adattatore nella derivazione RIO. I moduli ripetitori a fibre ottiche migliorano l'immunità ai disturbi della rete RIO e garantiscono al contempo il mantenimento della massima disponibilità dinamica della rete e il livello di integrità di sicurezza.

Il protocollo di comunicazione tra gli I/O di sicurezza e il PAC consente gli scambi sulla rete. Questo protocollo permette ad entrambi i dispositivi di verificare l'accuratezza dei dati ricevuti, di rilevare eventuali dati corrotti e di determinare se il modulo di trasmissione diventa non operativo. Pertanto, un loop di sicurezza può includere qualsiasi adattatore RIO e backplane non interferente, pagina 33.

Alimentazione per gli I/O di sicurezza

Gli I/O di sicurezza sono alimentati a 24 VCC e 3,3 VCC sul backplane mediante il M580 modulo alimentatore di sicurezza, pagina 132. Il modulo alimentatore di sicurezza monitora l'alimentazione fornita in modo che non superi 36 VCC.

Alimentazione per funzioni non di sicurezza:

5 VCC forniti dal backplane vengono utilizzati da ogni modulo di I/O di sicurezza per le proprie funzioni non di sicurezza.

Alimentazione esterna per gli I/O di sicurezza digitali:

Per il processo non di sicurezza (sensore, attuatore) è richiesto un alimentatore esterno, non superiore a 60 VCC, che può essere una bassissima tensione di protezione (SELV/PELV) di categoria di sovratensione II. L'alimentatore di processo non di sicurezza è controllato dal modulo di I/O di sicurezza, che rileva eventuali condizioni di sovratensione e sottotensione.

Diagnostica di un sistema di sicurezza M580

Introduzione

Questo capitolo fornisce informazioni sulle operazioni di diagnostica che possono essere eseguite in base agli indicatori hardware (basati sullo stato dei LED) e i bit o le parole di sistema per un sistema di sicurezza M580.

Diagnostica della CPU e del coprocessore di sicurezzaM580

Introduzione

Questa sezione descrive la diagnostica disponibile per le CPU di sicurezza e il coprocessore di sicurezza BME•58•040S BMEP58CPROS3.

Diagnostica della condizione di blocco

Introduzione

Le condizioni di blocco che si verificano durante l'esecuzione del programma di sicurezza o di processo derivano dal rilevamento di errori di sistema o dello stato HALT di un task nel quale è stato rilevato l'errore.

NOTA: il controller M580 Safety presenta due stati HALT indipendenti:

- HALT processo si applica ai task non di sicurezza (MAST, FAST, AUX0 e AUX1). Quando un task di processo entra nello stato HALT, anche tutti gli altri task di processo entrano nello stato HALT.
- SAFE HALT si applica solo al task SAFE.

Per una descrizione degli stati HALT e STOP, vedere la sezione *Stati operativi del controller M580 Safety*, pagina 265.

Diagnostica

Quando il controller rileva una condizione di blocco che provoca un errore di sistema, l'errore rilevato è descritto nella parola di sistema `%SW124`.

Quando il controller rileva una condizione di blocco che provoca uno stato HALT, l'errore rilevato è descritto nella parola di sistema `%SW125`.

Valori della parola di sistema `%SW124` e la corrispondente descrizione della condizione di blocco:

Valore `%SW124` (hex)	**Descrizione della condizione di blocco**
5AF2	Errore RAM rilevato nel controllo memoria
5AFB	Errore del codice firmware di sicurezza rilevato
5AF6	Overrun del watchdog di sicurezza rilevato sul controller.

Valore %SW124 (hex)	Descrizione della condizione di blocco
5AFF	Overrun del watchdog di sicurezza rilevato sul coprocessore
5B01	Coprocessore non rilevato all'avvio

Valori della parola di sistema %SW125 e la corrispondente descrizione della condizione di blocco:

Valore %SW125 (hex)	Descrizione della condizione di blocco
0•••	esecuzione di una funzione non determinabile
0002	caratteristica di firma della scheda SD (utilizzata con le funzioni *SIG_CHECK* e *SIG_WRITE*)
2258	esecuzione dell'istruzione HALT
2259	flusso di esecuzione diverso dal flusso di riferimento
23••	esecuzione di una funzione CALL verso una subroutine non definita
5AF3	errore di confronto rilevato dal controller
5AF9	errore di istruzione rilevato all'avvio o al runtime
5AFA	errore di confronto rilevato sul valore CRC
5AFC	errore di confronto rilevato dal coprocessore
5AFD	errore interno rilevato dal coprocessore; sottocodice in %SW126: 1 (risultato sconosciuto), 2 (applicazione CRC), 7 (contatore attività errato)
5AFE	rilevato errore di sincronizzazione coprocessore - solo controller; sottocodice in %SW126: 3 (diagnostica), 4 (fine UL), 5 (confronto), 6 (BC out), 8 (HALT durante UL), 9 HALT durante confronto), 10 (HALT durante BC out).
81F4	Nodo SFC non corretto
82F4	Codice SFC non accessibile
83F4	Workspace SFC non accessibile
84F4	Troppi passi SFC iniziali
85F4	Troppi passi SFC attivi
86F4	Sequenza codice SFC non corretta
87F4	Descrizione codice SFC non corretta
88F4	Tabella di riferimento SFC non corretta
89F4	errore di calcolo indice interno SFC rilevato
8AF4	Stato passo SFC non disponibile
8BF4	Memoria SFC troppo piccola dopo un cambio dovuto a un download
8CF4	Sezione Transazione/Azione non accessibile

Valore %SW125 (hex)	Descrizione della condizione di blocco
8DF4	Workspace SFC troppo piccolo
8EF4	Versione del codice SFC maggiore dell'interprete
8FF4	Versione del codice SFC più recente dell'interprete
90F4	descrizione insufficiente di un oggetto SFC: puntatore NULL
91F4	Identificativo azione non autorizzato
92F4	Definizione insufficiente del tempo di un identificativo azione
93F4	Impossibile trovare passo macro nella lista di passi attivi per disattivazione
94F4	Overflow nella tabella azione
95F4	Overflow nella tabella di attivazione/disattivazione dei passi
9690	Errore rilevato nel controllo CRC applicazione (checksum)
DE87	Errore virgola mobile rilevato nel calcolo
DEB0	Overrun watchdog del task (%S11 e %S19 sono impostati)
DEF0	Divisione per 0
DEF1	Errore di trasferimento stringa di caratteri
DEF2	Capacità superata
DEF3	Overrun indice
DEF4	Periodi del task incoerenti
DEF7	Errore di esecuzione SFC
DEFE	Passi SFC non definiti

Riavvio dell'applicazione

Dopo che si è verificata una condizione di blocco, occorre inizializzare il task arrestato. Se si è verificato un HALT per un:

- task di processo (MAST, FAST, AUX0 o AUX1), l'inizializzazione viene eseguita dal comando **Init** dal controller Control Expert o impostando il bit %S0 a 1.
- task SAFE, l'inizializzazione viene eseguita dal comando **Init Safety** del controller Control Expert.

Quando viene inizializzata, l'applicazione si comporta nel modo seguente:

- I dati riprendono il loro valore iniziale.
- I task vengono arrestati al termine del ciclo.

- L'immagine d'ingresso viene aggiornata.
- Le uscite vengono controllate nella posizione di sicurezza.

Il comando RUN riavvia l'applicazione o i task.

Diagnostica delle condizioni non bloccanti

Introduzione

Il sistema rileva una condizione non bloccante quando rileva un errore di ingresso/uscita sul bus del backplane (X Bus o Ethernet) o tramite l'esecuzione di un'istruzione, che può essere elaborata dal programma utente e che non modifica lo stato operativo del controller.

Questa sezione descrive alcuni bit e parole di sistema che possono essere utilizzati per rilevare lo stato del sistema di sicurezza e dei moduli che lo compongono.

NOTA: i bit e le parole di sistema disponibili non includono tutte le informazioni relative allo stato dei moduli di sicurezza. Utilizzare la struttura DDDT del controller di sicurezza e dei moduli I/O di sicurezza per determinare lo stato del sistema di sicurezza M580.

Per informazioni sul DDDT del controller M580 Safety, vedere la sezione *Struttura dati DDT standalone per controller M580* nel documento *Modicon M580 - Manuale di riferimento hardware*.

Per informazioni sui DDDT dei moduli di I/O di sicurezza M580, vedere le seguenti sezioni:

- Struttura dati BMXSAI0410, pagina 65 per il modulo di ingresso analogico di sicurezza
- Struttura dati BMXSDI1602, pagina 96 per il modulo di ingresso digitale di sicurezza
- Struttura dati BMXSDO0802, pagina 110 per il modulo di uscita digitale di sicurezza
- Struttura dati BMXSRA0405, pagina 127 per il modulo di uscita relè digitale di sicurezza

NOTA: è possibile eseguire la diagnostica avanzata dei dispositivi Ethernet tramite la messaggistica esplicita. Per questo scopo, utilizzare il:

- Blocco funzione READ_VAR (vedere EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi) per dispositivi Modbus TCP
- Blocco funzione DATA_EXCH (vedere Modicon M580, Hardware, Manuale di riferimento), specificando il protocollo CIP nel blocco ADDM, per i dispositivi EtherNet/IP

Condizioni associate alla diagnostica I/O

Una condizione non bloccante relativa agli I/O viene diagnosticata con le seguenti indicazioni:

- comportamento LED controller **I/O**: acceso fisso
- comportamento LED modulo **I/O**: acceso fisso
- bit di sistema (tipo di errore rilevato):
  - %S10 impostato a 0: errore I/O globale rilevato su uno dei moduli sul backplane Ethernet o X Bus locale o remoto
  - %S16 impostato a 0: errore di I/O rilevato nel task in corso su un backplane X Bus
  - %S40...%S47 impostati a 0: errore di I/O rilevato su un backplane X Bus all'indirizzo da 0 a 7
  - %S117 impostato a 0: errore RIO rilevato su un backplane X Bus remoto
  - %S119 impostato a 0: errore di I/O rilevato su un backplane X Bus locale

    NOTA: questi bit (%S10, %S16, %S40...%S47, %S117 e %S119) segnalano molti errori rilevati relativi ai moduli I/O di sicurezza.
- bit e parole di sistema relativi al canale in cui è stato rilevato un errore (numero di canale di I/O e tipo di errore rilevato) oppure informazioni Device DDT per modulo I/O (per i moduli configurati in modalità di indirizzamento Device DDT):
  - bit %Ir.m.c.ERR impostato a 1: errore del canale rilevato (scambi impliciti)
  - parola %MWr.m.c.2: il valore della parola indica il tipo di errore rilevato sul canale specificato e dipende dal modulo di I/O (scambi impliciti)

Condizioni relative all'esecuzione della diagnostica del programma

Una condizione non bloccante relativa all'esecuzione del programma viene diagnosticata con i seguenti bit e parole di sistema:

- bit di sistema - tipo di errore rilevato:
  - %S15 impostato a 1: rilevato errore di manipolazione della stringa di caratteri.
  - %S18 impostato a 1: overrun di capacità; errore rilevato su una virgola mobile o divisione per 0.

    (Per maggiori informazioni, vedere la sezione *Bit di sistema per l'esecuzione sicura dei task*, pagina 407.)

    Quando %S18 è impostato a 1, %SW17 contiene un descrizione dell'evento causale, pagina 409.
  - %S20 impostato a 1: overrun indice.

    NOTA: se il bit di sistema configurabile %S78 è impostato nel programma, il task SAFE entra nello stato HALT quando il bit di sistema %S18 è impostato a 1.

- parola di sistema - natura dell'errore rilevato:
  - `%SW125 (see Modicon M580, Hardware, Reference Manual)` (sempre aggiornato)

Diagnostica mediante LED della CPU M580 Safety

LED CPU

Utilizzare i LED sul lato frontale della CPU (vedere Modicon M580, Guida alla pianificazione del sistema di sicurezza), per la diagnostica generale sullo stato del PAC durante la messa in servizio o la risoluzione dei problemi.

⚠AVVERTIMENTO

RISCHIO DIAGNOSTICA IMPRECISA DEL SISTEMA

Non utilizzare i LED come indicatori operativi.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

In *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente*, consultare l'argomento Diagnostica LED per CPU M580 Hot Standby per informazioni su come diagnosticare i LED relativi alla ridondanza, tra cui **[A]**, **[B]**, **[PRIM]**, **[STBY]** e **[REMOTE RUN]**.

Stato del PAC	**Nomi e colori dei LED:**							
	RUN	**ERR**	**IO**[1]	**ETH MS**	**ETH NS**	**DL**	**SRUN**	**SMOD**
	Verde	**Rosso**	**Rosso**	**Verde/ Rosso**	**Verde/ Rosso**	**Verde**	**Verde**	**Verde**
Spegnimento								
Accensione • Autotest								
Non configurato					 Nessun cavo inserito e			

Stato del PAC	Nomi e colori dei LED:							
	RUN	ERR	IO[1]	ETH MS	ETH NS	DL	SRUN	SMOD
	Verde	Rosso	Rosso	Verde/ Rosso	Verde/ Rosso	Verde	Verde	Verde
					collegato a un altro dispositivo alimentato  Altrimenti			
Configurato: • Nessun errore esterno rilevato							–	–
• Errore esterno rilevato				–	–		–	–
• Nessun collegamento Ethernet, incluso il backplane Ethernet							–	–
• Indirizzo IP duplicato			–				–	–
• Stato STOP			 Rilevato errore su modulo, canale o configurazione di I/O  Nessun errore rilevato su ingresso/ uscita configurati		 Non collegato  Connesso		 Task SAFE in esecuzione OPPURE  Task SAFE arrestato	 Modalità di sicurezza OPPURE  Modalità di manutenzione

Stato del PAC	Nomi e colori dei LED:							
	RUN	**ERR**	**IO**[1]	**ETH MS**	**ETH NS**	**DL**	**SRUN**	**SMOD**
	Verde	**Rosso**	**Rosso**	**Verde/ Rosso**	**Verde/ Rosso**	**Verde**	**Verde**	**Verde**
					Nessun cavo			
• Stato RUN			–		Non collegato Connesso Nessun cavo		Task SAFE in esecuzione OPPURE Task SAFE arrestato	Modalità di sicurezza OPPURE Modalità di manutenzione
Stato HALT (errore reversibile rilevato)			–				Task SAFE in esecuzione Task SAFE arrestato	Modalità di sicurezza Modalità di manutenzione
Stato SAFE (errore irreversibile rilevato)								

Stato del PAC	Nomi e colori dei LED:							
	RUN	ERR	IO[1]	ETH MS	ETH NS	DL	SRUN	SMOD
	Verde	Rosso	Rosso	Verde/ Rosso	Verde/ Rosso	Verde	Verde	Verde
Aggiornamento SO								

1. Non tutti gli errori rilevati per un modulo I/O di sicurezza sono segnalati tramite LED. Per maggiori informazioni in merito, vedere i DDDT per i moduli di I/O di sicurezza.

Legenda:

Simbolo	Descrizione	Simbolo	Descrizione	Simbolo	Descrizione
	Verde fisso		Rosso fisso		Spento
	Verde lampeggiante (500 ms ON, 500 ms OFF)		Rosso lampeggiante (500 ms ON, 500 ms OFF)	–	Non applicabile

Diagnostica mediante LED del coprocessore di sicurezza M580

LED del coprocessore

I LED situati sul pannello anteriore del coprocessore (vedi Modicon M580, Guida alla pianificazione del sistema di sicurezza) permettono di effettuare la diagnostica dello stato del PAC, come indicato di seguito:

Stato del coprocessore	**Nomi e colori dei LED:**			
	SRUN	**ERR**	**SMOD**	**DL**
	Verde	**Rosso**	**Verde**	**Verde**
Alimentazione OFF				
Stato WAIT (attesa di dowload del firmware dalla CPU)				
Non configurato (nessuna applicazione)				
Configurato e funzionante in modalità di sicurezza: • Task SAFE arrestato				
• Task SAFE in esecuzione				
Configurato e funzionante in modalità Manutenzione: • Task SAFE arrestato				
• Task SAFE in esecuzione				
Task SAFE in HALT (errore reversibile rilevato)				
Stato SAFE (errore irreversibile rilevato)				

Legenda:

Simbolo	**Descrizione**		**Simbolo**	**Descrizione**		**Simbolo**	**Descrizione**
	Verde fisso			Rosso fisso			OFF

Simbolo	Descrizione		Simbolo	Descrizione		Simbolo	Descrizione
	Verde lampeggiante (500 ms ON, 500 ms OFF)			Rosso lampeggiante (500 ms ON, 500 ms OFF)			

LED di accesso alla scheda di memoria

Introduzione

Il LED verde di accesso alla scheda di memoria situato sotto lo sportellino della scheda di memoria SD indica l'accesso della CPU alla memoria quando si inserisce una scheda. Questo LED è visibile quando lo sportellino è aperto.

Stati dedicati del LED

I LEDs di **accesso alla scheda di memoria** indicano i seguenti stati:

Stato dei LED	Descrizione
Acceso	La scheda di memoria è riconosciuta, ma la CPU non vi accede.
Lampeggiante	La CPU sta accedendo alla scheda di memoria.
Lampeggiante	La scheda di memoria non è stata riconosciuta.
Spento	La scheda di memoria può essere rimossa dallo slot della CPU oppure la CPU non riconosce la scheda di memoria.

NOTA: Confermare che il LED sia spento prima di estrarre la scheda dallo slot.

Significati delle combinazioni di LED

La scheda di accesso LED opera insieme al LED (vedere Modicon M580, Hardware, Manuale di riferimento) **BKP**. La combinazione di questi LED indica le seguenti informazioni di diagnostica:

Stato della scheda di memoria	Condizioni	Stato della CPU	LED di accesso alla scheda di memoria	LED BKP
nessuna scheda di memoria nello slot	—	nessuna configurazione		
problema con la scheda di memoria	—	nessuna configurazione		
scheda di memoria senza progetto	—	nessuna configurazione		
scheda di memoria con progetto non compatibile	—	nessuna configurazione		
scheda di memoria con progetto compatibile	Viene rilevato un errore quando il progetto viene ripristinato dalla scheda di memoria alla RAM della CPU.	nessuna configurazione	durante il trasferimento:  fine del trasferimento: 	durante il trasferimento:  fine del trasferimento: 
	Nessun errore viene rilevato quando il progetto viene ripristinato dalla scheda di memoria alla RAM della CPU.	—	durante il trasferimento:  fine del trasferimento: 	durante il trasferimento:  fine del trasferimento: 
- nessuna condizione specifica o stato della CPU				

Questa legenda mostra i diversi stati del LED:

Simbolo	Significato	Simbolo	Significato
	spento		rosso fisso
	verde fisso		verde lampeggiante

Diagnostica dell'alimentatore di sicurezza del modulo M580

Introduzione

Questa sezione descrive la diagnostica disponibile per gli alimentatori di sicurezza M580.

Diagnostica mediante LED dell'alimentatore

LED dell'alimentatore

Gli alimentatori di sicurezza BMXCPS4002S, BMXCPS4022S, e BMXCPS3522S dispongono di un pannello anteriore che contiene i seguenti LED di diagnostica:

- **OK**: stato operativo
- **ACT**: attività
- **RD**: ridondanza (per strutture di alimentazione ridondanti)

I LED dell'alimentatore di sicurezza M580 possono fornire le seguenti informazioni di diagnostica:

LED	Descrizione
OK	• ON (verde) indica che tutte le condizioni seguenti sono vere: ◦ Tensione backplane 24 Vdc corretta. ◦ Tensione backplane 3,3 Vdc corretta. ◦ Il pulsante RESET non è stato attivato. • Il lampeggio indica che una delle seguenti condizioni è vera: ◦ Tensione backplane 24 Vdc non corretta. ◦ Tensione backplane 3,3 Vdc non corretta e pulsante RESET non attivato. • OFF indica che almeno una delle seguenti condizioni è vera: ◦ Tensione backplane 24 Vdc non corretta. ◦ Tensione backplane 3,3 Vdc non corretta. ◦ Il pulsante RESET è stato attivato.
ACT	• ON (verde) indica che l'alimentatore sta fornendo l'alimentazione. In una struttura con alimentazione ridondante, il modulo è l'alimentatore primario. • OFF indica che l'alimentatore non sta fornendo alimentazione. In una struttura con alimentazione ridondante, il modulo è l'alimentatore di standby.
RD	• ON (verde) indica che la comunicazione tra i due moduli alimentatori è corretta. • Il lampeggio indica che una delle seguenti condizioni è vera: ◦ Tensione backplane 24 Vdc non corretta. ◦ Tensione backplane 3,3 Vdc non corretta. • OFF indica che almeno una delle seguenti condizioni è vera: ◦ La comunicazione tra i due moduli alimentatori non è corretta. ◦ Esecuzione di autotest in corso.

Diagnostica degli ingressi analogici del BMXSAI0410

Introduzione

Questa sezione descrive i tool di diagnostica disponibili per il modulo di ingresso analogico di sicurezza BMXSAI0410.

Diagnostica DDDT BMXSAI0410

Introduzione

Il modulo di ingresso analogico di sicurezza BMXSAI0410 offre la seguente diagnostica mediante i propri `T_U_ANA_SIS_IN_4, pagina 65` elementi DDT del dispositivo:

- diagnostica degli ingressi
- rilevamento errori interni
- diagnostica del cablaggio del canale

Diagnostica degli ingressi

Viene monitorata la capacità dei sensori collegati ad ogni canale di misurare con precisione 10 valori di ingresso analogici compresi tra 4 e 20 mA. Se i test di misura degli ingressi non vengono superati, il bit `CH_HEALTH` nella struttura DDT `T_U_ANA_SIS_CH_IN, pagina 67` è impostato a 0; questo valore indica che non è operativo.

Rilevamento degli errori interni

Il modulo elabora il valore di ingresso mediante due circuiti paralleli separati. I due valori vengono confrontati per determinare se si è verificato un errore nell'elaborazione del modulo. Se i valori confrontati sono diversi, il bit `IC` nella struttura DDDT `T_U_ANA_SIS_CH_IN` viene impostato a 1; questo valore indica che non è operativo.

Per una descrizione visiva di questo processo, vedere il diagramma dell'architettura, pagina 145 del modulo di ingresso analogico di sicurezza BMXSAI0410.

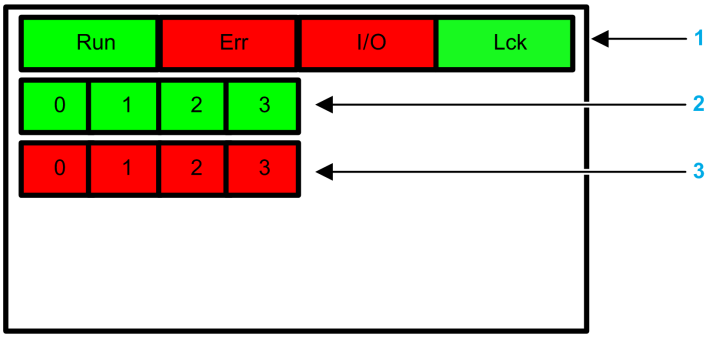
Diagnostica del cablaggio del canale

Viene effettuata costantemente la diagnostica del cablaggio del sensore al canale di ingresso per individuare un'eventuale condizione di conduttore interrotto, che viene rilevata quando la corrente di ingresso è inferiore a 3,75 mA o superiore a 20,75 mA. In questo caso, il bit `OOR` nella struttura DDDT `T_U_ANA_SIS_CH_IN` viene impostato a 1.

Diagnostica dei LED degli ingressi analogici del BMXSAI0410

LED, pannello

Il modulo di ingresso analogico BMXSAI0410 presenta il seguente pannello di LED sul lato frontale:



1 LED di stato del modulo

2 LED di stato del canale

3 LED di errore rilevati sul canale

NOTA:

- I LED dell'errore di canale rilevato sono funzionanti solo dopo che il modulo è stato configurato correttamente. Quando viene rilevato un errore di canale, il LED corrispondente resta acceso finché la condizione scatenante non è risolta.
- Dato che il modulo di ingresso dispone di quattro canali soltanto, i LED nelle posizioni 4...7 non sono utilizzati e non sono mai accesi.

Diagnostica del modulo

Utilizzare i quattro LED nella parte alta del pannello LED per diagnosticare la condizione del modulo di ingresso analogico BMXSAI0410:

LED del modulo				Stato del modulo	Soluzione possibile
Run	**Err**	**I/O**	**LCK**		
Lampeggiante[1]	Lampeggiante[1]	Lampeggiante[1]	Lampeggiante[1]	Autotest all'accensione.	–
Lampeggiante[1]	Acceso	Spento	Lampeggiante[1]	L'autotest all'accensione ha rilevato un errore interno sui canali di ingresso.	Sostituire il modulo.
Spento	Acceso	Spento	Spento	Errore interno rilevato.	Sostituire il modulo se la condizione persiste.
Spento	Lampeggiante[1]	Spento	X	Modulo I/O non configurato.	Configurare il modulo tramite il controller.
X	X	Acceso	X	Errore esterno rilevato su canale di ingresso.	Vedere oltre la sezione *Diagnostica del canale*, pagina 237.
Acceso	Lampeggiante[1]	X	X	Nessuna comunicazione tra controller e modulo I/O.	Verificare che: • Il controller sia un controller M580 Safety e che sia operativo. • Il backplane sia funzionante (se il modulo I/O si trova sul rack principale); • Il cavo tra il controller e il modulo I/O sia operativo e collegato correttamente (se il modulo I/O si trova su un rack di estensione o remoto).
Acceso	Sfarfallio[2]	X	Spento	Comunicazione non sicura e configurazione non bloccata.	Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 65 per l'istanza del modulo di I/O.
Acceso	Sfarfallio[2]	X	Acceso	Comunicazione non sicura e configurazione bloccata.	Verificare che: • La configurazione bloccata nel modulo sia uguale alla configurazione del modulo memorizzata nell'applicazione nel controller secondo le impostazioni effettuate in Control Expert.

LED del modulo				Stato del modulo	Soluzione possibile
Run	**Err**	**I/O**	**LCK**		
					• Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 65 per l'istanza del modulo di I/O.
Acceso	Acceso	Spento	X	Rilevato errore interno canale di ingresso	Sostituire il modulo se la condizione persiste.
Acceso	Spento	Spento	Spento	La comunicazione con il controller è regolare e la configurazione è sbloccata.	–
Acceso	Spento	Spento	Acceso	La comunicazione con il controller è regolare e la configurazione è bloccata.	–
X indica che lo stato del LED può essere Acceso o Spento. 1. Lampeggiante: acceso 500 ms / spento 500 ms. 2. Sfarfallio: acceso 50 ms /spento 50 ms.					

Diagnostica del canale

Usare tutti i LED sul modulo di ingresso analogico BMXSAI0410 per diagnosticare lo stato del canale:

LED del modulo				LED dei canali		Stato del canale	Soluzione possibile
Run	**Err**	**I/O**	**LCK**	**Stato del canale (LED 0...3)**	**Errore rilevato (LED 0...3)**		
Acceso	Spento	Spento	X	Acceso	Spento	La corrente di ingresso è compresa tra 4 e 20 mA sul canale.	–
Acceso	Spento	Acceso	X	OFF	Spento	La corrente di ingresso è compresa tra 4 e 20 mA sul canale.	Verificare che l'alimentatore esterno, il cablaggio esterno e il sensore siano funzionanti.
Acceso	Acceso	Spento	X	OFF	Acceso	Il canale non è operativo.	Sostituire il modulo se la condizione persiste.
X indica che lo stato del LED può essere Acceso o Spento.							

Diagnostica degli ingressi digitali del BMXSDI1602

Introduzione

Questa sezione descrive i tool di diagnostica disponibili per il modulo di ingresso digitale di sicurezza BMXSDI1602.

Diagnostica DDDT BMXSDI1602

Introduzione

Il modulo di ingresso digitale di sicurezza BMXSDI1602 fornisce la seguente diagnostica mediante i rispettivi elementi DDT del dispositivo `T_U_DIS_SIS_IN_16, pagina 96`:

- diagnostica degli ingressi
- rilevamento errori interni
- diagnostica del cablaggio del canale
- diagnostica di sovratensione e sottotensione

Diagnostica degli ingressi

Ogni canale di ingresso viene testato all'inizio di ogni ciclo (o scansione) per verificarne l'efficacia operativa. Ogni canale viene forzato nello stato alimentato e testato per verificare che lo stato alimentato sia stato raggiunto. Il canale viene quindi forzato nello stato non alimentato e viene nuovamente testato per verificare che lo stato non alimentato sia stato raggiunto.

Se il canale non commuta correttamente tra lo stato alimentato e quello non alimentato, il bit `CH_HEALTH` nella struttura DDDT `T_U_DIS_SIS_CH_IN, pagina 98` viene impostato a 0, per indicare che non è operativo.

Rilevamento degli errori interni

Ad ogni ciclo, il modulo esegue una sequenza di diagnostica degli ingressi. Il modulo elabora il valore di ingresso utilizzando due circuiti identici separati. I due valori vengono confrontati per determinare se nel processo interno del modulo si è verificato un errore interno. Se i valori confrontati sono diversi, il bit `IC` nella struttura DDDT `T_U_DIS_SIS_CH_IN` è impostato a 1 per indicare che non è operativo.

Vedere il diagramma dell'architettura, pagina 146 del modulo di ingresso digitale di sicurezza BMXSDI1602 per una descrizione visiva di questo processo.

Diagnostica del cablaggio del canale

Il cablaggio del sensore al canale di ingresso può essere diagnosticato in modo continuo per rilevare una delle seguenti condizioni:

- conduttore interrotto (circuito aperto)
- cortocircuito a 24 Vcc
- cortocircuito a 0 Vcc
- circuito incrociato tra due canali paralleli

La disponibilità di queste funzioni di diagnostica dipende dalla sorgente di alimentazione utilizzata dalla configurazione di cablaggio specifica, pagina 76, e dalla funzione di diagnostica attivata nella pagina di configurazione del modulo.

Se viene rilevata una di queste condizioni, la struttura DDDT `T_U_DIS_SIS_CH_IN` imposta il valore del bit associato a 1, nel seguente modo:

- il bit `OC` viene impostato a 1 se viene rilevata una condizione di conduttore aperto (interrotto) o di cortocircuito verso terra 0 Vdc.
- il bit `SC` viene impostato a 1 se viene rilevato un cortocircuito alla sorgente 24 Vdc o un circuito incrociato tra due canali.

Diagnostica di sovratensione e sottotensione

Il modulo effettua continuamente test per rilevare condizioni di sovratensione e sottotensione. Valgono i seguenti valori di soglia:

- Soglia di sottotensione = 18,6 Vdc
- Soglia di sovratensione = 33 Vdc

Se viene rilevata una di queste due condizioni, il modulo imposta il bit `PP_STS` nel DDT dispositivo `T_U_DIS_SIS_IN_16` a 0.

Diagnostica dei LED degli ingressi digitali del BMXSDI1602

LED, pannello

Il modulo di ingresso digitale BMXSDI1602 presenta il seguente pannello di LED sul lato frontale:

1 LED di stato del modulo

2 LED di stato canale per rank A

3 LED di errore rilevato sul canale per rank A

4 LED di stato canale per rank B

5 LED di errore rilevato sul canale per rank B

NOTA: Quando viene rilevato un errore di canale, il LED corrispondente resta acceso finché la condizione scatenante non è risolta.

Diagnostica del modulo

Utilizzare i quattro LED nella parte alta del pannello LED per diagnosticare la condizione del modulo di ingresso digitale BMXSDI1602:

LED del modulo				**Stato del modulo**	**Soluzione possibile**
Run	**Err**	**I/O**	**LCK**		
Lampeggio	Lampeggio[1]	Lampeggio[1]	Lampeggio[1]	Autotest all'accensione.	–
Lampeggio	Acceso	Spento	Lampeggio[1]	L'autotest all'accensione ha rilevato un errore interno sui canali di ingresso.	Sostituire il modulo.

LED del modulo				Stato del modulo	Soluzione possibile
Run	**Err**	**I/O**	**LCK**		
Lampeggio	Acceso	Acceso	Lampeggio[1]	• L'autotest all'accensione ha rilevato un errore interno nei canali di ingresso; oppure • Alimentazione 24VCC esterna fuori intervallo	Verificare che l'alimentazione esterna 24 Vcc dei preattuatori sia funzionante e collegare l'alimentazione 24 Vcc.
Spento	Acceso	Spento	Spento	Errore interno rilevato.	Sostituire il modulo se la condizione persiste.
Spento	Lampeggio[1]	Spento	X	Modulo I/O non configurato.	Configurare il modulo tramite la CPU.
X	XX	Acceso	X	• Alimentazione 24 Vcc esterna fuori intervallo; oppure • Errore esterno rilevato su canale di ingresso.	• Verificare che l'alimentazione esterna 24 Vcc dei preattuatori sia funzionante. • Vedere *Diagnostica del canale*, pagina 242.
Acceso	Lampeggio[1]	X	X	Nessuna comunicazione tra CPU e modulo.	Verificare che: • la CPU sia una CPU di sicurezza M580 funzionante; • il backplane sia funzionante (se il modulo I/O si trova sul rack principale); • il cavo tra la CPU e il modulo I/O sia funzionante e collegato correttamente (se il modulo I/O si trova su un rack esteso o remoto).
Acceso	Sfarfallio[2]	X	Spento	Comunicazione non sicura e configurazione non bloccata.	Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 96 per l'istanza del modulo di I/O.
Acceso	Sfarfallio[2]	X	Acceso	Comunicazione non sicura e configurazione bloccata.	• Verificare che la configurazione bloccata nel modulo sia uguale alla configurazione del modulo memorizzata nell'applicazione nella CPU secondo le impostazioni effettuate in Control Expert. • Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 96 per l'istanza del modulo di I/O.

LED del modulo				Stato del modulo	Soluzione possibile
Run	**Err**	**I/O**	**LCK**		
Acceso	Acceso	Spento	X	Rilevato errore interno canale di ingresso.	Sostituire il modulo se la condizione persiste.
Acceso	Spento	OFF	Spento	La comunicazione con la CPU è regolare e la configurazione è sbloccata.	–
Acceso	Spento	Spento	Acceso	La comunicazione con la CPU è regolare e la configurazione è bloccata.	–
X indica che lo stato del LED può essere Acceso o Spento. 1. Lampeggiante: acceso 500 ms /spento 500 ms. 2. Sfarfallio: acceso 50 ms /spento 50 ms.					

Diagnostica del canale

Usare tutti i LED sul modulo di ingresso digitale BMXSDI1602 per diagnosticare lo stato del canale:

LED del modulo				LED dei canali		Stato del canale	Soluzione possibile
Run	**Err**	**I/O**	**LCK**	**Stato del canale (LED 0...7, rank A/B)**	**Errore rilevato (LED 0...7, rank A/B)**		
Acceso	Spento	Spento	X	Acceso	Spento	Stato dell'ingresso ON.	–
Acceso	Spento	Spento	X	Spento	Spento	Stato dell'ingresso OFF.	–
Acceso	Acceso	Spento	X	OFF	Acceso	Stato dell'ingresso OFF. È stato rilevato un errore interno nel canale.	Sostituire il modulo se la condizione persiste.
Acceso	Acceso	Acceso	X	OFF	Acceso	Alimentazione 24 Vdc esterna fuori intervallo.	Verificare che l'alimentazione esterna 24 Vcc dei preattuatori sia funzionante.
Acceso	Spento	Acceso	X	X	Lampeggio[1]	L'ingresso si trova in: • Una condizione di circuito aperto, oppure • Una condizione di cortocircuito con 0 Vcc.	Verificare che il cablaggio sia funzionante e collegato correttamente.

LED del modulo				LED dei canali		Stato del canale	Soluzione possibile
Run	**Err**	**I/O**	**LCK**	**Stato del canale (LED 0...7, rank A/B)**	**Errore rilevato (LED 0...7, rank A/B)**		
Acceso	Spento	Acceso	X	X	Sfarfallio[2]	L'ingresso si trova in: • Una condizione di cortocircuito con 24 Vcc, oppure • Una condizione di cortocircuito con 0 Vcc.	Verificare che il cablaggio sia funzionante e collegato correttamente.
X indica che lo stato del LED può essere Acceso o Spento.							

Diagnostica delle uscite digitali del BMXSDO0802

Introduzione

Questa sezione descrive i tool di diagnostica disponibili per il modulo di uscita digitale di sicurezza BMXSDO0802.

Diagnostica DDDT BMXSDO0802

Introduzione

Il modulo di uscita digitale di sicurezza BMXSDO0802 offre le seguenti funzioni di diagnostica mediante i propri `T_U_DIS_SIS_OUT_8, pagina 111` elementi DDT del dispositivo:

- diagnostica delle uscite
- rilevamento errori interni
- diagnostica del cablaggio del canale
- diagnostica di sovratensione e sottotensione

Diagnostica delle uscite

Ogni canale di uscita viene testato all'inizio di ogni ciclo (o scansione) per verificarne l'efficacia operativa. Il test consiste nella commutazione degli stati dei contatti delle uscite (da ON a OFF, oppure da OFF a ON) per un periodo di tempo troppo breve per provocare una risposta dell'attuatore (meno di 1 ms). Se il canale non commuta correttamente tra lo stato alimentato e lo stato non alimentato, il bit `CH_HEALTH` nella struttura DDDT `T_U_DIS_SIS_CH_OUT, pagina 113` è impostato a 0, per indicare che non è operativo.

Rilevamento degli errori interni

Il modulo elabora il valore di uscita utilizzando due circuiti identici separati. Ogni circuito legge la tensione del punto intermedio sul canale. I due valori vengono confrontati e, se non corrispondono a quelli previsti, viene segnalato un errore interno impostando il bit `IC` nella struttura DDDT `T_U_DIS_SIS_CH_OUT` a 1, per indicare che non è operativo.

Vedere il diagramma dell'architettura, pagina 147 del modulo di uscita digitale di sicurezza BMXSDO0802 per una rappresentazione visiva di questo processo.

Diagnostica del cablaggio del canale

La diagnostica del cablaggio tra l'attuatore e il canale di uscita può essere effettuata in modo continuo per rilevare la presenza di una delle seguenti condizioni:

- conduttore interrotto (circuito aperto)
- cortocircuito a 24 Vcc
- cortocircuito a 0 Vcc
- circuito incrociato tra due canali paralleli
- sovraccarico del canale

  NOTA: Il sovraccarico del canale può essere rilevato solo se l'uscita non è alimentata.

La disponibilità di queste azioni di diagnostica dipende dalla funzione di diagnostica abilitata nella pagina di configurazione del modulo.

Se viene rilevata una di queste condizioni, la struttura DDDT `T_U_DIS_SIS_CH_OUT` imposta il valore del bit associato a 1, nel seguente modo:

- il bit `OC` viene impostato a 1 se viene rilevata una condizione di conduttore aperto (interrotto).
- il bit `SC` viene impostato a 1 se viene rilevato un cortocircuito alla sorgente 24 Vdc o un circuito incrociato tra due canali.
- il bit OL è impostato a 1 se viene rilevato un cortocircuito verso terra 0 Vdc o una condizione di sovraccarico del canale.

Diagnostica di sovratensione e sottotensione

Il modulo effettua continuamente test per rilevare condizioni di sovratensione e sottotensione. Valgono i seguenti valori di soglia:

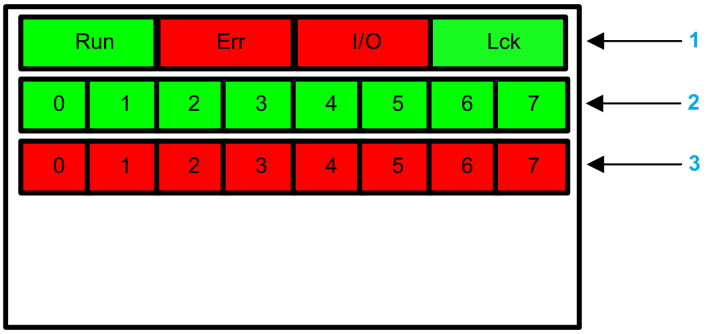
- Soglia di sottotensione = 18 Vdc
- Soglia di sovratensione = 31,8 Vdc

Se viene rilevata una di queste due condizioni, il modulo imposta il bit `PP_STS` nel DDT dispositivo `T_U_DIS_SIS_OUT_8` a 0.

Diagnostica dei LED delle uscite digitali del BMXSDO0802

LED, pannello

Il modulo di uscita digitale BMXSDO0802 presenta il seguente pannello di LED sul frontalino:



1 LED di stato del modulo

2 LED di stato del canale

3 LED di errore rilevati sul canale

NOTA: Quando viene rilevato un errore di canale, il LED corrispondente resta acceso finché la condizione scatenante non è risolta.

Diagnostica del modulo

Utilizzare i quattro LED nella parte alta del pannello LED per diagnosticare la condizione del modulo di uscita digitale BMXSDO0802:

LED del modulo				**Stato del modulo**	**Soluzione possibile**
Run	**Err**	**I/O**	**LCK**		
Lampeggio[1]	Lampeggio[1]	Lampeggio[1]	Lampeggio[1]	Autotest all'accensione.	–
Lampeggio[1]	Acceso	Spento	Lampeggio[1]	L'autotest all'accensione ha rilevato un errore interno sui canali di uscita.	Sostituire il modulo.

LED del modulo				Stato del modulo	Soluzione possibile
Run	**Err**	**I/O**	**LCK**		
Lampeggio[1]	Acceso	Acceso	Lampeggio[1]	• L'autotest all'accensione ha rilevato un errore interno nei canali di uscita; oppure • Alimentazione 24VCC esterna fuori intervallo	Verificare che l'alimentazione esterna 24 Vcc dei preattuatori sia funzionante e collegare l'alimentazione 24 Vcc.
Spento	Acceso	Spento	Spento	Errore interno rilevato.	Sostituire il modulo se la condizione persiste.
Spento	Lampeggio[1]	Spento	X	Modulo I/O non configurato.	Configurare il modulo tramite la CPU.
X	X	Acceso	X	• Alimentazione 24 Vcc esterna fuori intervallo; oppure • Errore esterno rilevato su canale di uscita.	• Verificare che l'alimentazione esterna 24 Vcc dei preattuatori sia funzionante. • Vedere oltre la sezione *Diagnostica del canale*, pagina 248.
Acceso	Lampeggio[1]	X	X	Nessuna comunicazione tra CPU e modulo. Il modulo è nello stato di posizionamento di sicurezza (o in reset se il modulo non è mai stato operativo normalmente).	Verificare che: • la CPU sia una CPU di sicurezza M580 funzionante; • il backplane sia funzionante (se il modulo I/O si trova sul rack principale); • il cavo tra la CPU e il modulo I/O sia funzionante e collegato correttamente (se il modulo I/O si trova su un rack esteso o remoto).
Acceso	Sfarfallio[2]	X	Spento	Comunicazione non sicura e configurazione non bloccata. Il modulo è nello stato di posizionamento di sicurezza (o in reset se il modulo non è mai stato operativo normalmente).	Per verificare le variabili disponibili per effettuare il debug della comunicazione sicura in DDDT
Acceso	Sfarfallio[2]	X	Acceso	Comunicazione non sicura e configurazione bloccata. Il modulo è nello stato di posizionamento di sicurezza.	• Verificare che la configurazione bloccata nel modulo sia uguale alla configurazione del modulo memorizzata nell'applicazione nella CPU secondo le impostazioni effettuate in Control Expert.

LED del modulo				Stato del modulo	Soluzione possibile
Run	**Err**	**I/O**	**LCK**		
					• Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 110 per l'istanza del modulo di I/O.
Acceso	Acceso	Spento	X	Errore interno rilevato su un canale di uscita.	Sostituire il modulo se la condizione persiste.
Acceso	Spento	OFF	Spento	La comunicazione con la CPU è sicura e la configurazione è sbloccata.	–
Acceso	Spento	Spento	Acceso	La comunicazione con la CPU è sicura e la configurazione è bloccata.	–
X indica che lo stato del LED può essere Acceso o Spento. 1. Lampeggiante: acceso 500 ms /spento 500 ms. 2. Sfarfallio: acceso 50 ms /spento 50 ms.					

Diagnostica del canale

Usare tutti i LED sul modulo di uscita digitale BMXSDO0802 per diagnosticare lo stato del canale:

LED del modulo				LED dei canali		Stato del canale	Soluzione possibile
Run	**Err**	**I/O**	**LCK**	**Stato del canale (LED 0...7)**	**Errore rilevato (LED 0...7)**		
Acceso	Spento	Spento	X	Acceso	Spento	Stato dell'uscita ON.	–
Acceso	Spento	Spento	X	OFF	Spento	Stato dell'uscita OFF.	–
Acceso	Acceso	Spento	X	OFF	Acceso	Stato dell'uscita OFF. Rilevato errore interno su canale di uscita.	Sostituire il modulo se la condizione persiste.
Acceso	Acceso	Acceso	X	OFF	Acceso	L'alimentatore esterno 24 Vdc dei preattuatori è fuori intervallo	Verificare che l'alimentatore 24 Vdc sia funzionante.
Acceso	Spento	Acceso	X	Spento	Lampeggio[1]	L'uscita si trova in:	Verificare che il cablaggio sia funzionante e collegato correttamente.

LED del modulo				LED dei canali		Stato del canale	Soluzione possibile
Run	**Err**	**I/O**	**LCK**	**Stato del canale (LED 0...7)**	**Errore rilevato (LED 0...7)**		
						• una condizione di circuito aperto, oppure • una condizione di cortocircuito con 0 Vdc, oppure • sovraccarico di tensione.	
Acceso	Spento	Acceso	X	Acceso	Sfarfallio[2]	L'uscita si trova in: • una condizione di cortocircuito con 24 Vdc, oppure • una condizione di cortocircuito con un altro canale di uscita attivo.	Verificare che il cablaggio sia funzionante e collegato correttamente.

X indica che lo stato del LED può essere Acceso o Spento.

1. Lampeggiante: acceso 500 ms /spento 500 ms.

2. Sfarfallio: acceso 50 ms /spento 50 ms.

Diagnostica delle uscite relè digitali del BMXSRA0405

Introduzione

Questa sezione descrive i tool di diagnostica disponibili per il modulo di uscita relè digitale di sicurezza BMXSRA0405.

Diagnostica DDDT BMXSRA0405

Introduzione

Il modulo di uscita relè digitale di sicurezza BMXSRA0405 offre la seguente diagnostica mediante i propri elementi DDT del dispositivo `T_U_DIS_SIS_OUT_4`, `pagina 128`:

- diagnostica dei contatti di uscita
- rilevamento errori interni

Diagnostica dei contatti di uscita

A seconda del numero di applicazione che è stato configurato per il modulo, il modulo può verificare automaticamente la sua capacità di cambiare gli stati dei contatti di uscita (da ON a OFF o da OFF a ON) per un tempo troppo breve per provocare una risposta dell'attuatore. Se il canale non cambia efficacemente dallo stato alimentato a quello non alimentato, il bit `CH_HEALTH` nella struttura DDDT `T_U_DIS_SIS_CH_ROUT`, `pagina 130` è impostato a 0, a indicare che non è operativo.

NOTA: I numeri di applicazione 2, 4, 6 e 8 eseguono questo test automatico del segnale. I numeri di applicazione 1, 3, 5 e 7 non lo eseguono e pertanto richiedono una transizione manuale quotidiana dello stato del canale di uscita per confermare la sua operatività.

Diagnostica dei comandi di uscita (rilevamento errori interni)

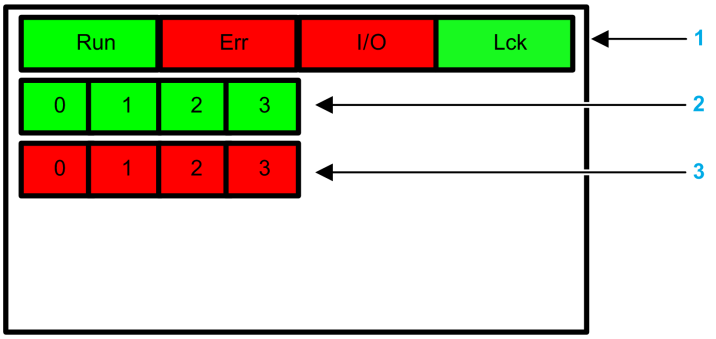
Il comando relè viene elaborato tramite due circuiti paralleli separati. I valori dei circuiti vengono confrontati. Se i valori confrontati sono diversi, il canale viene definito come non operativo e il bit `IC` nella struttura DDDT `T_U_DIS_SIS_CH_ROUT` è impostato a 1.

Per una descrizione visiva di questo processo, vedere il diagramma dell'architettura, pagina 148 del modulo relè di uscita digitale di sicurezza BMXSRA0405.

Diagnostica dei LED delle uscite relè digitali del BMXSRA0405

LED, pannello

Il modulo di uscita relè digitale BMXSRA0405 presenta il seguente pannello di LED sul lato frontale:



1 LED di stato del modulo

2 LED di stato del canale

3 LED di errore rilevati sul canale

NOTA:

- Quando viene rilevato un errore di canale, il LED corrispondente resta acceso finché la condizione scatenante non è risolta.
- Dato che il modulo di uscita relè dispone di quattro canali soltanto, i LED nelle posizioni 4...7 non sono utilizzati e non sono mai accesi.

Diagnostica del modulo

Utilizzare i quattro LED nella parte alta del pannello LED per diagnosticare la condizione del modulo di uscita relè digitale BMXSRA0405:

LED del modulo				**Stato del modulo**	**Soluzione possibile**
Run	**Err**	**I/O**	**LCK**		
Lampeggio[1]	Lampeggio[1]	Lampeggio[1]	Lampeggio[1]	Autotest all'accensione.	–
Lampeggio[1]	Acceso	Lampeggio[1]	Lampeggio[1]	L'autotest all'accensione ha rilevato un errore	–

LED del modulo				Stato del modulo	Soluzione possibile
Run	**Err**	**I/O**	**LCK**		
				interno sui canali di uscita.	
Spento	Acceso	Spento	Spento	Errore interno rilevato.	Sostituire il modulo se la condizione persiste.
Spento	Lampeggio[1]	Spento	X	Modulo I/O non configurato.	Configurare il modulo tramite la CPU.
Acceso	Lampeggio[1]	Spento	X	Nessuna comunicazione tra CPU e modulo. Il modulo è nello stato di posizionamento di sicurezza.	Verificare che: • la CPU sia una CPU di sicurezza M580 funzionante; • il backplane sia funzionante (se il modulo I/O si trova sul rack principale); • il cavo tra la CPU e il modulo I/O sia funzionante e collegato correttamente (se il modulo I/O si trova su un rack esteso o remoto).
Acceso	Sfarfallio[2]	Spento	Spento	Nessuna comunicazione tra CPU e modulo. Il modulo è nello stato di posizionamento di sicurezza (o in reset se il modulo non è mai stato operativo normalmente).	Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 127 per l'istanza del modulo di I/O.
Acceso	Sfarfallio[2]	Spento	Acceso	Comunicazione non sicura e configurazione bloccata. Il modulo è nello stato di posizionamento di sicurezza (o in reset se il modulo non è mai stato operativo normalmente).	• Verificare che la configurazione bloccata nel modulo sia uguale alla configurazione del modulo memorizzata nell'applicazione nella CPU secondo le impostazioni effettuate in Control Expert. • Effettuare il debug della condizione utilizzando le variabili DDDT, pagina 127 per l'istanza del modulo di I/O.
Acceso	Acceso	Spento	X	Errore interno rilevato sul canale di uscita.	Sostituire il modulo se la condizione persiste.
Acceso	Spento	OFF	Spento	La comunicazione con la CPU è sicura e la configurazione è sbloccata.	–

LED del modulo				Stato del modulo	Soluzione possibile
Run	**Err**	**I/O**	**LCK**		
Acceso	Spento	Spento	Acceso	La comunicazione con la CPU è sicura e la configurazione è bloccata.	–
X indica che lo stato del LED può essere Acceso o Spento. 1. Lampeggiante: acceso 500 ms /spento 500 ms. 2. Sfarfallio: acceso 50 ms /spento 50 ms.					

Diagnostica del canale

Usare tutti i LED sul modulo di uscita relè digitale BMXSRA0405 per dignosticare lo stato del canale:

LED del modulo				LED dei canali		Stato del canale	Soluzione possibile
Run	**Err**	**I/O**	**LCK**	**Stato del canale (LED 0...3)**	**Errore rilevato (LED 0...3)**		
Acceso	Spento	Spento	X	Acceso	Spento	Il relè di uscita è chiuso.	–
Acceso	Spento	Spento	X	OFF	Spento	Il relè di uscita è aperto.	–
Acceso	Acceso	Spento	X	OFF	Acceso	Il relè di uscita non è funzionante.	Sostituire il modulo se la condizione persiste.
X indica che lo stato del LED può essere Acceso o Spento.							

Utilizzo di un sistema di sicurezza M580

Introduzione

Questo capitolo fornisce informazioni su come operare un sistema di sicurezza M580.

Aree di processo, sicurezza e dati globali in Control Expert

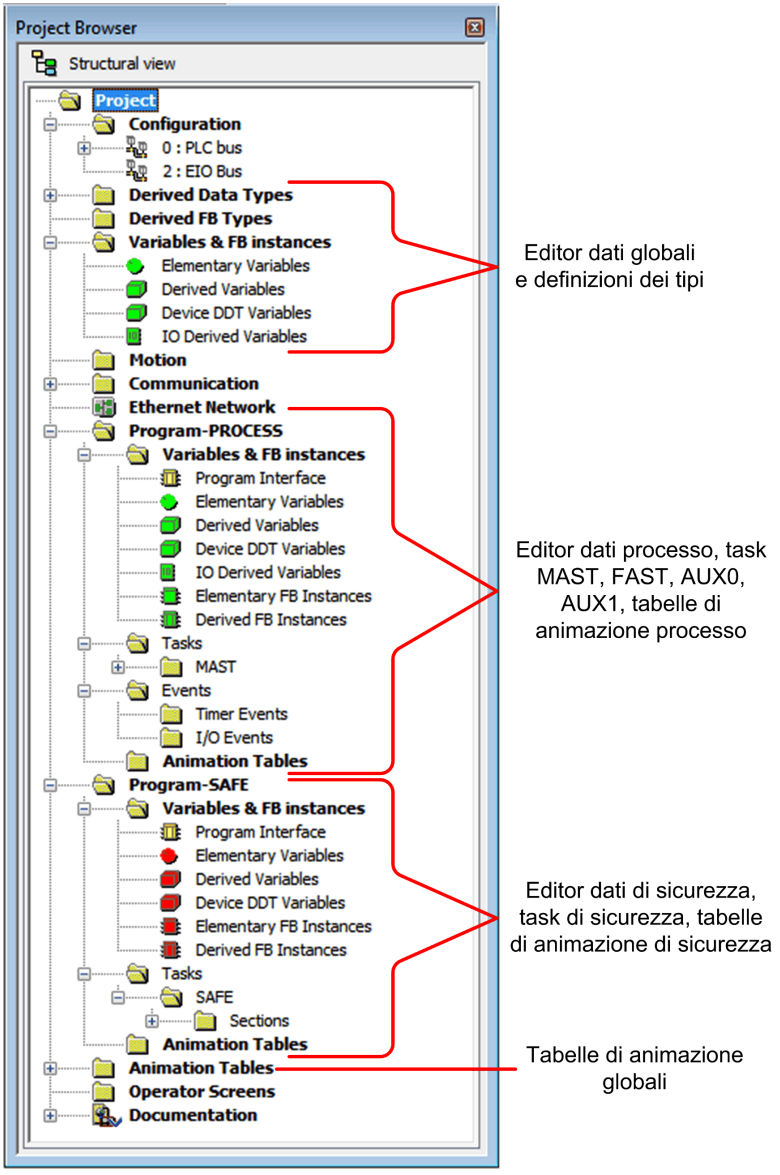
Introduzione

Questa sezione descrive la separazione delle aree dati in un progetto di sicurezza Control Expert M580.

Separazione dei dati in Control Expert

Area dati in Control Expert

La **Vista strutturale** del **Browser del progetto** visualizza la separazione dei dati in Control Expert.. Come indicato di seguito, ogni area dati dispone del proprio editor dati e raccolta di tabelle di animazione:



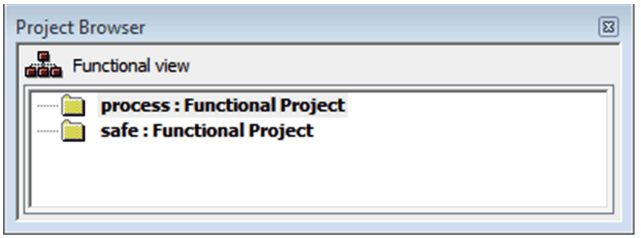
Osservando il **Browser di progetto** si potrà notare che:

- L'area sicura contiene un Editor dei dati di sicurezza, logica di sicurezza e istanze del blocco funzione utilizzati dal task SAFE. Tenere tuttavia presente che:
  - Eventi I/O, eventi timer e subroutine non sono supportati in un programma di sicurezza.
  - Le variabili IODDT non sono supportate dal task SAFE e non sono incluse nell'area di sicurezza.
  - Le icone rosse permettono di identificare le parti SAFE del programma.
- L'area di processo contiene un Editor dei dati di processo, logica di processo e istanze del blocco funzione utilizzati dai task non sicuri (ossia, MAST, FAST, AUX0 e AUX1).
- L'area globale contiene un Editor dati globali, dati derivati e tipi di blocco funzione instanziati nel processo e nei programmi di sicurezza.

  NOTA: Il termine *dati globali* utilizzato in questo argomento si riferisce all'intero ambito, globale, dell'applicazione di oggetti dati in un progetto di sicurezza. Non si riferisce al servizio Global Data supportato da molti moduli Ethernet Schneider Electric.

Browser di progetto nella vista funzionale

La **Vista funzionale** del **Browser di progetto** di Control Expert. per un sistema di sicurezza M580 presenta due progetti funzionali, uno per lo spazio dei nomi del processo, l'altro per lo spazio dei nomi sicuro:



La gestione di ciascun progetto funzionale in un sistema di sicurezza M580 è uguale alla gestione di un progetto nella vista funzionale di un sistema non sicuro M580, tranne per le tabelle di animazione e le sezioni di codice.

Effetto sulla vista strutturale:

Quando si aggiunge una sezione di codice o una tabella di animazione a un progetto funzionale, questo viene associato allo spazio dei nomi di questo progetto funzionale. Aggiungendo una sezione di codice o una tabella di animazione a:

- **processo: Progetto funzionale** il progetto viene associato allo spazio dei nomi di processo del progetto nella vista strutturale.
- **sicuro: Progetto funzionale** il progetto viene associato allo spazio dei nomi sicuro del progetto nella vista strutturale.

Disponibilità delle selezioni di task e linguaggio:

Quando si crea una nuova sezione codice per un progetto funzionale (selezionando **Crea > Nuova sezione...**), le selezioni di **Linguaggio** e **Task** disponibili dipendono dal progetto funzionale:

Quando si crea una nuova sezione codice per un progetto funzionale (selezionando **Crea > Nuova sezione...**), le selezioni di **Linguaggio** e **Task** disponibili dipendono dal progetto funzionale associato:

Progetto funzionale	**Task e linguaggi disponibili**	
	Linguaggi[1]	**Task**[2]
processo: Progetto funzionale	• IL • FBD • LD • segmento LL984 • SFC • ST	• MAST • FAST • AUX0 • AUX1
sicuro: Progetto funzionale	• FBD • LD	• SAFE
1. Selezionato nella scheda **Generale** della finestra di dialogo della nuova sezione. 2. Selezionato nella scheda **Identificazione** della finestra di dialogo della nuova sezione. Per impostazione predefinita, il task MAST è disponibile. Altre sezioni sono disponibili solo per la selezione dopo essere state create nel programma di processo.		

Icone con codifica colore

Per facilitare la distinzione tra le parti sicure e quelle di processo del processo, le parti sicure dell'applicazione sono contrassegnate con icone di colore rosso.

Modalità operative, stati operativi e task

Introduzione

Questa sezione descrive le modalità operative, gli stati operativi e i task supportati dal PAC di sicurezza M580.

Modalità operative del controller M580 Safety

Due modalità operative

Il controller M580 Safety dispone di due modalità operative:

- Modalità di sicurezza: la modalità operativa predefinita per le operazioni di sicurezza.
- Modalità di manutenzione: una modalità operativa opzionale a cui è possibile accedere temporaneamente per eseguire debug e modificare il programma applicativo o cambiare la configurazione.

Il software Control Expert Safety è uno strumento esclusivo che consente di gestire le transizioni tra le modalità operative.

NOTA: l'impostazione della modalità operativa di un controller Hot Standby di sicurezza, modalità di sicurezza o modalità di manutenzione, non è inclusa nel trasferimento di un'applicazione dal controller primario al controller di standby. In caso di commutazione, quando un controller di sicurezza passa da controller di standby a controller primario, la modalità operativa viene impostata automaticamente alla modalità di sicurezza.

Modalità di sicurezza e relative limitazioni

La modalità di sicurezza è la modalità predefinita del controller di sicurezza. Quando si accende il controller di sicurezza con un'applicazione valida presente, il controller entra in modalità di sicurezza. La modalità di sicurezza consente di controllare l'esecuzione della funzione di sicurezza. È possibile caricare, scaricare, avviare e arrestare il progetto in modalità di sicurezza.

Quando il controller M580 Safety funziona in modalità di sicurezza, le funzioni seguenti **non** sono disponibili:

- Download di una configurazione modificata da Control Expert al controller.
- Modifica e/o forzatura dei valori delle variabili e degli stati degli I/O di sicurezza.
- Debug della logica dell'applicazione, per mezzo di punti di interruzioni, punti di controllo ed esecuzione del codice passo passo.

- Utilizzo delle tabelle di animazione o richieste UMAS (ad esempio, da HMI) per scrivere su variabili di sicurezza e I/O di sicurezza.
- Modifica delle impostazioni di configurazione dei moduli di sicurezza tramite CCOTF. (Tenere presente che è supportato l'uso di CCOTF per moduli non interferenti.)
- Esecuzione della modifica online dell'applicazione di sicurezza.
- Impiego dell'animazione collegamento.

  NOTA: In modalità di sicurezza, tutte le variabili di sicurezza e gli stati degli I/O di sicurezza sono di sola lettura. Non è possibile modificare direttamente il valore di una variabile di sicurezza.

È possibile creare una variabile globale e utilizzarla per passare un valore tra una variabile di processo collegato (non sicuro) e una variabile di sicurezza collegata mediante le schede dell'interfaccia dell'Editor dati processo e dell'Editor dati di sicurezza. Dopo aver creato il collegamento, il trasferimento viene eseguito nel modo seguente:

- All'inizio di ciascun task SAFE, i valori della variabile non sicura vengono copiati nelle variabili sicure.
- Al termine del task SAFE, i valori della variabile di uscita sicura vengono copiati nelle variabili non sicure.

Funzionalità modalità manutenzione

La modalità di manutenzione è paragonabile alla modalità normale di un controller M580 non di sicurezza. Viene utilizzata solo per il debug e la regolazione del task SAFE dell'applicazione. La modalità di manutenzione è temporanea perché il controller di sicurezza entra automaticamente in modalità di sicurezza se la comunicazione tra Control Expert e il controller viene persa, oppure viene eseguito un comando di disconnessione. Nella modalità di manutenzione, gli utenti con le autorizzazioni appropriate possono leggere e scrivere nelle variabili di sicurezza e I/O di sicurezza configurati per accettare modifiche.

In modalità di manutenzione, avviene la doppia esecuzione del codice del task SAFE, ma i risultati non vengono confrontati.

Quando il controller M580 Safety funziona in modalità manutenzione, sono disponibili le funzioni seguenti:

- Download di una configurazione modificata da Control Expert al controller.
- Modifica e/o forzatura dei valori delle variabili e degli stati degli I/O di sicurezza.
- Debug della logica dell'applicazione, per mezzo di punti di interruzioni, punti di controllo ed esecuzione del codice passo passo.
- Utilizzo delle tabelle di animazione o richieste UMAS (ad esempio, da HMI) per scrivere su variabili di sicurezza e I/O di sicurezza.
- Modifica della configurazione tramite CCOTF.
- Esecuzione della modifica online dell'applicazione di sicurezza.

- Impiego dell'animazione collegamento.

In modalità di manutenzione, il livello SIL del controller di sicurezza non viene mantenuto.

⚠ AVVERTIMENTO
PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA Adottare le misure appropriate per garantire lo stato di sicurezza definito del sistema mentre il controller di sicurezza è in modalità di manutenzione. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Autorizzazione manutenzione

L'ingresso `%lr.m.c` può essere configurato per autorizzare l'esecuzione del controller di sicurezza in modalità **Manutenzione** come indicato di seguito:

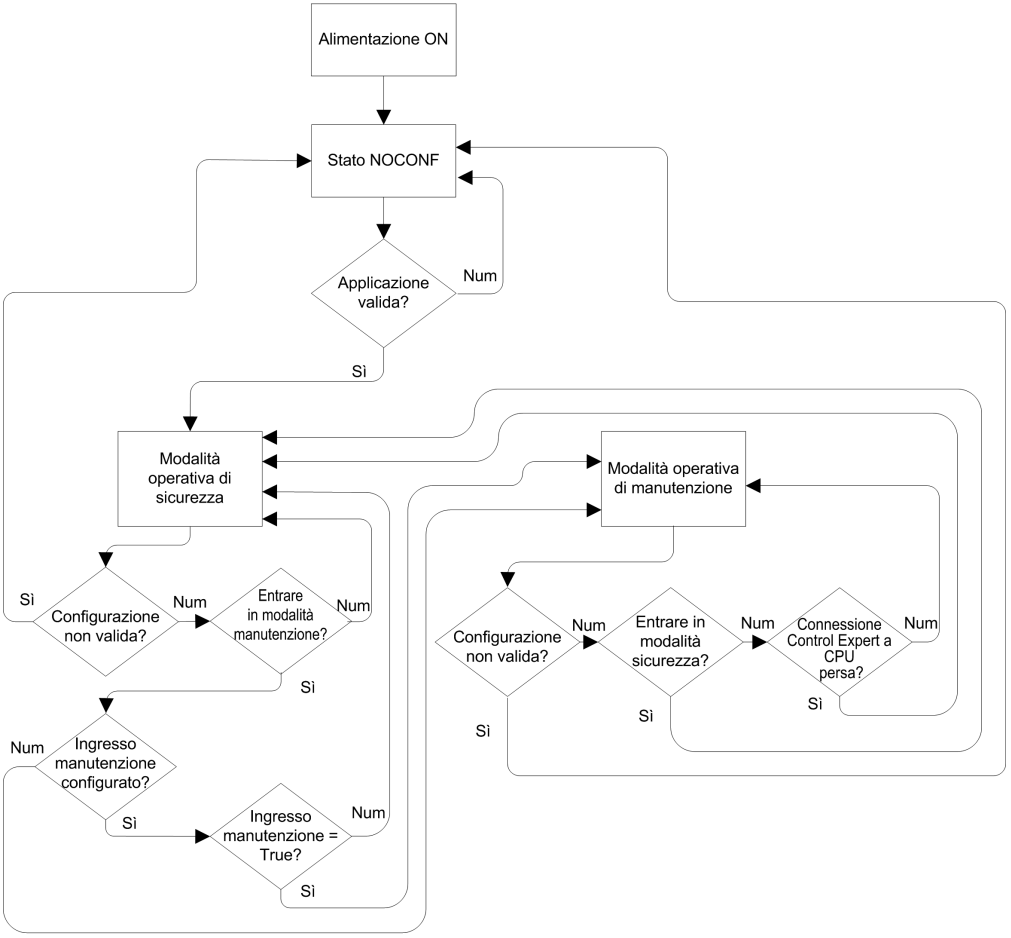
- `%lr.m.c` a 1: il controller di sicurezza può passare alla modalità **Manutenzione**.
- `%lr.m.c` a 0: il controller di sicurezza non può passare alla modalità **Manutenzione**.

  NOTA:

  - Se l'ingresso viene rilevato come in errore, `%lr.m.c` è considerato a 1 (**Manutenzione** commutabile). Per rimuovere questa autorizzazione nella schermata di configurazione, l'ingresso non deve essere rilevato in errore.
  - Il formato di ingresso è `%lr.m.c` o *DDT dispositivo* da un modulo di ingresso non di sicurezza.

Transizioni tra le modalità operative

Lo schema seguente mostra come il controller M580 Safety entri e quindi effettui la transizione tra modalità di sicurezza e di manutenzione:



Quando si alterna tra la modalità di sicurezza e la modalità di manutenzione:

- È corretto passare dalla modalità di manutenzione alla modalità di sicurezza con forzatura attiva. In questo caso, il valore della variabile forzata o lo stato degli I/O resta forzato dopo la transizione e fino a un'altra transizione dalla modalità di sicurezza a quella di manutenzione.

- La transizione dalla modalità di manutenzione alla modalità di sicurezza può essere effettuata nei modi seguenti:
  - Manualmente, tramite comando di menu o barra degli strumenti in Control Expert.
  - Automaticamente, dal controller di sicurezza, quando la comunicazione tra Control Expert e il controller viene persa per circa 50 secondi.
- La funzione ingresso di manutenzione, quando configurata, opera come controllo sulla transizione dalla modalità di sicurezza alla modalità di manutenzione. La funzione ingresso di manutenzione è configurata in Control Expert nella scheda **Configurazione** del controller:
  - Selezionando l'impostazione **Ingresso manutenzione** e
  - Specificando l'indirizzo topologico di un bit di ingresso (%I) per un modulo di ingresso digitale non interferente sul rack locale.

  Quando è configurato l'ingresso di manutenzione, la transizione dalla modalità di sicurezza alla modalità di manutenzione prende in considerazione lo stato del bit di ingresso designato (%I). Se il bit è impostato a 0 (false), il controller è bloccato in modalità di sicurezza. Se il bit è impostato a 1 (true), può verificarsi una transizione alla modalità di manutenzione.

Passaggio tra modalità di sicurezza e modalità di manutenzione in Control Expert

Il passaggio del controller di sicurezza dalla modalità di manutenzione alla modalità di sicurezza non è possibile se:

- Il controller è in modalità debug.
- È attivato un punto di interruzione in una sezione del task SAFE.
- È attivato un punto di controllo in una sezione del task SAFE.

Quando la modalità di debug non è attiva, non è attivato alcun punto di interruzione del task SAFE e non è impostato alcun punto di controllo del task SAFE, è possibile attivare manualmente una transizione tra modalità di sicurezza e modalità di manutenzione nel modo seguente:

- Per passare da modalità di sicurezza a modalità di manutenzione:
  - Selezionare **PLC > Manutenzione**, oppure
  - Fare clic sul pulsante della barra degli strumenti  .
- Per passare da modalità di manutenzione a modalità di sicurezza:
  - Selezionare **PLC > Sicurezza**, oppure
  - Fare clic sul pulsante della barra degli strumenti  .

NOTA: gli eventi di ingresso e uscita dalla modalità di sicurezza sono registrati nel server SYSLOG nel controller.

Determinazione della modalità operativa

È possibile determinare la modalità operativa corrente di un controller M580 Safety che utilizza i LED **SMOD** del controller e del coprocessore oppure Control Expert.

Quando i LED **SMOD** del controller e del coprocessore sono:

- Accesi *lampeggianti*, il controller è in modalità di manutenzione.
- Accesi *fissi*, il controller è in modalità di sicurezza.

Quando Control Expert è collegato al controller, viene identificata la modalità operativa del controller M580 Safety in diversi punti:

- Le parole di sistema %SW12 (coprocessore) e %SW13 (controller), pagina 409 insieme indicano la modalità operativa del controller, come indicato di seguito:
  - se %SW12 è impostata a 16#A501 (hex) e %SW13 è impostata a 16#501A (hex), il controller è in modalità di manutenzione;
  - se una o entrambe le parole di sistema sono impostate a 16#5AFE (hex), il controller è in modalità di sicurezza.
- Le schede secondarie **Task** e **Informazioni** della scheda **Animazione** del controller visualizzano la modalità operativa del controller.
- La barra delle applicazioni, al fondo della finestra principale di Control Expert, indica la modalità operativa come MANUTENZIONE o SICUREZZA.

Stati operativi del controller M580 Safety

Stati operativi

Gli stati operativi del controller M580 Safety sono descritti di seguito.

NOTA: Per una descrizione del rapporto tra stati operativi del controller M580 Safety e quelli del controller M580 Hot Standby, consultare il documento *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente* e le sezioni *Stati del sistema Hot Standby* e *Transizioni e assegnazioni dello stato Hot Standby*.

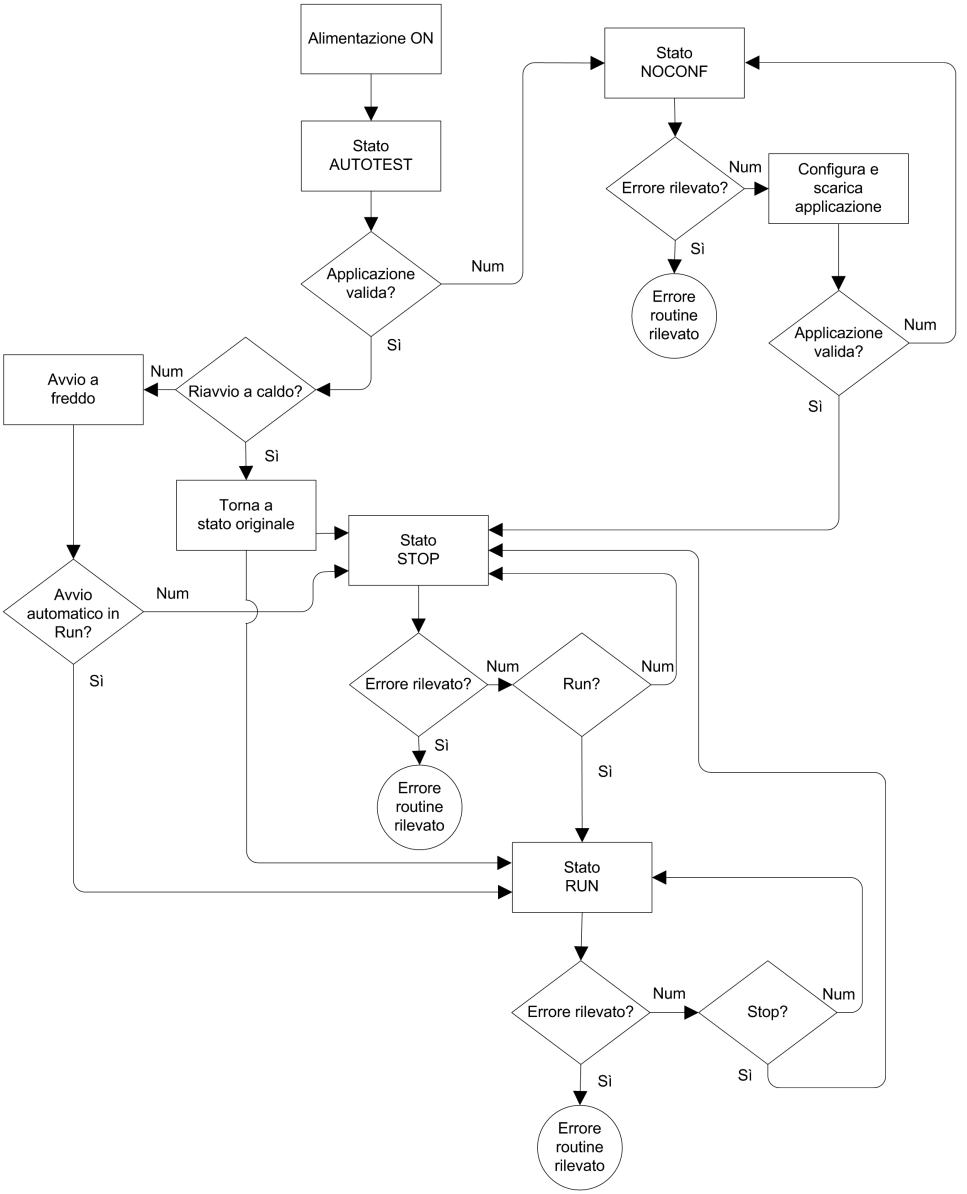
Stato operativo	Si applica a...	Descrizione
AUTOTEST	Controller	Il controller esegue test automatici interni. **NOTA:** se i backplane estesi sono collegati al backplane locale principale e le terminazioni di linea non sono inserite nei connettori inutilizzati sul modulo di estensione del backplane, il controller rimane in AUTOTEST al termine dei test automatici.
NOCONF	Controller	Il programma applicativo non è valido.
STOP	Controller o task	Il controller ha una applicazione valida e non è stato rilevato alcun errore, ma il funzionamento si è interrotto perché: • All'avvio non è impostato **Avvio automatico in Run** (modalità di sicurezza, pagina 260). • L'esecuzione è arrestata dall'esecuzione di un comando STOP (modalità di sicurezza, pagina 260 o manutenzione, pagina 261). • Sono stati impostati punti di interruzione in modalità manutenzione, quindi la connessione tra Control Expert e il controller è stata persa per più di 50 secondi. Il controller legge gli ingressi associati a ciascun task, ma non aggiorna le uscite, che entrano nel loro stato di posizionamento di sicurezza. Il controller può essere riavviato quando l'utente è pronto. **NOTA:** l'emissione di un comando STOP in Control Expert arresta tutti i task. L'evento STOP viene registrato nel server SYSLOG del controller.
HALT	Task	il controller M580 Safety presenta due stati HALT indipendenti: • HALT di processo si applica ai task non SAFE (MAST, FAST, AUX0 e AUX1). Quando un task di processo entra nello stato HALT, anche tutti gli altri task di processo entrano nello stato HALT. Il task SAFE non è influenzato da una condizione di HALT processo. • SAFE HALT si applica solo al task SAFE. I task di processo non sono influenzati da una condizione SAFE HALT. In ogni caso, le operazioni del task vengono interrotte perché è stata rilevata una condizione di blocco, con conseguente condizione ripristinabile, pagina 222. Il controller legge gli ingressi associati a ogni task arrestato, ma non aggiorna le uscite che si trovano nello stato di posizionamento di sicurezza.
RUN	Controller o task	Con un'applicazione valida e nessun errore rilevato, il controller legge gli ingressi associati a ciascun task, esegue il codice associato a ciascun task e aggiorna le uscite associate. • in modalità di sicurezza, pagina 260: la funzione di sicurezza viene eseguita e tutte le limitazioni applicate. • in modalità di manutenzione, pagina 261: il controller funziona come qualsiasi altro controller non di sicurezza. Avviene la doppia esecuzione del codice del task SAFE, ma i risultati non vengono confrontati. **NOTA:** l'emissione di un comando STOP in Control Expert avvia tutti i task. L'evento STOP viene registrato nel server SYSLOG del controller.

Stato operativo	Si applica a...	Descrizione
WAIT	Controller	Il controller è in uno stato transitorio mentre esegue il backup dei dati quando viene rilevata una condizione di disinserzione. Il controller si riavvia solo quando viene ripristinata l'alimentazione e viene rifornita la riserva di energia. WAIT, poiché è uno stato transitorio, potrebbe non essere visibile. Il controller esegue un riavvio a caldo, pagina 273 per uscire dallo stato WAIT.
ERROR	Controller	Il controller viene arrestato perché è stato rilevato un errore hardware o di sistema non ripristinabile, pagina 219. Lo stato ERROR attiva la funzione di sicurezza, pagina 20. Quando il sistema è pronto per il riavvio, eseguire un avvio a freddo, pagina 273 del controller per uscire dallo stato ERROR, spegnendo e riaccendendo o eseguendo un RESET.
OS DOWNLOAD	Controller	È in corso il download del firmware di un controller o coprocessore.

Vedere gli argomenti *Diagnostica LED del controller M580*, pagina 224 e *Diagnostica LED del coprocessore M580 Safety*, pagina 224 per informazioni sugli stati operativi del controller.

Transizioni stato operativo

Le transizioni tra più stati in un controller M580 Safety sono descritte di seguito:



Per informazioni su come vengono gestiti gli errori rilevati dal sistema di sicurezza, consultare *Elaborazione degli errori rilevati*, pagina 269.

Elaborazione degli errori rilevati

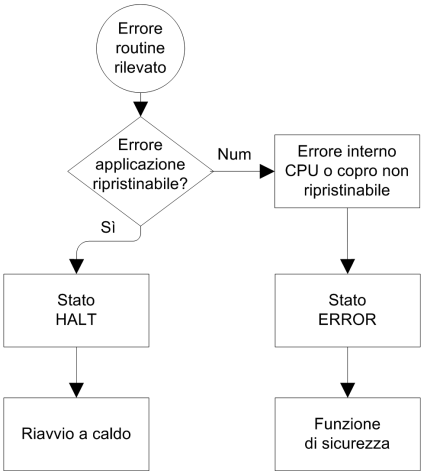
Il controller M580 Safety sicurezza gestisce i seguenti tipi di errori rilevati del controller:

- Errori rilevati dell'applicazione ripristinabili: questi eventi provocano l'ingresso degli eventi correlati nello stato HALT.

  NOTA: poiché i task MAST, FAST e AUX operano nella stessa area di memoria, un evento che provoca l'ingresso di uno di questi task nello stato HALT determina l'ingresso nello stato HALT anche degli altri task non sicuri. Poiché lo stato SAFE opera in un'area di memoria separata, i task non sicuri non vengono influenzati se il task SAFE entra nello stato HALT.

- Errori rilevati dell'applicazione non ripristinabili: errori interni rilevati del controller o del coprocessore: Questi eventi provocano l'ingresso del controller nello stato ERROR. La funzione di sicurezza viene applicata alla parte interessata del loop di sicurezza.

La logica del processo di gestione errori rilevati è descritta di seguito:



L'impatto degli errori rilevati sui singoli task è descritta di seguito:

	Stato del task			
Tipo di errore rilevato	**FAST**	**SAFE**	**MAST**	**AUX**
Overrun watchdog task FAST	HALT	RUN[1]	HALT	HALT
Overrun watchdog task SAFE	RUN	HALT[2]	RUN	RUN
Overrun watchdog task MAST	HALT	RUN	HALT	HALT
Overrun watchdog task AUX	HALT	RUN	HALT	HALT
errore di esecuzione codice doppio controller	RUN	HALT[2]	RUN	RUN
Overrun watchdog di sicurezza[3]	ERROR	ERROR[2]	ERROR	ERROR

Tipo di errore rilevato	Stato del task			
	FAST	SAFE	MAST	AUX
errore interno controller rilevato	ERROR	ERROR[2]	ERROR	ERROR

1. Poiché il task FAST è una priorità più alta del task SAFE, il ritardo del task FAST può provocare l'ingresso del task SAFE nello stato HALT o ERROR invece dello stato RUN.

2. Gli stati ERROR e HALT sul task SAFE provocano l'impostazione delle uscite di sicurezza allo stato configurabile dall'utente (posizionamento di sicurezza o mantenimento).

3. Il watchdog di sicurezza è impostato a 1,5 volte il watchdog del task SAFE.

Visualizzatore di stato di sicurezza della barra dei task

Quando Control Expert è collegato al controller M580 Safety, la barra dei task include un campo che descrive gli stati operativi combinati del task SAFE e dei task di processo (MAST, FAST, AUX0, AUX1), come indicato di seguito:

Stato task di processo	Stato task SAFE	Messaggio
STOP (tutti i task di processo in stato STOP)	STOP	STOP
STOP (tutti i task di processo in stato STOP)	RUN	RUN
STOP (tutti i task di processo in stato STOP)	HALT	SAFE HALT
RUN (almeno un task di processo in stato RUN)	STOP	RUN
RUN (almeno un task di processo in stato RUN)	RUN	RUN
RUN (almeno un task di processo in stato RUN)	HALT	SAFE HALT
HALT	STOP	PROC HALT
HALT	RUN	PROC HALT
HALT	HALT	HALT

Sequenze di avvio

Introduzione

Il controller M580 Safety può accedere alla sequenza di avvio nelle seguenti circostanze:

- All'accensione iniziale.
- In risposta a una interruzione di alimentazione.

In base al tipo di task e al contesto dell'interruzione dell'alimentazione, il controller M580 Safety può eseguire un avvio a freddo, pagina 273 o un avvio a caldo, pagina 273 al ripristino dell'alimentazione.

Avvio iniziale

All'avvio iniziale, il controller M580 Safety esegue un avvio a freddo. Tutti i task, compresi il task SAFE e i task non sicuri (MAST, FAST, AUX0, AUX1), entrano in stato STOP a meno che non sia attivato **Avvio automatico in RUN**, in tale caso tutti i task entrano nello stato RUN.

Avvio dopo un'interruzione dell'alimentazione

L'alimentatore M580 Safety fornisce una riserva di alimentazione che continua ad alimentare tutti i moduli del rack per un massimo di 10 ms in caso di interruzione dell'alimentazione. Quando la riserva di potenza si esaurisce, il controller M580 Safety esegue un ciclo di spegnimento-accensione completo.

Prima di spegnere il sistema, il controller di sicurezza memorizza i seguenti dati che definiscono il contesto operativo allo spegnimento:

- Data e ora dello spegnimento (memorizzate in %SW54...%SW58).
- Stato di ciascun task.
- Stato dei timer evento.
- Valori dei contatori in esecuzione.
- Firma dell'applicazione.
- Dati dell'applicazione (valori correnti delle variabili dell'applicazione)
- Checksum dell'applicazione.

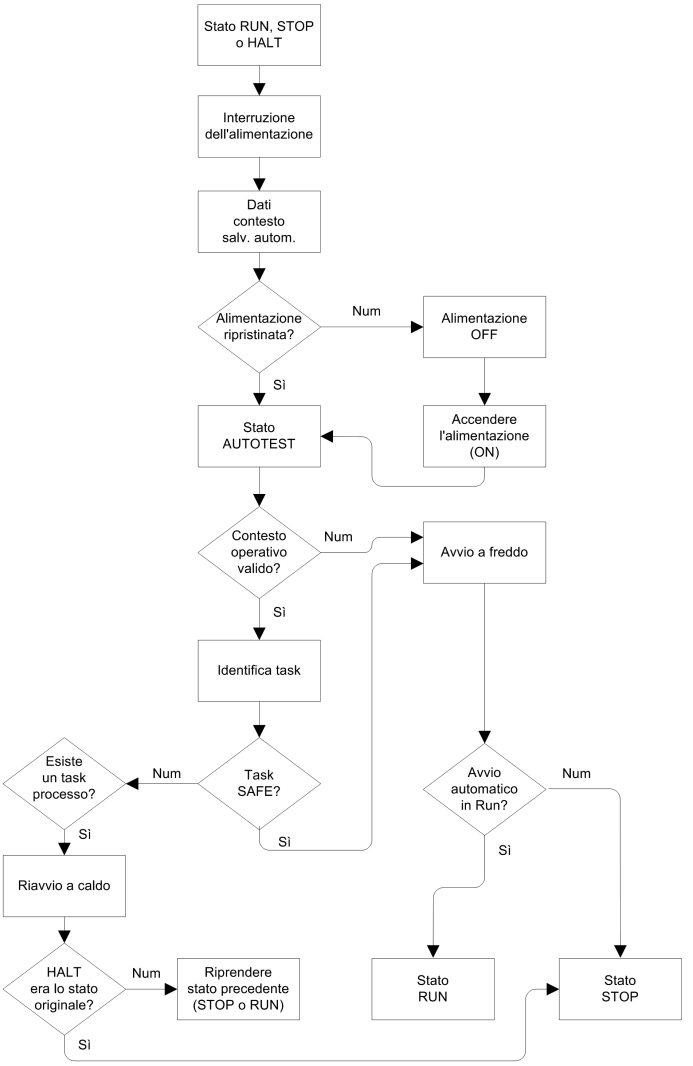
Dopo lo spegnimento, l'avvio può essere automatico (se l'alimentazione è stata ripristinata prima del completamento dell'arresto) o manuale (in caso contrario).

Successivamente, il controller M580 Safety esegue test automatici e verifica la validità dei dati del contesto operativo salvati allo spegnimento, come segue:

- Viene verificato il checksum dell'applicazione.
- Viene letta la scheda di memoria SD per confermare che contenga un'applicazione valida.
- Se l'applicazione nella scheda di memoria SD è valida, vengono controllate le firme per confermare che siano identiche.
- La firma dell'applicazione salvata viene verificata confrontandola con la firma dell'applicazione memorizzata.

Se il contesto operativo è valido, i task non sicuri eseguono un avvio a caldo. Se il contesto operativo non è valido, i task non sicuri eseguono un avvio a freddo. In un caso o nell'altro, il task SAFE esegue un avvio a freddo.

Dopo un'interruzione di alimentazione viene presentata la seguente sequenza di avvio:



Avvio a freddo

Un avvio a freddo provoca l'ingresso nello stato STOP di tutti i task, compresi i task SAFE e non sicuri (MAST, FAST, AUX0, AUX1), a meno che non sia attivato **Avvio automatico in RUN**, in questo caso tutti i task entrano nello stato RUN.

L'avvio a freddo determina le operazioni seguenti:

- Ai dati dell'applicazione (compresi bit interni, dati di I/O, parole interne e così via) vengono assegnati i valori iniziali definiti dall'applicazione.
- Le funzioni elementari vengono impostate ai valori predefiniti.
- I blocchi funzione elementari e le rispettive variabili vengono impostati ai valori predefiniti.
- Bit e parole di sistema vengono impostati ai valori predefiniti.
- Inizializza tutte le variabili forzate applicandone i valori predefiniti (inizializzati).

È possibile eseguire un avvio a freddo per dati, variabili e funzioni nello spazio dei nomi di processo selezionando **PLC > Init** in Control Expert, pagina 289 o impostando il bit di sistema %S0 (COLDSTART) a 1. Il bit di sistema %S0 non ha alcun effetto su dati e funzioni appartenenti allo spazio dei nomi sicuro.

NOTA: A seguito di un avvio a freddo, il task SAFE può avviarsi solo dopo l'avvio del task MAST.

Avvio a caldo

L'avvio a caldo determina per ciascun task di processo, compresi i task (MAST, FAST, AUX0, AUX1), l'ingresso nel relativo stato operativo al momento dell'interruzione di alimentazione. Al contrario, un avvio a caldo determina l'ingresso del task SAFE nello stato STOP, a meno che non sia selezionato **Avvio automatico in RUN**.

NOTA: Se un task era in stato HALT o in un punto di interruzione al momento dell'interruzione di alimentazione, tale task entra nello stato STOP dopo l'avvio a caldo.

L'avvio a caldo determina le operazioni seguenti:

- Ripristina l'ultimo valore conservato per le variabili dello spazio dei nomi di processo.
- Inizializza le variabili dello spazio dei nomi sicuro applicandone i valori predefiniti (inizializzati).
- Inizializza tutte le variabili forzate applicandone i valori predefiniti (inizializzati).
- Ripristina l'ultimo valore conservato per le variabili dell'applicazione.
- Imposta %S1 (WARMSTART) a 1.
- Le connessioni tra il controller e il controller vengono azzerate.
- I moduli di I/O vengono riconfigurati (se necessario) con le rispettive impostazioni memorizzate.

- Gli eventi, il task FAST e i task AUX vengono disattivati.
- Il task MAST viene riavviato dall'inizio del ciclo.
- %S1 viene azzerato al termine della prima esecuzione del task MAST.
- Gli eventi, il task FAST e i task AUX vengono attivati.

Se era in corso l'esecuzione di un task al momento dell'interruzione dell'alimentazione, dopo l'avvio a caldo il task riprende l'esecuzione dall'inizio.

⚠ AVVERTIMENTO
FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA Accertarsi che la selezione di **Avvio automatico in RUN** sia conforme al comportamento corretto del sistema; in caso contrario, disattivare la funzione. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Task del controller M580 Safety

Introduzione

Un controller M580 Safety può eseguire applicazioni con un solo task o con più task. A differenza di un'applicazione a task singolo che esegue solo il task MAST, un'applicazione a più task definisce la priorità di ogni task.

Il controller M580 Safety supporta i seguenti task:

- FAST
- SAFE
- MAST
- AUX0
- AUX1

Caratteristiche dei task

Caratteristiche dei task del controller M580 Safety:

Nome task	Priorità	Modello ora	Intervallo periodo	Periodo predefinito	Campo watchdog	Watchdog predefinito
FAST	1	Periodico	1...255 ms	5 ms	10...500 ms[2]	100 ms[2]
SAFE	2	Periodico	10...255 ms	20 ms	10...500 ms[2]	250 ms[2]
MAST[1]	3	Ciclico[4] o Periodico	1...255 ms	20 ms	10...1500 ms[2]	250 ms[2]
AUX0[3]	4	Periodico	10...2550 ms	100 ms	100...5000 ms[2]	2000 ms[2]
AUX1[3]	5	Periodico	10...2550 ms	200 ms	100...5000 ms[2]	2000 ms[2]

1. Il task MAST è richiesto e non può essere disattivato.

2. Se è attivato CCOTF (selezionando **Modifica online in RUN o STOP** nella scheda **Configurazione** della finestra di dialogo delle proprietà del controller), l'impostazione **Watchdog** minima è 64 ms.

3. Supportato da controller BMEP58•040S Safety standalone. Non supportato da controller BMEH58•040S Safety Hot Standby.

4. I controller BMEP58•040S Safety standalone supportano modelli di tempo ciclici e periodici. I controller BMEH58•040S Safety Hot Standby supportano solo il modello di tempo periodico.

Priorità task

I controller M580 Safety eseguono i task in sospeso in base alla loro priorità. Quando un task è in esecuzione, è possibile interromperlo con un altro task con priorità relativa più alta. Ad esempio, un task periodico, quando è pianificato per l'esecuzione del proprio codice, interrompe un task a priorità più bassa, ma attende fino al completamento di un task a priorità più alta.

Considerazioni sulla configurazione del task

Tutti i task non sicuri (MAST, FAST, AUX0 e AUX1) operano nella stessa area di memoria, mentre il task SAFE opera nella propria area di memoria separata. Risultato:

- Se un task non sicuro eccede il proprio watchdog, tutti i task non sicuri entrano in stato HALT, mentre il task SAFE continua a essere operativo.
- Se il task SAFE supera il proprio watchdog, solo il task SAFE entra in stato HALT, mentre i task non sicuri continuano a essere operativi.

Quando si creano e configurano task per l'applicazione, tenere presente le seguenti caratteristiche del task:

Task SAFE:

Progettare questo task periodico per eseguire solo sezioni di codice correlate alla sicurezza per i moduli I/O di sicurezza. Poiché al task SAFE è assegnata una priorità più bassa del task FAST, l'esecuzione del task SAFE può essere interrotta dal task FAST.

Definire il tempo di esecuzione massimo per il task SAFE impostando il valore appropriato di watchdog. Considerare il tempo richiesto per eseguire il codice e per leggere e scrivere i dati sicuri. Se il tempo per eseguire il task SAFE supera l'impostazione del watchdog, il task SAFE entra nello stato HALT e la parola di sistema %SW125 visualizza il codice di errore rilevato 16#DEB0.

NOTA:

- Poiché il task FAST ha una priorità più alta del task SAFE, è possibile includere un componente per il tempo di ritardo del task FAST nell'impostazione del watchdog del task SAFE.
- Se l'overrun dell'esecuzione del task SAFE è uguale al "Watchdog di sicurezza" (ossia un valore uguale a una volta e mezza l'impostazione del watchdog del task SAFE), il controller e il coprocessore entrano nello stato ERROR e viene applicata la funzione di sicurezza.

Task MAST:

Può essere configurato come ciclico o periodico. Quando si opera in modalità ciclica, definire un tempo di esecuzione massimo immettendo un valore appropriato del watchdog MAST. Aggiungere un piccolo intervallo di tempo a questo valore al termine di ogni ciclo per consentire l'esecuzione di altri task di sistema a bassa priorità. Poiché i task AUX hanno una priorità più bassa di MAST, se questo intervallo di tempo non viene fornito, i task AUX non possono mai essere eseguiti. Considerare l'aggiunta di un intervallo di tempo uguale al 10% del tempo di esecuzione del ciclo, con un minimo di 1 ms e un massimo di 10 ms.

Se il tempo per eseguire il task MAST ciclico supera l'impostazione del watchdog, il task MAST e tutti gli altri task non SAFE entrano in stato HALT e la parola di sistema %SW125 visualizza il codice errore rilevato 16#DEB0.

Quando si opera in modalità periodica, è possibile che il task MAST superi il proprio periodo. In tale caso, il task MAST opera in modalità ciclica e viene impostato il bit di sistema %S11.

Task FAST:

Lo scopo di questo task periodico è di eseguire una parte ad alta priorità dell'applicazione. Definire un tempo di esecuzione massimo impostando il valore di watchdog FAST. Poiché il task FAST interrompe l'esecuzione di tutti gli altri task, compreso il task SAFE, configurare il tempo di esecuzione del task FAST in modo che sia il più breve possibile. Un valore del watchdog del task FAST non deve essere maggiore del periodo FAST.

Il tempo di esecuzione del task FAST non deve superare la metà del periodo configurato per il task SAFE. Se si supera questo limite, il controller può arrestarsi.

Certamente, il tempo di esecuzione del task FAST non deve essere superiore alla metà del periodo configurato del task SAFE, altrimenti il watchdog di sicurezza potrebbe attivare e mettere il sistema in stato ERROR.

Se il tempo per eseguire il task FAST supera l'impostazione del watchdog, il task FAST e tutti gli altri task non SAFE entrano in stato HALT e la parola di sistema %SW125 visualizza il codice errore rilevato 16#DEB0.

Task AUX:

AUX0 e AUX1 sono task periodici opzionali. Il loro scopo è di eseguire una parte a bassa priorità dell'applicazione. I task AUX vengono eseguiti solo al termine dell'esecuzione dei task MAST, SAFE e FAST.

Definire un tempo di esecuzione massimo per i task AUX impostando il valore appropriato di watchdog. Se il tempo per eseguire un task AUX supera l'impostazione del watchdog, il task AUX e tutti gli altri task non SAFE entrano in stato HALT e la parola di sistema %SW125 visualizza il codice errore rilevato 16#DEB0.

Creazione di un progetto di sicurezza M580

Creazione di un progetto di sicurezza M580

Creazione di un progetto di sicurezza M580

Creazione di un progetto di sicurezza M580

Ilmenu **Crea** di Control Expert per Safety presenta tre diversi comandi di creazione e un comando Firma sicura, come indicato di seguito:

Comando	Descrizione
Crea modifiche	Compila solo le modifiche apportate al programma applicativo dal precedente comando di creazione e le aggiunge al programma generato in precedenza.
Ricrea tutto il progetto	Ricompila l'intero programma applicativo, sostituendo il programma creato in precedenza. **NOTA:** Per i moduli I/O di sicurezza M580, questo comando non genera un nuovo valore dell'identificativo esclusivo del modulo (MUID). Al contrario, viene conservato il valore MUID generato in precedenza.
Rinnova ID e Ricrea tutto	Ricompila l'intero programma applicativo, sostituendo il programma creato in precedenza. **NOTA:** • Eseguire questo comando solo quando i moduli I/O di sicurezza sono sbloccati, pagina 286. • Per i moduli I/O di sicurezza M580, questo comando genera un nuovo valore dell'identificativo esclusivo del modulo (MUID) e sostituisce il valore MUID esistente con uno nuovo.
Aggiorna Firma Safe	Da utilizzare per generare manualmente una firma di origini SAFE, pagina 278 per l'applicazione Safe. **NOTA:** Questo comando viene abilitato solo quando il parametro **Generale > Impostazioni crea > Gestione Firma Safe** è impostato su **Su richiesta utente**.

Firma Safe

Introduzione

I controller M580 Safety, standalone e Hot Standby, includono un meccanismo di produzione di un'impronta algoritmica SHA256 dell'applicazione sicura: la firma di origini SAFE. Durante il trasferimento dell'applicazione dal PC al controller, Control Expert confronta la firma di origini SAFE nel PC con la firma di origini SAFE nel controller per determinare se l'applicazione sicura nel PC è uguale o diversa dall'applicazione sicura nel controller.

La funzionalità firma sicura è opzionale. La generazione di una firma di origini SAFE può richiedere molto tempo, in base alla dimensione dell'applicazione sicura. Utilizzando le opzioni di gestione della firma sicura, è possibile generare una firma di origini SAFE che crea un valore algoritmico per l'applicazione sicura

- su ogni creazione oppure
- solo quando si desidera generare manualmente una firma di origini SAFE e aggiungerla alla creazione più recente oppure
- non apportare modifiche

Azioni che modificano la firma di origini SAFE

Sia le modifiche di configurazione che le modifiche di valore di variabili possono causare modifiche alla firma di origini SAFE.

Modifiche della configurazione: Le seguenti azioni di configurazione portano a una modifica della firma:

Dispositivo	**Azione**
Controller di sicurezza	Modificare il codice prodotto del controller tramite **Sostituisci processore...**
	Modificare la versione del controller tramite **Sostituisci processore...**
	Modificare qualsiasi parametro sulle schede di configurazione **Configurazione** o **Hot Standby** del controller.
	Modificare un parametro su una scheda dell'intestazione di comunicazione Ethernet del controller (**Sicurezza**, **Config IP**, **RSTP**, **SNMP**, **NTP**, **Porta Service**, **Sicurezza** ...).
Coprocessore di sicurezza	Non applicabile, in quanto il coprocessore non è configurabile.
Altro modulo di sicurezza	**Aggiungere**/**Eliminare**/**Spostare** un modulo: • Direttamente (con un comando) • Indirettamente (ad esempio, sostituendo un backplane Ethernet a 8 slot con un modulo di sicurezza nello slot 7, con un backplane Ethernet a 4 slot, eliminando quindi un modulo)
	Modifica di un parametro del modulo di sicurezza, situato sulla scheda **Configurazione** (ad esempio **Rilevamento cortocircuito a 24V**, **Rilevamento filo aperto**) e nel riquadro sinistro dell'editor (ad esempio **Funzione**, **Posizionamento di sicurezza**).
	Modifica dell'ID di un modulo tramite il comando **Rinnova ID e Ricrea tutto**.
	Modifica del nome istanza DDT del dispositivo.
Modulo CIP Safety	**Aggiungere**/**Rimuovere** un modulo.

Dispositivo	Azione
	Modifica di un parametro del modulo CIP Safety nell'editor DTM del dispositivo CIP Safety, oppure nell'**Elenco dispositivi** dell'editor DTM master del controller.
	Modifica del nome istanza DDT del dispositivo.
Alimentatore di sicurezza	**Aggiungere**/**Eliminare** un alimentatore di sicurezza.
Altre apparecchiature di sicurezza	Modifica di un indirizzo topologico di un'apparecchiatura di supporto ad un dispositivo di sicurezza, ad esempio: • Spostamento di un rack contenente un dispositivo di sicurezza. • Spostamento di un bus o una derivazione contenente un dispositivo di sicurezza.

Modifiche di valore: Ad eccezione di quanto definito, i seguenti elementi sono inclusi nel calcolo della firma di origini SAFE. Una modifica di tali valori causa una modifica della firma di origini SAFE:

Tipo	Componenti
Programma	Task SAFE e sezioni di codice correlate.
Variabili	Tutte le variabili dell'area sicura e i loro attributi.
DDT	Ciascun attributo DDT sicuro, eccetto quelli di data e di versione.
	Le variabili interne a ciascun DDT, compresi i loro attributi.
	I DDT sicuri, anche se non vengono utilizzati nell'applicazione sicura.
DFB	Ciascun attributo DFT sicuro, eccetto quelli di data e di versione.
	Le variabili interne a ciascun DFB, compresi i loro attributi.
	I DFB sicuri, anche se non vengono utilizzati nell'applicazione sicura.
Impostazioni di ambito sicuro	Tutte le **Impostazioni di progetto** per **Ambito** = sicuro.
Impostazioni di ambito comuni	Le seguenti **Impostazioni di progetto** per **Ambito** = comune:
	Variabili • Consenti cifre iniziali • Set di caratteri • Consenti l'uso di fronte EBOOL • Consenti INT/DINT al posto di ANY_BIT • Consenti estrazione bit di BYTE, INT, UINT, DINT, UDINT, WORD e DWORD • Variabili array rappresentate direttamente • Attiva analisi veloce per il trending • Forza inizializzazione riferimenti
	Programma > Linguaggi > Comune

Tipo	Componenti
	• Consenti procedure • Consenti commenti annidati • Consenti assegnazioni multiple [a:=b:=c;] (ST/LD) • Consenti parametri vuoti in chiamata non formale (ST/IL) • Mantieni collegamenti di output su EF disattivato (EN=0) • Visualizza commenti completi dell'elemento di struttura
	Programma > Linguaggi > LD • Rilevamento fronte di scansione singolo per EBOOL
	Generale > Tempo[1] • Fuso orario personalizzato • Fuso orario • Offset ora • Passa automaticamente all'ora legale ◦ Tutte le impostazioni START e END sotto Regola automaticamente per l'ora legale
1. Queste variabili non vengono esportate, ma qualsiasi modifica dei loro valori modifica la firma parziale della configurazione.	

Gestione della firma di origini SAFE

La firma di origini SAFE è gestita in Control Expert nella finestra **Strumenti > Impostazioni di progetto** selezionando **Generale > Impostazioni creazione**, quindi selezionando una delle seguenti impostazioni di **Gestione firma sicura**:

- **Automatico** (predefinito): genera una nuova firma di origini SAFE ogni volta che si esegue un comando **Crea**.
- **Su richiesta dell'utente**: genera una nuova firma di origini SAFE quando viene eseguito il comando **Crea > Aggiorna Firma sicura**.

  NOTA: Se si seleziona **Su richiesta dell'utente**, Control Expert genera una firma di origini sicura pari a 0 per ogni creazione. Se non si esegue il comando **Crea > Aggiorna Firma sicura**, si sceglie di non utilizzare la funzionalità Firma sicura.

Trasferimento di un'applicazione dal PC al controller

Quando si scarica un'applicazione dal PC al controller, Control Expert confronta la firma di origini sicure nell'applicazione scaricata con una presente nel controller. Control Expert si comporta come segue:

Nuova firma sicura	Firma sicura controller	Control Expert visualizza
Qualsiasi	Nessuna applicazione	Conferma trasferimento
Qualsiasi (eccetto 0)	0	Conferma trasferimento
0	0	Conferma trasferimento
0	Qualsiasi (eccetto 0)	Conferma trasferimento, seguito da un avviso “Ciò causerà un reset della Firma sicura”, seguito da una nuova conferma di trasferimento
XXXX = YYYY[2]	YYYY	Conferma trasferimento
XXXX ≠ YYYY[3]	YYYY	Conferma trasferimento, seguito da un avviso “Ciò causerà una modifica della Firma sicura”, seguito da una nuova conferma di trasferimento
1. Il valore "0" indica che una firma di origini SAFE non è stata generata automaticamente o manualmente. 2. L'applicazione sicura nel PC (XXXX) e l'applicazione sicura nel controller (YYYY) sono UGUALI. 3. L'applicazione sicura nel PC (XXXX) e l'applicazione sicura nel controller (YYYY) sono DIVERSE.		

Visualizzazione della firma di origini SAFE

Quando viene utilizzata, la firma di origini SAFE consiste di una serie di valori esadecimali e può essere molto lunga, rendendo difficoltosa la lettura diretta e il confronto del valore da parte dell'utente. Tuttavia, è possibile copiare e incollare la firma di origini SAFE in uno strumento di testo adeguato per effettuare confronti. La firma di origini SAFE può essere trovato in una delle seguenti destinazioni Control Expert:

- scheda (vedere EcoStruxure™ Control Expert, Modalità di funzionamento) **Proprietà del progetto > Identificazione**: Nel **Browser di progetto**, fare clic con il pulsante destro del mouse su **Progetto** e selezionare **Proprietà**.
- scheda (vedere EcoStruxure™ Control Expert, Modalità di funzionamento) **Schermata PLC > Informazioni**: Nel **Browser di progetto**, selezionare **Progetto > Configurazione > Bus PLC > <CPU>**, fare clic con il pulsante destro del mouse e selezionare **Apri**, quindi selezionare la scheda **Animazione**.
- Finestra di dialogo (vedere EcoStruxure™ Control Expert, Modalità di funzionamento) **Confronto PC < - - > PLC**: Selezionare questo comando dal menu **PLC**.
- Finestra di dialogo (vedere EcoStruxure™ Control Expert, Modalità di funzionamento) **Trasferisci progetto a PLC**: Selezionare questo comando dal menu **PLC** (o nella finestra di dialogo **Confronto PC < - - > PLC**.

Confronto tra la firma di origini SAFE e SAId

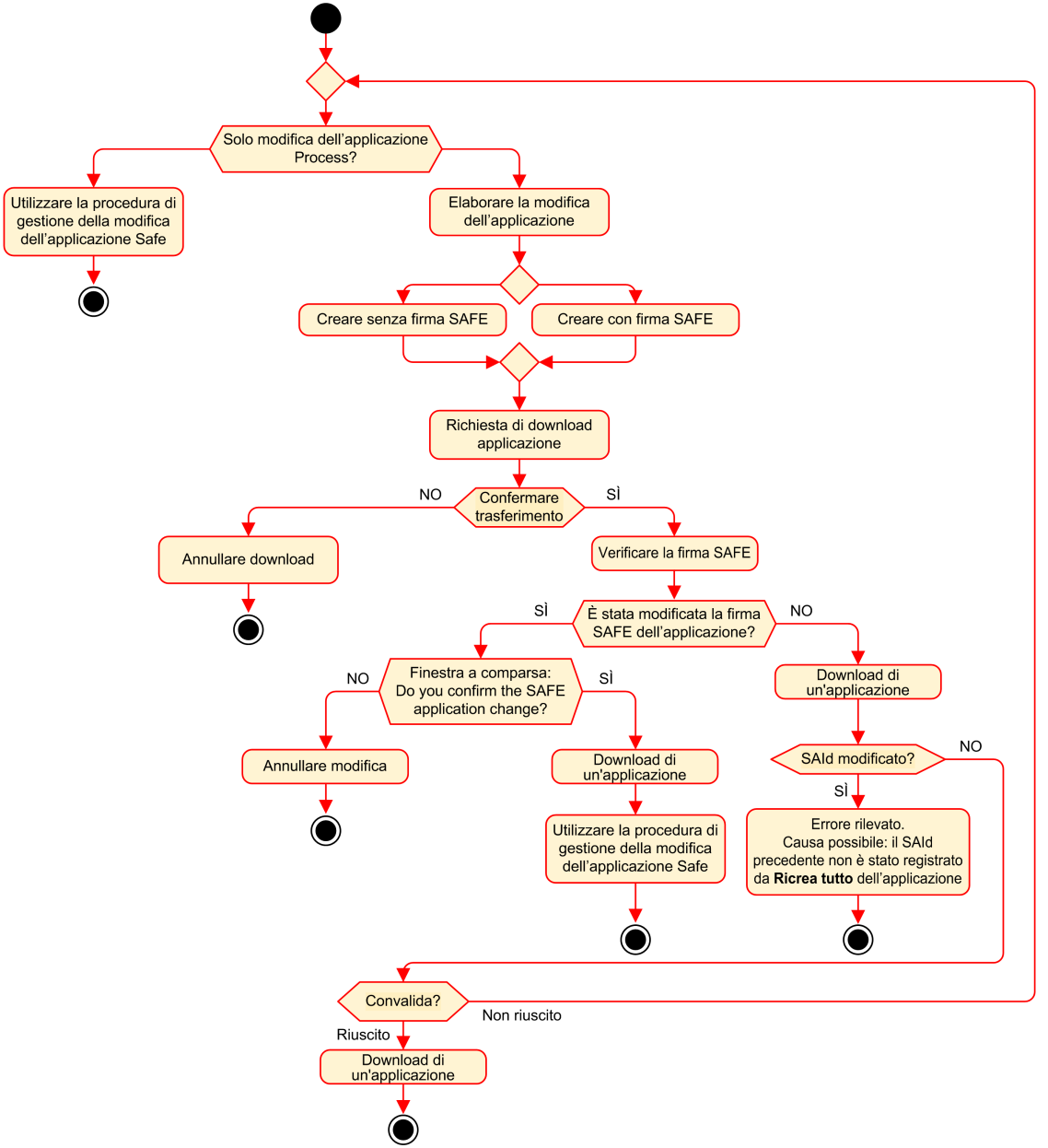
La firma di origini SAFE è stata creata per fornire una verifica *a priori* che l'applicazione non sia stata modificata. Utilizzare questa funzione ogni volta che l'applicazione di processo viene modificata, pagina 284 per evitare modifiche involontarie dell'applicazione sicura.

La firma di origini SAFE è un meccanismo affidabile, ma non è sufficiente per le applicazioni di sicurezza perché lo stesso codice sorgente può corrispondere a diversi codici binari (eseguibili), in base al tipo di creazione utilizzata dopo l'ultima modifica del codice sicuro.

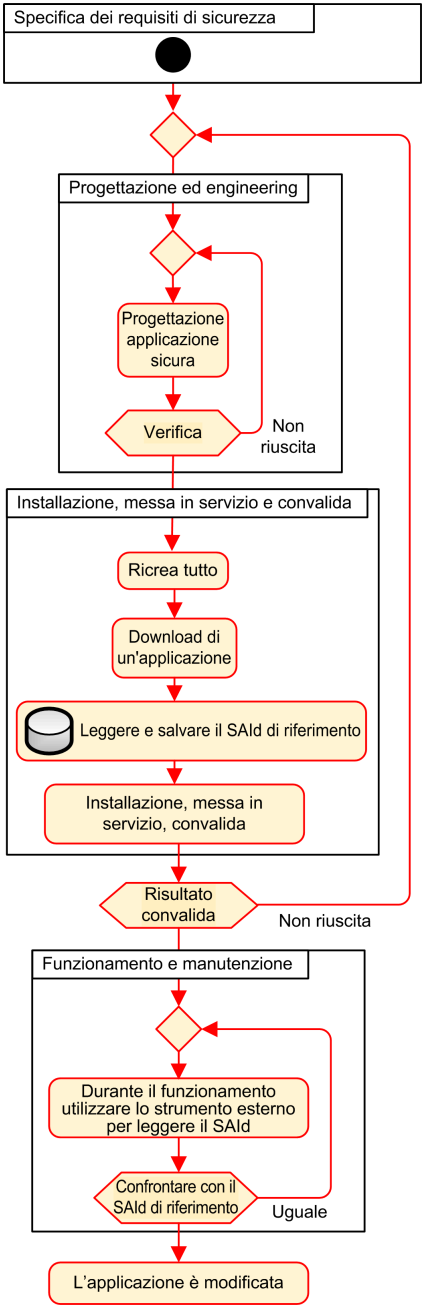
SAId, pagina 376 può essere valutato solo in fase di runtime. Il calcolo viene eseguito due volte e confrontato dal controller e dal coprocessore, in base al codice binario eseguito dall'applicazione sicura. Poiché SAId è sensibile a tutte le modifiche, incluse quelle che possono essere introdotte da un comando **Ricrea tutto** dopo una modifica di creazione, utilizzare un comando **Ricrea tutto** per generare una versione di riferimento dell'applicazione sicura. Questo processo, pagina 285 consente di utilizzare qualsiasi forma di creazione (**Ricrea tutto**, **Crea modifiche** online o offline) per le modifiche dell'applicazione di processo senza alcuna modifica apportata al SAId.

SAId è il metodo utilizzato per confermare che l'applicazione sicura è quella convalidata. Il valore SAId non viene verificato automaticamente dall'applicazione. Per questo motivo, verificare regolarmente SAId (ad esempio, utilizzando Control Expert o un HMI) leggendo l'uscita del blocco funzione S_SYST_STAT_MX o il contenuto della parola di sistema % SW169, pagina 409.

Modifiche del Processo semplificato di applicazione di processo



Gestione SAId



Blocco delle configurazioni del modulo I/O M580 di sicurezza

Blocco delle configurazioni del modulo I/O M580 Safety

Blocco della configurazione del modulo I/O di sicurezza

Ogni modulo I/O di sicurezza dispone di un pulsante di blocco configurazione (vedere Modicon M580, Guida alla pianificazione del sistema di sicurezza), in alto nella parte anteriore del modulo. Lo scopo della funzione di blocco è impedire modifiche indesiderate alla configurazione del modulo I/O. Ad esempio, il blocco della configurazione corrente del modulo I/O può impedire il tentativo di assegnare al modulo una configurazione falsa o semplicemente proteggere da errori di configurazione.

Per raggiungere il livello di sicurezza integrata (SIL) previsto, bloccare ogni modulo I/O di sicurezza dopo averlo configurato, ma prima di iniziare o riprendere le operazioni.

⚠AVVERTIMENTO

PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Bloccare ogni modulo I/O di sicurezza dopo averlo configurato ma prima di iniziare le operazioni.

Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

I meccanismi di blocco e sblocco funzionano come segue:

- Per bloccare la configurazione di un modulo I/O di sicurezza, tenere premuto il pulsante di blocco per oltre 3 secondi, quindi rilasciare il pulsante.
- Per sbloccare la configurazione di un modulo I/O di sicurezza, tenere premuto il pulsante di blocco per oltre 3 secondi, quindi rilasciare il pulsante.

Scenari per il blocco delle configurazioni del modulo I/O di sicurezza

La procedura da seguire per bloccare le configurazioni dei moduli I/O di sicurezza SIL3 varia in base allo scenario, che può essere:

- Prima configurazione dei moduli I/O
- Sostituzione dispositivo veloce dei moduli I/O

- Eseguire una modifica della configurazione al volo (CCOTF) per i moduli I/O

La procedura per ogni scenario è descritta di seguito.

Prima configurazione dei moduli di sicurezza I/O SIL3:

Passo	Azione
1	Collegare Control Expert al controller M580 Safety.
2	Utilizzare il comando **Trasferimento progetto dal PLC** per caricare il progetto dal controller in Control Expert.
3	Nella finestra **Bus PLC** in Control Expert, aprire ogni modulo I/O di sicurezza SIL3 e confermare che ogni modulo è configurato correttamente.
4	In una tabella di animazione in Control Expert, visualizzare il DDDT per ogni modulo I/O di sicurezza SIL3 e confermare che la configurazione di ogni modulo è la stessa del passo 3 precedente.
5	Bloccare la configurazione di ogni modulo I/O SIL3 tenendo premuto il pulsante di blocco configurazione (vedere Modicon M580, Guida alla pianificazione del sistema di sicurezza) per più di 3 secondi, quindi rilasciare il pulsante.
6	Verificare nella tabella di animazione la validità dello stato del bit di blocco (CONF_LOCKED) per ogni modulo I/O SIL3.

Sostituzione dispositivo veloce di un modulo di sicurezza I/O SIL3:

Passo	Azione
1	Sostituire il modulo I/O di sicurezza SIL3 con uno nuovo.
2	Collegare Control Expert al controller M580 Safety in modalità operativa di manutenzione, pagina 261.
3	Nella finestra **Bus PLC** in Control Expert, aprire ogni modulo I/O di sicurezza SIL3 e confermare che ogni modulo è configurato correttamente.
4	In una tabella di animazione in Control Expert, visualizzare il DDDT per ogni modulo I/O di sicurezza SIL3 e confermare che la configurazione di ogni modulo non è cambiata ed è la stessa del passo 3 precedente.
5	Bloccare la configurazione di ogni modulo I/O SIL3 tenendo premuto il pulsante di blocco configurazione (vedere Modicon M580, Guida alla pianificazione del sistema di sicurezza) per più di 3 secondi, quindi rilasciare il pulsante.
6	Verificare nella tabella di animazione la validità dello stato del bit di blocco (CONF_LOCKED) per ogni modulo I/O SIL3.

Esecuzione di CCOTF per aggiungere un nuovo modulo di sicurezza I/O SIL3:

Passo	Azione
1	Collegare Control Expert al controller M580 Safety in modalità operativa di manutenzione, pagina 261.
2	Aggiungere un nuovo modulo di I/O di sicurezza SIL3 alla configurazione e modificarne le impostazioni se necessario.
3	Eseguire il comando **Crea > Crea modifiche**.
4	Nella finestra **Bus PLC** in Control Expert, aprire ogni modulo I/O di sicurezza SIL3 e confermare che ogni modulo è configurato correttamente.
5	In una tabella di animazione in Control Expert, visualizzare il DDDT per ogni modulo I/O di sicurezza SIL3 e confermare che la configurazione di ogni modulo non è cambiata ed è la stessa del passo 3 precedente.
6	Bloccare la configurazione di ogni modulo I/O SIL3 tenendo premuto il pulsante di blocco configurazione (vedere Modicon M580, Guida alla pianificazione del sistema di sicurezza) per più di 3 secondi, quindi rilasciare il pulsante.
7	Verificare nella tabella di animazione la validità dello stato del bit di blocco (CONF_LOCKED) per ogni modulo I/O SIL3.
8	Nel menu **PLC** di Control Expert, comandare al controller di entrare in modalità di sicurezza, pagina 260.

Inizializzazione dei dati in Control Expert

Inizializzazione dei dati in Control Expert per il PAC M580 Safety

Due comandi di Init

Il menu **PLC** in Control Expert fornisce due comandi separati per l'inizializzazione dei dati:

- Il comando **Init** inizializza i dati per lo spazio dei nomi di processo (o non sicuro), utilizzabile dai task MAST, FAST, AUX0 e AUX1. È possibile eseguire questo comando se il PAC opera in modalità di sicurezza o manutenzione mentre il PAC è in stato STOP. Questo comando è analogo all'impostazione a 1 del bit di sistema %S0 (COLDSTART).

  NOTA: Impostando il bit %S0 a 1 si inizializzano i dati solo nello spazio dei nomi di processo. Non si influisce sui dati nello spazio dei nomi sicuro.

- Il comando **Iniz sicurezza** inizializza i dati solo per lo spazio dei nomi sicuro, dati utilizzabili esclusivamente dal task SAFE. È possibile eseguire questo comando solo se il task SAFE opera in modalità di manutenzione, mentre il task SAFE è in stato STOP o HALT. L'esecuzione di questo comando quando il task SAFE è in stato HALT determina il riavvio del task SAFE nello stato STOP.

Entrambi i comandi **Init** e **Iniz sicurezza** eseguono un avvio a freddo., pagina 273

Lavorare con le tabelle di animazione in Control Expert

Tabelle di animazione e schermate operatore

Introduzione

Un controller M580 Safety supporta tre tipi di tabelle di animazione, ciascuna associata a una delle seguenti aree dati:

- Le tabelle di animazione dell'area processo possono includere solo i dati nello spazio dei nomi processo.
- Le tabelle di animazione dell'area di sicurezza possono includere solo i dati nello spazio dei nomi sicuro.
- Le tabelle di animazione globali possono includere dati per l'intera applicazione, compresi i dati creati per gli spazi dei nomi sicuro e processo e variabili globali.

  NOTA: in una tabella di animazione globale, i nomi della variabile dati includono un prefisso che indica lo spazio dei nomi sorgente, come segue:

  - Una variabile dati dallo spazio dei nomi Sicuro viene visualizzata come "SAFE.<nomevariabile>".
  - Una variabile dati dallo spazio dei nomi Processo viene visualizzata come "PROCESS.<nome variabile>".
  - Una variabile dati dallo spazio dei nomi Globale (o Applicazione) visualizza solo il proprio <nome variabile>, senza prefisso dello spazio dei nomi.

I dati di processo e i dati di sicurezza di un controller M580 Safety sono accessibili anche da processi esterni (ad esempio, SCADA o HMI).

La possibilità di creare e modificare una tabella di animazione e la possibilità di eseguirne le funzioni dipendono dallo spazio dei nomi delle variabili interessate e dalla modalità operativa del progetto di sicurezza.

Condizioni per creare e modificare le tabelle di animazione

La creazione e modifica delle tabelle di animazione coinvolge l'aggiunta o la rimozione delle variabili dati. La possibilità di aggiungere variabili dati alla tabella di animazione o di eliminarle dipende da:

- Spazio dei nomi (sicuro o processo) in cui risiede la variabile dati.
- Modalità operativa (sicurezza o manutenzione) del controller M580 Safety.

Quando Control Expert è collegato al controller M580 Safety, è possibile creare e modificare le tabelle di animazione come segue:

- L'aggiunta o l'eliminazione di variabili dello spazio dei nomi processo a una tabella di animazione processo o globale è supportata mentre il controller M580 Safety opera in modalità sicura o in modalità di manutenzione.
- L'aggiunta o l'eliminazione di variabili dello spazio dei nomi da una tabella di animazione di sicurezza è supportata mentre il controller M580 Safety funziona in modalità di manutenzione.
- L'aggiunta o l'eliminazione di variabili dello spazio dei nomi da una tabella di animazione di sicurezza è supportata mentre il controller M580 Safety funziona in modalità di sicurezza solo se le impostazioni del progetto non includono tabelle di animazione nelle informazioni di caricamento.

  NOTA: le tabelle di animazione sono incluse o escluse dalle informazioni di caricamento in Control Expert selezionando **Strumenti > Impostazioni progetto...** per aprire la finestra **Impostazioni progetto...**, quindi selezionando **Impostazioni progetto > Generale > Dati integrati PLC > Informazioni di caricamento > Tabelle di animazione**.

Condizioni per il funzionamento delle tabelle di animazione

È possibile utilizzare le tabelle di animazione per forzare il valore di una variabile, annullare la forzatura del valore di una variabile, modificare un singolo valore di variabile o modificare più valori di variabili. La possibilità di eseguire queste funzioni dipende dallo spazio dei nomi in cui risiede una variabile e dalla modalità operativa del controller M580 Safety, come indicato di seguito:

- I valori della variabile di processo o globale possono essere letti o scritti in modalità operativa di sicurezza e manutenzione.
- I valori della variabile di sicurezza possono essere letti o scritti in modalità operativa di manutenzione
- I valori della variabile di sicurezza possono solo essere letti in modalità operativa di sicurezza.

Processo per la creazione di tabelle di animazione nello spazio dei nomi di processo o di sicurezza in Control Expert

Control Expert fornisce due modi per creare tabelle di animazione per lo spazio dei nomi di sicurezza o di processo:

- Da una finestra della sezione codice di sicurezza o processo, fare clic con il pulsante destro del mouse nella finestra codice, quindi selezionare:
  - **Inizializza tabella di animazione** per aggiungere l'oggetto dati a una tabella di animazione esistente nello spazio dei nomi di sicurezza o di processo, oppure
  - **Inizializza nuova tabella di animazione** per aggiungere l'oggetto dati a una nuova tabella di animazione nello spazio dei nomi di sicurezza o di processo.

  In ciascun caso, tutte le variabili nella sezione codice vengono aggiunte alla tabella di animazione nuova o esistente.
- Dal **Browser di progetto**, nell'area dati di processo o di sicurezza, fare clic con il pulsante destro del mouse sulla cartella **Tabelle di animazione** quindi selezionare **Nuova tabella di animazione**. Control Expert crea una nuova tabella di animazione vuota. È quindi possibile aggiungere singole variabili dallo spazio dei nomi (sicurezza o processo) correlato alla tabella.

Processo per creare tabelle di animazioni con ambito globale

Creare una tabella di animazione globale nel **Browser di progetto** facendo clic con il pulsante destro del mouse sulla cartella **Tabelle di animazione**, quindi selezionare **Nuova tabella di animazione**. È possibile aggiungere variabili alla nuova tabella di animazione in modi diversi:

- *Trascinamento della selezione*: è possibile trascinare una variabile da un editor di dati e rilasciarla nella tabella di animazione globale. Poiché l'ambito della tabella di animazione include l'intera applicazione, è possibile trascinare la variabile dall'**Editor dati di sicurezza**, dall'**Editor dati di processo** o dall'**Editor dati globali**.
- *Finestra di dialogo Selezione istanza*: è possibile fare doppio clic in una riga della tabella di animazione, quindi fare clic sul pulsante con i puntini di sospensione per aprire la finestra di dialogo **Selezione istanza**. Utilizzare l'elenco di filtraggio nella parte in alto a destra della finestra di dialogo per selezionare una delle seguenti aree di progetto:
  - SICURO: per visualizzare gli oggetti dati associati all'area di sicurezza.
  - PROCESSO: per visualizzare gli oggetti dati associati all'area di processo.
  - APPLICAZIONE: per visualizzare gli oggetti dati di ambito applicazione di più alto livello.

  Selezionare un oggetto dati, quindi fare clic su **OK** per aggiungere la voce alla tabella di animazione.

NOTA: gli oggetti dati aggiunti a una tabella di animazione globale da:

- Area Processo hanno il prefisso “PROCESS” che precede il nome della variabile (ad esempio PROCESS.variable_01
- Area Sicurezza hanno il prefisso “SAFE” che precede il nome della variabile (ad esempio SAFE.variable_02
- L'area Globale non ha alcun prefisso aggiunto al nome della variabile.

Visualizzazione dei dati sulle schermate operatore

È possibile visualizzare i dati su una schermata dell'operatore, ad esempio un'applicazione HMI, SCADA o FactoryCast, nello stesso modo in cui si collegano i dati in una tabella di animazione. Le variabili di dati disponibili per la selezione sono quelle incluse nel dizionario dati di Control Expert.

È possibile attivare il dizionario dati aprendo la finestra **Strumenti > Impostazioni progetto...**, quindi nell’area **Ambito > comune** della finestra, selezionando **Generale > Dati integrati PLC > Dizionario dati**.

Il dizionario dati rende le variabili dati disponibili nelle schermate operatore come segue:

- Le variabili dello spazio dei nomi sicuro includono sempre il prefisso "SAFE" e possono essere raggiunte solo mediante il formato "SAFE.<nome variabile>".
- Le variabili dello spazio dei nomi applicazione o globale non comprendono prefisso e possono essere raggiunte solo utilizzando il “<nome variabile>” senza prefisso.
- L’impostazione **Uso dello spazio dei nomi di processo** determina come una schermata operatore può raggiungere le variabili dello spazio dei nomi Processo.
  - Se si seleziona **Uso dello spazio dei nomi di processo**, la schermata operatore può leggere le variabili dell'area di processo solo mediante il formato "PROCESS. <nome variabile>".
  - Se si deseleziona **Uso dello spazio dei nomi di processo**, la schermata operatore può leggere le variabili dell'area di processo solo mediante il formato "<nome variabile>" senza il prefisso PROCESS.

    NOTA: se si dichiarano due variabili con lo stesso nome, una nello spazio dei nomi Processo e l'altra nello spazio dei nomi Globale, solo la variabile dello spazio dei nomi Globale è accessibile da un'applicazione HMI, SCADA o Factory Cast.

È possibile utilizzare la finestra di dialogo **Selezione istanza** per accedere ai singoli oggetti dati.

AVVISO
VALORE IMPREVISTO DELLA VARIABILE • Verificare che l'applicazione disponga delle corrette impostazioni di progetto. • Verificare la sintassi per accedere alle variabili nei diversi spazi dei nomi. **Il mancato rispetto di queste istruzioni può provocare danni alle apparecchiature.**

Per impedire di accedere alla variabile errata:

- Utilizzare nomi diversi per le variabili dichiarate nello spazio dei nomi Processo e nello spazio dei nomi Globale, oppure
- selezionare **Uso dello spazio dei nomi di processo** e utilizzare la sintassi seguente per accedere alle variabili con lo stesso nome:
  - "PROCESS.<nome variabile>" per le variabili dichiarate nello spazio dei nomi Processo.
  - “<nome variabile>” senza prefisso per le variabili dichiarate nello spazio dei nomi Globale

Strumento di trending

Lo strumento di Trending di Control Expert non è supportato per l'uso con un progetto di sicurezza M580.

Aggiunta di sezioni codice

Aggiunta di codice a un processo di sicurezza M580

Operazioni con i task in Control Expert

Nello spazio dei nomi di processo, Control Expert include il task MAST per impostazione predefinita. Il task MAST non può essere eliminato. Tuttavia, è possibile aggiungere i task FAST, AUX0 e AUX1. Tenere presente che la creazione di un task nella parte processo di un progetto di sicurezza è analoga alla creazione di un task in un progetto non di sicurezza. Per ulteriori informazioni, vedere l'argomento *Creazione e configurazione di un task* nel manuale *EcoStruxure™ Control Expert - Modalità operative*.

Nello spazio dei nomi sicuro, per impostazione predefinita, Control Expert include il task SAFE. Il task SAFE non può essere rimosso e non è possibile aggiungere altri task alla sezione **Sicurezza programma** del **Browser di progetto** in Control Expert. È possibile aggiungere più sezioni al task SAFE.

Configurazione delle proprietà del task SAFE

Il task SAFE supporta solo l'esecuzione del task periodico (l'esecuzione ciclica non è supportata). Le impostazioni **Periodo** e **Watchdog** del task SAFE vengono immesse nella finestra di dialogo **Proprietà di SAFE** e supportano il seguente campo di valori:

- Periodo task SAFE: 10...255 ms con valore predefinito di 20 ms.
- Watchdog task SAFE: 10...500 ms, in incrementi di 10 ms, con un valore predefinito di 250 ms.

Impostare il task SAFE **Periodo** a un valore minimo in base alla dimensione dati sicuri e al modello di PLC. Il periodo minimo del task SAFE può essere calcolato con le formule seguenti:

- Minimo assoluto necessario per la comunicazione sicura degli I/O:
  - 10 ms
- Tempo (in ms) necessario per trasferire e confrontare i dati sicuri tra la CPU e il COPRO:
  - (0.156 x Dimensione_dati_sicuri) + 2 ms (per BMEP584040S, BMEP586040S, BMEH584040S e BMEH586040S)
  - (0,273 x Dimensione_dati_sicuri) + 2 ms (per BMEP582040S e BMEH582040S)

  Dove Dimensione_dati_sicuri è la dimensione in KB dei dati sicuri.

- Tempo aggiuntivo (in ms) richiesto dai PAC Hot Standby per trasferire i dati sicuri dal PAC primario al PAC di standby:
  - $(K1 \times Task_{kb} + K2 \times Task_{DFB}) / 500$

  In questa formula:
  - $Task_{DFB}$ = il numero di DFB dichiarati nella parte sicura dell'applicazione.
  - $Task_{kb}$ = la dimensione (in KB) dei dati sicuri scambiati dal task SAFE tra i PAC primario e di standby.
  - K1 e K2 sono costanti, con valori determinati dal modulo CPU specifico utilizzato nell'applicazione:

Coefficiente	BMEH582040S	BMEH584040S e BMEH586040S
K1	32,0	10,0
K2	23,6	7,4

NOTA:

- Il valore prodotto da queste formule è un minimo assoluto per il periodo del task SAFE valido solo per una prima valutazione del limite del tempo di ciclo SAFE. Non comprende il tempo necessario per l'esecuzione del codice utente o per il margine necessario per il funzionamento previsto del sistema multi-task del PAC. Consultare l'argomento Considerazioni sul throughput del sistema in *Modicon M580 Standalone, Guida di pianificazione del sistema per architetture di utilizzo frequente*.
- Per impostazione predefinita, Dimensione_dati_sicuri e $Size_{kbyte}$ sono uguali. È possibile visualizzarne i valori, rispettivamente, nel menu **PLC > Consumo di memoria** e nella schermata **PLC > Hot Standby**.

Calcoli di esempio

I risultati di esempio del calcolo del periodo minimo del task SAFE sono indicati di seguito

Periodo minimo task SAFE (ms)					
$Size_{kbyte}$[1]	Nb_{DFB_Inst}	BMEP582040S	BMEP584040S oppure BMEP586040S	BMEH582040S	BMEH584040S oppure BMEH586040S
0	0	10	10	10	10
50	10	16	10	20	11
100	10	30	18	37	20
150	10	43	25	54	29
200	10	57	33	70	37

Periodo minimo task SAFE (ms)					
$Size_{kbyte}$[1]	**Nb_{DFB_Inst}**	**BMEP582040S**	**BMEP584040S oppure BMEP586040S**	**BMEH582040S**	**BMEH584040S oppure BMEH586040S**
250	10	71	41	87	46
300	20	84	49	105	55
350	20	98	57	121	64
400	20	112	64	138	73
450	20	125	72	155	81
500	20	139	80	172	90
550	30	-	88	-	99
600	30	-	96	-	108
650	30	-	103	-	117
700	30	-	111	-	126
750	30	-	119	-	134
800	40	-	127	-	143
850	40	-	135	-	152
900	40	-	142	-	161
950	40	-	150	-	170
1000	40	-	158	-	179
1. Si suppone che $Dimensione_{kbyte}$ e Dimensione_dati_sicuri siano uguali.					

NOTA: Configurare il watchdog del task SAFE con un valore maggiore del **Periodo** del task SAFE.

Consultare l'argomento *Tempo di sicurezza del processo*, pagina 157, per informazioni su come la configurazione del task SAFE influisce sul tempo di sicurezza del processo.

Consultare l'argomento *Task PAC M580 Safety*, pagina 274 per informazioni sulla descrizione della priorità di esecuzione del task SAFE.

Creazione di sezioni codice

Fare clic con il pulsante destro del mouse sulla cartella **Sezione** di un task e selezionare **Nuova sezione...** per aprire una finestra di dialogo di configurazione. Per i task di sicurezza e processo, sono disponibili i seguenti linguaggi di programmazione:

Linguaggio	Task di sicurezza	Task di processo			
	SAFE	MAST	FAST	AUX0	AUX1
IL	–	✓	✓	✓	✓
FBD	✓	✓	✓	✓	✓
LD	✓	✓	✓	✓	✓
segmento LL984	–	✓	✓	✓	✓
SFC	–	✓	✓	✓	✓
ST	–	✓	✓	✓	✓
✓: disponibile – : non disponibile					

Tranne queste limitazioni sulla disponibilità del linguaggio di programmazione per il task SAFE, la finestra di dialogo di configurazione Nuova sezione ha la stessa funzionalità per un progetto non di sicurezza M580. Per ulteriori informazioni, vedere l'argomento *Finestra di dialogo delle proprietà per sezioni FBD, LD, IL o ST* nel manuale *EcoStruxure™ Control Expert - Modalità operative*.

Aggiunta di dati alle sezioni di codice

Poiché il task SAFE è separato dai task di processo, solo i dati accessibili nell'**Editor dati di sicurezza** sono disponibili per l'aggiunta a una sezione di codice del task SAFE. Tali dati comprendono:

- Variabili di sicurezza non identificate (ossia senza indirizzo %M o %MW) create nell'**Editor dati di sicurezza**.
- Oggetti dati che fanno parte delle strutture DDT dispositivo del modulo di sicurezza M580.

Analogamente, i dati disponibili per sezioni di codice del task non di sicurezza comprendono tutti i dati nell'ambito dello spazio dei nomi di processo. Questi comprendono tutti i dati di progetto tranne:

- Dati esclusivamente disponibili nello spazio dei nomi SAFE (vedere sopra).
- Oggetti dati creati nell'**Editor dati globali**.

Analisi del codice

Quando si analizza o crea un progetto, Control Expert visualizza un messaggio di errore rilevato se:

- I dati appartenenti allo spazio dei nomi di processo sono inclusi nel task SAFE.
- I dati appartenenti allo spazio dei nomi sicuro sono inclusi in un task di processo (MAST, FAST, AUX0, AUX1).
- Bit (%M) o parole (%MW) identificati sono inclusi in una sezione del task SAFE.

Richiesta diagnostica

Introduzione

La richiesta diagnostica è disponibile solo per alimentatori di sicurezza M580 situati su un rack principale utilizzando il blocco funzione PWS_DIAG. Un rack principale è un rack con indirizzo 0 e una CPU o un modulo adattatore di comunicazione (CRA) nello slot 0 o 1. Un rack di estensione non è un rack principale.

La CPU può effettuare una richiesta diagnostica di alimentatori ridondanti sul rack locale e, tramite un modulo adattatore di comunicazione (CRA), di alimentatori ridondanti su un rack remoto. Se gli alimentatori master e slave sono funzionanti, l'alimentatore master entra in modalità diagnostica master e l'alimentatore slave entra in modalità diagnostica slave. I LED indicano che il test è in corso.

NOTA: Questa richiesta non è implementata all'accensione (Power On)

Una volta terminato il test di diagnostica, il master torna allo stato operativo normale e lo slave passa allo stato normale o di errore a seconda dei risultati dei test. I risultati dei test vengono archiviati nella memoria degli alimentatori.

Dati restituiti dalla richiesta diagnostica

Le informazioni di diagnostica inviate alla CPU dagli alimentatori sono le seguenti:

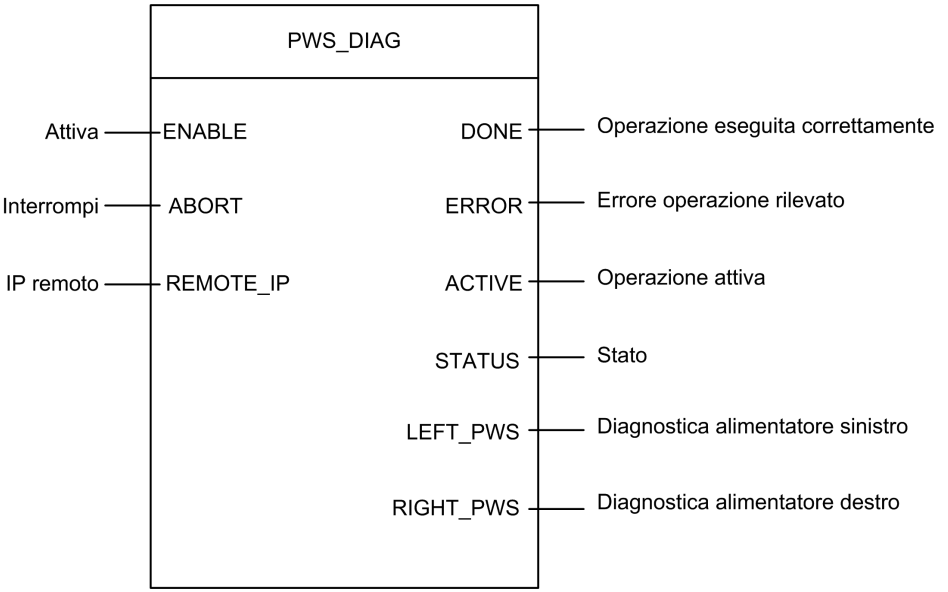
- Temperatura ambiente dell'alimentatore.
- Tensione e corrente sulla linea backplane 3,3V.
- Tensione e corrente sulla linea backplane 24V.
- Energia cumulata totale dell'alimentatore dalla data di fabbricazione sulle linee backplane 3,3V e 24V.
- Tempo operativo come master dall'ultima accensione e dal momento della produzione
- Tempo operativo come master dall'ultima accensione e dalla produzione.
- Durata di vita residua in percentuale (LTPC): il tempo che intercorre prima della manutenzione preventiva, dal 100% allo 0%.

  NOTA: Nessuna sostituzione a 0%.

- Numero di volte in cui l'alimentatore è stato inserito.

  NOTA: Dda SCADA è possibile resettare il numero di inserzioni dal momento dell'installazione ed effettuare tutte le altre operazioni di diagnostica.
- Numero di volte in cui la tensione principale BMXCPS4002S è scesa sotto il livello di sottotensione 1 (95 Vca).
- Numero di volte in cui la tensione principale BMXCPS4002S è salita oltre il livello di sovratensione 2 (195 Vca).
- Numero di volte in cui la tensione principale BMXCPS4022S è scesa sotto il livello di sottotensione 1 (20 Vcc).
- Numero di volte in cui la tensione principale BMXCPS4022S è salita oltre il livello di sovratensione 2 (40 Vcc).
- Numero di volte in cui la tensione principale BMXCPS3522S è scesa sotto il livello di sottotensione 1 (110 Vcc).
- Numero di volte in cui la tensione principale BMXCPS3522S è salita oltre il livello di sovratensione 2 (140 Vcc).
- Stato corrente dell'alimentatore (master/slave/non funzionante).

Rappresentazione in FBD



Parametri

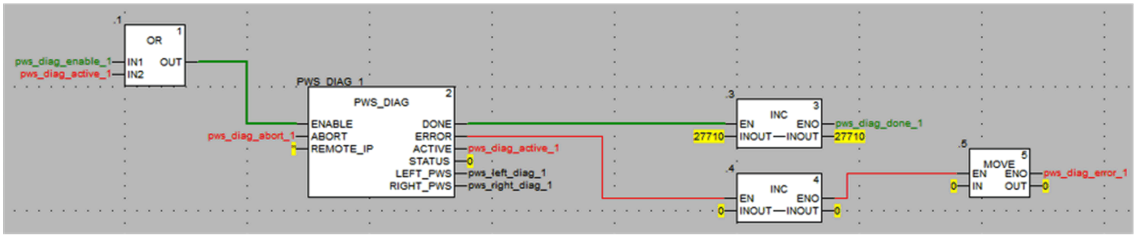
Parametri di ingresso:

Nome parametro	Tipo di dati	Descrizione
ENABLE	BOOL	Quando è ON, l'operazione è attivata.
ABORT	BOOL	Quando è ON, l'operazione corrente viene interrotta.
REMOTE_IP	STRING	Indirizzo IP ("ip1.ip2.ip3.ip4") della derivazione che contiene il modulo alimentatore. Lasciare in questo campo una stringa vuota ("") oppure non associare alcuna variabile al relativo contatto per indirizzare l'alimentatore nel rack locale.

Parametri di uscita:

Nome parametro	Tipo di dati	Descrizione
DONE	BOOL	ON quando l'operazione viene conclusa correttamente.
ERROR	BOOL	ON quando l'operazione non è eseguita correttamente e viene interrotta.
ACTIVE	BOOL	ON quando l'operazione è attiva.
STATUS	WORD	Identificatore errore rilevato.
LEFT_PWS	ANY	Dati diagnostici per alimentatore sinistro. Utilizzare una variabile di tipo PWS_DIAG_DDT_V2, pagina 138 per un'interpretazione corretta.
RIGHT_PWS	ANY	Dati diagnostici per alimentatore destro. Utilizzare una variabile di tipo PWS_DIAG_DDT_V2 per un'interpretazione corretta.

Esempio



pws_left_diag_1		PWS_DIAG_DDT	
pws_right_diag_1		PWS_DIAG_DDT	
PwsMajorVersion	153	BYTE	Power Supply major version
PwsMinorVersion	162	BYTE	Power Supply minor version
Model	0	BYTE	Power Supply Model identifier
State	12	BYTE	Power Supply state
I33BacPos	0	UINT	Measure current of 3V3 Bac in nominal role (producer)
V33Buck	0	UINT	Measure voltage of 3V3 Buck
I24Bac	0	UINT	Measure current of 24V Bac
V24Int	0	UINT	Measure voltage of 24V Int
Temperature	0	INT	Measure of Ambient Temperature
OperTimeMaster...	16935	DINT	Operating Time as Master since last Power ON
OperTimeSlaveSi...	2	DINT	Operating Time as Slave since last Power ON
OperTimeMaster	282128	DINT	Operating Time as Master since Manufacturing
OperTimeSlave	44	DINT	Operating Time as Slave Since Manufacturing
Work	0	DINT	Work supplied since Manufacturing
RemainingLTPC	0	UINT	Remaining Life Time in percent
NbPowerOn	0	UINT	Number of Power ON since Manufacturing
NbVoltageLowFail	0	UINT	Number of failure detected on Primary Voltage by Low Threshold
NbVoltageHighFail	0	UINT	Number of failure detected on Primary Voltage by High Threshold

Comandi Scambia e Azzera

Introduzione

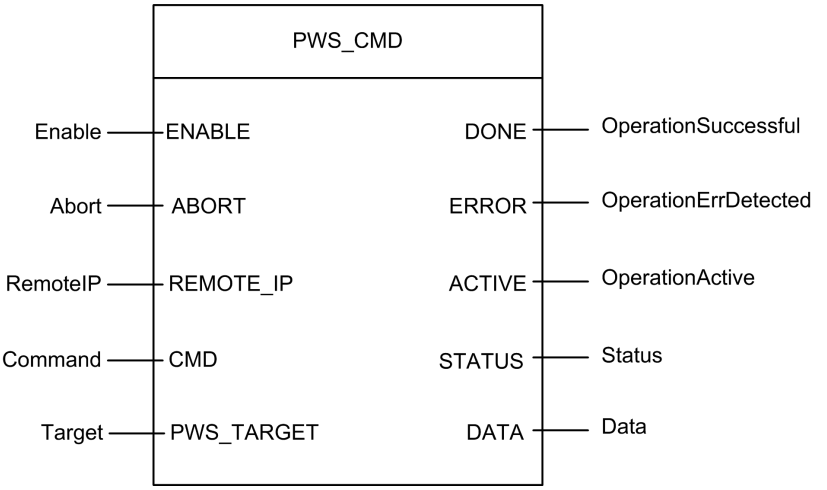
Il blocco funzione PWS_CMD può essere utilizzato per emettere due comandi:

- Richiesta Scambia: questo comando richiede all'alimentatore di operare come master. Se sono operativi entrambi gli alimentatori, l'alimentatore specificato diventa il master e l'altro diventa lo slave.
- Richiesta Azzera: questo comando azzera i contatori del numero di volte in cui:
  - la tensione principale è scesa sotto il livello di sottotensione 1.
  - la tensione principale è scesa sotto il livello di sottotensione 2.
  - l'alimentatore è stato inserito.

Entrambe le richieste sono disponibili solo per gli alimentatori che si trovano nel rack principale. Un rack principale è un rack con indirizzo 0 e una CPU o un modulo adattatore di comunicazione (CRA) nello slot 0 o 1. Un rack di estensione non è un rack principale.

I LED indicano che il comando è in corso. Una registrazione dell'evento viene memorizzata nell'alimentatore.

Rappresentazione in FBD



Parametri

Parametri di ingresso:

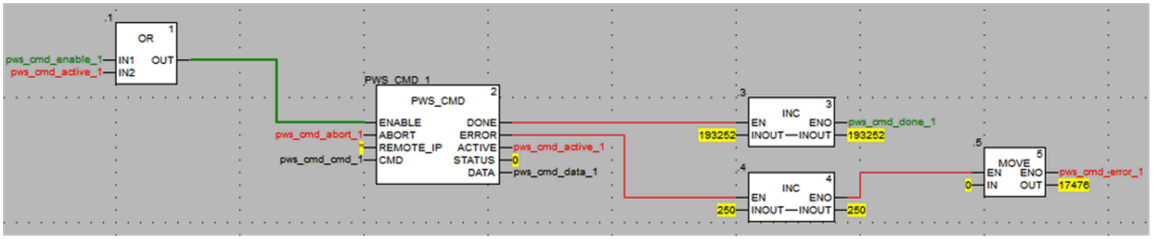
Nome parametro	Tipo di dati	Descrizione
ENABLE	BOOL	Quando è ON, l'operazione è attivata.
ABORT	BOOL	Quando è ON, l'operazione corrente viene interrotta.
REMOTE_IP	STRING	Indirizzo IP ("ip1.ip2.ip3.ip4") della derivazione che contiene il modulo alimentatore. Lasciare in questo campo una stringa vuota ("") oppure non associare alcuna variabile al relativo contatto per indirizzare l'alimentatore nel rack locale.
CMD	ANY	Usare una variabile di tipo PWS_CMD_DDT per un'interpretazione corretta. Codice di comando disponibile: • 1 = Scambia • 3 = Azzera
PWS_TARGET	BYTE	Alimentatore da indirizzare: • 1 = sinistro • 2 = destro • 3 = entrambi

Parametri di uscita:

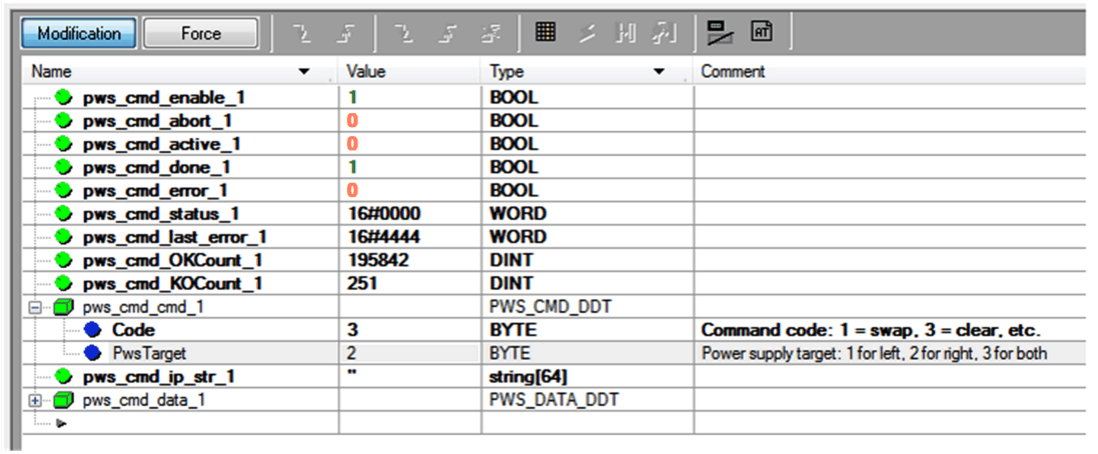
Nome parametro	Tipo di dati	Descrizione
DONE	BOOL	ON quando l'operazione viene conclusa correttamente.
ERROR	BOOL	ON quando l'operazione non è eseguita correttamente e viene interrotta.
ACTIVE	BOOL	ON quando l'operazione è attiva.
STATUS	WORD	Identificatore errore rilevato.
DATA	ANY	Dati di risposta (a seconda del codice di comando)- Nessun dato segnalato per i comandi di scambio e azzeramento.

Esempio

Il seguente diagramma descrive un blocco PWS_CMD utilizzato per una richiesta di scambio:



La seguente schermata dell'editor di dati mostra i valori delle variabili di una richiesta di scambio:



Gestione della sicurezza dell'applicazione

Introduzione

Control Expert consente di limitare l'accesso al PAC di sicurezza M580 agli utenti con password assegnate. Questa sezione fa riferimento ai processi di assegnazione password disponibili in Control Expert.

Protezione dell'applicazione

Panoramica

EcoStruxure Control Expert dispone di un meccanismo di password che impedisce l'accesso non autorizzato all'applicazione.

La password di EcoStruxure Control Expert protegge queste azioni:

- Apertura dell'applicazione in EcoStruxure Control Expert.
- Connessione al controller in EcoStruxure Control Expert.

L'impostazione della password di un'applicazione impedisce la modifica, il download o l'apertura indesiderati dei file dell'applicazione. La password è crittografata nell'applicazione.

Oltre a impostare la password, è possibile crittografare i file `.STU`, `.STA` e `.ZEF`. La funzionalità di crittografia file in EcoStruxure Control Expert consente di impedire le modifiche e rafforza la protezione della proprietà intellettuale. L'opzione di crittografia file è protetta da un meccanismo di password.

NOTA: quando un controller è gestito come parte di un progetto di sistema, la password dell'applicazione e la crittografia del file sono disattivate in Editor Control Expert e gestite con Topology Manager.

Creazione della password

La costruzione della password è conforme allo standard IEEE 1686-2013.

Una password valida contiene almeno 8 caratteri e include almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere non alfanumerico ($, %, &, ecc.).

NOTA: la password dell'applicazione viene cancellata quando si esporta un progetto non crittografato in un file `.XEF` o `.ZEF`.

Creazione di un nuovo progetto

Per impostazione predefinita, una nuova applicazione (progetto) di EcoStruxure Control Expert Classic ha le seguenti caratteristiche:

- Il progetto non è protetto da una password.
- I file dell'applicazione di progetto non sono crittografati.

Quando si crea un progetto, è possibile esercitare queste opzioni nella finestra di dialogo **Applicazione sicurezza**:

- Impostare una password per l'applicazione.
- Applicare la crittografia ai file dell'applicazione tramite una password di crittografia file.

Accedere alla finestra di dialogo **Applicazione sicurezza** in EcoStruxure Control Expert Classic:

Passo	Azione
1	Aprire la finestra **Nuovo progetto** in EcoStruxure Control Expert (**File > Nuovo**).
2	Selezionare un controller per il progetto.
3	Fare clic sul pulsante **OK** per aprire la finestra di dialogo **Applicazione sicurezza**.
4	Scegliere se creare un progetto con o senza password e seguire le istruzioni nella tabella appropriata di seguito.

Nessuna password: creare un progetto senza una password dell'applicazione:

Passo	Azione
1	Accedere alla finestra di dialogo **Applicazione sicurezza**.
2	Nella finestra di dialogo **Applicazione sicurezza** selezionare **Non si desidera impostare una password dell'applicazione per questo progetto**.
3	Fare clic sul pulsante **OK** per continuare.

Con password: per creare un progetto con una password dell'applicazione e una password (opzionale) di crittografia file, procedere come segue.

NOTA: è possibile configurare una data di scadenza per queste password nella scheda **Criteri** nell'Editor sicurezza.

Passo	Azione
1	Accedere alla finestra di dialogo **Applicazione sicurezza**.
2	Nella finestra di dialogo **Password applicazione**, creare una password per proteggere l'applicazione e aumentare la sicurezza di accesso al controller: • Specificare una password nel campo **Immissione**. • Reinserire la password nel campo **Conferma**.
3	Nella casella di gruppo **Password crittografia file** creare una password per proteggere la proprietà intellettuale: • Specificare una password nel campo **Immissione**. • Reinserire la password nel campo **Conferma**. **NOTA:** • È possibile configurare una password di crittografia file solo dopo aver configurato una password dell'applicazione. • Utilizzare password diverse per la password dell'applicazione e la password di crittografia file.
4	Premere il pulsante **OK** per applicare le impostazioni della password e chiudere la finestra di dialogo **Applicazione sicurezza**.

NOTA:

- Se non si immette alcuna password, i file dell'applicazione non vengono crittografati. In questo caso, alla successiva apertura del progetto EcoStruxure Control Expert, viene visualizzata la finestra di dialogo **Password**. Per accedere al progetto, non digitare una password e fare clic su **OK**. Quindi utilizzare le istruzioni seguenti per impostare una password dell'applicazione e attivare la crittografia dei file.
- È possibile creare o modificare la password di un'applicazione in qualsiasi momento, ma non è possibile cancellare la password dell'applicazione quando si configura una password di crittografia file per il progetto.

Impostazione di una password dell'applicazione

Impostare una password dell'applicazione

Passo	Azione
1	Fare clic con il pulsante destro del mouse su **Progetto** nel **Browser di progetto**.
2	Selezionare **Proprietà** dal menu di scelta rapida per aprire la finestra **Proprietà del progetto**.

Passo	Azione
3	Selezionare la scheda **Protezione progetto e controller**.
4	Nel campo **Applicazione**, fare clic su **Modifica password...** per aprire la finestra **Modifica password**.
5	Immettere la nuova password nel campo **Immissione**.
6	Immettere la conferma della nuova password nel campo **Conferma**.
7	Fare clic su **OK** per confermare.
8	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare le modifiche.

Modifica della password dell'applicazione

Modificare la password di protezione dell'applicazione:

Passo	Azione
1	Fare clic con il pulsante destro del mouse su **Progetto** nel **Browser di progetto**.
2	Selezionare **Proprietà** dal menu di scelta rapida per aprire la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione progetto e controller**.
4	Nel campo **Applicazione**, fare clic su Modifica password... per aprire la finestra **Modifica password**.
5	Immettere la password precedente nel campo **Password precedente**.
6	Immettere la nuova password nel campo **Immissione**.
7	Immettere la conferma della nuova password nel campo **Conferma**.
8	Fare clic su **OK** per confermare.
9	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare le modifiche.

Eliminazione della password dell'applicazione

La cancellazione della password dell'applicazione non è consentita se è abilitata la crittografia dei file.

Cancellare la password di protezione dell'applicazione:

Passo	Azione
1	Fare clic con il pulsante destro del mouse su **Progetto** nel **Browser di progetto**.
2	Selezionare il comando **Proprietà** dal menu di scelta rapida per aprire la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione progetto e controller**.
4	Nel campo **Applicazione**, fare clic su Cancella password... per aprire la finestra **Password**.
5	Immettere la password nel campo **Password**.
6	Fare clic su **OK** per confermare.
7	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare le modifiche.

Funzione di blocco automatico

Per esercitare l'opzione di limitazione dell'accesso allo strumento EcoStruxure Control Expert dopo un periodo di inattività configurato, selezionare la casella di controllo **Blocco automatico** e immettere un valore nella casella **Minuti prima del blocco** per impostare il timeout per il tempo di inattività.

Una funzione di blocco automatico opzionale limita l'accesso allo strumento di programmazione software EcoStruxure Control Expert dopo un periodo di inattività configurato. È possibile attivare la funzione di blocco automatico con la casella di controllo **Blocco automatico** e selezionare il timeout per il tempo di inattività con **Minuti prima del blocco**.

Se la funzione di blocco automatico è attivata e il tempo di inattività configurato scade, viene visualizzata una finestra di dialogo che riciede la password dell'applicazione. Dietro la finestra di dialogo, gli editor rimangono aperti nella stessa posizione. Di conseguenza, chiunque può leggere il contenuto delle finestre di EcoStruxure Control Expert ma non può continuare a lavorare con EcoStruxure Control Expert.

NOTA: se non è stata assegnata una password al progetto, la finestra di dialogo non viene visualizzata.

Condizione di richiesta password

Apertura di un'applicazione esistente (progetto):

Quando si apre un file di applicazione, viene visualizzata una finestra di dialogo **Password applicazione**.

Immettere la password e fare clic su **OK**.

Risultato: se la password è corretta, l'applicazione si apre. Se la password è errata, un messaggio su schermo indica che la password non è valida e viene visualizzata una nuova finestra di dialogo **Password applicazione**.

Se si fa clic su **Annulla**, l'applicazione non viene aperta.

Accesso all'applicazione in EcoStruxure Control Expert dopo un blocco automatico, quando EcoStruxure Control Expert non è collegato al controller o quando il progetto in EcoStruxure Control Expert è *uguale* al progetto nel controller:

Allo scadere del tempo di blocco automatico, viene visualizzata una finestra di dialogo **Password applicazione**.

Immettere la password e fare clic su **OK**.

Risultato: se la password è corretta, EcoStruxure Control Expert diventa nuovamente attivo. Se la password è errata, un messaggio su schermo indica che la password non è valida e viene visualizzata una nuova finestra di dialogo Password applicazione .

Fare clic su **Chiudi** per chiudere l'applicazione non salvata.

Accesso all'applicazione nel controller dopo un blocco automatico, quando EcoStruxure Control Expert è collegato al controller e l'applicazione in EcoStruxure Control Expert è *diversa* dall'applicazione nel controller:

Alla connessione, se l'applicazione software EcoStruxure Control Expert e l'applicazione del controller non sono uguali, viene visualizzata una finestra di dialogo **Password applicazione**.

Immettere la password e fare clic su **OK**.

Risultato: se la password è corretta viene stabilito il collegamento. Se la password è errata, un messaggio indica che è stata immessa una password errata e viene visualizzata una nuova finestra di dialogo **Password applicazione**.

Se si fa clic su **Annulla**, la connessione non viene stabilita.

NOTA: alla connessione, se l'applicazione software EcoStruxure Control Expert e le applicazioni del controller sono uguali, non viene richiesta la password. Se inizialmente non è stata immessa alcuna password (lasciata vuota alla creazione del progetto), fare clic su **OK** per stabilire la connessione alla richiesta della password.

NOTA:

- Dopo tre tentativi con password errata, attendere un intervallo di tempo crescente tra ogni nuovo tentativo di inserimento della password. Il periodo di attesa aumenta da 15 secondi a 1 ora, con l'incremento che aumenta di un fattore di 2 dopo ogni tentativo non riuscito con password errata.
- Per le password dimenticate, consultare le istruzioni per le password perse, pagina 324.

Abilitazione dell'opzione di crittografia file

NOTA: Impostare una password dell'applicazione *prima* di attivare la crittografia del file.

Abilitare l'opzione di crittografia file:

Passo	Azione
1	Fare clic con il pulsante destro del mouse su **Progetto** nel **Browser di progetto**.
2	Selezionare il comando **Proprietà** dal menu di scelta rapida per aprire la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione progetto e controller**.
4	Selezionare la casella di controllo **Crittografia file attiva** per aprire la finestra **Crea password**.
5	Immettere la password nel campo **Immissione**.
6	Confermare la password nel campo **Conferma**.
7	Fare clic su **OK** per confermare.
8	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare le modifiche.

Disbilitazione dell'opzione di crittografia file

Disbilitare l'opzione di crittografia file

Passo	Azione
1	Fare clic con il pulsante destro del mouse su **Progetto** nel **Browser di progetto**.
2	Selezionare il comando **Proprietà** dal menu di scelta rapida per aprire la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione progetto e controller**.
4	*Deselezionare* la casella di controllo **Crittografia file attiva** per aprire la finestra **Password di crittografia file**.
5	Immettere la password e fare clic su **OK** per confermare che l'applicazione non è crittografata.
6	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche.

Modifica della password di crittografia del file

Modificare la password di crittografia del file:

Passo	Azione
1	Fare clic con il pulsante destro del mouse su **Progetto** nel **Browser di progetto**.
2	Selezionare il comando **Proprietà** dal menu di scelta rapida per aprire la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione progetto e controller**.
4	Nel campo **Crittografia file**, fare clic su Modifica password... per aprire la finestra **Modifica password**.
5	Immettere la password precedente nel campo **Password precedente**.
6	Immettere la nuova password nel campo **Immissione**.
7	Immettere la conferma della nuova password nel campo **Conferma**.
8	Fare clic su **OK** per confermare.
9	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare le modifiche.

Cancellazione della password di crittografia file

Cancellare la password di crittografia del file:

Passo	Azione
1	Fare clic con il pulsante destro del mouse su **Progetto** nel **Browser di progetto**.
2	Selezionare il comando **Proprietà** dal menu di scelta rapida per aprire la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione progetto e controller**.
4	Nel campo **Crittografia file**, fare clic su Modifica password... per aprire la finestra **Password**.
5	Immettere la password nel campo **Password**.
6	Fare clic su **OK** per confermare.
7	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare le modifiche.

NOTA: Per le password di crittografia dei file dimenticate, consultare le istruzioni per le password perse, pagina 324.

Regole di compatibilità

Non è possibile aprire file di applicazione `.STA` e `.ZEF` crittografati in EcoStruxure Control Expert 15.0 Classic o versioni precedenti.

Non è possibile importare file di applicazione `.ZEF` crittografati in EcoStruxure Control Expert con Topology Manager.

Le regole di compatibilità tra la versione dell'applicazione e la versione di EcoStruxure Control Expert/Unity Pro si applicano ai file `.ZEF` esportati senza crittografia.

NOTA: Quando la crittografia dei file è attivata per il progetto, non è possibile salvare i file dell'applicazione archiviati (`.STA`) senza crittografia.

Protezione tramite password dell'area di sicurezza

In breve

I controller di sicurezza includono una funzione di protezione tramite password dell'area di sicurezza, accessibile dalla finestra di dialogo **Proprietà** del progetto. Questa funzione consente di proteggere gli elementi del progetto situati nell'area di sicurezza del progetto di sicurezza funzionale.

NOTA: Quando la funzione di protezione tramite password dell'area di sicurezza è attiva, le parti di sicurezza dell'applicazione non possono essere modificate

Le modifiche alle seguenti parti di sicurezza non sono consentite quando è abilitata la protezione tramite password dell'area di sicurezza:

Parte relativa alla sicurezza	**Azione vietata (offline E online)**
Configurazione	Modificare le caratteristiche del controller
	Aggiungere, eliminare, modificare un modulo di sicurezza nel rack
	Modificare l'alimentazione di sicurezza
Tipi	Creare, eliminare, modificare un DDT di sicurezza
	Cambiare un attributo DDT: da NON SICURO->STATO SICURO definito
	Cambiare un attributo DDT: da STATO SICURO definito->NON SICURO
	Creare, eliminare, modificare un DFB di sicurezza
	Cambiare un attributo DFB: da NON SICURO->STATO SICURO definito
	Cambiare un attributo DFB: da STATO SICURO definito->NON SICURO
Programma SAFE	Qualsiasi modifica nel nodo **Variabili e istanze FB**
	Creare task
	Importare task
	Modificare task
	Creare sezione

Parte relativa alla sicurezza	Azione vietata (offline E online)
	Eliminare sezione
	Importare sezione
	Modificare sezione
Impostazioni progetto	Modificare impostazioni di progetto SAFE
	Modificare impostazioni di progetto COMMON

NOTA:

- Se è attivata una password di sicurezza, immettere la password per entrare in modalità Manutenzione.
- Nel caso in cui la password dell'applicazione e il blocco automatico siano attivati: quando la password dell'applicazione è richiesta a causa di inattività e EcoStruxure Control Expert Classic è collegato al controller di sicurezza in modalità di programmazione e il controller di sicurezza è in esecuzione in modalità di manutenzione, il controller di sicurezza passa in modalità di sicurezza dopo 5 minuti se non si immette la password.

NOTA:

- Se è attivata una password di sicurezza, immettere la password per entrare in modalità Manutenzione.
- Se sono attivati la password dell'applicazione e il blocco automatico:

  Quando le condizioni seguenti sono vere, il controller di sicurezza passa alla modalità di sicurezza dopo cinque minuti se non si immette la password:

  La password dell'applicazione è richiesta a causa dell'inattività.

  EcoStruxure Control Expert Classic è collegato al controller di sicurezza in modalità Programmazione.

  Il controller di sicurezza è in esecuzione in modalità Manutenzione.

Crittografia

La password dell'area di sicurezza utilizza la crittografia standard SHA-256.

Funzione della password dell'area di sicurezza rispetto alle autorizzazioni utente del progetto di sicurezza funzionale

L'attivazione della password dell'area di sicurezza e l'implementazione delle autorizzazioni utente create nell'**Editor di sicurezza** sono funzioni di sicurezza che si escludono a vicenda, come segue:

- Se all'utente che avvia EcoStruxure Control Expert è stato assegnato un profilo utente, tale utente può accedere alle aree di sicurezza dell'applicazione di sicurezza se l'utente immette la password dell'area di sicurezza e gli sono state concesse le autorizzazioni di accesso nell'**Editor di sicurezza**.
- Se i profili utente non sono stati assegnati, un utente può accedere alle aree sicure dell'applicazione di sicurezza immettendo la password dell'area di sicurezza.

Indicatori visivi in EcoStruxure Control Expert

Lo stato della funzione di protezione dell'area relativa alla sicurezza può essere rilevato visivamente tramite il nodo **Programma SAFE** nel **Browser di progetto**:

- Un lucchetto chiuso indica che è stata creata e attivata una password dell'area di sicurezza.
- Un lucchetto aperto indica che è stata creata ma non attivata una password dell'area di sicurezza.

  NOTA: Se l'applicazione di sicurezza viene chiusa e riaperta, la password dell'area relativa alla sicurezza viene attivata automaticamente alla riapertura.
- Nessun lucchetto indica che non è stata creata alcuna password dell'area di sicurezza.

Compatibilità

A partire da EcoStruxure Control Expert versione 14.0, la funzione della password dell'area di sicurezza esiste per controller M580 Safety dalla versione firmware 2.80.

NOTA:

- I file di programma applicativo `.STU`, `.STA` e `.ZEF` (creati a partire da EcoStruxure Control Expert versione 14.0) non possono essere aperti in Unity Pro versione 13.1 o precedente.
- La sostituzione di un controller M580 Safety in un'applicazione EcoStruxure Control Expert versione 14.0 ha il seguente effetto:
  - L'aggiornamento dal firmware 2.70 a 2.80 (o da qualsiasi versione successiva di supporto) aggiunge la funzionalità della password dell'area di sicurezza alla scheda **Protezione programma e Safety** della finestra **Progetto > Proprietà**.
  - Il downgrade dal firmware 2.80 (e da qualsiasi versione successiva comparabile) a 2.70 rimuove la funzionalità della password dell'area di sicurezza.

Attivazione della protezione e creazione della password

Procedura per l'attivazione delle sezioni e la creazione della passwird:

Passo	Azione
1	Nel browser di progetto, fare clic con il pulsante destro del mouse su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione programma e Safety**.
4	Nell'area **Sicurezza**, attivare la protezione selezionando la casella **Protezione attiva**. **Risultato**: viene visualizzata la finestra di dialogo **Modifica password**.
5	Immettere una password nel campo **Immissione**.
6	Confermare la password nel campo **Conferma**.
7	Fare clic su **OK** per confermare.
8	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto** tutte le modifiche vengono annullate.

Modifica della password

Procedura per modificare la password di protezione delle sezioni del progetto:

Passo	Azione
1	Nel browser di progetto, fare clic con il pulsante destro del mouse su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione programma e Safety**.
4	Nell'area **Sicurezza**, fare clic su **Modifica password...**. **Risultato**: viene visualizzata la finestra di dialogo **Modifica password**.
5	Immettere la password precedente nel campo **Password precedente**.
6	Immettere la nuova password nel campo **Immissione**.
7	Immettere la conferma della nuova password nel campo **Conferma**.
8	Fare clic su **OK** per confermare.
9	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto** tutte le modifiche vengono annullate.

Eliminazione della password

Procedura per eliminare la password di protezione delle sezioni del progetto:

Passo	Azione
1	Nel browser di progetto, fare clic con il pulsante destro del mouse su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione programma e Safety**.
4	Nell'area **Sicurezza**, fare clic su **Cancella password...**. **Risultato**: viene visualizzata la finestra di dialogo **Controllo accesso**:
5	Immettere la password precedente nel campo **Password**.
6	Fare clic su **OK** per confermare.
7	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto** tutte le modifiche vengono annullate.

Protezione di Unità programma, sezione e subroutine

In breve

La funzione di protezione è accessibile dalla schermata **Proprietà** del progetto in modalità offline.

Questa funzione permette di proteggere gli elementi del programma (sezioni, Unità programma).

NOTA: la protezione non è attiva finché la protezione non viene attivata nel progetto.

NOTA: la protezione del progetto è attiva solo per gli elementi di programma contrassegnati. Ciò non impedisce le seguenti operazioni:

- Collegamento al PLC
- Caricamento di un'applicazione dalla CPU
- Modifica della configurazione
- Aggiunta di nuove Unità programma e/o sezioni
- Modifica della logica in una nuova sezione (non protetta)

Attivazione della protezione e creazione della password

Procedura per attivare la protezione e creare la password per sezioni e Unità programma:

Passo	Azione
1	Nel browser del progetto fare clic su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione programma e Safety**.
4	Nel campo **Unità programma e sezioni**, attivare la protezione selezionando la casella di controllo **Protezione attiva**. **Risultato**: viene visualizzata la finestra di dialogo **Modifica password**:
5	Specificare una password nel campo **Immissione**.
6	Confermare la password nel campo **Conferma**.
7	Selezionare la casella di controllo **Criptata** se è necessaria un'ulteriore protezione mediante password. **NOTA:** un progetto con una password criptata non può essere modificato con Unity Pro V4.0 e versioni precedenti.

Passo	Azione
8	Fare clic su **OK** per confermare.
9	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto**, tutte le modifiche vengono annullate.

Note:

Se un elemento di programma è configurato con una protezione (lettura o lettura/scrittura), la protezione attiva viene indicata da un lucchetto chiuso al livello della sezione.

Se l'elemento di programma è configurato con una protezione ma la protezione è disabilitata, al livello dell'elemento di programma viene visualizzato un lucchetto aperto.

Modifica della password

Procedura per cambiare la password di protezione progetto per sezioni e Unità programma:

Passo	Azione
1	Nel browser del progetto fare clic su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione programma e Safety**.
4	Nel campo **Unità programma e sezioni**, fare clic su **Modifica password...**. **Risultato**: viene visualizzata la finestra di dialogo **Modifica password**:
5	Immettere la password precedente nel campo **Password precedente**.
6	Immettere la nuova password nel campo **Immissione**.
7	Confermare la nuova password nel campo **Conferma**.
8	Selezionare la casella di controllo **Criptata** se è necessaria un'ulteriore protezione mediante password. **NOTA:** un progetto con una password criptata non può essere modificato con Unity Pro V4.0 e versioni precedenti. Unity Pro è il nome precedente di Control Expert per versione 13.1 o precedenti.
9	Fare clic su **OK** per confermare.
10	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto**, tutte le modifiche vengono annullate.

Eliminazione della password

Procedura per eliminare la password di protezione progetto per sezioni e Unità programma:

Passo	Azione
1	Nel browser del progetto fare clic su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione programma e Safety**.
4	Nel campo **Unità programma e sezioni**, fare clic su **Azzera password...**. **Risultato**: viene visualizzata la finestra di dialogo **Controllo accesso**:
5	Immettere la password precedente nel campo **Password**.
6	Fare clic su **OK** per confermare.
7	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto**, tutte le modifiche vengono annullate.

Protezione del firmware

Panoramica

La protezione del firmware tramite password consente di impedire l'accesso non autorizzato al firmware del modulo.

Password

La password differenzia tra maiuscole e minuscole e contiene da 8 a 16 caratteri alfanumerici. La sicurezza della password è aumentata quando contiene un misto di lettere maiuscole e minuscole, caratteri alfabetici, alfanumerici e caratteri speciali.

NOTA: Quando si importa un file ZEF, la password del firmware viene memorizzata nel modulo solo se è selezionata l'opzione **Crittografia file**.

Modifica della password

È possibile modificare la password in qualsiasi momento.

NOTA: Il valore predefinito della password del firmware nell'applicazione Control Expert è: **`fwdownload`**.

- Per il firmware V4.01 e versioni successive, è necessario modificare il valore predefinito della password del firmware, altrimenti non sarà possibile creare l'applicazione Control Expert.
- Per le versioni del firmware precedenti alla V4.01 non è obbligatorio, ma è consigliabile modificare il valore predefinito della password del firmware.

Procedura per la modifica della password di protezione del firmware:

Passaggio	Azione
1	Nel browser del progetto fare clic su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione progetto e controller**.
4	Nel campo **Firmware** , fare clic su **Cambia password...**. **Risultato**: viene visualizzata la finestra **Modifica password**.
5	Immettere la password precedente nel campo **Password precedente**.
6	Immettere la nuova password nel campo **Immissione**.
7	Confermare la nuova password nel campo **Conferma**.
8	Fare clic su **OK** per confermare.
9	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto**, tutte le modifiche vengono annullate.

Ripristino della password

Se si reimposta la password, il valore predefinito viene assegnato alla password del firmware nell'applicazione Control Expert se viene confermata la password corrente.

Per reimpostare la password, procedere come segue:

Passaggio	Azione
1	Nel browser del progetto fare clic su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.

Passaggio	Azione
3	Selezionare la scheda **Protezione progetto e controller**.
4	Nel campo **Firmware** , fare clic su **Azzera password...**. **Risultato**: viene visualizzata la finestra **Password**.
5	Immettere la password corrente nel campo **Password**.
6	Fare clic su **OK** per confermare.
7	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. La nuova password è quella predefinita: **`fwdownload`**. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto**, tutte le modifiche vengono annullate.

Protezione Web/Memorizzazione dati

Panoramica

La protezione tramite password impedisce l'accesso non autorizzato all'area di memorizzazione dati della scheda di memoria SD (se nella CPU è inserita una scheda valida).

Per le CPU Modicon M580 in un progetto creato da Control Expert con:

- Versione precedente a 15.1, è possibile fornire una protezione tramite password per l'accesso alla memorizzazione dati.
- Dalla versione 15.1, è possibile fornire la protezione tramite password sia per la diagnostica Web sia per l'accesso alla memorizzazione dei dati.

  NOTA: Se un controller è gestito come parte di un progetto di sistema, la password di **Diagnostica Web/Memorizzazione dati** è disattivata in Editor Control Expert e deve essere gestita tramite Topology Manager.

Password

La password differenzia tra maiuscole e minuscole e contiene da 8 a 16 caratteri alfanumerici. La sicurezza della password è aumentata quando contiene un misto di lettere maiuscole e minuscole, caratteri alfabetici, alfanumerici e caratteri speciali.

NOTA: Quando si importa un file ZEF, la password Web/memorizzazione dati viene memorizzata all'interno del modulo solo se è selezionata l'opzione **Crittografia file**.

Modifica della password

È possibile modificare la password in qualsiasi momento.

NOTA: La password memorizzazione dati/Web ha un valore predefinito nell'applicazione Control Expert. Questo valore predefinito dipende dalla versione di Control Expert:

- **`datadownload:`** versioni di Control Expert precedenti alla 15.1
- **`webuser:`** versioni di Control Expert da 15.1

La modifica della password predefinita è obbligatoria o meno, a seconda della versione firmware del modulo:

- Dalla versione 4.01 del firmware, è necessario modificare il valore predefinito della password di Memorizzazione dati/Web, altrimenti non sarà possibile creare l'applicazione Control Expert.
- Per le versioni firmware precedenti alla 4.01 non è obbligatorio, ma si consiglia di modificare il valore predefinito della password di Memorizzazione dati/Web.

Procedura per la modifica della password Web/memorizzazione dati:

Passo	Azione
1	Nel browser di progetto, fare clic con il pulsante destro del mouse su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione progetto e controller**.
4	Nel campo **Memorizzazione dati** (o **Diagnostica Web/Memorizzazione dati**), fare clic su **Modifica password...**. **Risultato**: viene visualizzata la finestra **Modifica password**.
5	Immettere la password precedente nel campo **Password precedente**.
6	Immettere la nuova password nel campo **Immissione**.
7	Immettere la conferma della nuova password nel campo **Conferma**.
8	Fare clic su **OK** per confermare.
9	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto** tutte le modifiche vengono annullate.

Ripristino della password

Ripristinando la password se ne assegna il valore predefinito alla password Web/ memorizzazione dati nell'applicazione Control Expert se la password corrente è confermata.

Per reimpostare la password, procedere come segue:

Passo	Azione
1	Nel browser di progetto, fare clic con il pulsante destro del mouse su **Progetto**.
2	Selezionare il comando **Proprietà** nel menu a comparsa. **Risultato**: viene visualizzata la finestra **Proprietà del progetto**.
3	Selezionare la scheda **Protezione progetto e controller**.
4	Nel campo **Memorizzazione dati** (o **Diagnostica Web/Memorizzazione dati**), fare clic su **Reimposta password...**. **Risultato**: viene visualizzata la finestra **Password**.
5	Immettere la password corrente nel campo **Password**.
6	Fare clic su **OK** per confermare.
7	Fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. La nuova password è quella predefinita: **`datadownload`**. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto**, tutte le modifiche vengono annullate.

Perdita della password

Panoramica

Se si dimentica la password, procedere nel modo indicato nella seguenti procedure e contattare l'assistenza tecnica di Schneider Electric.

NOTA: La procedura di ripristino della password dell'applicazione varia a seconda che l'opzione di crittografia del file sia attivata o disattivata.

Password applicazione Control Expert senza opzione di crittografia file

La procedura seguente per reimpostare la password dell'applicazione è valida quando l'opzione di crittografia file è disattivata o per il file dell'applicazione gestito con Control Expert 15.0 Classic o versioni precedenti.

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme `SHIFT +F2` nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**, è necessario rispettare le condizioni seguenti:

- Al momento dell'apertura, selezionare l'applicazione; viene visualizzata la finestra di dialogo **Password**.
- Al momento del blocco automatico, viene visualizzata la finestra di dialogo **Password**. Se non si ricorda la password, selezionare **Chiudi**. Riaprire l'applicazione; viene visualizzata la finestra di dialogo **Password**.

  NOTA: Se si chiude l'applicazione senza immettere una password dopo un blocco automatico, tutte le modifiche vanno perse.

Procedura per reimpostare la password dell'applicazione:

Passo	Azione
1	**Condizione:** viene visualizzata la finestra di dialogo **Password**.
2	Premere `SHIFT+F2`. **Risultato**: si apre la finestra a comparsa **Password dimenticata** e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. **NOTA:** la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password.
6	Modificare la password (vecchia password = password fornita dall'assistenza tecnica Schneider Electric).
7	Fare clic su **Crea** > **Crea modifiche**.
8	**Salvare** l'applicazione.

Password dell'applicazione Control Expert con opzione di crittografia file

Se si dimentica la password dell'applicazione quando la crittografia file è attivata, è necessario inviare il file dell'applicazione all'assistenza tecnica Schneider Electric. Viene quindi ricevuto il file dell'applicazione crittografata con una nuova password dell'applicazione file dall'assistenza tecnica Schneider Electric.

NOTA: Modificare la password dell'applicazione al primo utilizzo.

Password applicazione controller

Procedura per il ripristino della password dell'applicazione controller se il rispettivo file **.STU* è disponibile:

Passo	Azione
1	Aprire il rispettivo file **.STU*.
2	Quando viene visualizzata la finestra di dialogo **Password**, premere `SHIFT+F2`. **Risultato**: si apre la finestra a comparsa **Password dimenticata** e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. **Nota**: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password.
6	Modificare la password (vecchia password = password fornita dall'assistenza tecnica Schneider Electric).
7	**Connettersi** al controller.
8	Fare clic su **Crea** > **Crea modifiche**.
9	**Salvare** l'applicazione.

Procedura per reimpostare la password dell'applicazione del controller se il file **.STU* rispettivo non è disponibile:

Passo	Azione
1	**Condizione:** al momento della connessione, viene visualizzata la finestra di dialogo **Password**.
2	Premere `SHIFT+F2`. **Risultato**: si apre la finestra a comparsa **Password dimenticata** e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. **Nota**: la password fornita dall'assistenza tecnica Schneider Electric è temporanea e valida finché non si modifica l'applicazione.
5	Immettere questa password.
6	Caricare l'applicazione dal controller.
7	**Salvare** l'applicazione.
8	Modificare la password (vecchia password = quella fornita dall'assistenza tecnica Schneider Electric).

Passo	Azione
9	Fare clic su **Crea** > **Crea modifiche**.
10	**Salvare** l'applicazione.

Password di crittografia file

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme `SHIFT +F2` nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**:

- Selezionare **Progetto > Proprietà del progetto > Protezione progetto e controller**
- Nel campo **Crittografia file**, fare clic su **Cancella password...**. Viene visualizzata la finestra di dialogo **Password**.

Procedura per reimpostare la password di crittografia file:

Passo	Azione
1	**Condizione:** viene visualizzata la finestra di dialogo **Password**.
2	Premere `SHIFT+F2`. **Risultato**: si apre la finestra a comparsa **Password dimenticata** e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. **Nota**: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password e fare clic su **OK** per chiudere la finestra di dialogo **Password**.
6	Fare clic su **Modifica password** e modificare la password (password precedente = password fornita dall'assistenza Schneider Electric).
7	Fare clic su **OK** per chiudere la finestra di dialogo **Modifica password**, quindi fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto** tutte le modifiche vengono annullate.

Password area sicura

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme `SHIFT +F2` nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**:

- Selezionare **Progetto > Proprietà del progetto > Protezione programma e Safety**
- Nel campo **Sicurezza**, fare clic su **Modifica password...**. Viene visualizzata la finestra di dialogo **Password**.

Procedura per reimpostare la password dell'area sicura:

Passo	Azione
1	**Condizione:** viene visualizzata la finestra di dialogo **Password**.
2	Premere `SHIFT+F2`. **Risultato**: si apre la finestra a comparsa **Password dimenticata** e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. **Nota**: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password e fare clic su **OK** per chiudere la finestra di dialogo **Password**.
6	Fare clic su **Modifica password** e modificare la password (password precedente = password fornita dall'assistenza Schneider Electric).
7	Fare clic su **OK** per chiudere la finestra di dialogo **Modifica password**, quindi fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto** tutte le modifiche vengono annullate.

Password del firmware

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme `SHIFT +F2` nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**:

- Selezionare **Progetto > Proprietà del progetto > Protezione progetto e controller**
- Nel campo **Firmware**, fare clic su **Reimposta password...**. Viene visualizzata la finestra di dialogo **Password**.

Procedura per reimpostare la password del firmware:

Passo	Azione
1	**Condizione:** viene visualizzata la finestra di dialogo **Password**.
2	Premere `SHIFT+F2`.

Passo	Azione
	Risultato: si apre la finestra a comparsa **Password dimenticata** e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. **Nota**: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password e fare clic su **OK** per chiudere la finestra di dialogo **Password**.
6	Fare clic su **Modifica password** e modificare la password (password precedente = password fornita dall'assistenza Schneider Electric).
7	Fare clic su **OK** per chiudere la finestra di dialogo **Modifica password**, quindi fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto** tutte le modifiche vengono annullate.

Password Web/Memorizzazione dati

L'assistenza tecnica Schneider Electric richiede una stringa di caratteri alfanumerici visualizzata nella finestra a comparsa **Password dimenticata** non appena si preme `SHIFT +F2` nella finestra di dialogo **Password**.

Per accedere alla finestra di dialogo **Password**:

- Selezionare **Progetto > Proprietà del progetto > Protezione progetto e controller**
- Nel campo **Memorizzazione dati**, fare clic su **Reimposta password...**. Viene visualizzata la finestra di dialogo **Password**.

Procedura per ripristinare la password della memorizzazione dei dati:

Passo	Azione
1	**Condizione:** viene visualizzata la finestra di dialogo **Password**.
2	Premere `SHIFT+F2`. **Risultato**: si apre la finestra a comparsa **Password dimenticata** e viene visualizzata una stringa di caratteri alfanumerici.
3	Copiare questa stringa e consegnarla all'assistenza tecnica Schneider Electric.
4	Si riceve la password generata dall'assistenza tecnica Schneider Electric. **Nota**: la password è temporanea, valida finché non si modifica l'applicazione.
5	Immettere questa password e fare clic su **OK** per chiudere la finestra di dialogo **Password**.

Passo	Azione
6	Fare clic su **Modifica password** e modificare la password (password precedente = password fornita dall'assistenza Schneider Electric).
7	Fare clic su **OK** per chiudere la finestra di dialogo **Modifica password**, quindi fare clic su **OK** o **Applica** nella finestra **Proprietà del progetto** per confermare tutte le modifiche. Se si fa clic su **Annulla** nella finestra **Proprietà del progetto** tutte le modifiche vengono annullate.

Gestione della sicurezza della workstation

Introduzione

Schneider Electric fornisce lo strumento di gestione di accesso dell'*Editor di sicurezza* utilizzabile per limitare e controllare l'accesso alle workstation su cui è installato il software Control Expert. Questa sezione descrive le funzionalità di questo strumento correlato esclusivamente ai progetti di sicurezza M580.

Gestione dell'accesso a EcoStruxure Control Expert

Introduzione

Schneider Electric fornisce lo strumento di configurazione *Editor di sicurezza* utilizzabile per gestire l'accesso al software EcoStruxure Control Expert installato su una o più workstation. (L'uso di questo strumento è opzionale.)

NOTA: la gestione dell'accesso si riferisce all'hardware, in genere workstation, su cui è installato il software EcoStruxure Control Expert. Il progetto stesso ha un proprio sistema di protezione.

Per ulteriori informazioni, consultare *EcoStruxure™ Control Expert, Editor sicurezza, Guida operativa*.

NOTA: anche i profili utente di sicurezza richiedono autorizzazioni per accedere alla parte processo dell'applicazione di sicurezza. Quando si creano o modificano i profili utente, confermare che tutte le modifiche applicabili siano state eseguite.

Categorie di utenti

L'*Editor di sicurezza* supporta le seguenti categorie di utenti:

- *SecurityAdmin:* solo il *SecurityAdmin* può gestire la sicurezza di accesso per il software. Questo utente amministrativo specifica chi può accedere al software e i relativi diritti di accesso. Durante l'installazione di EcoStruxure Control Expert su una workstation, solo il *SecurityAdmin* può accedere alla configurazione di sicurezza senza alcuna limitazione dei diritti (senza una password).

  NOTA: l'utente *SecurityAdmin* esegue il ruolo amministrativo che era gestito dal ruolo *Supervisore* (*super user*) nelle versioni precedenti di EcoStruxure Control Expert (precedenti alla versione 15.3).

- *Utenti*: gli utenti del software sono definiti nell'elenco di utenti dal *SecurityAdmin* quando la protezione dell'accesso è attiva per EcoStruxure Control Expert. L'utente, il cui nome è incluso nell'elenco utenti, può accedere a un'istanza del software immettendo il proprio nome (esattamente come appare nell'elenco) e la relativa password.

Profilo utente

I profili utente includono tutti i diritti di accesso per gli utenti corrispondenti. Il *SecurityAdmin* può definire in modo personalizzato questi profili, oppure crearli applicando un profilo preconfigurato incluso nello strumento *Editor di sicurezza*.

Profili utente preconfigurati

L'*Editor di sicurezza* offre questi profili utente preconfigurati che si applicano al programma di sicurezza o al programma di processo:

Profilo	Tipo di programma applicabile		Descrizione
	Processo	Sicurezza	
Sola lettura	✓	✓	L'utente può accedere al progetto solo in modalità di lettura, tranne che per l'indirizzo PAC, che può essere modificato. L'utente può inoltre copiare o scaricare il progetto.
Operativo	✓	—	L'utente dispone degli stessi diritti concessi al profilo **Sola lettura**, a cui è stata aggiunta la possibilità di modificare i parametri di esecuzione del programma di processo (costanti, valori iniziali, durate dei cicli di task e così via).
Sicurezza_ Operativo	—	✓	L'utente dispone degli stessi diritti concessi al profilo **Operativo** ma rispetto al programma di sicurezza, con le seguenti eccezioni: • Il trasferimento dei valori dei dati al PAC non è consentito. • Il comando del programma di sicurezza per entrare in modalità di manutenzione è consentito.
Regolazione	✓	—	L'utente dispone degli stessi diritti concessi al profilo **Operativo**, con la possibilità aggiuntiva di caricare un progetto (trasferimento al PAC) e di modificare la modalità operativa del PAC (**Run**, **Stop**, ...)
Regolazione_ Sicurezza	—	✓	L'utente dispone degli stessi diritti concessi al profilo **Regolazione** ma rispetto al programma di sicurezza, con le seguenti eccezioni: • Il trasferimento dei valori dei dati al PAC non è consentito.

Profilo	Tipo di programma applicabile		Descrizione
	Processo	Sicurezza	
			• Il comando del programma di sicurezza per entrare in modalità di manutenzione è consentito.
Debug	✓	—	L'utente dispone degli stessi diritti concessi al profilo **Regolazione**, con la possibilità aggiuntiva di utilizzare gli strumenti di debug.
Debug_Sicurezza	—	✓	L'utente dispone degli stessi diritti concessi al profilo **Debug** ma rispetto al programma di sicurezza, con le seguenti eccezioni: • L'arresto o l'avvio del programma non è consentito. • L'aggiornamento dei valori di inizializzazione non è consentito. • Il trasferimento dei valori dei dati al PAC non è consentito. • La forzatura di ingressi, uscite o bit interni non è ammessa. • Il comando del programma di sicurezza per entrare in modalità di manutenzione è consentito.
Programma	✓	—	L'utente dispone degli stessi diritti concessi al profilo **Debug**, con la possibilità aggiuntiva di modificare il programma.
Programma_ Sicurezza	—	✓	L'utente dispone degli stessi diritti concessi al profilo **Programma** ma rispetto al programma di sicurezza, con le seguenti eccezioni: • L'arresto o l'avvio del programma non è consentito. • L'aggiornamento dei valori di inizializzazione non è consentito. • Il trasferimento dei valori dei dati al PAC non è consentito. • Il ripristino del progetto nel PAC da un backup salvato non è consentito. • La forzatura di ingressi, uscite o bit interni non è ammessa. • Il comando del programma di sicurezza per entrare in modalità di manutenzione è consentito.
Disattivato	✓	—	Gli utenti non possono accedere al progetto.

Assegnazione di un utente preconfigurato

Il *SecurityAdmin* può assegnare un utente preconfigurato, derivato da un profilo preconfigurato, a un utente specifico nella scheda **Utenti** dell'*Editor di sicurezza*. Sono disponibili le seguenti selezioni utente preconfigurate:

- Regolazione_utente_sicurezza
- Debug_utente_sicurezza
- Operativo_utente_sicurezza
- Programma_utente_sicurezza
- Regolazione_utente
- Debug_utente
- Operativo_utente
- Programma_utente

Vedere la descrizione del *certificate whitelist* in *EcoStruxure EcoStruxure Control Expert, Editor di sicurezza, Guida al funzionamento*.

Diritti di accesso

Introduzione

Questa sezione presenta i diritti di accesso disponibili per ciascuno dei profili utente preconfigurati.
I diritti di accesso di EcoStruxure Control Expert sono raggruppati nelle categorie seguenti:

- Topology Manager

I diritti di accesso di EcoStruxure Control Expert Classic sono raggruppati nelle categorie seguenti:

- Servizi del progetto
- Regolazione/debug
- Librerie
- Modifica globale
- Modifica elementare di una variabile
- Modifica elementare di dati composti DDT
- Modifica elementare di un tipo DFB
- Modifica elementare di un'istanza DFB
- Editor di configurazione del bus
- Editor di configurazione degli I/O
- Schermate di runtime
- Sicurezza informatica
- Sicurezza

NOTA: i diritti di accesso di EcoStruxure Control Expert Classic si applicano anche a Editor Control Expert.

Topology Manager

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Create progetto di sistema	–	–	–	–	–	–	✓	✓
Modify progetto di sistema	–	–	–	–	–	–	✓	✓
Import progetto di sistema	–	–	–	–	–	–	✓	✓
Delete progetto di sistema	–	–	–	–	–	–	✓	✓
Manage progetto di sistema settings	–	–	–	–	–	–	✓	✓

✓ : incluso

– : non incluso

Servizi del progetto

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Crea un nuovo progetto	–	–	–	–	–	–	✓	✓
Apri un progetto esistente	✓	✓	✓	✓	✓	✓	✓	✓
Salva un progetto	–	–	–	–	–	–	✓	✓
Salva un progetto con nome	✓	✓	✓	✓	✓	✓	✓	✓

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Importa un progetto	–	–	–	–	–	–	✓	✓
Crea offline	–	–	–	–	–	–	✓	✓
Arrestare build online	–	–	–	–	–	–	✓	✓
Eseguire build online	–	–	–	–	–	–	✓	✓
Avvia, arresta o inizializza il PAC*	✓	–	✓	–	–	–	✓	✓
Aggiorna i valori iniz con i valori correnti (solo dati non sicuri)	–	–	✓	–	–	–	✓	✓
Trasferimento del progetto dal PAC	✓	✓	✓	✓	✓	✓	✓	✓
Trasferimento del progetto al PAC	✓	✓	✓	✓	–	–	✓	✓
Trasferimento dei valori dei dati da file a PAC (solo dati non sicuri)	✓	–	✓	–	✓	–	✓	✓
Ripristina backup progetto nel PAC	–	–	–	–	–	–	✓	✓
Salva nel backup progetto nel PAC	–	–	–	–	–	–	✓	✓
Imposta indirizzo	✓	✓	✓	✓	✓	✓	✓	✓
Modifica opzioni	✓	✓	✓	✓	✓	✓	✓	✓

* Solo i task processo vengono avviati o arrestati. Per un PAC non di sicurezza, questo significa che il PAC viene avviato o arrestato. Per un PAC M580 Safety, questo significa che i task diversi dal task SAFE vengono avviati o arrestati.

✓ : Incluso

– : non incluso

Regolazione/debug

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_ Sicurezza	Debug	Debug_ Sicurezza	Operativo	Operativo_ Sicurezza	Programma	Programma_ Sicurezza
Modifica valori variabili	✓	–	✓		✓		✓	✓
Modifica valori variabile di sicurezza	–	✓	–	✓	–	✓	–	✓
Forza bit interni	–	–	✓	–	–	–	✓	✓
Forza uscite	–	–	✓	–	–	–	✓	✓
Forza ingressi	–	–	✓	–	–	–	✓	✓
Gestione task	–	–	✓	–	–	–	✓	✓
Gestione task SAFE	–	–	–	✓	–	–	–	✓
Modifica del periodo di ciclo del task	✓	–	✓		✓	–	✓	✓
Modifica durata ciclo task SAFE	–	✓	–	✓	–	✓	–	✓
Elimina messaggio nel visualizzatore	✓	✓	✓	✓	✓	✓	✓	✓
Debug dell'eseguibile	–	–	✓	✓	–	–	✓	✓
Sostituisci una variabile del progetto	–	–	–	–	–	–	✓	✓
Sostituisci una variabile del progetto di sicurezza	–	–	–	–	–	–	–	✓

✓ : incluso

– : non incluso

Librerie

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_ Sicurezza	Debug	Debug_ Sicurezza	Operativo	Operativo_ Sicurezza	Programma	Programma_ Sicurezza
Crea librerie o famiglie	–	–	–	–	–	–	✓	✓
Crea famiglie o librerie di sicurezza	–	–	–	–	–	–	–	✓
Elimina librerie o famiglie	–	–	–	–	–	–	✓	✓
Elimina famiglie o librerie di sicurezza	–	–	–	–	–	–	–	✓
Poni l'oggetto nella libreria	–	–	–	–	–	–	✓	✓
Poni l'oggetto nella libreria di sicurezza	–	–	–	–	–	–	–	✓
Elimina un oggetto dalla libreria	–	–	–	–	–	–	✓	✓
Elimina un oggetto dalla libreria di sicurezza	–	–	–	–	–	–	–	✓
Recupera oggetto da una libreria	–	–	–	–	–	–	✓	✓
Recupera un oggetto dalla libreria di sicurezza	–	–	–	–	–	–	–	✓

✓ : incluso

– : non incluso

Modifica globale

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_ Sicurezza	Debug	Debug_ Sicurezza	Operativo	Operativo_ Sicurezza	Programma	Programma_ Sicurezza
Modifica documentazione	✓	✓	✓	✓	✓	✓	✓	✓
Modifica la vista funzionale	–	–	–	–	–	–	✓	✓

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica le tabelle di animazione	✓	✓	✓	✓	✓	✓	✓	✓
Modifica valore delle costanti	✓	–	✓	–	✓	–	✓	✓
Modifica valore delle costanti di sicurezza	–	✓	–	✓	–	✓	–	✓
Modifica la struttura del programma	–	–	–	–	–	–	✓	✓
Modifica la struttura del programma di sicurezza	–	–	–	–	–	–	–	✓
Modifica sezioni programma	–	–	–	–	–	–	✓	✓
Modifica sezioni programma di sicurezza	–	–	–	–	–	–	–	✓
Modifica le impostazioni del progetto	–	–	–	–	–	–	✓	✓
✓ : incluso – : non incluso								

Modifica elementare di una variabile

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Rimozione/aggiunta variabile	–	–	–	–	–	–	✓	✓
Rimozione/aggiunta variabili di sicurezza	–	–	–	–	–	–	–	✓
Modifica attributi principali della variabile	–	–	–	–	–	–	✓	✓

Diritto di accesso	Profilo utente preconfigurato							
	Rego-lazione	Rego-lazio-ne_ Sicu-rezza	Debug	De-bug_ Sicu-rezza	Operati-vo	Operati-vo_ Sicurez-za	Program-ma	Pro-gram-ma_ Sicurez-za
Modifica attributi principali variabili di sicurezza	–	–	–	–	–	–	–	✓
Modifica attributi secondari della variabile	✓	–	✓	–	✓	–	✓	✓
Modifica attributi secondari variabili di sicurezza	–	✓	–	✓	–	✓	–	✓
✓ : incluso – : non incluso								

Modifica elementare di dati composti DDT

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regola-zione	Regola-zione_ Sicurez-za	Debug	Debug_ Sicurez-za	Operati-vo	Operati-vo_ Sicurez-za	Program-ma	Pro-gram-ma_ Sicurez-za
Rimozione/ aggiunta DDT	–	–	–	–	–	–	✓	✓
Modifiche DDT	–	–	–	–	–	–	✓	✓
✓ : incluso – : non incluso								

Modifica elementare di un tipo DFB

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_ Sicurezza	Debug	Debug_ Sicurezza	Operativo	Operativo_ Sicurezza	Programma	Programma_ Sicurezza
Rimozione/aggiunta tipo DFB	–	–	–	–	–	–	✓	✓
Rimozione/aggiunta tipo DFB di sicurezza	–	–	–	–	–	–	–	✓
Modifica struttura tipo DFB	–	–	–	–	–	–	✓	✓
Modifica struttura tipo DFB di sicurezza	–	–	–	–	–	–	–	✓
Modifica sezioni tipo DFB	–	–	–	–	–	–	✓	✓
Modifica sezioni tipo DFB di sicurezza	–	–	–	–	–	–	–	✓
✓ : incluso – : non incluso								

Modifica elementare di un'istanza DFB

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_ Sicurezza	Debug	Debug_ Sicurezza	Operativo	Operativo_ Sicurezza	Programma	Programma_ Sicurezza
Modifica istanza DFB	–	–	–	–	–	–	✓	✓
Modifica istanza DFB di sicurezza	–	–	–	–	–	–	–	✓
Modifica attributi secondari istanza DFB	✓	–	✓	–	✓	–	✓	✓
Modifica attributi secondari istanza DFB di sicurezza	–	✓	–	✓	–	✓	–	✓
✓ : incluso – : non incluso								

Editor di configurazione del bus

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica configurazione	–	–	–	–	–	–	✓	✓
Modifica della configurazione di sicurezza	–	–	–	–	–	–	–	✓
Rilevamento I/O	–	–	–	–	–	–	✓	✓

✓ : incluso

– : non incluso

Editor di configurazione degli I/O

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica configurazione I/O	–	–	–	–	–	–	✓	✓
Modifica della configurazione degli I/O di sicurezza	–	–	–	–	–	–	–	✓
Regola I/O	✓	–	✓	–	✓	–	✓	✓
Regola I/O di sicurezza	–	✓	–	✓	–	✓	–	✓
Salva_param	–	–	✓	–	–	–	✓	✓
Ripristina_param	–	–	✓	–	–	–	✓	✓

✓ : incluso

– : non incluso

Schermate di runtime

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Modifica schermate	–	–	–	–	–	–	✓	✓
Modifica messaggi	–	–	–	–	–	–	✓	✓
Aggiungi/rimuovi schermate o famiglie	–	–	–	–	–	–	✓	✓
✓ : incluso – : non incluso								

Sicurezza informatica

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	Regolazione_Sicurezza	Debug	Debug_Sicurezza	Operativo	Operativo_Sicurezza	Programma	Programma_Sicurezza
Crea o modifica password applicazione	–	–	–	–	–	–	✓	✓
Entra in modalità manutenzione	–	✓	–	✓	–	✓	–	✓
Adatta timeout blocco automatico	✓	✓	✓	✓	✓	✓	✓	✓
✓ : incluso – : non incluso								

Sicurezza

Questa categoria dispone dei seguenti diritti d'accesso:

Diritto di accesso	Profilo utente preconfigurato							
	Regolazione	**Regolazione_ Sicurezza**	**Debug**	**Debug_ Sicurezza**	**Operativo**	**Operativo_ Sicurezza**	**Programma**	**Programma_ Sicurezza**
Entra in modalità manutenzione	–	✓	–	✓	–	✓	–	✓

✓ : incluso

– : non incluso

Modifiche a Control Expert per il sistema di sicurezza M580

Introduzione

Questa sezione descrive la funzionalità Control Expert che è stata modificata o limitata per il sistema di sicurezza M580.

Trasferimento e importazione di codice e progetti di sicurezza M580 in Control Expert

Trasferimento di un progetto di sicurezza da Control Expert al PAC di sicurezza

È possibile utilizzare il comando **PLC > Trasferisci progetto al PLC** per trasferire il progetto da Control Expert al PAC quando:

- Control Expert è collegato in modalità di programmazione (vedi EcoStruxure™ Control Expert, Modalità operative) al PAC di sicurezza M580 e
- in Control Expert è aperto un progetto e
- tutti i task PAC sono in stato STOP.

NOTA: Un'applicazione di sicurezza può essere trasferita solo a un PAC di sicurezza. Non si può trasferire un'applicazione di sicurezza a un PAC non di sicurezza.

Trasferimento di un progetto di sicurezza dal PAC di sicurezza a Control Expert

Analogamente, è possibile utilizzare il comando **PLC > Trasferisci progetto dal PLC** per trasferire il progetto dal PAC a Control Expert quando:

- Control Expert è collegato in modalità di programmazione (vedi EcoStruxure™ Control Expert, Modalità operative) al PAC di sicurezza M580 e
- non vi sono progetti aperti in Control Expert.

È possibile trasferire il contenuto relativo a qualsiasi task (SAFE, MAST, FAST, AUX0 o AUX1) nella modalità operativa di sicurezza o di manutenzione.

Importazione di progetti e di sezioni di codice in Control Expert

Control Expert Safety supporta l'importazione sia di progetti interi (tramite **File > Apri**) sia di sezioni di codice (via **Task > Importa...** o **Sezioni > Importa...**), secondo le condizioni seguenti:

- Solo i tipi di funzioni o di blocchi funzione esistenti nella libreria di sicurezza (**Data Scope Editor > <Libset> > Safety**) oppure nella libreria personalizzata (**Data Scope Editor > <Libset> > Libreria personalizzata**, possono essere inclusi in una sezione di codice gestita dal task SAFE.
- Solo i tipi di funzioni o di blocchi funzione esistenti in librerie diverse dalla libreria di sicurezza possono essere inclusi in una sezione del codice non SAFE gestita da un task di processo (MAST, FAST, AUX0 o AUX1).

Salvataggio e ripristino di dati tra un file e il PAC

Funzioni di salvataggio e ripristino per i dati non di sicurezza

Control Expert supporta i comandi **PLC > Salva i dati dal PLC al file** e **PLC > Recupera i dati dal file al PLC** per i dati dell'area di processo e globali. Tuttavia, i dati salvati e ripristinati non includono le variabili e le istanze di blocchi funzione create nello spazio dei nomi sicuro.

Per informazioni su come utilizzare questi comandi per i dati non sicuri, vedere l'argomento *Salvataggio/ripristino di dati tra un file e il PLC* nel documento *EcoStruxure™ Control Expert - Modalità operative*.

CCOTF per un PAC di sicurezza M580

Modifica al volo della configurazione

La funzione di modifica al volo della configurazione (CCOTF) permette di modificare una configurazione di Control Expert mentre il PAC è in funzione. Le funzioni supportate possono includere:

- Aggiunta di una derivazione.
- Aggiunta di un modulo di I/O.
- Eliminazione di un modulo di I/O.

- Modifica della configurazione di un modulo di I/O, incluso:
  - Modifica di un'impostazione dei parametri.
  - Aggiunta di una funzione del canale.
  - Eliminazione di una funzione del canale.
  - Modifica di una funzione del canale.

  NOTA: Le funzioni CCOTF non si applicano ai dispositivi CIP Safety.

La funzione CCOTF viene attivata selezionando **Modifica online in modalità RUN o STOP** nella scheda **Configurazione** del modulo CPU.

La funzionalità di base della funzione CCOTF è stata implementata nel PAC di sicurezza M580, con le limitazioni descritte sotto.

Per una descrizione completa della funzione CCOTF, vedere *Modicon M580 Modifica della configurazione al volo Guida utente*.

Limitazioni di CCOTF per un PAC di sicurezza M580

La funzione CCOTF è implementata nel PAC di sicurezza M580 con una serie di limitazioni legate alla funzione specifica e dal tipo di modulo di I/O, nel seguente modo:

Funzione CCOTF	**Tipo di modulo di I/O e modalità operativa**			
	I/O non interferenti		**I/O di sicurezza SIL3**	
	Modalità di manutenzione	**Modalità di sicurezza**	**Modalità di manutenzione**	**Modalità di sicurezza**
Aggiungi derivazione	✓	✓	✓[1]	✓
Aggiungi modulo	✓	✓	✓[1]	**X**
Elimina modulo	✓	✓	✓	**X**
Modifica configurazione modulo I/O	✓	✓	**X**	**X**

✓: Consentita

X: Non consentita

1.Per aggiungere una derivazione e un modulo di sicurezza sono necessarie due sessioni CCOTF: una sessione CCOTF per aggiungere la derivazione e una seconda sessione CCOTF per aggiungere il modulo di sicurezza. Queste azioni non possono essere eseguite in una sola sessione CCOTF.

NOTA: Le modifiche effettuate in una sola sessione CCOTF possono riferirsi solo a un singolo task (SAFE, MAST, FAST, AUX0 o AUX1).

Modifiche dei tool del PAC di sicurezza M580

Introduzione

Il PAC di sicurezza M580 supporta l'uso di vari tool correlati. Alcuni di questi tool sono stati modificati per essere utilizzati insieme al PAC di sicurezza M580. In questa sezione sono descritti alcuni di questi tool.

Uso della memoria

La schermata **Uso della memoria** contiene le seguenti informazioni:

- la distribuzione fisica del PAC (memoria iniziale e scheda di memoria)
- lo spazio di memoria utilizzato da un progetto (dati, programma, configurazione, sistema)

Per il PAC di sicurezza M580, questa schermata contiene due nuovi parametri specifici – **Dati di sicurezza dichiarati** e **Codice di sicurezza eseguibile** – che sono descritti di seguito.

NOTA: Si può anche usare il comando **Pack** in questa schermata per riorganizzare la memoria laddove possibile.

Per ulteriori informazioni vedere la sezione *Uso della memoria* nel manuale utente *EcoStruxure™ Control Expert, Modalità operative*.

Per il PAC di sicurezza M580 vengono visualizzati i seguenti parametri:

Parametro	Descrizione
Dati utente	Questo campo indica lo spazio di memoria (in parole) occupato dai dati utente (oggetti relativi alla configurazione): • **Dati**: dati identificati associati al processore (%M, %MW, %S, %SW, etc.) o ai moduli di ingresso/uscita. • **Dati dichiarati**: dati non localizzati (dichiarati nell'editor dati di processo) salvati dopo un'interruzione dell'alimentazione. • **Dati dichiarati non salvati**: dati non localizzati (dichiarati nell'editor dati di processo) non salvati dopo un'interruzione dell'alimentazione. • **Dati di sicurezza dichiarati**: dati non localizzati (dichiarati nell'editor dati di sicurezza) non salvati dopo un'interruzione dell'alimentazione.
Programma utente	Questo campo indica lo spazio di memoria (in parole) occupato dal programma del progetto: • **Costanti**: costanti statiche associate al processore (%KW) e ai moduli di ingresso/uscita; valori dati iniziali. • **Codice eseguibile**: codice eseguibile della parte area di processo del programma del progetto, tipi EF, EFB e DFB. • **Informazioni di caricamento**: informazioni per il caricamento di un progetto (codice grafico di linguaggi, simboli, ecc.).

Parametro	Descrizione
	• **Codice di sicurezza eseguibile**: codice eseguibile della parte area di sicurezza del programma del progetto, tipi EF, EFB e DFB.
Altro	Questo campo indica lo spazio di memoria (in parole) occupato dagli altri dati relativi alla configurazione e alla struttura del progetto: • **Configurazione**: altri dati relativi alla configurazione (hardware o software). • **Sistema**: dati utilizzati dal sistema operativo (stack di task, cataloghi, ecc.), • **Diagnostica**: informazioni relative alla diagnostica del processo o del sistema, buffer di diagnostica. • **Dizionario dati**: dizionario delle variabili simbolizzate con le rispettive caratteristiche (indirizzo, tipo, ecc.).
Memoria interna	Questo campo mostra l'organizzazione della memoria PAC interna. Indica anche lo spazio di memoria disponibile (**Totale**), lo spazio di memoria contiguo più grande possibile (**Valore più alto**) e il livello di frammentazione (a causa delle modifiche online).

Visualizzatore eventi

Visualizzatore eventi è una utility MS Windows che cattura gli eventi registrati da Control Expert. Si può usare *Visualizzatore eventi* per visualizzare una cronologia di eventi registrati.

Accedere a *Visualizzatore eventi* in MS Windows nella cartella *Strumenti di amministrazione* del *Pannello di controllo*. Quando si apre l'utility, selezionare **Mostra riquadro di azioni**, quindi fare clic su **Crea visualizzazione personalizzata** per aprire la finestra di dialogo. Qui si può creare una visualizzazione personalizzata per eventi Control Expert.

NOTA: Nella finestra di dialogo **Crea visualizzazione personalizzata**, selezionare prima **Per origine**, quindi selezionare **TraceServer** come origine per visualizzare eventi Control Expert.

CIP Safety

Panoramica

Questo capitolo descrive le comunicazioni CIP Safety IEC 61784-3 supportate dalle CPU di sicurezza indipendenti BMEP58•040S M580.

Introduzione di CIP Safety per PAC Safety M580

Comunicazione CIP Safety

Introduzione

I controller di sicurezza standalone BMEP58•040S supportano la comunicazione CIP Safety (IEC 61784-3) e possono utilizzare questo protocollo per stabilire una connessione con un dispositivo CIP Safety su EtherNet/IP.

CIP Safety utilizza un meccanismo utilizzatore-produttore per lo scambio di dati tra nodi sicuri su EtherNet/IP (la comunicazione DeviceNet o Sercos III non è supportata). Il controller svolge un ruolo di origine che stabilisce una connessione EtherNet/IP Unicast (uno a uno) con ogni dispositivo di sicurezza di destinazione. Il controller può stabilire una connessione CIP Safety con i dispositivi di destinazione che supportano il protocollo CIP Safety e una connessione CIP (non di sicurezza) con i dispositivi di destinazione che supportano il protocollo CIP.

Come per tutti i controller di sicurezza, il controller CIP Safety e il coprocessore eseguono due volte lo stack CIP Safety in parallelo e confrontano i risultati di elaborazione.

Architetture supportate

I controller di sicurezza standalone M580 supportano i dispositivi CIP Safety situati nei cloud DIO.

NOTA: Al momento, non esiste un dispositivo CIP Safety in grado di supportare RSTP che possa essere installato su un rack eX80. Pertanto, attualmente i dispositivi CIP Safety non possono essere collegati alle doppie porte della rete di dispositivi del controller, ma possono essere collegati alla porta Service del controller.

I cloud DIO richiedono solo una connessione unica (non ad anello) in rame e possono essere collegati a:

- un modulo di switch opzionale di rete BMENOS0300
- la porta service del controller.
- la porta service del modulo adattatore Ethernet I/O eX80 BM•CRA312•0 su una derivazione RIO.
- una porta in rame di uno switch a doppio anello Ethernet.

NOTA: Quando un dispositivo CIP Safety è collegato alla porta service di un modulo adattatore Ethernet I/O eX80 BM•CRA312•0 su una derivazione RIO, il dispositivo CIP Safety di destinazione potrebbe non avviarsi automaticamente durante il caricamento della configurazione CRA. Per aprire nel modo previsto le connessioni CIP Safety, potrebbe essere necessario gestire il bit di controllo della connessione CIP Safety nel DDDT di destinazione (CTRL_IN o CTRL _OUT) commutandolo da False a True dopo il caricamento della configurazione di BM•CRA312•0.

Come per tutte le apparecchiature situate nei cloud DIO, i dispositivi CIP Safety non vengono analizzati come parte dell'anello principale RIO e il loro stato di connessione non viene riflesso nei LED del controller.

Per maggiori informazioni sui cloud DIO, consultare *Guida di pianificazione del sistema Modicon M580 indipendente per le architetture utilizzate più di frequente* e *Guida di pianificazione del sistema Modicon M580 per le topologie complesse*.

Panoramica della configurazione

La configurazione delle comunicazioni CIP Safety comprende tre attività di configurazione distinte:

- Configurare il controller standalone M580 Safety con le impostazioni CIP Safety in Control Expert, pagina 355. Ciò comprende la creazione di un Identificativo di rete univoco dell'origine (OUNID) che identifica in modo univoco il controller. L'OUNID creato in Control Expert è formato dalla concatenazione di due elementi:
  - Numero di rete di sicurezza (SNN): Un identificativo per il controller creato in Control Expert.
  - Indirizzo IP principale del controller, immesso in Control Expert come parte delle impostazioni dell'indirizzo IP del controller.

  Configurare l'impostazione OUNID del controller una sola volta, nella configurazione iniziale. Se successivamente si modifica l'impostazione OUNID, sarà necessario riconfigurare anche tutti i dispositivi CIP Safety collegati al controller.
- Configurare il dispositivo CIP Safety, pagina 359, utilizzando uno strumento di configurazione di rete di sicurezza (SNCT) offerto dal fornitore del dispositivo. Ciò comprende due attività:
  - Creazione di un identificativo di configurazione di sicurezza (SCID): noto anche come firma di configurazione, lo SCID viene creato nell'SNCT e utilizzato da Control Expert quando si configura la connessione CIP Safety tra l'origine (controller) e la destinazione (dispositivo CIP Safety).
  - Assegnazione di un numero di rete di sicurezza (SNN): l'SNN viene generalmente creato per il dispositivo CIP Safety da Control Expert e assegnato al dispositivo dall'SNCT.

- Configurare la connessione CIP Safety tra il controller e il dispositivo CIP Safety, pagina 361. La connessione viene identificata da un TUNID, creato utilizzando la connessione di dispositivo DTM in Control Expert e utilizzando un DTM CIP Safety, che può essere basato su un file EDS fornito dal produttore o utilizzato singolarmente se non sono disponibili file EDS.

Gestione delle connessioni di dispositivo CIP Safety

Il controller CIP Safety stabilisce una connessione con un dispositivo CIP configurato, quindi gestisce il dispositivo collegato. Questo perché Control Expert supporta sia il protocollo CIP che il protocollo CIP Safety e può gestire le connessioni CIP verso:

- i dispositivi CIP, che implementano CIP, ma non CIP Safety, su EtherNet/IP.
- i dispositivi CIP Safety, che implementano CIP Safety, ma non CIP, su Ethernet/IP.
- i dispositivi ibridi CIP, che implementano sia CIP che CIP Safety su EtherNet/IP.

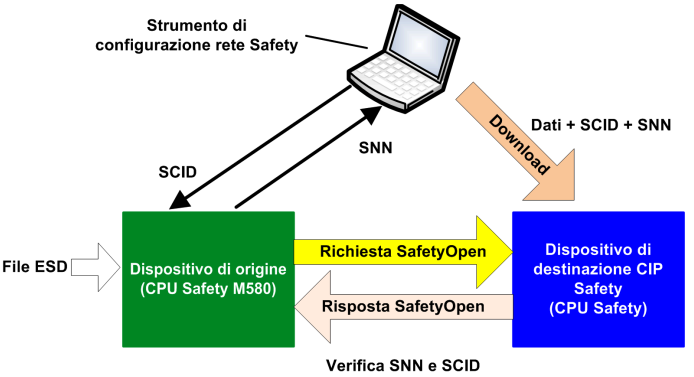
NOTA: Per la configurazione, i dispositivi CIP e CIP Safety necessitano ciascuno di un unico DTM. Un dispositivo ibrido CIP, che ingloba i protocolli CIP e CIP Safety, necessita di due DTM, uno configurato come dispositivo CIP, l'altro come dispositivo CIP Safety.

Come stabilire una connessione origine -> destinazione

Il controller standalone M580 utilizza solo la richiesta apertura di sicurezza di tipo 2 per stabilire una connessione con un dispositivo CIP Safety. Una connessione apertura di sicurezza di tipo 2 può essere stabilita verso un dispositivo di sicurezza solo dopo che il dispositivo sia stato configurato come SNCT. Ne caso in cui il dispositivo Cip Safety sia un prodotto di terze parti, Control Expert non possiede e non può scaricare un file di configurazione su un dispositivo CIP Safety e non può essere utilizzato come SNCT.

NOTA: Al contrario, una connessione apertura di sicurezza di tipo 1 può fornire al dispositivo di sicurezza le proprie impostazioni di configurazione e stabilire la connessione. I controller M580 CIP Safety non supportano la richiesta di connessione apertura di sicurezza di tipo 1.

Lo schema seguente presenta una panoramica della modalità di creazione di una connessione CIP Safety tra il controller come origine di connessione e il dispositivo CIP Safety come destinazione di connessione:



In questo diagramma si verificano i seguenti eventi:

1. Control Expert utilizza un file EDS offerto dal fornitore come base per la creazione di un DTM per la connessione tra il controller e il dispositivo CIP Safety.
2. Il dispositivo SNN viene creato in Control Expert, quindi immesso nell'SNCT.
3. L'SNCT crea lo SCID per il dispositivo, che viene inserito in Control Expert come parte della configurazione di connessione.
4. L'SNCT scarica sul dispositivo le proprie impostazioni di configurazione, lo SCID creato dall'SNCT e l'SNN creato da Control Expert per la connessione.
5. Il controller come origine invia al dispositivo una Richiesta apertura di sicurezza di tipo 2.
6. Il dispositivo CIP Safety invia una Risposta di apertura di sicurezza al controller.
7. Se il checksum corrisponde sia nella richiesta che nella risposta, la connessione viene stabilita.

Configurazione della CPU CIP Safety M580

Panoramica

Questa sezione descrive le modalità di configurazione della CPU indipendente CIP Safety come origine per le comunicazioni CIP Safety.

Configurazione dell’OUNID CPU

CPU come origine

Utilizzare la scheda**Sicurezza** della (vedi Modicon M580, Hardware, Manuale di riferimento) CPU di sicurezza indipendente M580 per configurare la CPU come CIP Safety origine, assegnandole un Identificativo di rete univoco di origine (OUNID).

Un OUNID è un valore esadecimale concatenato da 10 byte, composto da:

- Numero di rete di sicurezza (6 byte)
- Indirizzo IP (4 byte)

NOTA: Le modifiche all'OUNID possono essere effettuate solo offline. Dopo la creazione della configurazione modificata, l'applicazione può essere scaricata sul PAC.

Numero di rete di sicurezza

Il Numero di rete di sicurezza componente dell'OUNID può essere generato automaticamente da Control Expert, o generato dall'utente con immissione manuale. Creare l’SNN::

- Automaticamente, selezionando**Basato su tempo**, quindi facendo clic sul pulsante **Genera**. Il valore generato automaticamente viene visualizzato nel campo **Numero**.
- Manualmente, selezionando **Manuale**, quindi immettendo una stringa esadecimale da 6 byte nel campo **Numero**.

NOTA: È necessario che l'utente assegni un SNN univoco a ciascuna origine CPU M580 collegata alla stessa rete di sicurezza.

Indirizzo IP

L'impostazione di sola lettura viene inserita automaticamente, in base all'impostazione dell'**Indirizzo IP principale** della CPU nella scheda **IPConfig** Modicon M580, Hardware, Manuale di riferimento.

OUNID

Dopo la creazione, l'OUNID viene utilizzato come parametro nella Richiesta di apertura di sicurezza di tipo 2,, pagina 376 stabilendo una connessione tra la CPU come origine e il dispositivo CIP Safety come destinazione.

Configurazione del dispositivo CIP Safety di destinazione

Panoramica

Questa sezione descrive il processo di configurazione del dispositivo CIP Safety, compresa la sua configurazione con l'utilizzo di uno strumento di configurazione offerto dal fornitore.

Panoramica di configurazione del dispositivo CIP Safety

Introduzione

La configurazione del dispositivo CIP Safety di destinazione comprende due attività:

- Configurare le impostazioni del dispositivo di destinazione CIP Safety, pagina 359 utilizzando uno strumento di configurazione di rete di sicurezza (SNCT) offerto dal fornitore.
- Configurare la connessione tra l'origine della CPU CIP Safety e il dispositivo CIP di destinazione, utilizzando un DTM in Control Expert. Il DTM può essere:
  - basato su un file EDS offerto dal fornitore.
  - un DTM generico di Control Expert, se non sono disponibili file EDS.

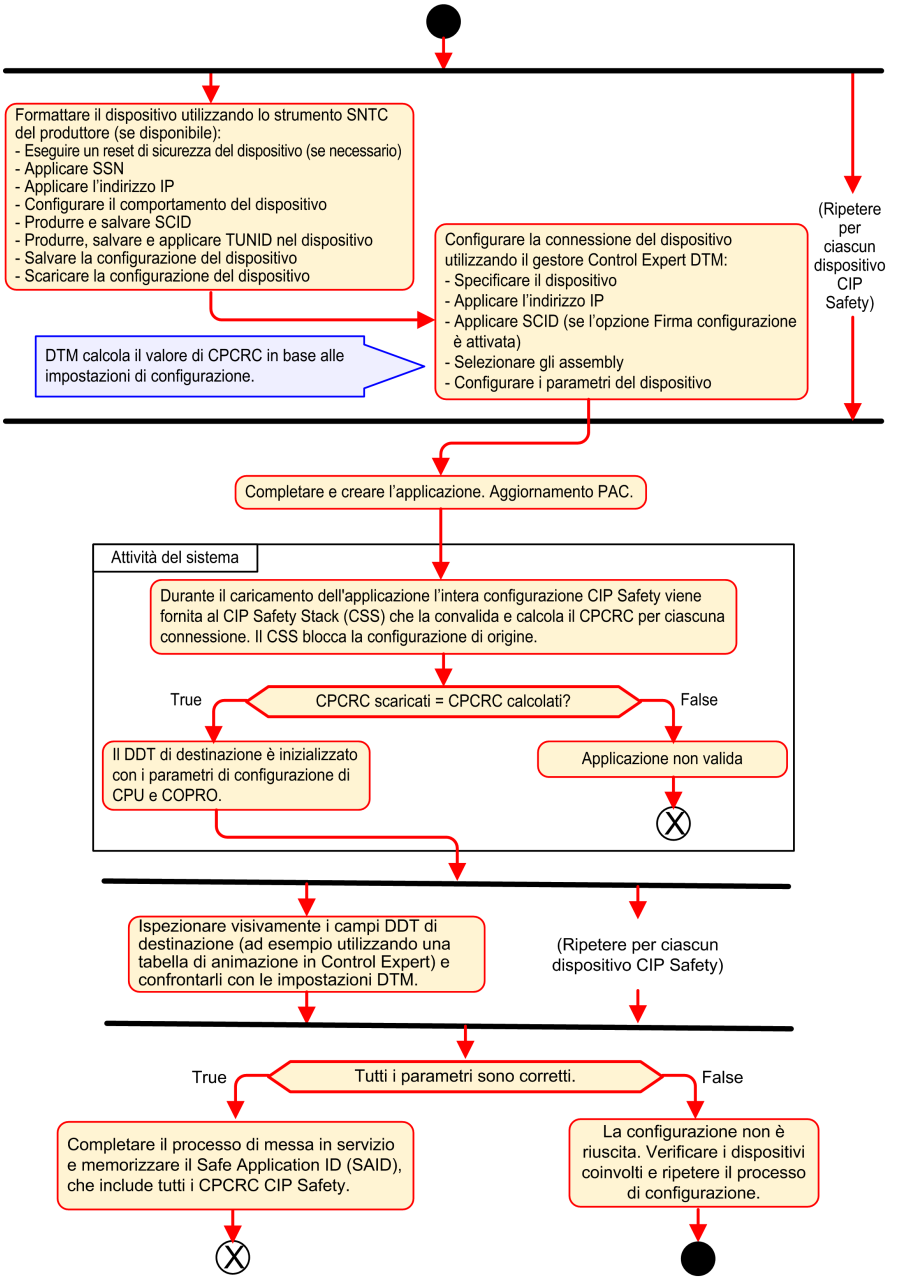
Verifica di configurazione doppia

I seguenti due processi, insieme, forniscono una conferma di integrità elevata che la configurazione creata con il software Control Expert è stata scaricata e salvata in modo corretto nella CPU CIP Safety M580 come origine:

- Un confronto visivo eseguito dall'utente (dopo il completamento dell'operazione) dei parametri di configurazione della connessione CIP Safety visualizzati nella destinazione DDDT rispetto agli stessi parametri visualizzati nel DTM di destinazione.
- Un confronto automatico, eseguito da CPU e Copro, del parametro di connessione CPCRC CRC calcolato dal DTM rispetto al CPCRC calcolato dallo stack CIP Safety (CSS) in esecuzione in CPU e Copro.

Panoramica del processo di configurazione

Il processo di configurazione e convalida del dispositivo CIP Safety:



Configurazione del dispositivo CIP Safety con l'utilizzo di uno strumento offerto dal fornitore

Introduzione

Il dispositivo di destinazione CIP Safety viene configurato utilizzando uno strumento di configurazione di rete di sicurezza (SNCT). Non è configurato con il software Control Expert. L'SNCT viene offerto dal fornitore del dispositivo CIP Safety, quindi è collegato al dispositivo.

Usare l'SNCT per:

- Configurare e scaricare sul dispositivo le impostazioni necessarie al suo funzionamento.
- Configurare, quindi copiare e trasferire al software Control Expert, un Identificativo di configurazione di sicurezza specifico per il dispositivo (SCID). Lo SCID viene denominato Firma di configurazione del dispositivo. Viene utilizzato in Control Expert per la configurazione della connessione Origine -> Destinazione., pagina 366
- Assegnare al dispositivo il TUNID univoco, composto da:
  - Numero di rete di sicurezza (SNN), pagina 365 e
  - Indirizzo IP univoco.

    NOTA: L'SNN viene solitamente generato da un software di configurazione Control Expert (come parte della configurazione di connessione Origine -> Destinazione) e applicato al dispositivo. L'indirizzo IP viene immesso sia nell'SNCT che nel DTM di connessione del dispositivo in Control Expert.

Configurazione dello SCID

Lo SCID viene impostato nell'SNCT e svolge la funzione di identificativo univoco di configurazione esadecimale per il dispositivo di destinazione CIP Safety. È una concatenazione di:

- Configurazione di sicurezza CRC (SCCRC): un valore di controllo di ridondanza ciclico (CRC) delle impostazioni di configurazione del dispositivo CIP Safety, costituito da 4 byte.
- Timestamp di configurazione di sicurezza (SCTS): un valore timestamp esadecimale di data e ora costituito da 6 byte.

NOTA: Se si configura un controller M580 come origine CIP Safety, testare e verificare il comportamento funzionale di CIP Safety del sistema prima di utilizzare la comunicazione CIP Safety per controllare la funzione di sicurezza correlata. Dopo aver completato correttamente il test e la verifica, abilitare la firma di configurazione di destinazione CIP Safety (se presente) nei DTM CIP Safety di Control Expert.

Dopo aver creato lo SCID con SNCT, è possibile immettere gli elementi dello SCID nella scheda **Sicurezza** del DTM dispositivo in Control Expert:

- **ID**: Immettere il valore SCCRC.
- **Data:** immettere la data di creazione dello SCID (mm/gg/aaaa).
- **Ora**: immettere l'ora di creazione dello SCID (hh/mm/ss/ms).

Sequenza di configurazione del dispositivo CIP Safety

Questa sequenza descrive un tipico processo di configurazione del dispositivo CIP Safety:

1. Ottenere l'SNN del dispositivo (ricevuto da Control Expert).
2. Applicare l'SNN nell'SNCT del fornitore.
3. Eseguire un reset di sicurezza del dispositivo (opzionale: se l'OUNID di origine è cambiato dall'ultimo collegamento del dispositivo).
4. Applicare il TUNID nel dispositivo.
5. Determinare le impostazioni di configurazione che controllano il comportamento del dispositivo.
6. Configurare il dispositivo con l'SNCT del fornitore (strumento di configurazione di rete di sicurezza).
7. Bloccare la configurazione e verificarne l'accuratezza.
8. Registrare e salvare i parametri per un futuro utilizzo nella configurazione di origine (SCID, Numeri gruppo, indirizzo IP e così via).
9. Salvare una copia della configurazione del dispositivo per un futuro utilizzo (ad esempio, in caso il dispositivo debba essere sostituito).

Configurazione dei DTM del dispositivo di sicurezza

Panoramica

Questa sezione descrive la configurazione dei dispositivi di sicurezza di destinazione e le relative connessioni alla CPU di origine, utilizzando i DTM in Control Expert.

Lavorare con i DTM

Lavorare con i DTM

La configurazione della connessione tra l'origine CPU e il dispositivo CIP Safety di destinazione viene effettuata utilizzando un DTM. Control Expert supporta l'utilizzo dei seguenti DTM, in base al profilo del dispositivo:

- DTM CIP Safety: per configurare una connessione a un dispositivo CIP Safety. Questa operazione può essere eseguita con un file EDS del fornitore o con il file *EDS di sicurezza generico* incluso in Control Expert.
- DTM generico: per configurare una connessione standard (ossia non di sicurezza) a un dispositivo, basata su un file EDS del fornitore.

Le impostazioni immesse con l'utilizzo di un DTM vengono archiviate nel DDDT, pagina 386 T_CIP_SAFETY_CONF e utilizzate dalla Richiesta di apertura di sicurezza di tipo 2, pagina 376per stabilire una connessione tra la CPU origine e il dispositivo di destinazione.

Quando è disponibile un file EDS

Quando per un dispositivo è disponibile un file EDS del fornitore, utilizzarlo per creare un nuovo DTM e aggiungerlo al **Catalogo DTM** in Control Expert come segue:

Passo	Azione
1	In Control Expert, selezionare **Strumenti** > **Browser DTM**.
2	In **Browser DTM**, fare clic con il pulsante destro del mouse su DTM CPU (BMEP58_ECPU_EXT) per aprire il menu contestuale.

Passo	Azione
3	Selezionare il **menu Dispositivo > Funzioni aggiuntive > Aggiungi EDS a libreria**. Si apre la procedura guidata **Aggiunta EDS**.
4	Vedere l'argomento Aggiunta di un file EDS al catalogo hardware (vedere EcoStruxure™ Control Expert, Modalità di funzionamento) per le istruzioni dettagliate su come completare il processo di aggiunta di un file EDS al Catalogo DTM.

Dopo aver aggiunto un DTM al **Catalogo DTM**, è possibile aggiungerlo al progetto Control Expert.

Quando un file EDS non è disponibile

Control Expert include un DTM di sicurezza generico nel **Catalogo DTM**. È possibile utilizzarlo per configurare un dispositivo CIP Safety quando non è disponibile un file EDS per quel dispositivo.

Dispositivi ibridi

Un dispositivo ibrido è un singolo dispositivo in grado di supportare sia connessioni di sicurezza che standard. Quando si aggiunge un dispositivo ibrido al **Catalogo DTM** con il comando **Aggiungi EDS alla libreria**, vengono creati due DTM nel **Catalogo DTM** per il dispositivo: un DTM standard e un DTM di sicurezza.

Quando un dispositivo ibrido viene aggiunto al progetto, è necessario configurare sia il DTM standard che quello di sicurezza per singolo dispositivo.

Aggiunta di un DTM al Progetto Control Expert

Per aggiungere un DTM al Progetto Control Expert:

Passo	Azione
1	Nel **Browser DTM**, fare clic con il pulsante destro del mouse sul DTM CPU (BMEP58_ECPU_EXT) e selezionare **Aggiungi...** Si apre la finestra di dialogo **Aggiungi.**
2	Selezionare il DTM da aggiungere. Può essere: • Un DTM CIP Safety creato da un file EDS del dispositivo CIP Safety del fornitore, o • Un DTM CIP Safety senza un file EDS del fornitore.

Passo	Azione
3	Fare clic su **Aggiungi DTM**. Il DTM selezionato compare nel **Browser DTM** sotto il DTM CPU.
4	Fare clic con il pulsante destro del mouse sul nuovo DTM selezionare **Apri**. Si apre la finestra di configurazione del DTM

Configurazione del DTM

Il DTM CIP Safety, creato con o senza file EDS del fornitore, presenta una serie di schermate di configurazione simili in Control Expert:

Struttura ad albero / Schede di configurazione	Tipo DTM	
	Con EDS del fornitore	Senza EDS del fornitore
<Nodo superiore>	✓	✓
Nodo generale		
Scheda dispositivo	✓	**X**
Scheda di sicurezza	✓	✓
<Connessioni>		
Scheda di connessione	✓	✓
Scheda Verifica identità	✓	✓
Scheda Impostazioni di configurazione	✓	**X**
Scheda di verifica configurazione	✓	✓

< > indica il nome definito dall'utente.

✓ = incluso

X = non incluso

I seguenti argomenti descrivono diverse schede di configurazione presentate da Control Expert per ogni tipo di DTM.

DTM dispositivo di sicurezza - Informazioni su file e fornitore

Introduzione

Il DTM CIP Safety, creato o meno da file EDS, presenta una descrizione del file EDS di origine e del fornitore del dispositivo. Per un:

- DTM CIP Safety creato da file EDS del fornitore queste informazioni sono di sola lettura ed è possibile accedervi solo selezionando il <Nodo superiore> della struttura ad albero del DTM (pannello sinistro).
- DTM CIP Safety creato senza un file EDS queste informazioni sono visibili in due posizioni differenti:
  - con la selezione <Nodo superiore>vengono visualizzate le informazioni di sola lettura del file EDS.

    NOTA: Il riferimento del file EDS è un file EDS di sicurezza generico interno con fornitore Schneider Electric, che viene utilizzato da Control Expert per creare il DTM CIP Safety.
  - Con la selezione della scheda **Generale > Dispositivo** vengono visualizzate le informazioni modificabili sul fornitore.

Informazioni sul file EDS

Le informazioni sul file EDS comprendono i seguenti dati di sola lettura:

- Descrizione
- Data creazione del file
- Ora creazione del file
- Data ultima modifica
- Ora ultima modifica
- Revisione EDS

Informazioni sul fornitore

Le seguenti informazioni sul fornitore solo di sola lettura per un DTM CIP Safety creato da un file EDS del fornitore:

- Nome del fornitore
- Tipo di dispositivo

- Revisione maggiore
- Revisione minore
- Nome prodotto

Le seguenti informazioni sul fornitore sono di lettura-scrittura per un DTM CIP Safety creato senza un file EDS del fornitore:

- ID fornitore
- Tipo prodotto
- Codice prodotto
- Revisione maggiore
- Revisione minore

NOTA: Per le configurazioni di DTM effettuate senza un file EDS, immettere le impostazioni del fornitore con le informazioni fornite da quest'ultimo. Per impostazione predefinita, i valori del fornitore DTM sono impostati su 0, quando i valori a 0 non sono supportati.

DTM del dispositivo di sicurezza - Numero di rete di sicurezza

Numero di rete di sicurezza

Utilizzare la scheda **Generale > Sicurezza** del DTM del dispositivo CIP Safety per configurare un Numero di rete di sicurezza (SNN) per il dispositivo di sicurezza. L'SNN viene utilizzato per impostare l'Identificativo univoco di rete di destinazione (TUNID). TUNID identifica il dispositivo CIP Safety ed è un componente essenziale della Richiesta di apertura di sicurezza di tipo 2, pagina 376 emessa dal controller di origine per avviare una connessione CIP Safety.

Configurazione dell'SNN

L'SNN è un valore esadecimale che fa parte sia della configurazione di connessione CIP Safety (configurata utilizzando Control Expert) sia della configurazione del dispositivo CIP Safety (configurato utilizzando un SNCT). Tipicamente, l'SNN viene creato in Control Expert, quindi copiato (o immesso nuovamente) nel SNCT. Quindi l'SNCT produce il TUNID sulla base di SNN e indirizzo IP e trasferisce tale valore CIP Safety.

È anche possibile inviare l'SNN direttamente dal DTM di connessione CIP Safety in Control Expert al dispositivo di destinazione, pagina 384.

Per configurare l'SNN:

Passo	Azione
1	Nella scheda **Generale > Sicurezza**, fare clic sul pulsante con i puntini di sospensione (...). Si apre la finestra di dialogo **Numero di rete di sicurezza**.
2	Nella finestra di dialogo **Numero di rete di sicurezza** selezionare uno dei seguenti: • **Basato sul tempo**: per generare un valore esadecimale basato su giorno, mese, anno, ora, minuto, secondo e millisecondo al momento della generazione. • **Manuale**: per generare un valore basato su un valore decimale immesso da 1 a 9999, concatenato con due valori esadecimali, come segue: ◦ parola 1: 0004 (fissa) ◦ parola 2: 0000 (fissa) ◦ parola 3: 0001...270F (il valore esadecimale del valore immesso da 1 a 9999) • **Specifico del fornitore**: un identificativo specifico del fornitore basato su 3 parole esadecimali immesse: ◦ parola 1: 05B5...2DA7 (dal fornitore) ◦ parola 2: 0000 (fissa) ◦ parola 3: 0001...270F (dal fornitore) • Un valore esadecimale immesso direttamente (digitato o incollato), composto da: ◦ parola 1: 2DA8...FFFE ◦ parole 2 e 3: 00000000...05265BFF
3	Per un formato basato sul tempo, manuale o specifico del fornitore, fare clic su **Genera**. Se è stato immesso direttamente un valore esadecimale, fare clic su **Imposta.**
4	Fare clic su **OK** per salvare l'SNN e chiudere la finestra di dialogo. L'SNN viene visualizzato nel campo **Numero di rete di sicurezza**.

Configurazione dello SCID

Lo SCID, chiamato anche Firma di configurazione, viene impostato nello strumento di configurazione di rete di sicurezza offerto dal fornitore (SNCT) e rappresenta l'identificativo di configurazione esadecimale univoco per il dispositivo CIP Safety. È composto da:

- Il CRC di configurazione di sicurezza (SCCRC): è un valore di controllo di ridondanza ciclico (CRC) delle impostazioni di configurazione del dispositivo di sicurezza, sotto forma di un valore esadecimale formato da 4 byte.
- Timestamp configurazione di sicurezza (SCTS): un valore timestamp esadecimale di data e ora formato da 6 byte.

Per inserire lo SCID:

Passo	Azione
1	Ottenere dal dispositivo che utilizza l'SNCT per la connessione i seguenti: • SCCRC • Data (mm/gg/aaaa) e ora (hh/mm/ss/ms) in cui è stata eseguita la configurazione SNCT.
2	Selezionare **Firma di configurazione**.
3	Inserire l'SCCRC nel campo **ID**.
4	Immettere i valori di data e ora nei campi **Data** e **Ora**.

NOTA: Se si configurano le connessioni di sicurezza con uno SCID = 0 (configura SCID disattivato), verificare che l'origine di sicurezza M580 e le destinazioni CIP Safety abbiano le configurazioni corrette.

DTM dispositivo di sicurezza - Verifica e convalida della configurazione

Verifica visiva della configurazione DTM

Utilizzare la scheda **Generale > Verifica configurazione** per il DTM CIP Safety, creato con o senza file EDS del fornitore, per confrontare i parametri definiti in questo DTM (e visualizzati in questa scheda) con quelli impostati nel dispositivo di destinazione DDDT. È anche possibile utilizzare la tabella di animazione in Control Expert, quando quest'ultimo è in modalità connesso ed è collegato a una CPU.

NOTA: Dopo aver scaricato un'applicazione, è necessario verificare visivamente per ciascuna destinazione CIP Safety che tutti i parametri di configurazione CIP Safety scaricati nell'origine M580 per una certa destinazione siano identici a quelli configurati nel DTM di destinazione. Ciò si realizza confrontando i parametri di configurazione visualizzati nella destinazione DDDT di CIP Safety (utilizzando una tabella di animazione con Control Expert in modalità connesso) con quelli configurati nel DTM e visualizzati nella scheda di verifica di configurazione.

Convalida della configurazione scaricata

Dopo aver scaricato tutte le configurazioni CIP Safety, la verifica utente è lo strumento per mezzo del quale vengono convalidati tutti i download. Una delle verifiche di convalida è un test delle configurazioni di connessione di sicurezza dopo il loro utilizzo in un'origine per confermare che la connessione di destinazione stia funzionando nel modo previsto.

DTM del dispositivo di sicurezza - Connessioni I/O

Introduzione

Il DTM CIP Safety, creato con o senza file EDS del fornitore, è dotato di nodi di connessione di sicurezza. Sia i nodi di ingresso che di uscita sono supportati, secondo le funzionalità, da un dispositivo specifico. La scheda **Connessione** presenta i parametri per la connessione di ingresso o di uscita selezionata.

Per i DTM creati con un file EDS del fornitore, le connessioni predefinite sono preselezionate. È possibile utilizzare i comandi **Rimuovi connessione** e **Aggiungi connessione** per adattare le impostazioni di connessione alle esigenze della propria applicazione.

Impostazioni di connessione dell'ingresso di sicurezza

Ciascuna connessione di ingresso di sicurezza presenta i seguenti parametri:

- **Dimensioni ingresso** (Lettura-Scrittura): la dimensione dei dati di ingresso configurati nel dispositivo CIP Safety, in byte. Impostate su 0 per impostazione predefinita.

  NOTA: È necessario sostituire il valore predefinito con le impostazioni offerte dal fornitore. Il valore 0 non è supportato.

- **Requested Packet Interval** (Lettura-Scrittura): RPI rappresenta il periodo di aggiornamento della connessione. Impostato nello stesso modo di (periodo di task SAFE)/2 per impostazione predefinita.

  NOTA: È possibile impostare il periodo task SAFE (Tsafe) nella finestra di dialogo **Proprietà di SAFE** (**Browser di progetto > Task > SAFE > Proprietà**) in Control Expert.

- **Aspettativa_tempo_di_rete** (Lettura-Scrittura): il tempo, in millisecondi, impiegato dalla comunicazione, pagina 166 CIP Safety. Se il valore è inferiore all'*Aspettativa_tempo_di_rete minima* viene visualizzata una notifica di rilevamento di errore. Per impostazione predefinita, il valore dovrebbe essere pari a *Aspettativa_tempo_di_rete minima* * 1,5.

- **Moltiplicatore_timeout** (Lettura-Scrittura): un componente nella produzione dell'*Aspettativa_tempo_di_rete minima*, il Moltiplicatore_timeout è uguale all'Aspettativa_tempo_di_rete /128 µSec. *Aspettativa_tempo_di_rete minima* = RPI * Moltiplicatore_timeout + Tsafe + 40.

- **Trasmissione_di_rete_max** (Lettura-Scrittura): l'età peggiore (più lontana, in ms) di data al momento del ricevimento del pacchetto da parte dell'utilizzatore. Questo parametro è utilizzato per il calcolo del valore minimo da immettere in Aspettativa_tempo_di_rete (come descritto sotto). Il parametro può essere perfezionato verificando il valore *Età_dati-max* nel dispositivo utilizzatore dopo l'esecuzione della comunicazione CIP Safety per un periodo di tempo significativo sulla rete.

  Questo parametro è utilizzato per il calcolo del valore minimo del "Aspettativa_tempo_di_rete", come segue:

  Min (Aspettativa tempo di rete) = RPI * Moltiplicatore_timeout + Trasmissione_di_rete_max

  Quando viene modificato Tsafe, il valore di questo parametro deve cambiare e, di conseguenza, il valore minimo dell'*Aspettativa_tempo_di_rete* deve cambiare a sua volta.

  A questo parametro si applicano i seguenti attributi:

  - Valore minimo = 1- ms
  - Valore massimo = 5800 ms
  - Valore predefinito = 40 + Tsafe

Il DTM di dispositivo utilizza queste impostazioni di ingresso per effettuare i seguenti calcoli:

Variabile	**Valore**		
	Predefinito	**Minimo**	**Max.**
Safeperiod (ms)	20	10	255
Intervallo ripetizione pacchetti in ingresso (ms)	RPI = Tsafe / 2	5	500
Moltiplicatore timeout	2	1	255
Trasmissione_di_rete_max (ms)	40 + 2 * Tsafe	10	5800
Aspettativa tempo di rete	Aspettativa_tempo_di_rete valore minimo* 1.5	RPI * Moltiplicatore_timeout + Trasmissione_di_rete_max	5800

Impostazioni di connessione di uscita di sicurezza

Ciascuna uscita di sicurezza presenta i seguenti parametri:

- **Dimensioni uscita** (Lettura-Scrittura): la dimensione dei dati di uscita configurati nel dispositivo CIP Safety, in byte. Impostate su 0 per impostazione predefinita.

  NOTA: È necessario sostituire il valore predefinito con le impostazioni offerte dal fornitore. Il valore 0 non è supportato.

- **Requested Packet Interval** (Lettura-Scrittura): RPI rappresenta il periodo di aggiornamento della connessione. Impostato nello stesso modo del periodo task SAFE (Tsafe).
- **Aspettativa tempo di rete** (Lettura-Scrittura): il tempo, in millisecondi, impiegato dalla comunicazione, pagina 166 CIP Safety. Se il valore è inferiore all'*Aspettativa_tempo_di_rete minima* viene visualizzata una notifica di rilevamento di errore. Per impostazione predefinita, il valore dovrebbe essere pari a *Aspettativa_tempo_di_rete minima* * 1,5.
- **Moltiplicatore timeout** (Lettura-Scrittura): un componente nella produzione dell'*Aspettativa_tempo_di_rete minima*, il Moltiplicatore timeout è uguale all'Aspettativa_tempo_di_rete /128 µSec. *Aspettativa_tempo_di_rete minima* = RPI * Moltiplicatore_timeout + Tsafe + 40.
- **Trasmissione_di_rete_max** (Lettura-Scrittura): l'età peggiore (più lontana, in ms) di data al momento del ricevimento del pacchetto da parte dell'utilizzatore. Questo parametro è utilizzato per il calcolo del valore minimo da immettere in Aspettativa_tempo_di_rete (come descritto sotto). Il parametro può essere perfezionato verificando il valore *Età_dati-max* nel dispositivo utilizzatore dopo l'esecuzione della comunicazione CIP Safety per un periodo di tempo significativo sulla rete.

  Questo parametro è utilizzato per il calcolo del valore minimo del "Aspettativa_tempo_di_rete", come segue:

  Min (Aspettativa tempo di rete) = RPI * Moltiplicatore_timeout + Trasmissione_di_rete_max

  Quando viene modificato Tsafe, il valore di questo parametro deve cambiare e, di conseguenza, il valore minimo dell'*Aspettativa_tempo_di_rete* deve cambiare a sua volta.

  A questo parametro si applicano i seguenti attributi:

  - Valore minimo = 1- ms
  - Valore massimo = 5800 ms
  - Valore predefinito = 40 + 2*Tsafe

Il DTM di dispositivo utilizza queste impostazioni di uscita per effettuare i seguenti calcoli:

Variabile	**Valore**		
	Predefinito	**Minimo**	**Max.**
Safeperiod (ms)	20	10	255
Intervallo ripetizione pacchetti in ingresso (ms)	RPI = Tsafe	10	255
Moltiplicatore timeout	2	1	255
Trasmissione_di_rete_max (ms)	40 + 2 * Tsafe	10	5800
Aspettativa tempo di rete	Aspettativa_tempo_di_rete valore minimo* 1.5	RPI * Moltiplicatore_timeout + Trasmissione_di_rete_max	5800

Checking Remote Device Identity

Use this tab to specify the degree to which a remote device (detected on the network) conforms to the configuration settings for the same remote device in the Control Expert application project. Control Expert does not maintain connections to a remote device that does not pass this identity check.

NOTA: This page appears only for generic DTM types that support connections, for example, Generic Device DTM, Advanced Generic DTM, and Generic Safety DTM.

The Generic Device Explicit Msg DTM does not support connections.

To open this page:

Step	Action
1	Double-click on the remote device in the **DTM Browser** to open its DTM in the **Device Editor**.
2	In the navigation tree in the left pane of the **Device Editor** select the connection node you want to configure.
3	In the right pane of the **Device Editor**, click the **Identity Check** tab.

NOTA: When this page is open, you can use the **Remove Connection** command to delete the selected connection.

Remote Device Identity Properties

A connection to a remote Schneider Electric device can present these properties:

Property	Description
Check Identity	This property defines the rule that Control Expert uses to compare the configured versus the actual remote device. These are the available settings: • **Must match exactly**: The DTM or EDS file exactly matches the remote device. • **Disable**: The checking function does not run. The identity portion of the connection is filled with zero values (the default setting). • **Must be compatible**: When the remote device is not the same as defined by the DTM/EDS, it emulates the DTM/EDS definitions. • **None**—no checking occurs; the identity portion of the connection is omitted • **Custom**: Enable the following parameter settings individually.
When **Check identity** is set to **Custom**, complete these fields:	
Compatibility Mode	• **True**: For each of the following selected tests, the DTM/EDS and remote device are compatible. • **False**: For each of the following selected tests, the DTM/EDS and remote device match exactly.
Minor Version	For each of these, select a setting:

Property	Description
Major Version	• **Compatible**: Include the parameter in the test. • **Not checked**: Do not include the parameter in the test.
Product Code	
Product Type	
Product Vendor	

DTM del dispositivo di sicurezza - Impostazioni di connessione I/O

Introduzione

Il DTM CIP Safety, se creato senza un file EDS del fornitore, comprende la scheda **Impostazioni di configurazione** del nodo di connessione.

Utilizzare la scheda **Impostazioni di configurazione** per completare la configurazione della connessione tra la CPU e il dispositivo remoto.

Parametri

La scheda **Impostazioni di configurazione** include i seguenti parametri:

- **Istanza d'ingresso**: il numero gruppo specifico del gruppo dispositivo associato con le trasmissioni di ingresso (T→O).
- **Istanza di uscita**: il numero gruppo specifico del dispositivo associato con le trasmissioni di uscita (O→T).
- **Istanza di configurazione**: il numero gruppo specifico del dispositivo associato con le impostazioni di configurazione del dispositivo.

Impostazioni dell'indirizzo IP del dispositivo di sicurezza

Modiche del DTM master della CPU M580

Le impostazioni dell'indirizzo IP e DHCP per un dispositivo CIP Safety sono configurabili in DTM Master della CPU M580.

NOTA: Diversamente dalle altre impostazioni di configurazione della connessione per i dispositivi di destinazione, l'indirizzo IP del dispositivo non è impostato nel DTM di connessione del dispositivo.

Accesso alle impostazioni dell'indirizzo IP del dispositivo di sicurezza

Eseguire questa sequenza di passaggi per modificare l'indirizzo IP e i parametri DHCP del dispositivo CIP Safety:

Passo	Azione
1	Disconnettere Control Expert dal dispositivo di destinazione ed eseguire le seguenti modifiche offline.
2	Nel **Browser DTM** di Control Expert, fare doppio clic su DTM Master della CPU M580 (BMEP58_ ECPU_EXT) per aprire la sua configurazione.
3	Nella struttura di navigazione, espandere l'Elenco dispositivi per visualizzare le istanze degli slave associate.
4	Selezionare il dispositivo che corrisponde al dispositivo CIP Safety.
5	Selezionare la scheda **Impostazione indirizzo**.

Configurazione delle impostazioni dell'indirizzo IP del dispositivo di sicurezza

Nella scheda **Impostazione indirizzo**, modificare questi parametri per il dispositivo di sicurezza selezionato:

Campo	Parametro	Descrizione
Configurazione IP	**Indirizzo IP**	Immettere l'indirizzo IP del dispositivo selezionato.
	Maschera di sottorete	La maschera di sottorete del dispositivo. **NOTA:** Impostare la subnet mask in modo tale che l'indirizzo IP del dispositivo risieda nella stessa subnet dell'indirizzo IP principale della CPU di origine.
	Gateway	L'indirizzo gateway utilizzato per raggiungere questo dispositivo. Il valore predefinito 0.0.0.0 indica che il dispositivo si trova sulla stessa subnet della CPU di origine.
Server di indirizzi	**DHCP per questo dispositivo**	• **Disattivato** (predefinito) disattiva il client DHCP per il dispositivo. • **Attivato** attiva il client DHCP in questo dispositivo.

Campo	Parametro	Descrizione
	Identificato da	Se il servizio DHCP per questo dispositivo è Attivato, selezionare il tipo di identificativo del dispositivo: • **Indirizzo MAC.** • **Nome dispositivo**.
	Identificativo	Se il DHCP è Attivato e il **Nome dispositivo** selezionato, immettere il valore del nome dispositivo.

Per maggiori informazioni sulla configurazione dei parametri del dispositivo DTM Master della CPU M580, vedere l'argomento Parametri elenco dispositivi (vedi Modicon M580, Hardware, Manuale di riferimento).

Operazioni con CIP Safety

Panoramica

Questa sezione descrive le operazioni con CIP Safety.

Trasferimento di un’applicazione CIP Safety da Control Expert al PAC

Iniziare il download dell'applicazione

Utilizzare il comando **PLC > Trasferisci progetto a PLC** per iniziare il download.

Se il PLC è configurato con un'applicazione preesistente (la “vecchia applicazione”), viene invalidato all'inizio del download della nuova applicazione. Se la vecchia applicazione comprende dispositivi configurati, il PAC chiude le connessioni con tali dispositivi.

Fine del download dell'applicazione

La configurazione CIP Safety viene scritta nel CIP Safety Stack (CSS) della CPU, che calcola un parametro di connessione CRC (CPCRC) per ciascuna connessione. Quindi, ciascun CPCRC calcolato da CSS viene confrontato con il CPCRC corrispondente archiviato nella configurazione e calcolato dal DTM di destinazione. In caso di:

- Non corrispondenza di CPCRC, il CSS rifiuta l’applicazione e il PAC resta in stato NOCONF.
- Uguaglianza:
  - Il CPCRC e i valori dei parametri di connessione vengono copiati nel DDDT di destinazione, pagina 385 corrispondente.
  - Il parametro CSIO_HEALTH, pagina 392 all’interno del DDDT della CPU (T_BMEP58_ECPU_EXT) è impostato su 0.
  - I bit DDDT HEALTH del dispositivo, pagina 385 di destinazione CIP Safety sono impostati su 0.
  - Il PAC apre le connessioni dei dispositivi configurati tramite le Richieste di apertura di sicurezza di tipo 2, pagina 376

Nel caso di non corrispondenza di CPCRC, il CSS rifiuta l’applicazione e il PAC resta in stato NOCONF.

Ricalcolo dell'ID dell'applicazione di sicurezza

L'ID dell'applicazione di sicurezza (SAId) è una firma della parte sicura dell'applicazione Control Expert. È archiviata come parola di sistema %SW169, pagina 409. Il CSS calcola un CRC su tutte le istanze di CPCRC. Questo CRC viene aggiunto al calcolo del SAId. Quindi, una modifica alla configurazione della destinazione CIP Safety modifica il valore SAId.

Struttura della richiesta di apertura di sicurezza di tipo 2

Struttura del frame di connessione di apertura di sicurezza di tipo 2 CIP

Le CPU di sicurezza indipendenti M580 supportano le connessioni CIP Safety create da richieste di connessione di apertura di sicurezza di tipo 2 La struttura della richiesta di connessione è descritta di seguito:

Nome parametro		**Descrizione**
Moltiplicatore timeout di connessione		Per l'utilizzatore di una connessione, è utile a determinare se una delle tre connessioni standard debba essere in timeout. Il valore di timeout per la connessione è definito come segue: RPI di connessione * (CTM+1) * 4
O_to_T RPI		Intervallo pacchetto richiesto da origine a destinazione.
T_to_O RPI		Intervallo pacchetto richiesto da destinazione a origine.
Electronic Key.Vendor ID		Identificativo del fornitore
Electronic Key.Prod Type		Tipo di dispositivo
Electronic Key.Prod Code		Codice prodotto dispositivo
Electronic Key.Compatible/Major Rev		Revisione maggiore
Electronic Key.Minor Rev		Revisione minore
SCID	Configurazione di sicurezza CRC	Identificativo configurazione di sicurezza: fornito dallo strumento di configurazione di rete di sicurezza (SNCT), viene utilizzato durante la messa in servizio, la formazione di una connessione e la sostituzione del dispositivo.
	Data configurazione	
	Ora di configurazione	
TUNID	Data TUNID	Identificativo di rete univoco di destinazione: identifica la destinazione della richiesta di apertura di sicurezza.
	Ora TUNID	
	ID del nodo di destinazione	

Nome parametro		Descrizione
OUNID	Data OUNID	Identificativo di rete univoco di origine: identifica l'origine della richiesta di apertura di sicurezza.
	Ora OUNID	
	ID del nodo di origine	
Moltiplicatore_EPI_Intervallo_ping		Definisce l'Intervallo_conteggio_ping per la connessione.
Moltiplicatore_min_Msg_ Coord_Tempo		Il numero minimo di incrementi di 128 µS necessari al Messaggio di coordinamento di tempo per passare dall'utilizzatore al produttore.
Moltiplicatore_Aspettativa_tempo_rete		L'età massima dei dati di sicurezza, misurata con incrementi di 128 µS, consentita da un utilizzatore.
Moltiplicatore_Timeout		Il numero di tentativi di produzione dati da includere nell'equazione per il rilevamento di connessioni fallite.
Numero_errore_max		Il numero di pacchetti errati che può essere derivato prima della chiusura della connessione.
CRC parametri di connessione (CPCRC)		CRC parametri di connessione. Un CRC-S32 di parametri di connessione di destinazione contenuti nella richiesta di apertura di sicurezza di tipo 2.

Operazioni del dispositivo CIP Safety

Introduzione

Questa sezione descrive le operazioni del dispositivo CIP Safety, compresi i meccanismi di rilevamento e risposta agli errori di sistema e lo stato operativo del dispositivo:

- autotest all'accensione
- risposta a errore rilevato non ripristinabile
- errore rilevato ripristinabile
- gestione dello stato della connessione di destinazione
- stato Run / Idle del dispositivo CIP Safety

Autotest all'accensione dell'origine e della destinazione CIP Safety

All'accensione, e ogni qualvolta viene caricata una nuova applicazione, il sistema CIP Safety esegue le seguenti operazioni:

- Il controller trasferisce i parametri di configurazione allo Stack CIP Safety (CSS) nel controller e nel coprocessore.
- Il CSS, nel controller e nel coprocessore, valuta il CPCRC per ogni connessione.
- Per ogni connessione, il sistema CIP Safety confronta il CPCRC scaricato (calcolato dal DTM di origine) con quelli calcolati dal controller e dal coprocessore.
- Il CSS blocca la configurazione di origine.
- L'applicazione avvia le richieste di apertura di sicurezza di tipo 2 per una connessione a ogni dispositivo CIP Safety.
- Ogni dispositivo CIP Safety:
  - Calcola il proprio CPCRC e lo confronta con quello ricevuto dall'origine.
  - Confronta lo SCID ricevuto con quello archiviato internamente (Nota: questa verifica si applica solo ai dispositivi configurabili).

Gli scambi di I/O tra dispositivi di origine e di destinazione iniziano solo se tutte le verifiche hanno esito positivo.

NOTA: Oltre agli autotest all'accensione descritti in precedenza, il sistema esegue tutti gli autotest di runtime richiesti dagli standard CIP di sicurezza IEC 61784-3.

Risposta a errore non reversibile rilevato

Se il controller o la diagnostica I/O rileva un errore irreversibile, il sistema di sicurezza imposta la parte interessata nello stato sicuro definito. La parte coinvolta del sistema viene spenta e non alimentata, con gli ingressi di sicurezza impostati su 0. Tutte le uscite di sicurezza coinvolte sono portate nello stato di posizionamento di sicurezza configurato.

Risposta a errore reversibile rilevato

Gli errori reversibili rilevati tipicamente comprendono eventi quali la perdita di connessione di un modulo e così via. Tali errori sono riportati nei bit Stato del DDDT del dispositivo (T_CIP_SAFETY_IO, pagina 385), che contiene il valore logico AND dei bit Status_IN e Status_OUT. Nel caso di un errore reversibile rilevato per un ingresso, il valore di tale ingresso viene forzato nello stato sicuro definito e impostato a 0.

Gestione dello stato di connessione destinazione

Lo stato di una connessione verso una destinazione CIP Safety è riportato nel bit Stato dei parametri Status_IN e Status_OUT come descritti nel tipo dati T_CIP_SAFETY_STATUS, pagina 386. Lo stato della destinazione può essere aperto, operativo o di errore rilevato.

Per gli ingressi, lo stato di connessione viene fornito dal convalidatore di sicurezza del server, per le uscite , lo stato di connessione viene fornito dal convalidatore di sicurezza del client.

Run / Inattivo

Lo stato operativo di un dispositivo CIP Safety, run o inattivo, è riportato nel bit Run_Inattivo del parametro Status_IN o Status_OUT come descritto nel tipo dati T_CIP_SAFETY_STATUS, pagina 386.

Per un dispositivo di ingresso:

Quando viene stabilita una connessione con un modulo di ingresso, il bit Run_Inattivo viene impostato su Inattivo (0) dal produttore (ingresso) fino a quando la sequenza di coordinamento di tempo iniziale viene completata. Dopodiché, il valore del bit può essere 1 (stato Run) o 0 (stato Inattivo). Se il bit Run_Inattivo è impostato a 0 (stato Inattivo), i valori dei dati di ingresso sono forzati a 0 (stato sicuro definito).

Per un dispositivo di uscita:

Il bit Run_Inattivo per le uscite viene impostato a 1 dall'origine (controller) quando il controller si trova nello stato Run e la sequenza di coordinamento di tempo iniziale viene completata correttamente. Lo stato Run/Inattivo per le uscite viene impostato a 0 dall'origine (controller) quando il controller è nello stato Stop o Halt, o quando la sequenza di coordinamento di tempo iniziale non è stata completata correttamente, o quando la connessione è chiusa. Se il bit Run_Inattivo viene impostato su 0 (stato Inattivo), il dispositivo di uscita deve impostare le proprie uscite sul loro stato di posizionamento di sicurezza.

Interazioni tra le operazioni del controller di sicurezza e la connessione di destinazione

Introduzione

Questo argomento tratta delle interazioni tra i seguenti stati/operazioni dell'origine controller di sicurezza e la connessione del dispositivo di destinazione:

- tempo di reazione del sistema
- stato run
- stato stop / halt
- ciclo di spegnimento-accensione / riavvio
- comando iniz safety

- Modalità di manutenzione
- CCOTF
- Connessione / Disconnessione / sostituzione di un dispositivo

Tempo di reazione del sistema

Il tempo impiegato dalla comunicazione CIP Safety, chiamato *aspettativa tempo di rete*, viene aggiunto e diventa parte del *tempo di reazione del sistema* di M580 Safety. Per ulteriori informazioni, vedere l'argomento *Impatto delle comunicazioni CIP Safety sul tempo di reazione del sistema di sicurezza*

Stato Run

Quando il sistema CIP Safety sta funzionando in stato Run:

- I bit di stato nel DDDT, pagina 385 di comunicazione del dispositivo CIP Safety vengono aggiornati all'inizio del ciclo task SAFE.
- I valori di ingresso vengono aggiornati all'inizio del ciclo task SAFE, sulla base del valore ricevuto più recentemente.
- Dopo l'esecuzione del programma task SAFE i valori di uscita sono aggiornati e trasmessi.
- Il bit Run_Inattivo per le uscite nel DDDT di comunicazione del dispositivo CIP Safety viene impostato su 1.
- I bit di stato nel DDDT di comunicazione del dispositivo CIP Safety vengono aggiornati.

Stato Stop

Quando il task SAFE entra nello stato Stop, ad esempio se il task SAFE viene arrestato o ha raggiunto il punto di interruzione:

- La connessione da origine a destinazione resta aperta.
- Vengono eseguiti gli scambi di dati tra il controller e il dispositivo CIP Safety.
- I bit di stato nel DDDT, pagina 385 di comunicazione del dispositivo CIP Safety continuano ad essere aggiornati.
- Il bit Run_Inattivo per le uscite nel DDDT di comunicazione del dispositivo CIP Safety viene impostato su 0 e i dispositivi di uscita applicano l'impostazione di posizionamento di sicurezza configurata.

Stato Halt

Nello stato Halt, i valori di uscita non vengono inviati dal controller al dispositivo CIP Safety e i bit di stato del dispositivo CIP Safety sono impostati a 0.

Ciclo accen/spegn o Reset

In un ciclo accen/spegn o reset:

- La parte di sicurezza dell'applicazione esegue un riavvio a freddo, pagina 273.
- Il controller esegue la stessa sequenza di operazioni che viene eseguita per il download dell'applicazione, pagina 375.

Comando Iniz Safety

L'esecuzione del comando **PLC > Iniz Safety** in Control Expert inizializza i valori del DDDT di comunicazione del dispositivo CIP Safety, pagina 385, impostandoli sui valori predefiniti di fabbrica.

Modalità di manutenzione

IL funzionamento del controller M580 Safety in modalità manutenzione, pagina 261 non influisce sul funzionamento del dispositivo CIP Safety. Il controller continua a confrontare i calcoli eseguiti separatamente dal controller e dal coprocessore. Tuttavia, non vi saranno confronti aggiuntivi ai valori nel DDDT di destinazione. Quindi, il funzionamento del controller in modalità manutenzione non è considerato sicuro.

CCOTF

La funzione di modifica della configurazione in corso d'opera (CCOTF) non è supportata dai dispositivi CIP Safety. Poiché un dispositivo CIP Safety ottiene le impostazioni di configurazione da uno strumento di configurazione di rete di sicurezza offerto dal fornitore (SNCT) e non dal controller di origine, le modifiche alle impostazioni del dispositivo non possono essere effettuate dal controller.

Connessione / Disconnessione / sostituzione di un dispositivo CIP Safety

Per impostazione predefinita, sulla base dell'avvio dell'applicazione o l'esecuzione di un comando **PLC > Iniz Safety**, i bit CTRL_IN e CTRL_OUT in DDDT, pagina 385 sono impostati su Attivato (1). Quando un dispositivo è collegato a un controller in modalità Stop o Run e il bit CTRL_IN o CTRL_OUT del dispositivo è impostato su Attivato (1), il dispositivo avvia automaticamente gli scambi di dati.

NOTA: Siccome i bit CTRL_IN e CTRL_OUT sono impostati su Attivato in un ciclo di accensione/spegnimento, è necessario adottare misure adeguate nell'applicazione del task SAFE per evitare funzionamenti non previsti quando viene eseguito un ciclo accensione/spegnimento.

⚠ AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Non utilizzare i bit CTRL_IN o CTRL_OUT come misura di sicurezza per impostare i dati di destinazione in uno stato sicuro definito.

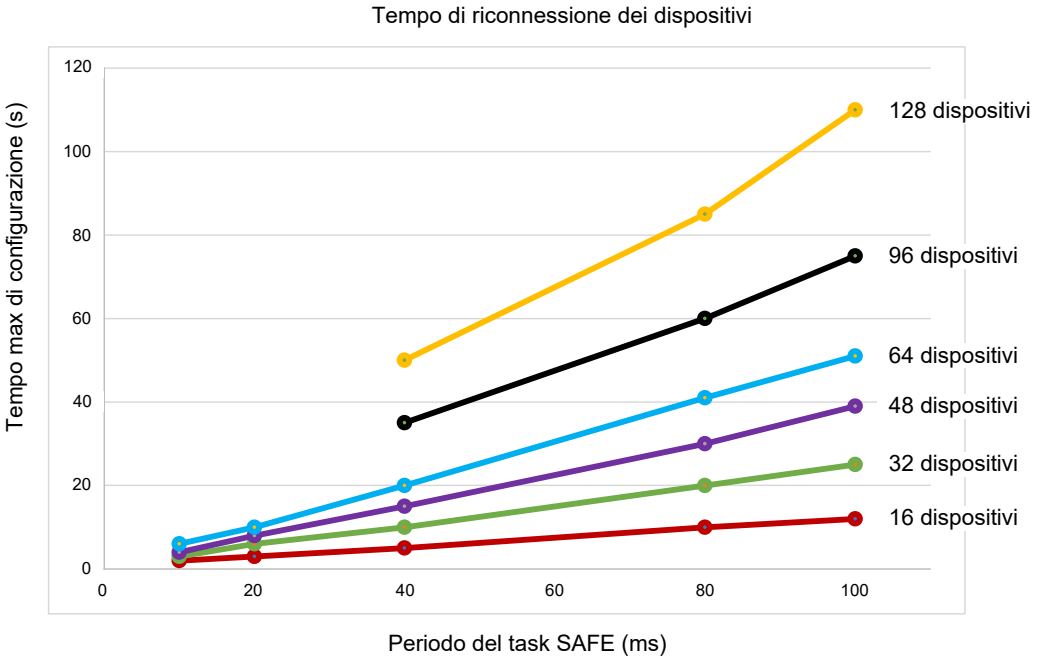
Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.

Il controller, quando rileva un errore che richiede la chiusura di una connessione del dispositivo, imposta il bit CTRL_IN o CTRL_OUT corrispondente su Disattivato (0). Il dispositivo resta in stato disabilitato e ritorna nello stato Attivato (1) se la transizione è stata prevista. Ad esempio, se l'errore viene azzerato e viene eseguita una richiesta di riapertura di connessione.

È possibile eseguire una richiesta di riapertura di connessione reimpostando il bit di controllo corrispondente (CTRL_IN o CTRL_OUT) da Disattivato (0) a Attivato (1) nel DDDT.

Quando un dispositivo viene nuovamente connesso, il tempo di connessione dipende dal periodo task SAFE e il numero di dispositivi connessi:

- Per un dispositivo singolo con un periodo task SAFE inferiore a 100 ms, il tempo stimato per la connessione è inferiore a 2 secondi.
- Per dispositivi multipli, vedere il grafico seguente per i tempi di connessione stimati.



Il controller CIP Safety tratta la sostituzione del dispositivo come la disconnessione e la riconnessione. Le operazioni per riconfigurare il nuovo dispositivo con le stesse impostazioni del dispositivo sostituito sono locali per il dispositivo e non coinvolgono il controller.

Comandi DTM CIP Safety

Introduzione

Il DTM CIP Safety comprende la scheda **Sicurezza**, che presenta i seguenti comandi:

- **RESET proprietà**
- **Mettere TUNID**

È possibile accedere a questi comandi selezionando una connessione nella struttura ad albero del DTM, quindi vengono abilitati soltanto quando il DTM collegato al dispositivo CIP Safety è in funzione online.

Proprietà RESET

utilizzare il comando **Proprietà RESET** per eseguire un reset delle impostazioni di configurazione del dispositivo CIP Safety ai valori out-of-the-box predefiniti di fabbrica. Un reset può essere eseguito solo se:

- Il comando viene eseguito dalla CPU di origine identificata con l'OUNID archiviato nel dispositivo.
- Le impostazioni di configurazione del modulo non sono bloccate.

Dopo il reset, il modulo non ha proprietario e può essere configurato da un'altra origine.

NOTA: Se viene eseguito un reset su un modulo con connessioni operative, il comando reset non avrà efficacia.

Mettere TUNID

Utilizzare il comando **Mettere TUNID** per impostare il Numero di rete di sicurezza (SNN) nel dispositivo CIP Safety di destinazione. In esecuzione, il Numero di rete di sicurezza, pagina 365 archiviato nella configurazione del DTM del dispositivo CIP Safety viene trasferito al dispositivo di destinazione e sovrascrive il valore SNN già esistente nel dispositivo.

NOTA: Prima di eseguire questo comando, confermare che si è identificato il dispositivo corretto per la ricezione dell'SNN che si intende trasferire.

Diagnostica CIP Safety

Panoramica

Questa sezione presenta gli strumenti di diagnostica per il dispositivo CIP Safety, la connessione tra il dispositivo e la CPU indipendente Safety M580.

DDDT del dispositivo CIP Safety

T_CIP_SAFETY_IO DDDT

Ciascuna istanza al dispositivo CIP Safety è descritta da T_CIP_SAFETY_IO DDDT, composto dai seguenti parametri:

Parametro	Tipo di dati	Descrizione
Stato	BOOL	Stato globale = AND logico di • Status_IN.Health • Status_OUT.Health Consultare i tipi di dati T_CIP_SAFETY_STATUS, pagina 386 per una descrizione di queste parti di stato.
Status_IN	T_CIP_SAFETY_STATUS	Stato ingresso.
Status_OUT	T_CIP_SAFETY_STATUS	Stato uscita.
CTRL_IN	BOOL	Attivare/disattivare la connessione di ingresso.
CTRL_OUT	BOOL	Attivare/disattivare la connessione di uscita.
Conf_In	T_CIP_SAFETY_CONF	Le firme e i parametri CIP per la connessione di ingresso.
Conf_Out	T_CIP_SAFETY_CONF	Le firme e i parametri CIP per la connessione di uscita.
Ingresso	Array[0...n] di BYTE	Valori di ingresso, la dimensione dipende dal tipo di dispositivo. Modulo allineato da 4 byte con dimensione configurata all'interno del DTM.
Uscita	Array[0...m] di BYTE	Valori di uscita, la dimensione dipende dal tipo di dispositivo. Modulo allineato da 4 byte con dimensione configurata all'interno del DTM.

I tipi di dati CIP Safety a cui si è fatto riferimento sopra sono descritti di seguito.

T_CIP_SAFETY_STATUS

Il tipo di dati T_CIP_SAFETY_SATATUS è composto dai seguenti parametri:

Parametro	Tipo di dati	Descrizione
Stato operativo	BOOL	Stato ingresso o uscita: • Per ingresso: ◦ 1: la comunicazione in ingresso è aperta e funzionante. ◦ 0: errore rilevato per la comunicazione in ingresso dal convalidatore di sicurezza del server. • Per uscita: ◦ 1: la comunicazione in uscita è aperta e funzionante. ◦ 0: errore rilevato per la comunicazione in uscita dal convalidatore di sicurezza del client.
Run_Inattivo	BOOL	Stato degli ingressi o delle uscite del dispositivo CIP Safety: • Per gli ingressi, è impostato dal produttore (ingresso): ◦ 1: se l'ingresso è in stato Run. ◦ 0: se l'ingresso è in stato Inattivo, o fino al corretto completamento della sequenza di coordinamento di tempo iniziale. • Per le uscite, è impostato dall'origine (CPU): ◦ 1: se il PAC è in stato Run, o dopo il corretto completamento della sequenza di coordinamento di tempo iniziale. ◦ 0: se il PAC è in stato Stop o Halt, se la connessione è chiusa, o se la sequenza di coordinamento di tempo iniziale non è stata completata.
Codice_errore	WORD	Vedere l'elenco dei codici di errore individuati, pagina 388.
Sottocodice_errore	WORD	Vedere l'elenco dei sottocodici di errore individuati, pagina 389.

T_CIP_SAFETY_CONF

Il tipo di dati T_CIP_SAFETY_CONF è composto dai seguenti parametri, che vengono trasmessi nella Richiesta di apertura di sicurezza di tipo 2, pagina 376:

Parametro	Tipo di dati	Descrizione
TO_MULTIPLIER	BYTE	Moltiplicatore timeout. Per l'utilizzatore di una connessione, è utile a determinare se una delle tre connessioni standard debba essere in timeout. Il valore di timeout per la connessione è definito come segue: RPI di connessione * (CTM+1) * 4
RPI_uscita	UDINT	Intervallo pacchetto richiesto della connessione O→T.
RPI_ingresso	UDINT	Intervallo pacchetto richiesto della connessione T→O.
ID_fornitore_dispositivo	UINT	Identificativo del fornitore ODVA.
Tipo_dispositivo	UINT	Raggruppamento ODVA a cui appartiene il dispositivo.
Codice_prodotto_dispositivo	UINT	Codice prodotto assegnato da ODVA.
Revisione_maggiore	BYTE	Numero della revisione maggiore del firmware del dispositivo.
Revisione_minore	BYTE	Numero della revisione minore del firmware del dispositivo.
Nb_assembly_configurazione	UINT	Il numero gruppo specifico del dispositivo associato con le impostazioni di configurazione del dispositivo.
Nb_assembly_uscita	UINT	Il numero gruppo specifico del dispositivo associato con le trasmissioni di uscita (O→T).
Nb_assembly_ingresso	UINT	Il numero gruppo specifico del dispositivo associato con le trasmissioni di ingresso (T→O).
CRC_SC	UDINT	Configurazione di sicurezza CRC. Un controllo di ridondanza ciclico (CRC) della configurazione del dispositivo CIP Safety.
Data_configurazione	UINT	Mese, giorno e anno della creazione della configurazione.
Ora_configurazione	UDINT	Ora, minuto, secondo e millisecondo della creazione della configurazione.
Ora_TUNID	UDINT	Mese, giorno e anno in cui è stato generato l'identificativo univoco di rete di destinazione.
Data_TUNID	UINT	Ora, minuto, secondo e millisecondo in cui è stato generato l'identificativo univoco di rete di destinazione.
IDnodo_TUNID	UDINT	Un identificativo univoco di rete per il dispositivo di destinazione.
Ora_OUNID	UDINT	Mese, giorno e anno in cui è stato generato l'identificativo univoco di rete dell'origine.
Data_OUNID	UINT	Ora, minuto, secondo e millisecondo in cui è stato generato l'identificativo univoco di rete dell'origine.

Parametro	Tipo di dati	Descrizione
IDnodo_OUID	UDINT	Un identificativo univoco di rete per il dispositivo di origine.
Moltiplicatore_EPI_Intervallo_ping	UINT	Definisce l'Intervallo_conteggio_ping per la connessione.
Moltip_min_mess_coordinamento_tempo	UINT	Il numero minimo di incrementi di 128 µS necessari al Messaggio di coordinamento di tempo per passare dall'utilizzatore al produttore.
Moltip_aspettative_tempo_rete	UINT	L'età massima dei dati di sicurezza, misurata con incrementi di 128 µS, consentita da un utilizzatore.
Moltiplicatore_Timeout	BYTE	Il numero di tentativi di produzione dati da includere nell'equazione per il rilevamento di connessioni fallite.
Numero_errore_max	UDINT	Il numero di pacchetti errati che può essere derivato prima della chiusura della connessione.
CPCRC	UDINT	CRC parametri di connessione. Un CRC-S32 di parametri di connessione di destinazione contenuto nella richiesta di apertura di sicurezza di tipo 2.

Codici di errore del dispositivo CIP Safety

Codici di errore rilevati

I seguenti codici e sottocodici di errore rilevato si applicano al tipo di dati T_CIP_SAFETY_STATUS e sono inclusi nei parametri Status_IN e Status_OUT del DDDT del dispositivo CIP Safety.

Codici di errore rilevato

Codice di errore rilevato	Significato
0001	Connessione aperta, nessuna risposta
0002	Connessione aperta, rilevato errore di risposta dal dispositivo
0003	Connessione aperta, risposta non valida dal dispositivo
0004	Il server (utilizzatore) non è in funzione
0005	Il client (produttore) non è in funzione

Sottocodici di errore rilevato

NOTA: Tutti i sottocodici di errore rilevato diversi da quelli elencati di seguito sono previsti per il solo utilizzo interno di Schnieder Electric. In tal caso, è necessario riferire il sottocodice di errore rilevato al personale di Schnieder Electric.

Sottocodici di errore rilevato per le connessioni aperte:

Sottocodice di errore rilevato (hex)	Significato
0100	Connessione in uso o Forward_Open doppio.
0103	Classe di trasporto e combinazione di trigger non supportate.
0105	La configurazione appartiene già ad un'altra origine.
0106	L'uscita appartiene già ad un'altra origine.
0107	Connessione di destinazione non trovata (Invia_Chiusura).
0108	Parametro di connessione di rete non valido
0109	Dimensioni connessione non valide
0110	Dispositivo non configurato.
0111	O->T RPI, T->O RPI o RPI correzione di tempo non supportato.
0113	Tutte le istanze del convalidatore di sicurezza sono in uso.
0114	ID_fornitore_dispositivo o Codice_prodotto_dispositivo specificati nella chiave elettronica non corrispondono.
0115	Il Tipo_dispositivo specificato nella chiave elettronica non corrisponde.
0116	Revisione_maggiore o Revisione_minore specificate nella chiave elettronica non corrispondono.
0117	Percorso applicazione prodotto o consumato non valido
0118	Percorso applicazione configurazione non valido o incoerente
011A	Oggetto destinazione fuori da connessioni
011B	RPI inferiore a tempo inibizione produzione.
011C	Classe di trasporto non supportata.
011D	Trigger di produzione non supportato.
011E	Direzione non supportata.
0123	Tipo di connessione di rete da origine a destinazione non valido
0124	Tipo di connessione di rete da destinazione a origine non valido
0126	Dimensione configurazione non valida

Sottocodice di errore rilevato (hex)	Significato
0127	Dimensione da origine a destinazione non valida
0128	Dimensione da destinazione a origine non valida
0129	Percorso applicazione configurazione non valido
012A	Percorso applicazione utilizzatrice non valido
012B	Percorso applicazione produttrice non valido
012C	Il simbolo di configurazione non esiste.
012D	Il simbolo di utilizzo non esiste.
012E	Il simbolo di produzione non esiste.
012F	Combinazione percorso applicazione incoerente
0130	Formato dati consumo incoerente
0131	Formato dati di produzione incoerente
0203	Timeout connessione.
0204	La destinazione non risponde a richieste non collegate.
0205	Errore rilevato parametro in richiesta di apertura di sicurezza.
0207	Riconoscimento non collegato senza risposta.
0315	Tipo di segmento non valido in percorso connessione.
031B	Connessione modulo già stabilita.
031C	Non può essere applicato nessun altro codice di stato esteso.
031F	Nel modulo di produzione non sono più disponibili i collegamenti configurabili alle risorse per l'utilizzatore.
0801	Moltiplicatore_EIP_Intervallo_Ping o Numero_consumatore_max non valido per unione multicast.
0802	Dimensione di connessione di sicurezza non valida.
0803	Formato di connessione di sicurezza non valido.
0804	Parametri di connessione correzione di tempo non validi.
0805	Moltiplicatore_EIP_intervallo_ping non valido
0806	Moltiplicatore min_Msg_coordinamento_tempo non valido
0807	Moltiplicatore_aspettativa_tempo_rete non valido
0808	Moltiplicatore timeout non valido
0809	Numero max utilizzatore non valido

Sottocodice di errore rilevato (hex)	Significato
080A	CPCRC non valido
080B	ID di connessione di correzione di tempo non valido
080C	SCID non corrispondente
080D	TUNID non impostato
080E	TUNID non corrispondente
080F	Funzionamento di configurazione non consentito.

Sottocodici di errore rilevato per server o client:

Sottocodice di errore rilevato (hex)	Significato
271D	Il messaggio di coordinamento di tempo è stato ricevuto con un bit Risposta_ping non impostato.
2730	Messaggio di coordinamento di tempo non ricevuto nel tempo assegnato.
2732	Verifica messaggio di coordinamento di tempo: messaggio con stesso time stamp già ricevuto da questo utilizzatore.
2733	Verifica messaggio coordinamento di tempo: errore rilevato controllo parità.
2734	Verifica messaggio coordinamento di tempo: errore rilevato controllo Ack_Byte_2.
2735	Verifica messaggio di coordinamento di tempo non ricevuto entro il limite di circa 5 secondi.
2736	Verifica messaggio di coordinamento di tempo non ricevuto entro lo stesso o il successivo intervallo di ping.
2738	Verifica messaggio coordinamento di tempo: CRC non corrispondente.
2820	CRC di time stamp non corrispondente.
2821	Delta timestamp zero.
2822	Delta timestamp maggiore dell'aspettativa rime di rete.
2823	Età dati di un messaggio superiore all'aspettativa rime di rete.
2824	Età dati di un messaggio valido sotto altri aspetti maggiore dell'aspettativa tempo di rete.
2825	CRC dati effettivi non corrispondente.
2826	CRC dati complementari non corrispondente.
282E	CRC dati effettivi non corrispondente (nessuna chiusura della connessione).

Sottocodice di errore rilevato (hex)	Significato
282F	CRC dati complementari non corrispondente (nessuna chiusura della connessione).
2832	Timeout del monitor di attività dell'utilizzatore.

DDDT CPU indipendente CIP Safety

Aggiunte CIP Safety a T_BMEP58_ECPU_EXT

Il DDDT CPU di sicurezza indipendente M580 (T_BMEP58_ECPU_EXT) comprende due variabili CIP Safety:

- CSIO_SCANNER: lo stato del bit di controllo dello scanner I/O CIP Safety. Questo campo Booleano può essere:
  - 1: il servizio funziona correttamente.
  - 0: il servizio non funziona correttamente.

Per ulteriori informazioni, vedere l'elenco dei parametri di ingresso (vedere Modicon M580, Hardware, Manuale di riferimento) SERVER_STATUS2 DDDT.

- CSIO_HEALTH: lo stato dei dispositivi CIP Safety collegati. Questa variabile è un array di 128 valori Booleani, in cui ciascun bit indica lo stato di un singolo dispositivo collegato:
  - 1: il servizio funziona correttamente.
  - 0: il servizio non funziona correttamente.

Per ulteriori informazioni, vedere l'argomento Stato dispositivo (vedere Modicon M580, Hardware, Manuale di riferimento).

Diagnostica DTM del controller

Diagnostica tramite DTM del controller M580

Il DTM del controller M580 fornisce i seguenti servizi di diagnostica:

- Rilevamento dispositivo
- Stato del dispositivo I/O CIP Safety

Rilevamento dispositivo di sicurezza CIP

Quando Control Expert funziona online, è possibile utilizzare il suo servizio di rilevamento del bus di campo per rilevare i dispositivi CIP Safety di primo livello, ossia i dispositivi collegati direttamente al controller, nella rete. Sono individuabili solo i dispositivi con un DTM che corrisponde al DTM registrato nel **Catalogo DTM** del PC host.

Il rilevamento del dispositivo viene eseguito facendo clic con il pulsante destro del mouse sul DTM del controller (BMEP58_ECPU_EXT) nel **Browser DTM**, quindi selezionando **Rilevamento bus di campo** per aprire una finestra di dialogo con lo stesso nome, che visualizza i dispositivi rilevati. È possibile utilizzare gli strumenti di questa finestra di dialogo per aggiungere i DTM dispositivo al proprio progetto. I dispositivi aggiunti vengono visualizzati sotto il controller nel **Browser DTM** e nella struttura di navigazione del DTM del controller.

Per ulteriori informazioni su come utilizzare questo servizio, vedere la sezione Servizio di rilevamento del bus di campo (vedere EcoStruxure™ Control Expert, Modalità di funzionamento).

Stato connessione dispositivo CIP Safety

Quando Control Expert è in funzione online, la struttura del DTM del controller visualizza un'icona che indica lo stato di ciascuna connessione per i dispositivi di I/O CIP Safety aggiunti al progetto:

-  indica che la connessione è in stato RUN.
-  indica che la connessione è in stato STOP, non collegata o non determinabile.

Per ulteriori informazioni su come utilizzare questa funzionalità, consultare l'argomento Introduzione della diagnostica nel DTM Control Expert (vedere Modicon M580, Hardware, Manuale di riferimento).

Diagnostica di connessione del dispositivo CIP Safety

Introduzione

I nodi di connessione di un DTM CIP Safety includono due schede utilizzabili per identificare e diagnosticare la connessione del dispositivo:

- modulo, informazioni
- stato, informazioni

Scheda Informazioni del modulo

Il DTM CIP Safety presenta la scheda **Informazioni del modulo** che fornisce valori statici per i seguenti parametri di identificazione del modulo:

- ID fornitore
- tipo di prodotto
- codice prodotto
- revisione software
- numero di serie
- nome prodotto
- indirizzo MAC

Scheda Informazioni di stato

Il DTM CIP Safety presenta la scheda **Informazioni di stato** che fornisce valori dinamici per la connessione del controller al dispositivo CIP Safety:

Stato	Descrizione
Stato CIP Safety	Lo stato corrente del dispositivo, come definito dalla sezione 5-4.2.1.5 Stato dispositivo dello standard CIP Safety: • 0: non definito • 1: test automatico • 2: inattivo • 3: eccezione test automatico • 4: in esecuzione • 5: interruzione • 6: errore critico • 7: configurazione • 8: attesa TUNID • 9...50: riservato • 51: attesa TUNID con coppia consentita Vedere NOTA • 52: esecuzione con coppia consentita Vedere NOTA • 53...99: specifico del dispositivo • 100...255: specifico del fornitore **NOTA:** Consentiti e definiti solo nei profili del dispositivo movimento di sicurezza: 0x2E, 0x2F.
Stato di eccezione	Un attributo a byte singolo il cui valore indica lo stato degli allarmi e degli errori per il dispositivo. Può essere fornito come metodo di base o espanso. Per ulteriori dettagli, consultare la sezione 5-4.2.1.6 Stato di eccezione dello standard CIP Safety.

Stato	Descrizione
Errore grave	Condizione specifica del dispositivo. Per maggiori dettagli, vedere il Manuale dispositivo.
Errore non grave	Condizione specifica del dispositivo. Per maggiori informazioni, vedere il manuale del dispositivo.
Indirizzo IP	Indirizzo IP del dispositivo CIP Safety, impostato nel DTM del controller, pagina 372 M580.
TUNID	Identificativo di rete univoco di destinazione
OUNID	Identificativo di rete univoco di origine, pagina 355
Stato di blocco	Lo stato della configurazione del dispositivo, come configurato utilizzando uno strumento di configurazione di rete di sicurezza (SNCT): • Bloccato: configurazione di sola lettura. • Sbloccato: configurazione lettura-scrittura.
Firma configurazione	La connessione del dispositivo di destinazione Identificativo di configurazione di sicurezza (SCID, pagina 366).

Appendici

Contenuto della sezione

Introduzione

Le appendici contengono informazioni su IEC 61508 e la relativa policy SIL. Inoltre, sono forniti i dati tecnici dei moduli di sicurezza e non interferenti con esecuzione di calcoli di esempio.

IEC 61508

Contenuto del capitolo

Introduzione

Questo capitolo fornisce informazioni sui concetti Safety del IEC 61508 in generale e sulla relativa policy SIL in particolare.

Informazioni generali su IEC 61508

Introduzione

I sistemi correlati alla sicurezza sono sviluppati per l'uso nei processi in cui i rischi per le persone, l'ambiente, l'apparecchiatura e la produzione devono essere tenuti a un livello accettabile. Il rischio dipende dalla gravità e dalla probabilità, quindi definendo le necessarie misure di protezione.

Per quanto riguarda la sicurezza dei processi, occorre considerare due aspetti:

- le normative e i requisiti definiti dagli enti ufficiali per la protezione di persone, ambiente, apparecchiatura e produzione
- le misure per cui tali normative e requisiti vengono soddisfatti

Descrizione di IEC 61508

Lo standard tecnico che definisce i requisiti per i sistemi correlati alla sicurezza è

- l'IEC 61508.

Il suo scopo è la sicurezza funzionale di sistemi correlati alla sicurezza elettrici, elettronici o elettronici programmabili. Un sistema di sicurezza è un sistema che deve eseguire una o più funzioni specifiche per garantire che i rischi siano mantenuti a un livello accettabile. Queste funzioni sono definite funzioni di sicurezza (Safety Functions). Un sistema viene definito sicuro dal punto di vista funzionale se guasti casuali, sistematici o di causa comune non inducono un malfunzionamento del sistema e non provocano lesioni o morte delle persone, danni ambientali e perdite di apparecchiature e di produzione.

Lo standard definisce un approccio generico a tutte le attività nel ciclo di vita dei sistemi utilizzati per eseguire funzioni di sicurezza. È costituito dalle procedure da utilizzare per la progettazione, lo sviluppo e la convalida di hardware e software applicati nei sistemi correlati alla sicurezza. Inoltre, determina le regole che riguardano la gestione della sicurezza funzionale e la documentazione.

Descrizione di IEC 61511

I requisiti di sicurezza funzionale definiti nella IEC 61508 sono perfezionati appositamente per l'industria di processo nei seguenti standard tecnici:

- IEC 61511: sicurezza funzionale - sistemi strumentali di sicurezza per l'industria di processo

Questo standard guida l'utente nell'applicazione di un sistema correlato alla sicurezza, a partire dalla fase iniziale di un progetto, proseguendo con l'avvio, contemplando modifiche ed eventuali attività di dismissione dal servizio. Riepilogando, si occupa del ciclo di vita di sicurezza di tutti i componenti di un sistema correlato alla sicurezza utilizzato nell'industria di processo.

Descrizione dei rischi

IEC 61508 si basa sui concetti di analisi del rischio e funzione di sicurezza. Il rischio dipende da gravità e probabilità: Può essere ridotto a un livello tollerabile applicando una funzione di sicurezza che consiste di un sistema elettrico, elettronico o elettronico programmabile. Inoltre, deve essere ridotto a un livello che sia il più basso ragionevolmente praticabile.

Riepilogando, IEC 61508 vede i rischi come segue:

- Il rischio zero non è mai raggiungibile.
- La sicurezza deve essere considerata fin dall'inizio.
- I rischi intollerabili devono essere ridotti.

Politica SIL

Introduzione

Il valore SIL valuta la robustezza di un'applicazione rispetto ai guasti, indicando perciò la capacità di un sistema di eseguire una funzione di sicurezza in una probabilità definita. Lo standard IEC 61508 specifica quattro livelli di prestazioni di sicurezza in base al rischio o agli impatti causati dal processo per cui viene utilizzato il sistema di sicurezza. Più pericolosi sono i possibili impatti sulla comunità e sull'ambiente, maggiori sono i requisiti di sicurezza per ridurre il rischio.

Descrizione valore SIL

Livello discreto (1 su 4 possibili) per la specifica dei requisiti di integrità di sicurezza delle funzioni di sicurezza da assegnare ai sistemi di sicurezza, dove il livello di integrità di sicurezza 4 è il più alto e il livello 1 il più basso. Vedere la sezione SIL per domanda bassa.

Descrizione dei requisiti SIL

Per raggiungere la sicurezza funzionale, sono necessari due tipi di requisiti:

- requisiti della funzione di sicurezza, che definiscono quali funzioni di sicurezza devono essere eseguite
- requisiti di integrità di sicurezza, che definiscono il grado di certezza necessario per l'esecuzione delle funzioni di sicurezza

I requisiti della funzione di sicurezza sono derivati dall'analisi del pericolo e quelli dell'integrità di sicurezza dalla valutazione del rischio.

Consistono delle seguenti quantità:

- tempo medio tra i guasti
- probabilità di guasto
- tassi di guasto
- copertura diagnostica
- frazione guasti di sicurezza
- tolleranza di errore hardware

A seconda del livello di integrità di sicurezza, queste quantità devono essere comprese tra limiti definiti.

NOTA: la combinazione di dispositivi con livelli di integrità di sicurezza differenti su una rete o una funzione di sicurezza richiede un elevato livello di attenzione relativamente ai requisiti di IEC 61508 e genera implicazioni progettuali e operative.

Descrizione della classificazione SIL

Come definito nella normativa IEC 61508, il valore SIL è limitato dalla frazione guasti di sicurezza (SFF) e dalla tolleranza ai guasti hardware (HFT) del sottosistema che esegue la funzione di sicurezza. Un HFT pari a n significa che n+1 guasti potrebbero causare la perdita della funzione di sicurezza; non è possibile accedere allo stato di sicurezza definito. SFF dipende dalla frequenza guasti e dalla copertura diagnostica.

La tabella seguente mostra la relazione tra SFF, HFT e SIL per sottosistemi di sicurezza complessi in base a IEC 61508-2, in cui non è possibile definire completamente le modalità di guasto di tutti i componenti:

SFF	**HFT = 0**	**HFT = 1**	**HFT = 2**
SFF ≤ 60%	-	SIL1	SIL2
60% < SFF ≤ 90%	SIL1	SIL2	SIL3
90% < SFF ≤ 99%	SIL2	SIL3	SIL4
SFF > 99%	SIL3	SIL4	SIL4

Esistono due modi per raggiungere un determinato livello di integrità di sicurezza:

- aumentando l'HFT fornendo ulteriori percorsi di arresto indipendenti
- aumentando SFF tramite diagnostica aggiuntiva

Descrizione della relazione a richiesta SIL

La normativa IEC 61508 distingue tra modalità di domanda bassa e modalità di domanda alta (o continua) di funzionamento.

Nella modalità a bassa richiesta, la frequenza della richiesta di funzionamento fatta su un sistema correlato alla sicurezza non è superiore a 1 all'anno e non è superiore al doppio della frequenza dei test di tenuta. Il valore SIL per un sistema correlato alla sicurezza a bassa richiesta è legato direttamente alla probabilità media dell’impossibilità di eseguire la propria funzione di sicurezza su richiesta oppure, semplicemente, alla probabilità di guasto su richiesta (PFD).

Nella modalità ad alta richiesta o continua, la frequenza della richiesta di funzionamento fatta su un sistema correlato alla sicurezza è maggiore di 1 all'anno e maggiore del doppio della frequenza dei test di tenuta. Il valore SIL per un sistema correlato alla sicurezza ad alta

richiesta è legato direttamente alla probabilità che si verifichi un guasto pericoloso all'ora o, semplicemente, alla probabilità di guasto all'ora (PFH).

SIL per bassa richiesta

La tabella seguente elenca i requisiti per un sistema nella modalità di funzionamento a bassa richiesta:

Livello di integrità di sicurezza (SIL)	Probabilità di guasto su richiesta (PFD)
4	≥ 10^{-5} - < 10^{-4}
3	≥ 10^{-4} - < 10^{-3}
2	≥ 10^{-3} - < 10^{-2}
1	≥ 10^{-2} - < 10^{-1}

SIL per alta richiesta

La tabella seguente elenca i requisiti per un sistema nella modalità di funzionamento ad alta richiesta:

Livello di integrità di sicurezza (SIL)	Probabilità di guasto all'ora (PFH)
4	≥ 10^{-9} - < 10^{-8}
3	≥ 10^{-8} - < 10^{-7}
2	≥ 10^{-7} - < 10^{-6}
1	≥ 10^{-6} - < 10^{-5}

Per SIL3, le probabilità richieste di guasto per il sistema integrato di sicurezza completo sono:

- PFD ≥ 10^{-4} - < 10^{-3} per bassa richiesta
- PFH ≥ 10^{-8} - < 10^{-7} per alta richiesta

Descrizione del loop di sicurezza

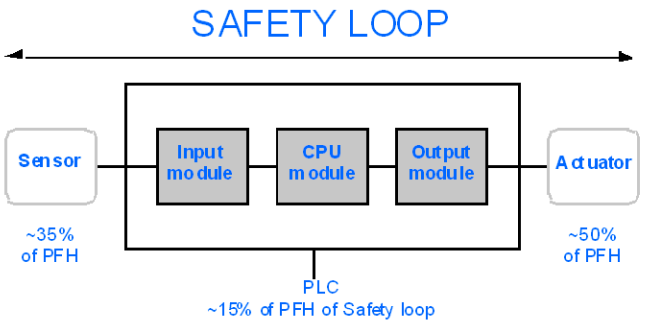
Il loop di sicurezza a cui appartiene il controller M580 Safety è costituito dalle 3 parti seguenti:

- Sensori

- Controller M580 Safety con alimentatore di sicurezza, controller di sicurezza, coprocessore di sicurezza e moduli I/O di sicurezza
- Attuatori

Un backplane o una connessione remota comprendente uno switch o un CRA non distrugge un loop di sicurezza. I backplane, gli switch e i moduli CRA sono parte di un black channel. Questo significa che i dati scambiati dagli I/O e dal controller non possono essere danneggiati senza rilevamento da parte del ricevitore.

La figura seguente mostra un loop di sicurezza tipico:



Come illustrato nella figura precedente, il contributo del controller è solo del 10-20% in quanto la probabilità di guasto di sensori e attuatori è generalmente piuttosto elevata.

Un presupposto conservativo del 10% per il contributo del controller di sicurezza alla probabilità complessiva lascia più margine per l'utente e determina le seguenti probabilità richieste di guasto per il controller di sicurezza:

- PFD ≥ 10^{-5} - < 10^{-4} per bassa richiesta
- PFH ≥ 10^{-9} - < 10^{-8} per alta richiesta

Descrizione dell'equazione PFD

Lo standard IEC 61508 presuppone che metà dei guasti finisca in uno stato sicuro definito. Perciò, la frequenza di guasto λ viene divisa in

- λ_S - il guasto di sicurezza e
- λ_D - l'avaria, composta da
  - λ_{DD} - avaria rilevata dalla diagnostica interna
  - λ_{DU} - avaria non rilevata.

La frequenza di guasto può essere calcolata mediante il tempo medio tra guasti (MTBF), un valore specifico del modulo, come segue:

$\lambda = 1/MTBF$

L'equazione per calcolare la probabilità di guasto su richiesta è:

$PFD(t) = \lambda_{DU} \times t$

t rappresenta il tempo tra due test di tenuta.

La probabilità di guasto all'ora implica un intervallo di tempo di un'ora. Quindi, l'equazione PFD si riduce a quella seguente:

$PFH = \lambda_{DU}$

Oggetti di sistema

Contenuto del capitolo

Introduzione

Questo capitolo descrive i bit e le parole di sistema del PAC M580 Safety.

NOTA: i simboli associati a ciascun oggetto bit o parola di sistema menzionati nelle tabelle descrittive di questi oggetti non sono implementati come standard nel software, ma possono essere immessi con l'ausilio dell'editor di dati.

Bit di sistema M580 Safety

Bit di sistema per esecuzione task SAFE

I seguenti bit di sistema si applicano al PAC M580 Safety. Per una descrizione dei bit di sistema validi per PAC M580 Safety e PAC M580 non di sicurezza, consultare la presentazione di *Bit di sistema* in *EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento*.

Tali bit di sistema sono correlati all'esecuzione del task SAFE, ma non sono direttamente accessibili nel codice del programma di sicurezza. È possibile accedervi solo tramite i blocchi `S_SYST_READ_TASK_BIT_MX` e `S_SYST_RESET_TASK_BIT_MX`.

Bit **Simbolo**	**Funzione**	**Descrizione**	**Stato iniziale**	**Tipo**
%S17 `CARRY`	Uscita rotazione	Durante un'operazione di rotazione, questo bit assumerà lo stato del bit in uscita.	0	R/W
%S18 `OVERFLOW`	Errore aritmetico o di superamento del limite rilevato	Normalmente impostato a 0, questo bit viene impostato a 1 nel caso in cui si verifichi un superamento della capacità: • Un risultato maggiore di + 32 767 o minore di - 32 768, in lunghezza singola. • Un risultato maggiore di + 65 535, in intero senza segno. • Un risultato maggiore di + 2 147 483 647 o minore di - 2 147 483 648, in lunghezza doppia • Un risultato maggiore di +4 294 967 296, in lunghezza doppia o intero senza segno. • Divisione per 0. • Radice di un numero negativo. • Forzatura a un passo inesistente su un tamburo. • Riempimento di un registro già completo, svuotamento di un registro già vuoto.	0	R/W
%S21 `1RSTTASKRUN`	Prima scansione task SAFE in RUN	Provato nel task SAFE, questo bit indica il primo ciclo di questo task. Viene impostato a 1 all'inizio del ciclo e azzerato alla fine. **NOTA:** • Il primo ciclo dello stato del task può essere letto mediante l'uscita `SCOLD` del blocco funzione di sistema `S_SYST_STAT_MX`. • Questo bit non è efficace per sistemi M580 Safety Hot Standby.	0	R/W

Note relative ai bit di sistema specifici non di sicurezza

Bit di sistema	Descrizione	Note
%S0	avvio a freddo	Può essere utilizzato solo nei task di processo (non SAFE) e non influisce sul task SAFE.
%S9	uscite impostate su posizionamento di sicurezza	Non influisce sui moduli di uscita Safety.
%S10	Errore globale rilevato su I/O	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.
%S11	overflow del watchdog	Prende in considerazione un overrun su task SAFE.
%S16	errore task rilevato su I/O	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.
%S19	overrun del periodo di task	Informazioni per overrun task SAFE non disponibili.
%S40...47	errore rilevato su I/O rack *n*	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.
%S78	STOP su errore rilevato	Si applica ai task di processo e al task SAFE. Se è impostato il bit, se ad esempio si verifica un errore di overflow %S18, il task SAFE entra in stato HALT.
%S94	salva i valori regolati	Non si applica alle variabili SAFE. I valori iniziali SAFE non sono modificabili dall'attivazione di questo bit.
%S117	Errore rilevato RIO sulla rete I/O Ethernet	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.
%S119	generale nell'errore rack rilevato	Segnala alcuni, ma non tutti i possibili errori rilevati relativi ai moduli di I/O di sicurezza.

Parole di sistema M580 Safety

Parole di sistema per controller M580 Safety

Le seguenti parole di sistema si applicano al controller M580 Safety. Per una descrizione delle parole di sistema valide per il controller M580 Safety e per i controller M580 non di sicurezza, consultare la presentazione di *Parole di sistema* in *EcoStruxure™ Control Expert - Bit e parole di sistema - Manuale di riferimento*.

Questi valori e parole di sistema sono correlati al task SAFE. È possibile accedervi dal codice del programma applicativo nelle sezioni non di sicurezza (MAST, FAST, AUX0 o AUX1), ma non dal codice nella sezione del task SAFE.

Word	Funzione	Tipo
%SW4	Periodo del task SAFE definito nella configurazione. Il periodo non è modificabile dall'operatore.	R
%SW12	Indica la modalità operativa del modulo coprocessore: • 16#A501 = modalità di manutenzione • 16#5AFE = modalità di sicurezza Qualsiasi altro valore è interpretato come errore rilevato.	R
%SW13	Indica la modalità operativa del controller: • 16#501A = modalità di manutenzione • 16#5AFE = modalità di sicurezza Qualsiasi altro valore è interpretato come errore rilevato.	R
%SW42	Ora corrente task SAFE. Indica il tempo di esecuzione dell'ultimo ciclo del task SAFE (in ms).	R
%SW43	Durata max. task SAFE. Indica il tempo di esecuzione del task SAFE più lungo dall'ultimo avvio a freddo (in ms).	R
%SW44	Durata min. task SAFE. Indica il tempo di esecuzione del task SAFE più breve dall'ultimo avvio a freddo (in ms).	R
%SW110	Percentuale del carico del controller di sistema utilizzato dal sistema per servizi interni.	R
%SW111	Percentuale del carico del controller di sistema utilizzato dal task MAST.	R
%SW112	Percentuale del carico del controller di sistema utilizzato dal task FAST.	R
%SW113	Percentuale del carico del controller di sistema utilizzato dal task SAFE.	R
%SW114	Percentuale del carico del controller di sistema utilizzato dal task AUX0.	R
%SW115	Percentuale del carico del controller di sistema utilizzato dal task AUX1.	R
%SW116	Carico totale del controller di sistema.	R

Word	Funzione	Tipo
%SW124	Contiene la causa dell'errore irreversibile rilevato quando il controller M580 Safety è in stato Halt: • 0x5AF2: Errore RAM rilevato nel controllo memoria • 0x5AFB: Errore del codice firmware di sicurezza rilevato • 0x5AF6: Errore di overrun del watchdog di sicurezza rilevato sul controller. • 0x5AFF: Errore di overrun watchdog di sicurezza rilevato sul coprocessore. • 0x5B01: Coprocessore non rilevato all'avvio. • 0x5AC03: Errore irreversibile CIP Safety rilevato dal controller. • 0x5AC04: Errore irreversibile CIP Safety rilevato dal coprocessore. **NOTA:** Quanto indicato sopra non costituisce un elenco completo. Per ulteriori informazioni, consultare *EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento*.	R
%SW125	Contiene la causa dell'errore reversibile rilevato nel controller M580 Safety: • 0x5AC0: La configurazione CIP Safety non è corretta (rilevata dal controller). • 0x5AC1: La configurazione CIP Safety non è corretta (rilevata dal coprocessore). • 0x5AF3: Errore di confronto rilevato dal controller principale. • 0x5AFC: Errore di confronto rilevato dal coprocessore. • 0x5AFD: Errore interno rilevato dal coprocessore. • 0x5AFE: Errore di sincronizzazione rilevato tra controller e coprocessore. • 0x9690: Errore di checksum del programma applicativo rilevato. **NOTA:** Quanto indicato sopra non costituisce un elenco completo. Per ulteriori informazioni, consultare *EcoStruxure™ Control Expert, Bit e parole di sistema, Manuale di riferimento*.	R
%SW126 %SW127	Queste due parole di sistema contengono informazioni per uso interno Schneider Electric per consentire di analizzare nei dettagli un errore rilevato.	R
%SW128	Con firmware del controller 3.10 o precedente, forzare la sincronizzazione dell'ora tra ora NTP e ora sicura nei moduli I/O di sicurezza e nel task SAFE: • Il cambiamento di valore da 16#1AE5 a 16#E51A forza la sincronizzazione. Vedere la sezione *Procedura per sincronizzare le impostazioni dell'ora NTP*, pagina 182. • Altre sequenze e valori non forzano la sincronizzazione.	L/S
%SW142	Contiene la versione del firmware del coprocessore di sicurezza in quattro cifre BCD: ad esempio, la versione firmware 21.42 corrisponde a %SW142 = 16#2142.	R
%SW148	Conteggio degli errori ECC (Error Correcting Code, codice di correzione errori) rilevati dal controller.	R
%SW152	Con il firmware del controller 3.10 o precedente, lo stato dell'ora del controller NTP aggiornato dal modulo di comunicazione Ethernet (ad esempio BMENOC0301 o BMENOC0311) sul backplane X Bus tramite la funzione di sincronizzazione dell'ora forzata opzionale: • 0: l'ora del controller non viene aggiornata dal modulo di comunicazione Ethernet.	R

Word	Funzione	Tipo
	• 1: l'ora del controller viene aggiornata dal modulo di comunicazione Ethernet.	
%SW169	ID applicazione di sicurezza: Contiene un ID della parte codice di sicurezza dell'applicazione. L'ID viene modificato automaticamente quando si modifica il codice applicazione sicuro. **NOTA:** • Se il codice di sicurezza è stato modificato ed è stato eseguito un comando **Crea modifiche** dal precedente comando **Ricrea tutto** (cambiando perciò l'ID applicazione di sicurezza), l'esecuzione di un comando **Ricrea tutto** può di nuovo cambiare l'ID applicazione di sicurezza. • L'identificativo univoco del programma SAFE può essere letto mediante l'uscita `SAID` del blocco funzione di sistema `S_SYST_STAT_MX`.	R
%SW171	Stato dei task FAST: • 0: Non esistono task FAST • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	R
%SW172	Stato del task SAFE: • 0: Non esiste alcun task SAFE • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	R
%SW173	Stato del task MAST: • 0: Non esiste alcun task MAST • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	R
%SW174	Stato del task AUX0: • 0: Nessun task AUX0 esistente • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	R

Word	Funzione	Tipo
%SW175	Stato del task AUX1: • 0: Non esiste alcun task AUX1 • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	R
%SW176	Stato di conteggio bit forzato per le variabili SAFE del programma: • Incrementa ogni volta che viene forzato un bit digitale. • Decrementa ogni volta che viene annullata la forzatura di un bit digitale.	R

Riferimenti SRAC

Il piano di verifica delle condizioni di applicazione relative alla sicurezza (SRAC) fornisce un quadro generico per giustificare il rispetto delle istruzioni del manuale di installazione e sicurezza associato. Queste istruzioni nella documentazione *Modicon M580, Manuale di sicurezza* sono elencate come requisiti.

La tabella seguente fornisce il titolo del paragrafo dove è possibile trovare il requisito relativo al ciclo di vita dell'applicazione:

Requisito del ciclo di vita dell'applicazione	
Id	**In questa posizione**
LC #1	Passo 9: Specifica dei requisiti di sicurezza del sistema E/E/PE, pagina 41
LC #2	Passo 9: Specifica dei requisiti di sicurezza del sistema E/E/PE, pagina 41
LC #3	Passo 10: Realizzazione dei sistemi di sicurezza E/E/PE, pagina 41
LC #4	Passo 12: Installazione e messa in servizio globali, pagina 45
LC #5	Passo 12: Installazione e messa in servizio globali, pagina 45
LC #6	Passo 13: Convalida sicurezza globale, pagina 46
LC #7	Passo 14: Funzionamento, manutenzione e riparazione globali, pagina 47
LC #8	Passo 15: Modifica e retrofit globale, pagina 47

La tabella seguente fornisce il titolo del paragrafo dove è possibile trovare i requisiti relativi al Messaggio informativo di sicurezza:

Requisito del messaggio informativo di sicurezza	
Id	**In questa posizione**
SM #1	Informazioni preliminari, pagina 10
SM #2	Avviamento e verifica, pagina 11
SM #3	Loop di sicurezza, pagina 21
SM #4	Moduli non interferenti, pagina 33

Requisito del messaggio informativo di sicurezza	
Id	**In questa posizione**
SM #5	Alimentazione esterna utilizzata con gli I/O di sicurezza digitali, pagina 51
SM #6	Esempi di cablaggio dell'applicazione di ingresso BMXSAI0410, introduzione, pagina 58
SM #7	Esempi di cablaggio applicazione di ingresso BMXSAI0410, SIL3 Cat2/PLd, pagina 60
SM #8	Esempi di cablaggio applicazione di ingresso BMXSAI0410, SIL3 Cat2/PLd con alta disponibilità, pagina 61
SM #9	Esempi di cablaggio applicazione di ingresso BMXSAI0410, SIL3 Cat4/PLe, pagina 62
SM #10	Esempi di cablaggio dell'applicazione di ingresso BMXSAI0410, SIL3 Cat4/PLe con alta disponibilità, pagina 63
SM #11	Connettore di cablaggio BMXSDI1602, alimentazione di processo, pagina 70
SM #12	Connettore di cablaggio BMXSDI1602, fusibile, pagina 71
SM #13	Esempi di cablaggio dell'applicazione di ingresso BMXSDI1602, introduzione, pagina 76
SM #14	Diagnostica cablaggio configurabile in Control Expert, pagina 77
SM #15	Esempi di cablaggio applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd, pagina 78
SM #16	Esempi di cablaggio applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd, pagina 78
SM #17	Esempi di cablaggio applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd, pagina 78
SM #18	Esempi di cablaggio applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 80
SM #19	Esempi di cablaggio applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 80
SM #20	Esempi di cablaggio applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 80
SM #21	Esempi di cablaggio applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 80
SM #22	Esempi di cablaggio applicazione di ingresso BMXSDI1602, SIL3 Cat2/PLd con alta disponibilità, pagina 80
SM #23	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 84

Requisito del messaggio informativo di sicurezza	
Id	**In questa posizione**
SM #24	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 84
SM #25	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 84
SM #26	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 84
SM #27	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 84
SM #28	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 84
SM #29	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 84
SM #30	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe, pagina 84
SM #31	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 90
SM #32	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 90
SM #33	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 90
SM #34	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 90
SM #35	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 90
SM #36	Esempi di cablaggio applicazione di ingresso BMXSDI1602, Cat4/PLe con alta disponibilità, pagina 90
SM #37	Connettore di cablaggio BMXSDO0802, fusibile, pagina 102
SM #38	Esempi di cablaggio dell'applicazione di uscita BMXSDO0802, introduzione, pagina 104
SM #39	Esempi di cablaggio dell'applicazione di uscita BMXSDO0802, introduzione, pagina 104
SM #40	Diagnostica di cablaggio configurabile in Control Expert, pagina 105
SM #41	Riepilogo diagnostica del cablaggio delle uscite, pagina 108
SM #42	Riepilogo diagnostica del cablaggio delle uscite, pagina 108

Requisito del messaggio informativo di sicurezza	
Id	**In questa posizione**
SM #43	Riepilogo diagnostica del cablaggio delle uscite, pagina 108
SM #44	Riepilogo diagnostica del cablaggio delle uscite, pagina 108
SM #45	Riepilogo diagnostica del cablaggio delle uscite, pagina 108
SM #46	Riepilogo diagnostica del cablaggio delle uscite, pagina 108
SM #47	Connettore di cablaggio BMXSRA0405, fusibile, pagina 116
SM #48	Applicazione_1: 4 uscite, SIL2 / Cat2 / PLc, stato non alimentato, nessun test automatico del segnale, pagina 119
SM #49	Applicazione_3: 4 uscite, SIL2 / Cat2 / PLc, stato alimentato, nessun test automatico del segnale, pagina 120
SM #50	Applicazione_5: 2 uscite, SIL3 / Cat4 / PLe, stato non alimentato, nessun test automatico del segnale, pagina 121
SM #51	Applicazione_7: 2 uscite, SIL3 / Cat4 / PLe, stato alimentato, nessun test automatico del segnale, pagina 122
SM #52	Alimentatori M580 Safety, Introduzione, pagina 133
SM #53	Descrizione del tempo per moduli di uscita, pagina 160
SM #54	Configurazione dei periodi massimi dei task SAFE e FAST della CPU, pagina 164
SM #55	Funzioni e blocchi funzione di sicurezza certificati, pagina 169
SM #56	Configurazione della sincronizzazione dell'ora con firmware della CPU 3.10 o precedente, Introduzione, pagina 180
SM #57	Modifica dell'impostazione dell'ora NTP durante il funzionamento, pagina 181
SM #58	Procedura per sincronizzare le impostazioni dell'ora NTP, pagina 182
SM #59	Procedura per sincronizzare le impostazioni dell'ora NTP, pagina 182
SM #60	Configurazione del DFB S_WR_ETH_MX, pagina 194
SM #61	Configurazione del DFB S_RD_ETH_MX, pagina 196

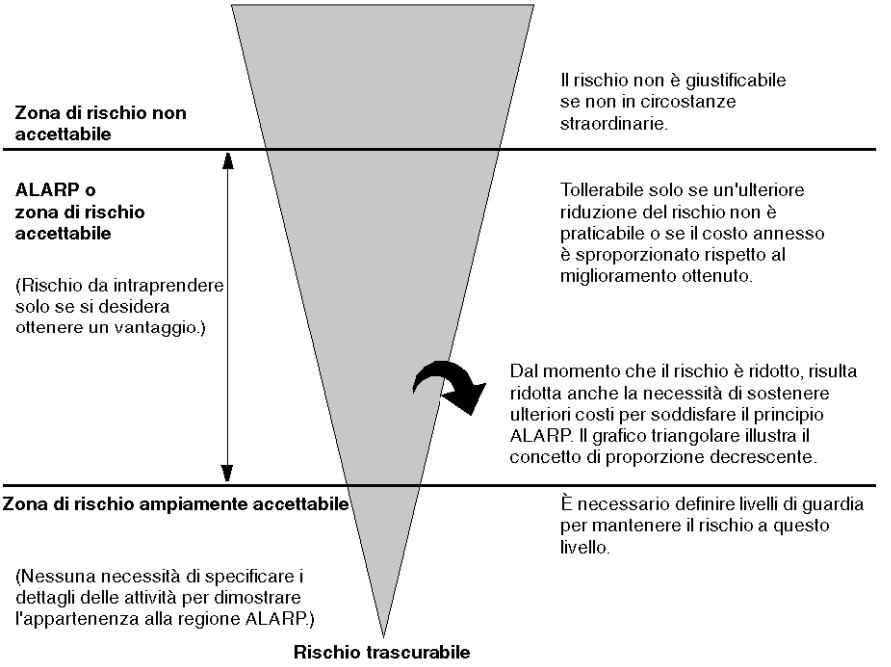
Requisito del messaggio informativo di sicurezza	
Id	**In questa posizione**
SM #62	Configurazione del DFB S_WR_ETH_MX2, pagina 207
SM #63	Configurazione del DFB S_RD_ETH_MX2, pagina 210
SM #64	Comunicazioni black channel M580, pagina 213
SM #65	Comunicazioni black channel M580, pagina 213
SM #66	Diagnostica LED CPU M580 Safety, pagina 224
SM #67	Funzionalità modalità manutenzione, pagina 261
SM #68	Sequenze di avvio, avvio a caldo, pagina 273
SM #69	Blocco della configurazione del modulo I/O di sicurezza, pagina 286
SM #70	Visualizzazione dei dati nelle schermate operatore, pagina 293
SM #71	Configurazione del dispositivo CIP Safety mediante uno strumento offerto dal fornitore, pagina 359
SM #72	Interazioni tra le operazioni del PAC di sicurezza e la connessione di destinazione, pagina 382

Glossario

A

ALARP:

(*il più basso prevedibile*) (Definizione di IEC 61508)



C

CCF:

(*Common cause failure, guasto da causa comune*) Guasto risultante da uno o più eventi che causano guasti concomitanti su due o più canali separati in un sistema a più canali, provocando un guasto del sistema. (Definizione di IEC 61508) La causa comune in un sistema a due canali è un fattore cruciale per la probabilità di guasto su domanda (PFD, probability of failure on demand) per l'intero sistema.

CPCRC:

(*controllo di ridondanza ciclica del parametro di connessione*) Un CRC-S32 dei parametri di connessione di destinazione prodotto dal CSS per ciascuna connessione CIP Safety e contenuto nella richiesta di apertura di sicurezza di tipo 2.

D

DDDT:

(*Device derived data type, tipo dati derivati dispositivo*) Un DDT predefinito dal produttore e non modificabile dall'utente. Contiene gli elementi di linguaggio di I/O di un modulo di I/O.

Derivazione RIO:

Un rack di moduli I/O Ethernet, gestito da un adattatore RIO, con ingressi e uscite inclusi nella scansione RIO della CPU. Una derivazione può essere un rack singolo o un rack principale con un rack esteso.

DRS:

(*switch a doppio anello*) Uno switch a gestione estesa ConneXium configurato per il funzionamento su una rete Ethernet. I file di configurazione predefinita sono forniti da Schneider Electric per lo scaricamento su un DRS per supportare funzionalità speciali dell'architettura dell'anello principale / del sotto-anello.

DTM:

(*Device Type Manager*) Un DTM è un driver del dispositivo eseguito sul PC host. Fornisce una struttura unificata per l'accesso ai parametri, la configurazione e il funzionamento dei dispositivi e la diagnostica dei problemi. I DTM possono essere una semplice interfaccia utente grafica (Graphical User Interface, GUI) per l'impostazione dei parametri dei dispositivi su un'applicazione altamente sofisticata che supporta l'esecuzione di calcoli complessi in tempo reale a scopo di diagnostica e manutenzione. Nel contesto di un DTM, un dispositivo può essere un modulo di comunicazione o un sistema di rete remoto.

Vedere FDT.

E

EDS:

(*Electronic Data Sheet*) Gli EDS sono semplici file di testo che descrivono le capacità di configurazione di un dispositivo. I file EDS sono elaborati e forniti dal costruttore del dispositivo.

EUC:

(*Equipment under control, apparecchiatura sotto controllo*) (Definizione IEC 61508) Questo termine indica apparecchiature, macchine, sistemi o impianti utilizzati per attività di produzione, elaborazione, trasporto, medicali o di altro tipo.

H

HFT:

(*Hardware Fault Tolerance, tolleranza degli errori hardware*) (Definizione IEC 61508)

Una tolleranza degli errori hardware pari a N significa che N + 1 errori potrebbero provocare la perdita delle funzioni di sicurezza, ad esempio:

- HFT = 0: il primo errore può causare la perdita della funzione di sicurezza.
- HFT = 1: 2 errori combinati potrebbero causare la perdita della funzione di sicurezza. (Vi sono due percorsi possibili per passare a uno stato di sicurezza. Perdita della funzione di sicurezza significa che non è stato possibile passare a uno stato di sicurezza.)

O

OUNID:

(*identificativo di rete univoco dell'origine*) Un valore che identifica in modo univoco il dispositivo da cui ha origine la connessione (tipicamente una CPU) su una rete CIP Safety. OUNID consiste in:

- un numero di rete di sicurezza (SNN), che può essere un Time stamp o un altro valore definito dall'utente.
- un indirizzo di nodo (per reti EtherNet/IP, l'indirizzo IP).

P

PST:

(*Process safety time, tempo di sicurezza processo*) Il tempo di sicurezza del processo è il periodo di tempo che intercorre tra un errore verificatosi in un EUC o nel sistema di controllo dell'EUC (potenzialmente in grado di provocare un evento pericoloso) e il verificarsi dell'evento pericoloso qualora non venga eseguita la funzione di sicurezza. (Definizione IEC 61508)

R

Rete DIO:

Una rete contenente apparecchiature distribuite nella quale la scansione I/O viene eseguita da una CPUDIO con servizio di scansione sul rack locale. Il traffico di rete DIO è fornito dopo il traffico RIO, che ha la priorità in una rete di dispositivi.

S

SAId:

(*identificativo dell'applicazione di sicurezza*) Una firma calcolata con un algoritmo della parte sicura dell'applicazione Control Expert, archiviata in %SW169.

SCID:

(*identificativo di configurazione di sicurezza*) Vedere TUNID.

SFF:

(*Safe Failure Fraction, frazione di guasti di sicurezza*)

SNCT:

(*strumento di configurazione di rete di sicurezza*) Uno strumento offerto dal fornitore per la configurazione dei dispositivi CIP Safety. Vedere TUNID.

SRAC:

(*Safety Related Application Condition*, condizione dell'applicazione di sicurezza)

SRT:

(*System reaction time, tempo di reazione del sistema*) Il tempo di reazione del sistema è il periodo di tempo tra il rilevamento di un segnale al terminale del modulo di ingresso e la reazione di impostazione di un'uscita al terminale del modulo di uscita.

T

TFFR:

(*tolerable functional failure rate*, tasso guasti funzionali tollerabili) Un tasso orario secondo le norme EN 5012x per il settore ferroviario.

TUNID:

(*identificativo di rete univoco della destinazione*) Un valore che identifica in modo univoco il dispositivo di destinazione della connessione su una rete CIP Safety. TUNID consiste in:

- un numero di rete di sicurezza (SNN), che può essere un Time stamp o un altro valore definito dall'utente.
- un identificativo di configurazione di sicurezza (SCID), anche detto firma di configurazione, creato con uno strumento di configurazione di rete di sicurezza offerto dal fornitore (SNCT) e che consiste in:
  - un CRC di configurazione di sicurezza (SCCRC), che è un valore CRC delle impostazioni di configurazione del dispositivo di sicurezza, sotto forma di un valore esadecimale formato da 4 byte.
  - Un Time stamp di configurazione di sicurezza (SCTS), un valore time stamp esadecimale di data e ora formato da 6 byte.

Indice

A

B

C

D

E

F

S

T

U

V

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

Poiché gli standard, le specifiche tecniche e la progettazione possono cambiare di tanto in tanto, si prega di chiedere conferma delle informazioni fornite nella presente pubblicazione.

QGH46985.06