Modicon M580

Guida alla pianificazione del sistema di sicurezza

Traduzione delle istruzioni originali

QGH60286.08
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 7
Prima di iniziare 8
Avviamento e verifica 9
Funzionamento e regolazioni 10
Informazioni sul manuale 11
Moduli supportati del sistema di sicurezza M580 17
Moduli certificati del sistema di sicurezza M580 18
Moduli non interferenti 20
Selezione di una topologia del sistema di sicurezza M580 25
Progettazione di una topologia del sistema di sicurezza M580 26
Topologie M580 Safety 30
CPU e coprocessore M580 Safety 38
Caratteristiche fisiche di coprocessore e CPU M580 Safety 39
Descrizione fisica di coprocessore e CPU di sicurezza M580 39
Display a LED per coprocessore e CPU M580 Safety 45
Porte Ethernet 47
Porta USB 50
Socket SFP 52
Scheda di memoria SD 52
Sigilli anti-manomissione e sportello della scheda SD bloccabile 54
Caratteristiche della prestazioni di coprocessore e CPU M580 Safety 57
Caratteristiche delle prestazioni di coprocessore e CPU M580 57
Alimentatori M580 Safety 60
Descrizione fisica degli alimentatori M580 Safety 61
Caratteristiche prestazionali dell'alimentatore M580 Safety 67
Relé allarme alimentatore M580 Safety 72
Moduli I/O M580 Safety 73
Descrizione fisica dei moduli I/O M580 Safety 74
Descrizione fisica dei moduli I/O M580 74
Caratteristiche delle prestazioni I/O M580 Safety 80
Caratteristiche prestazionali del modulo di ingresso analogico BMXSAI0410 Safety 80

Caratteristiche prestazionali del modulo di ingresso digitale BMXSDI1602 Safety 82
Caratteristiche prestazionali del modulo di uscita digitale BMXSDO0802 Safety 83
Modulo di uscita relé digitale BMXSRA0405 Safety 85
Installazione del PAC M580 Safety 87
Installazione di moduli di estensione e rack M580 88
Pianificazione dell'installazione del rack locale 88
Montaggio dei rack 93
Estensione di un rack 95
Installazione di CPU M580, copro, alimentatore e I/O 98
Installazione di CPU e coprocessore 98
Installazione di un modulo di alimentazione 101
Installazione I/O M580 Safety 105
Installazione di una scheda di memoria SD in una CPU 107
Aggiornamento del firmware del controller M580 Safety 110
Aggiornamento del firmware alla versione 4.21 111
Downgrade del firmware dalla versione 4.21 o successiva 111
Utilizzo di un sistema di sicurezza M580 113
Aree di processo, sicurezza e dati globali in Control Expert 114
Separazione dei dati in Control Expert 115
Modalità operative, stati operativi e task 119
Modalità operative del PAC M580 Safety 119
Stati operativi del PAC M580 Safety 124
Sequenze di avvio 129
Task del PAC M580 Safety 133
Creazione di un progetto di sicurezza M580 137
Creazione di un progetto di sicurezza M580 137
Firma Safe 137
Blocco delle configurazioni del modulo I/O M580 di sicurezza 145
Blocco delle configurazioni del modulo I/O M580 Safety 145
Inizializzazione dei dati in Control Expert 148
Inizializzazione dei dati in Control Expert per il PAC M580 Safety 148
Lavorare con le tabelle di animazione in Control Expert 149
Tabelle di animazione e schermate operatore 149

Aggiunta di sezioni codice 154
Aggiunta di codice a un processo di sicurezza M580 154
Richiesta diagnostica 158
Comandi Scambia e Azzera 161
Gestione della sicurezza dell'applicazione 164
Protezione dell'applicazione 164
Protezione tramite password dell'area di sicurezza 172
Protezione di Unità programma, sezione e subroutine 177
Protezione del firmware 179
Protezione Web/Memorizzazione dati 181
Perdita della password 183
Gestione della sicurezza della workstation 190
Gestione dell'accesso a EcoStruxure Control Expert 190
Diritti di accesso 193
Impostazioni del progetto di sicurezza M580 204
Impostazioni progetto per un progetto M580 Safety in Control Expert 204
Appendici 209
IEC 61508 210
Informazioni generali su IEC 61508 211
Policy SIL 213
Oggetti di sistema 218
Bit di sistema M580 Safety 219
Parole di sistema M580 Safety 221
Riferimenti SRAC 225
Glossario 227
Indice 229

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

Ambito del documento

La presente Guida alla pianificazione del sistema di sicurezza descrive i moduli del sistema M580 Safety con particolare attenzione a come soddisfano ai requisiti di sicurezza della normativa IEC 61508. Fornisce informazioni dettagliate su come installare, operare ed eseguire la manutenzione del sistema in modo corretto per proteggere le persone e impedire danni ad ambiente, apparecchiatura e produzione.

La presente documentazione è dedicata a personale qualificato con conoscenze dei sistemi di sicurezza funzionale e Control Expert XL 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 di validità

Il presente documento è valido per EcoStruxure™ Control Expert 16.0 con ControlExpert_V160_HF001 M580 Safety o versione 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/.

Le caratteristiche dei prodotti descritti in questo documento corrispondono a quelle disponibili su www.se.com. Nell'ambito della nostra strategia aziendale per un miglioramento costante, è possibile che il contenuto della documentazione venga revisionato nel tempo per migliorare la chiarezza e la precisione. Se si notano differenze tra le caratteristiche riportate in questo documento e quelle riportate su www.se.com, considerare www.se.com contenente le informazioni più recenti.

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, Manuale di sicurezza	QGH46982 (Inglese), QGH46983 (Francese), QGH46984 (Tedesco), QGH46985 (Italiano), QGH46986 (Spagnolo), QGH46987 (Cinese)
EcoStruxure™ Control Expert, Safety, Block Library	QGH60275 (Inglese), QGH60278 (Francese), QGH60279 (Tedesco), QGH60280 (Italiano), QGH60281 (Spagnolo), QGH60282 (Cinese)
Sistemi di controller Modicon - Sicurezza informatica - Guida utente	EIO0000001999 (Inglese), EIO0000002001 (Francese), EIO0000002000 (Tedesco), EIO0000002002 (Italiano), EIO0000002003 (Spagnolo), EIO0000002004 (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, Topologie complesse, Guida di sistema	NHA58892 (Inglese), NHA58893 (Francese), NHA58894 (Tedesco), NHA58895 (Italiano), NHA58896 (Spagnolo), NHA58897 (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)
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

RISCHIO DI SCOSSA ELETTRICA, ESPLOSIONE O ARCO ELETTRICO

- Mettere fuori tensione tutte le apparecchiature, inclusi i dispositivi collegati, prima di rimuovere qualunque coperchio o sportello, o prima di installare/disinstallare accessori, hardware, cavi o fili, tranne che per le condizioni specificate nell'apposta Guida hardware per questa apparecchiatura.
- Per verificare che l'alimentazione sia isolata, usare sempre un rilevatore di tensione correttamente tarato.
- Prima di riattivare l'alimentazione dell'unità rimontare e fissare tutti i coperchi, i componenti hardware e i cavi e verificare la presenza di un buon collegamento di terra.
- Quando si utilizza questa apparecchiatura e qualunque prodotto associato, usare esclusivamente la 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 i controlli di prevenzione e 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 morte, gravi infortuni o danni alle apparecchiature.

[1] Per ulteriori informazioni, vedere 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 morte, gravi infortuni o danni alle apparecchiature.

Marchi commerciali

QR Code è un marchio registrato di DENSO WAVE INCORPORATED in Giappone e in altri paesi.

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:

Standard	**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 61496-1:2013 Sicurezza	Sicurezza dei macchinari: 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.
IEC 61508-2:2010	Sicurezza funzionale dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili: Requisiti dei sistemi di sicurezza elettrici/elettronici/elettronici programmabili.

Standard	Descrizione
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

Inoltre, i termini utilizzati nelle informazioni qui contenute possono essere utilizzate indirettamente in quanto derivate da altre norme quali:

Norma	Descrizione
Serie IEC 60034	Macchine elettriche rotative
Serie IEC 61800	Variatori di velocità elettrici regolabili
Serie IEC 61158	Comunicazioni dati digitali per misure 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 o meno applicarsi 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.

Informazioni sulla terminologia non inclusiva o insensibile

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

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 fornisce tutta la funzionalità di Control Expert L ed è utilizzabile con CPU di sicurezza BMEP582040S e BMEH582040S.
- Control Expert XL Safety fornisce tutta la funzionalità di Control Expert XL ed è utilizzabile per l'intera gamma di CPU 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 M580 Safety è un sistema di sicurezza certificato da TÜV Rheinland Group, in base a:

- SIL3 / IEC 61508 / IEC 61511
- SIL4 / EN 50128 (IEC 62279), EN 50129 (IEC 62245), EN 50126 (IEC 62278)
- 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: www.certipedia.com o www.fs-products.com.

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

- CPU standalone BMEP582040S
- CPU standalone BMEP584040S
- CPU standalone BMEP586040S
- CPU Hot Standby BMEH582040S
- CPU Hot Standby BMEH584040S
- CPU Hot Standby BMEH586040S
- 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 20.

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 indicato SIL2 o SIL3 senza un riferimento standard, si tratta di 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 una CPU

È possibile sostituire una CPU BME•58•040S con un'altra 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 CPU di sicurezza e Hot Standby.
- Per una descrizione delle limitazioni della CPU, *Caratteristiche prestazionali della CPU e del coprocessore M580*, pagina 57 del documento *Modicon M580, Guida alla pianificazione del sistema di sicurezza*.

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 in-rack (BMEx, BMXx, PMXx e PMEx), esistono due tipi di moduli non interferenti:

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

  Per moduli Mx80 non in-rack, tutta l'apparecchiatura Ethernet (DIO o DRS) può essere considerata come non interferente e perciò utilizzabile 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 di TÜV Rheinland all'indirizzo www.certipedia.com.

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 avanzato X80 1 CH	BMXCRA31210
Comunicazione: adattatore derivazione Ethernet avanzato 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 rack	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
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

Tipo di modulo	Codice prodotto modulo
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 In 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
Digitale: Dig 16Q Trans Source 0.5A	BMXDDO1602
Digitale: Dig 16 O Trans Sink	BMXDDO1612

Tipo di modulo	Codice prodotto modulo
	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 rack possono essere considerati 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 di TÜV Rheinland all'indirizzo www.certipedia.com.

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
Alimentazione standard ridondante 24/48 VCC	BMXCPS4022
Alimentazione CA standard ridondante	BMXCPS4002

Tipo di modulo	Codice prodotto modulo
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 rack dei moduli M580 Safety) sono non interferenti di Tipo 2.

Selezione di una topologia del sistema di sicurezza M580

Introduzione

Questo capitolo descrive le topologie supportate da un sistema di sicurezza M580.

Progettazione di una topologia del sistema di sicurezza M580

Supporto per PAC standalone e Hot Standby

Un sistema di sicurezza M580 supporta applicazioni SIL3 per PAC standalone e Hot Standby. Ciascun rack di CPU comprende una CPU e un modulo coprocessore.

NOTA: Per una descrizione dei rack disponibili e del loro utilizzo consentito, consultare l'argomento *Utilizzo dei rack*, pagina 88.

Posizionamento dei moduli di sicurezza nell'anello principale RIO

Installare i moduli di sicurezza M580 solo nell'anello principale RIO, che include:

- Il rack locale principale. I PAC di sicurezza standalone possono includere fino a sette rack di estensione locali opzionali.
  - Il rack locale principale deve comprendere un alimentatore di sicurezza, una CPU di sicurezza e un coprocessore di sicurezza.
  - Per un PAC di sicurezza standalone, il rack principale locale e i rack di estensione locali possono anche comprendere I/O di sicurezza. Il PAC M580 Hot Standby non supporta I/O sul rack principale locale o sui rack di estensione locali.

    NOTA: La distanza massima tra rack principale e l'ultimo rack di estensione è di 30 m.
- Fino a 31 derivazioni RIO per la CPU BME•586040S, 16 derivazioni RIO per la CPU BME•584040S e 8 derivazioni RIO per la CPU BME•582040S), ciascuna comprendente un rack principale remoto e un rack esteso remoto opzionale.

Qualsiasi rack con moduli di sicurezza richiede un alimentatore di sicurezza.

NOTA: Un rack che contiene moduli di sicurezza può anche comprendere moduli non interferenti di tipo 1, pagina 20. Tuttavia, i moduli non interferenti di tipo 2, pagina 23 possono non essere posizionati nello stesso rack dei moduli di sicurezza. I moduli non interferenti di tipo 2 possono essere posizionati su rack senza moduli di sicurezza, ad esempio in rack di apparecchiatura distribuita. Altri moduli non di sicurezza possono non essere inclusi in un sistema di sicurezza M580.

Estensione di un rack principale

Utilizzare i moduli di estensione rack BMXXBE1000 per il collegamento a margherita dei rack principale e di estensione. Collegare ciascuna coppia di moduli con i cavi del connettore BMXXBC•••K e terminare ciascuna estremità della serie con terminatori di linea TSXELYEX.

Comunicazioni rack locale con una derivazione RIO

Per supportare le derivazioni RIO in un sistema di sicurezza M580 con firmware della CPU 3.10 o precedente, configurare la CPU di sicurezza M580 come server NTP o come client NTP (con un altro dispositivo configurato come server NTP). Senza un orologio correttamente configurato (NTP), la comunicazione I/O di sicurezza potrebbe non funzionare correttamente.

Utilizzare un modulo adattatore remoto BM•CRA312•0 (un BM•CRA31200 per rack remoto contenente solo moduli non interferenti e un adattatore BM•CRA31210 per rack remoto contenente modulo I/O di sicurezza e/o non interferenti per collegare la derivazione RIO all'anello principale RIO. Collegare ciascuna estremità dell'anello principale RIO alle due doppie porte sulla CPU di sicurezza BME•58•040S.

Se il collegamento avviene tramite cavo in rame di Cat5e, la distanza massima tra le derivazioni è di 100 m.

NOTA: In alternativa, è possibile collegare il rack principale locale all'adattatore remoto BM•CRA312•0 nella derivazione RIO posizionando un modulo ripetitore in fibra ottica BMXNRP020• in ciascun rack. Per ulteriori informazioni, consultare l'argomento *Utilizzo dei moduli di conversione in fibra ottica* nella *Modicon M580 Standalone, Guida di pianificazione del sistema per architetture di utilizzo frequente*.

Collegamento di due PAC M580 Safety

Un sistema di sicurezza M580 supporta inoltre comunicazione a canale nero peer-to-peer tra due PAC di sicurezza. In genere, questa connessione avviene tramite un BMENOC0321 in ciascun sistema di sicurezza. Per ulteriori informazioni, vedere la sezione comunicazioni peer-to-peer nel *Modicon M580, Manuale di sicurezza*.

NOTA: per supportare comunicazioni black channel tra due PAC con firmware della CPU 3.10 o precedente, attivare il servizio NTP in entrambi i PAC. È possibile configurare un PAC come server NTP e l'altro come client NTP. In alternativa, è possibile configurare ciascun PAC come client NTP, con un altro dispositivo configurato come server NTP.

Aggiunta di apparecchiature distribuite a un sistema di sicurezza M580

È possibile includere apparecchiature distribuite nel sistema di sicurezza M580. In genere, l'apparecchiatura distribuita viene collegata a margherita senza loop o con loop a margherita.

È possibile collegare un loop a margherita dell'apparecchiatura distribuita alle due porte di rete di uno dei moduli seguenti sull'anello principale RIO:

- un modulo di comunicazioni Ethernet BMENOC0301/11.
- uno switch opzionale di rete Ethernet BMENOS0300.
- uno switch ad anello doppio ConneXium.

È inoltre possibile utilizzare la porta service di un modulo di comunicazione Ethernet BMENOC0301/11, uno switch opzionale di rete Ethernet BMENOS0300 o la CPU di sicurezza BME•58•040S per collegare l'apparecchiatura distribuita a margherita senza loop.

NOTA: Posizionare solo moduli non interferenti di tipo 1 e 2 in una rete di apparecchiature distribuite. Posizionare i moduli di sicurezza solo nel rack locale (principale o di estensione) e nella rete RIO. Escludere i moduli non di sicurezza non interferenti di tipo 1 o 2 dal progetto di sicurezza.

Consultare l'argomento *Selezione della corretta topologia* in *Modicon M580 Standalone, Guida di pianificazione del sistema per le architetture di utilizzo frequente* per ulteriori informazioni sulla connessione delle apparecchiature distribuite a una CPU M580.

Aggiunta di apparecchiature CIP Safety ad un sistema di sicurezza M580

È possibile includere dispositivi I/O CIP Safety (CSIO) nel sistema di sicurezza M580 come apparecchiatura distribuita CSIO.

È possibile collocare un'apparecchiatura distribuita CSIO all'anello principale RIO tramite:

- la porta di servizio di un modulo adattatore CPU o EIO X80 BM•CRA31210.
- uno switch opzionale di rete Ethernet BMENOS0300.
- uno switch a doppio anello (DRS) ConneXium.

Ciascun tipo di I/O (CSIO, RIO, DIO) presenta dei limiti. Per mantenere un livello accettabile di prestazioni, non utilizzare il massimo di tutti i tipi di I/O nella stessa architettura.

Basare un'architettura M580 CIP Safety tipica su una topologia remota o distribuita:

Limitazioni **topologia remota**:

	Dispositivi CSIO	**Dispositivi DIO**	**Derivazioni RIO**
BMEP582040S	10	10	8
BMEP584040S	32	10	16
BMEP586040S	(n. CSIO) + 0,5*(n. DIO) + (n. RIO) ≤ 128		

Limitazioni **topologia distribuita**:

	Dispositivi CSIO	**Dispositivi DIO**	**Derivazioni RIO**
BMEP582040S	16	61	2
BMEP584040S	64	61	2
BMEP586040S	(n. CSIO) + 0,5*(n. DIO) + (n. RIO) ≤ 128		

Il contributo del tempo CSIO al task SAFE è di circa 100 µs/apparecchiatura con una CPU BMEP584040S o BMEP586040S e 400 µs/apparecchiatura con una CPU BMEP582040S

Topologie M580 Safety

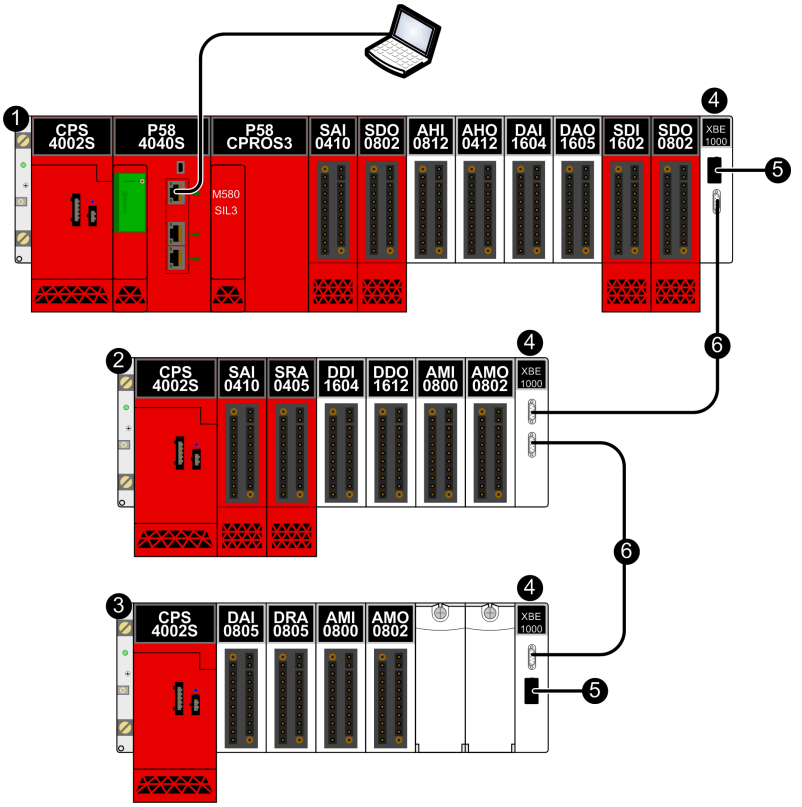
Introduzione

Gli schemi seguenti presentano esempi di topologie di sicurezza M580. Questa raccolta di topologie di esempio non comprende ogni topologia potenziale supportata da un sistema di sicurezza M580.

Consultare *Modicon M580 Standalone, Guida di pianificazione del sistema per architetture di utilizzo frequente*, *Modicon M580 Guida di pianificazione del sistema per le topologie complesse* e *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente* per ulteriori informazioni sulla configurazione di una topologia M580.

Estensione del rack principale locale

Lo schema seguente presenta un rack principale locale con due rack di estensione. Tenere presente che il sistema di sicurezza M580 supporta un singolo rack principale locale più un massimo di sette rack di estensione su una lunghezza massima di 30 m:



1 Rack principale locale con moduli di sicurezza e di tipo 1 non interferenti

2 Rack di estensione locale con moduli di sicurezza e di tipo 1 non interferenti

3 Rack di estensione locale con moduli di tipo 1 non interferenti

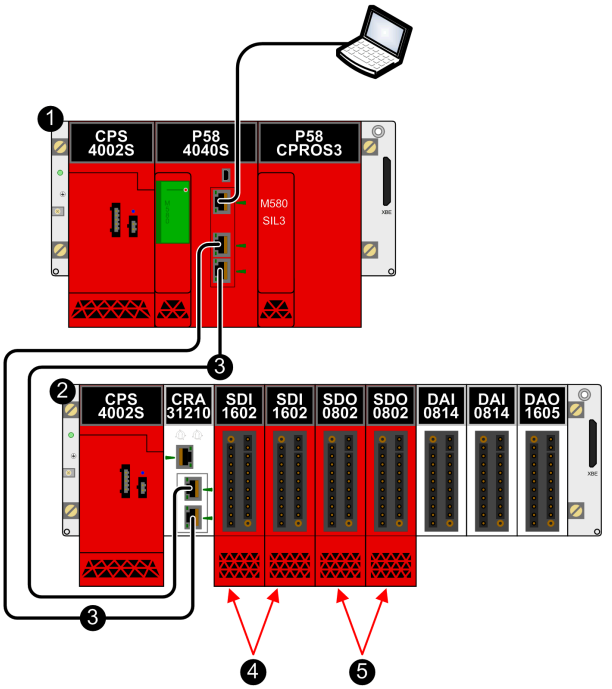
4 Moduli di estensione rack BMXXBE1000

5 Terminazioni di linea TSXELYEX

6 Cavi connettore BMXXBC•••K

Topologie di I/O ad alta disponibilità

Lo schema seguente presenta un esempio di I/O ridondanti nella stessa derivazione RIO:



1 Rack principale locale

2 Derivazione RIO

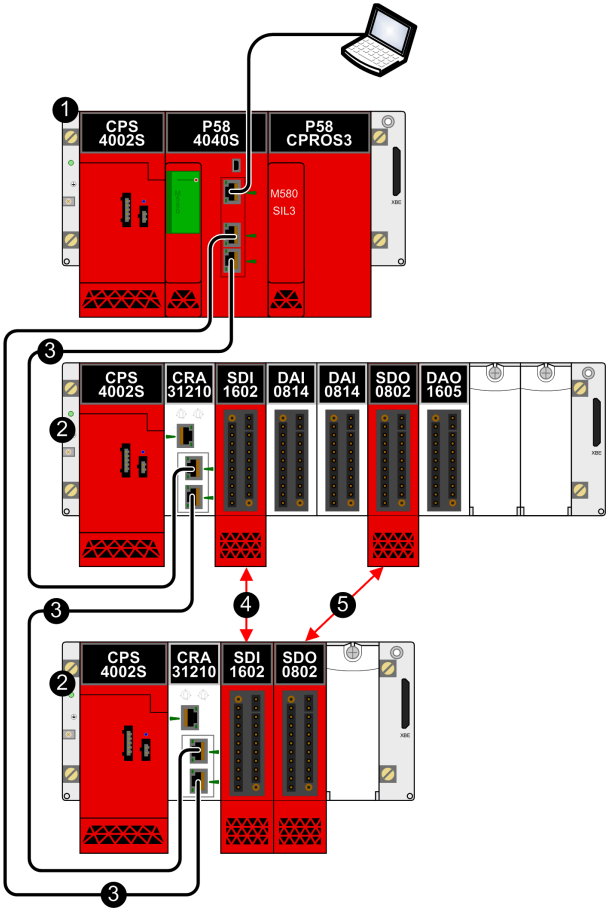
3 Anello principale RIO

4 Due moduli di ingresso ridondanti nella stessa derivazione RIO

5 Due moduli di uscita ridondanti nella stessa derivazione RIO

NOTA: Con firmware della CPU 3.10 o precedente, attivare il servizio NTP per il PAC di sicurezza M580 per supportare la comunicazione black channel tra il rack principale locale e le derivazioni RIO sull'anello principale RIO e configurare l'ora nel PAC se il PAC deve essere il server NTP. Il PAC Safety può essere il server NTP o il client NTP (con un altro dispositivo configurato come server NTP).

Lo schema seguente presenta un esempio di posizionamento di I/O ridondanti in due derivazioni RIO separate:



1 Rack principale locale

2 Derivazione RIO

3 Anello principale RIO

4 Due moduli di ingresso ridondanti in derivazioni RIO separate

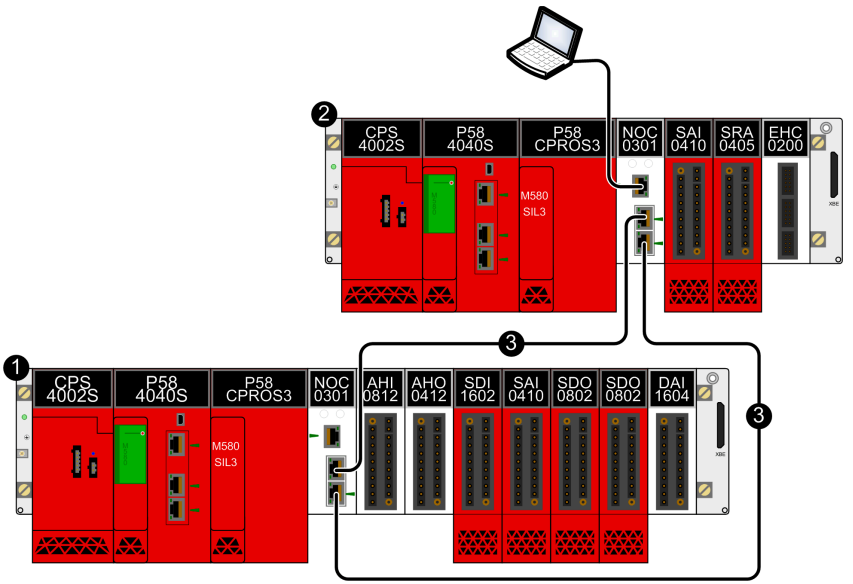
5 Due moduli di uscita ridondanti in derivazioni RIO separate

NOTA:

- Posizionare i moduli di I/O di sicurezza ridondanti in derivazioni RIO separate.
- Con firmware della CPU 3.10 o precedente, attivare il servizio NTP per il PAC M580 Safety per supportare la comunicazione black channel tra il rack principale locale e le derivazioni RIO sull'anello principale RIO. Il PAC di sicurezza può essere il server NTP o il client NTP (con un altro dispositivo configurato come server NTP).

Topologia peer-to-peer per due PAC di sicurezza standalone

Lo schema seguente mostra un esempio di come collegare due PAC di sicurezza M580 separati. In questo esempio, un sensore collegato a un modulo di ingresso di sicurezza nel PAC 1 può essere configurato per provocare una risposta da un attuatore collegato a un modulo di uscita di sicurezza nel PAC 2:



1 PAC 1 di sicurezza M580 standalone

2 PAC 2 di sicurezza M580

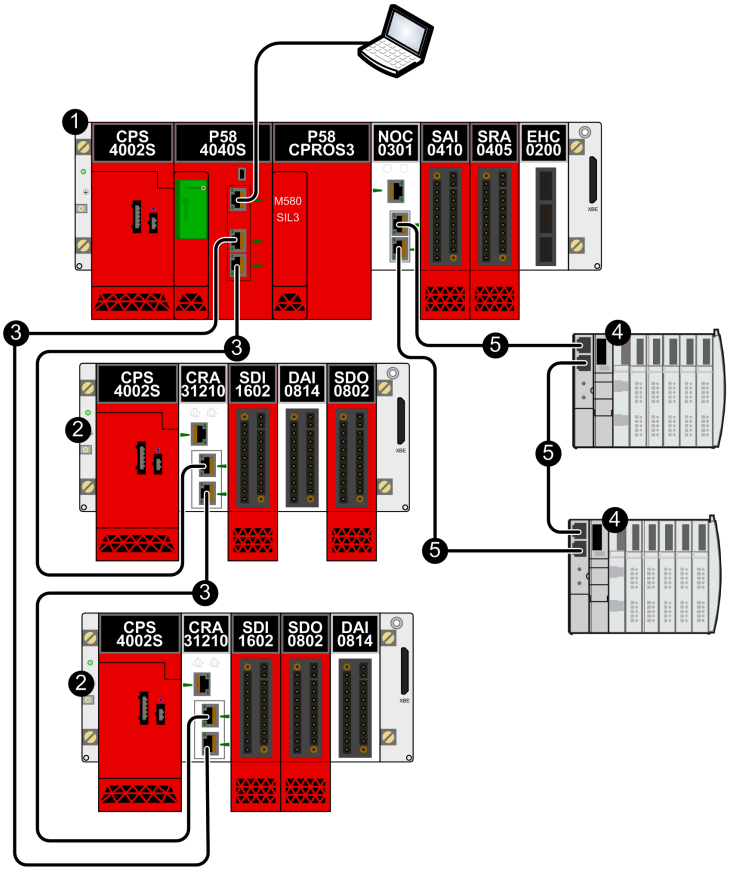
3 Comunicazione black channel tra PAC

NOTA: per supportare comunicazioni black channel tra due PAC con firmware della CPU 3.10 o precedente, attivare il servizio NTP in entrambi i PAC. È possibile configurare un PAC come server NTP e l'altro come client NTP. In alternativa, è possibile configurare ciascun PAC come client NTP, con un altro dispositivo configurato come server NTP.

Aggiunta di apparecchiatura distribuita al PAC di sicurezza M580

È possibile aggiungere moduli non interferenti di tipo 1 e tipo 2 al progetto di sicurezza M580 come apparecchiatura distribuita, in una configurazione a margherita senza loop o con loop a margherita.

Lo schema seguente descrive un esempio di apparecchiatura distribuita aggiunta come collegamento a margherita senza loop. In questo esempio, l'apparecchiatura distribuita con collegamento a margherita si connette al PAC tramite le porte EIO ETH2 ed ETH3 di un modulo di comunicazioni Ethernet BMENOC0301/11:



1 Rack principale locale con backplane Ethernet

2 Derivazione RIO con moduli di sicurezza e di tipo 1 non interferenti

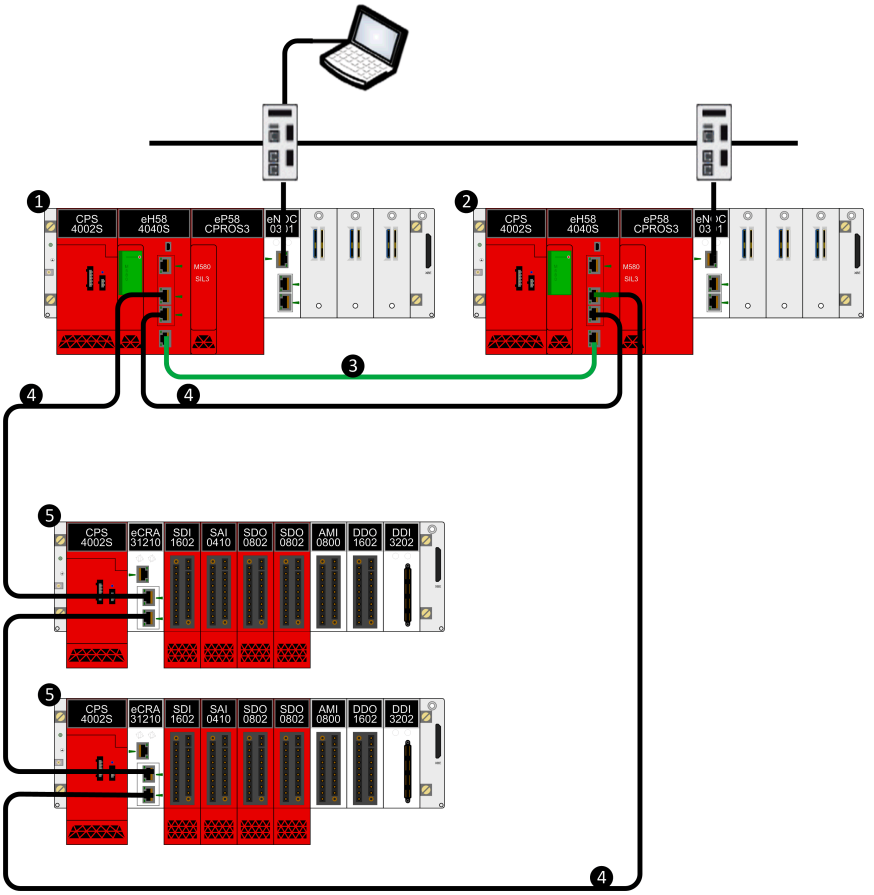
3 Anello principale RIO

4 Apparecchiatura distribuita

5 Anello di apparecchiatura distribuita

Topologia Hot Standby

Lo schema seguente presenta una topologia Hot Standby:



1 Rack locale primario con CPU primaria

2 Rack locale di standby con CPU di standby

3 Collegamento di comunicazione Hot Standby

4 Anello principale Ethernet RIO

5 Derivazione (e)X80 RIO

CPU e coprocessore M580 Safety

Introduzione

Questo capitolo descrive le CPU BME•58•040S e il Coprocessore (Copro) BMEP58CPROS3.

Caratteristiche fisiche di coprocessore e CPU M580 Safety

Introduzione

Questa sezione descrive le caratteristiche fisiche comuni delle CPU BME•58•040S e del coprocessore BMEP58CPROS3 (Copro).

Descrizione fisica di coprocessore e CPU di sicurezza M580

Posizione sul rack locale

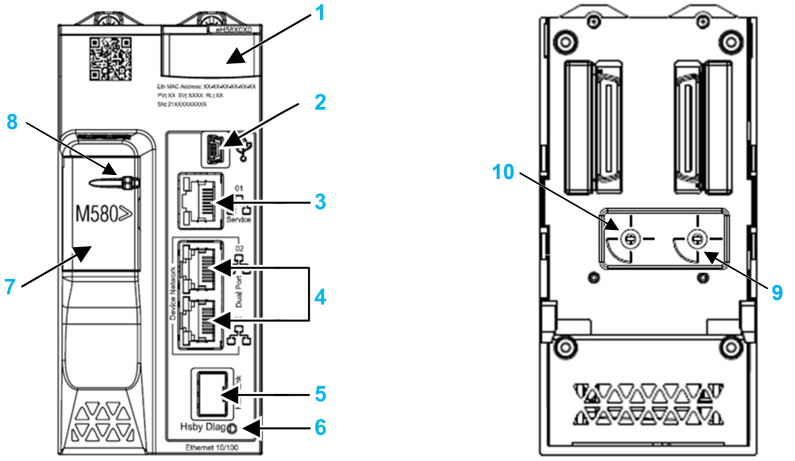
Ogni sistema di sicurezza SIL3 M580 standalone richiede una CPU BME•58•040S e un coprocessore (Copro) BMEP58CPROS3. La CPU richiede due slot del modulo ed è posizionata negli slot 0 e 1 immediatamente a destra dell'alimentatore nel rack locale principale. Anche il copro richiede due slot del modulo ed è posizionato negli slot 2 e 3 immediatamente a destra della CPU. La CPU e il copro non possono essere posizionati in altre posizioni di slot o in altri rack. Se sono presenti rack di estensione in una configurazione di un rack locale, assegnare l'indirizzo 00 al rack che ospita la CPU and Copro.

NOTA: CPU e copro di sicurezza possono essere installati solo su un rack Ethernet BMEXBP••••. Per una descrizione dei rack M580 disponibili, consultare l'argomento *Rack locali e remoti* in *Modicon M580 - Manuale di riferimento hardware*.

Viste anteriore e posteriore della CPU

La CPU BME•58•040S di sicurezza supporta la scansione RIO e DIO.

Caratteristiche fisiche della CPU:



Legenda:

1 Pannello di visualizzazione diagnostica a LED

2 Porta USB Mini-B per la configurazione del modulo tramite PC con Control Expert

3 Connettore porta di servizio Ethernet RJ45

4 Connettori RJ45 che insieme fungono da porta doppia alla rete Ethernet

5 Socket SFP per collegamento Hot Standby in rame o fibra ottica

6 LED di collegamento di stato Hot Standby

7 Slot scheda di memoria SD (dietro lo sportello)

8 Sportello bloccabile della scheda di memoria SD

9 Selettore a rotazione della modalità operativa, con impostazioni **Communication Security Reset**, **Secured**, **Standard**

> **NOTA:** il selettore a rotazione della modalità operativa sarà operativo per le future versioni del prodotto. Per questa release del prodotto, la modalità operativa viene impostata automaticamente su **Standard**, indipendentemente dalla posizione del selettore.

10 Selettore a rotazione A/B/Clear, utilizzato per impostare il PAC come PAC A o PAC B o per cancellare l'applicazione Control Expert esistente

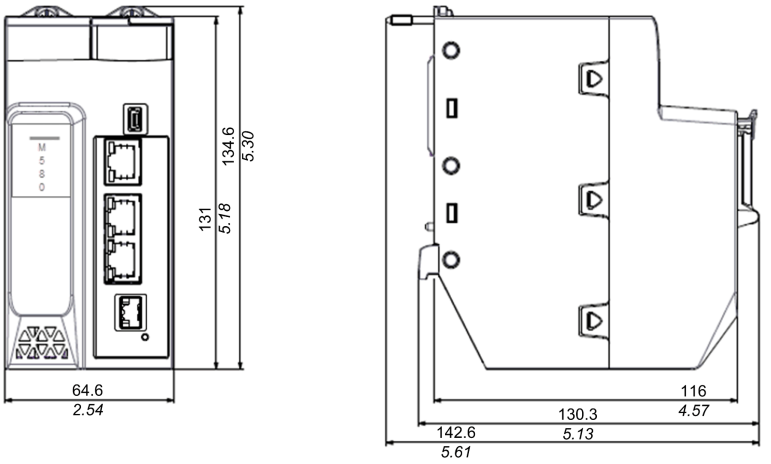
Pannello frontale del coprocessore

Il coprocessore BMEP58CPROS3 presenta solo un display a LED sul lato anteriore.

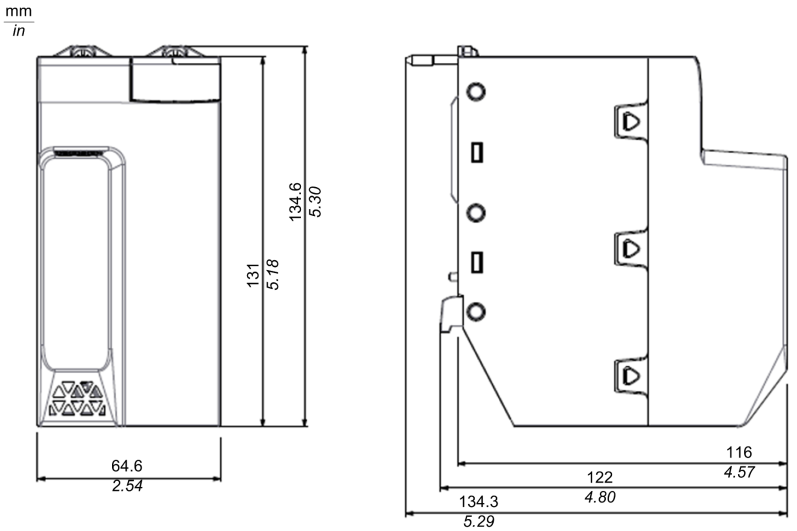
Dimensioni di CPU e copro

Le CPU BME•58•040S di sicurezza presentano le seguenti dimensioni fisiche:

mm
in



Il copro BMEP58CPROS3 presenta le seguenti dimensioni fisiche: A differenza della CPU, il copro non presenta connettori fisici o etichette correlate

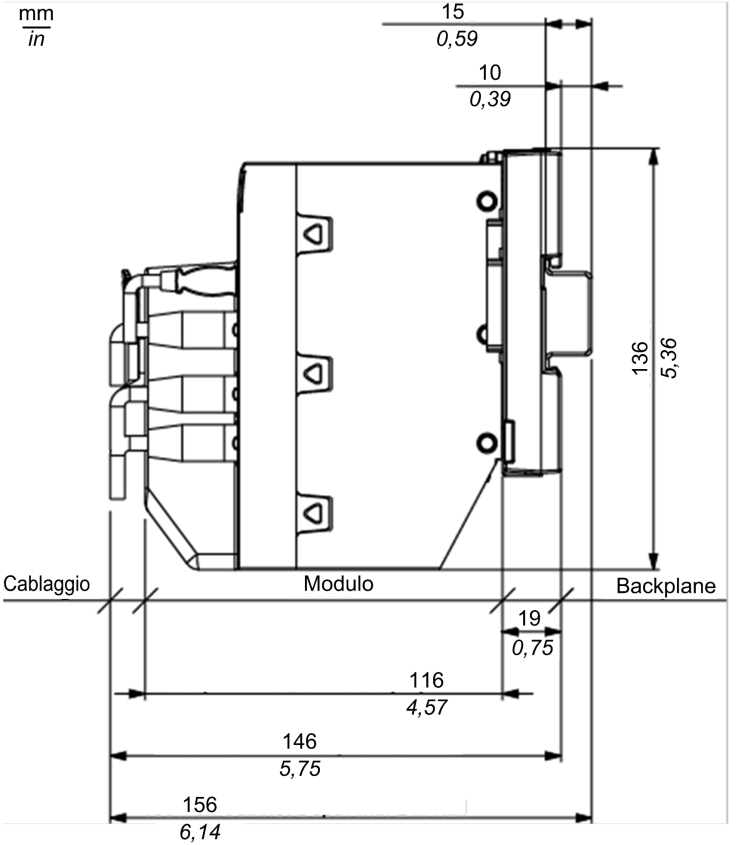


NOTA: Considerare l'altezza di CPU e copro quando si pianifica l'installazione del rack locale. CPU e copro si estendono oltre il bordo inferiore del rack di:

- 29,49 mm (1.161 in.) per un rack Ethernet
- 30,9 mm (1.217 in.) per un rack X Bus

Dimensioni di cablaggio CPU

Le CPU BME•58•040S di sicurezza presentano le seguenti dimensioni quanto montate su una guida DIN con relativo cablaggio:

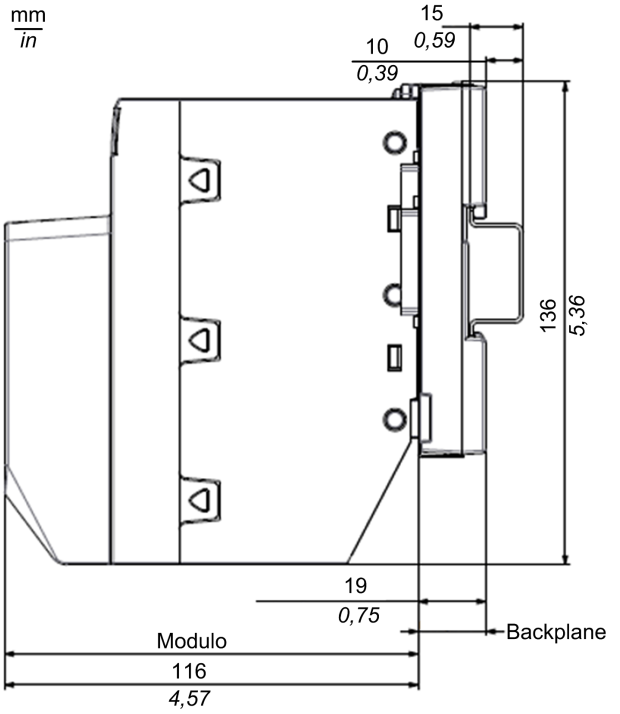


La profondità globale della CPU è:

- 146 mm con cablaggio
- 156 mm con cablaggio più guida DIN

Dimensioni di cablaggio copro

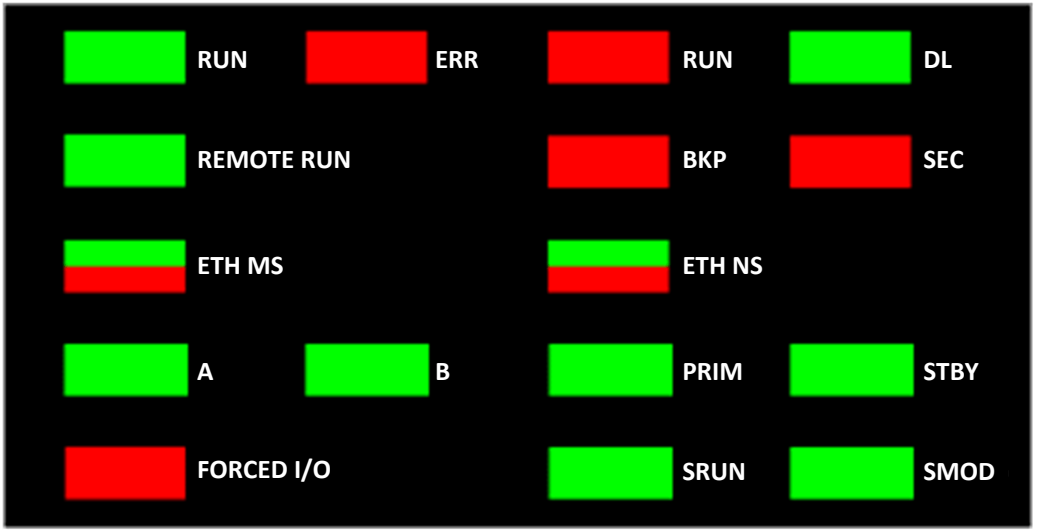
Il copro BMEP58CPROS3 presenta le seguenti dimensioni quando è montato su una guida DIN:



Display a LED per coprocessore e CPU M580 Safety

CPU LED Display

Un display a LED si trova sul pannello frontale della CPU:



NOTA: Il LED **SEC**, che indica lo stato di comunicazione sicuro, non è implementato per questa versione.

NOTA: Il display LED Copro è un sottoinsieme del display della CPU e include i seguenti LED:

- **ERR**
- **DL**
- **SRUN**
- **SMOD**

Descrizioni dei LED

NOTA: Consultare gli argomenti:

- *Diagnostica LED CPU M580 Safety* e *Diagnostica LED coprocessore M580* nel *Modicon M580, Manuale di sicurezza* per informazioni su come utilizzare i LED di CPU e copro per diagnosticare lo stato del PAC di sicurezza.
- *Diagnostica LED per CPU Hot Standby M580* in *Modicon M580 - Guida alla pianificazione del sistema Hot Standby per architetture di utilizzo frequente* per informazioni su come utilizzare i LED **A**, **B**, **PRIM**, **STBY**, e **REMOTE RUN** della CPU Hot Standby.

Indicatore LED	Si applica a...		Descrizione
	CPU	Copro	
RUN	✓	–	**Acceso**: la CPU gestisce le uscite e almeno un task è in stato RUN.
ERR	✓	✓	**acceso**: la CPU ha rilevato un errore interno della CPU (ad esempio, nessuna configurazione, errore watchdog rilevato, errore autotest rilevato.)
I/O	✓	–	**Acceso**: la CPU ha rilevato un errore, esterno alla CPU, in uno o più moduli di I/O.
DL (*Download*)	✓	+	• **Acceso**: è in corso un aggiornamento del firmware nella CPU, nel Copro, nel backplane o in un altro modulo nel rack. • **Spento**: nessun aggiornamento del firmware in corso.
BKP	✓	–	**Acceso**: • La scheda di memoria o la memoria flash della CPU è assente o non funzionante. • La scheda di memoria è inutilizzabile (formato errato, tipo non riconosciuto). • La scheda di memoria o il contenuto della memoria flash della CPU non è coerente con l'applicazione corrente. • La scheda di memoria è stata rimossa e reinserita. • È stato eseguito un comando **PLC > Backup progetto... > Cancella backup** mentre non era presente alcuna scheda di memoria. Il LED **BKP** rimane **acceso** fino al completamento del backup del progetto.
			Spento: la scheda di memoria o il contenuto della memoria flash della CPU è valido e l'applicazione nella memoria di esecuzione è identica.
ETH MS	✓	–	MOD STATUS (verde/rosso): il motivo indica lo stato di configurazione della porta Ethernet. **NOTA:** nel caso del rilevamento di un errore recuperabile, il LED **ETH MS** può essere verde o rosso e acceso o spento.
ETH NS	✓	–	NET STATUS (verde/rosso): Il motivo indica lo stato della connessione Ethernet.

Indicatore LED	Si applica a...		Descrizione
	CPU	Copro	
FORCED I/O	✓	–	**Acceso**: almeno un ingresso o un'uscita su un modulo di I/O digitale è forzato.
SRUN	✓	✓	**Acceso**: il PAC gestisce le uscite di sicurezza e il task SAFE è in stato RUN.
SMOD	✓	✓	• **Acceso**: il PAC funziona in modalità di sicurezza, pagina 119. • **Lampeggiante**: il PAC funziona in modalità di manutenzione, pagina 120.
✓: Applicabile – : Non applicabile.			

Porte Ethernet

Introduzione

Tre porte RJ45 Ethernet sono presenti sulla parte frontale della CPU, una porta per manutenzione e due porte di rete per dispositivi. Tutte le porte hanno le seguenti caratteristiche.

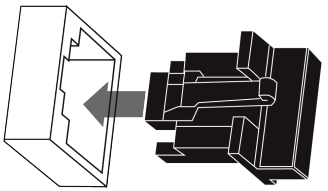
Caratteristiche comuni

Tutte e tre le porte hanno lo stesso connettore RJ45 e usano lo stesso tipo di cavi Ethernet.

NOTA: Le tre porte Ethernet sono collegate alla messa a terra dello chassis e il sistema richiede una messa a terra equipotenziale.

Coperchio antipolvere

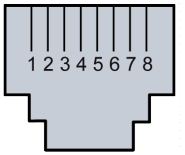
Per impedire che entri polvere nelle porte Ethernet non utilizzate, proteggerle con l'apposito coperchietto:



Porte Ethernet:

Ogni connettore RJ45 dispone di una coppia di indicatori LED:

La posizione dei pin, i pin di uscita e i collegamenti dei cavi sono gli stessi sulle tre porte RJ45 Ethernet:

Pin	Descrizione	
1	TD+	Pin di uscita: 
2	TD-	
3	RD+	
4	Non collegato	
5	Non collegato	
6	RD-	
7	Non collegato	
8	Non collegato	
—	Terra involucro/chassis	

NOTA: I pin TD (1 e 2) e i pin RD (3 e 6) sono auto MDIX compatibili e invertono automaticamente i loro ruoli in base al supporto collegato (ossia, cavi diritti o incrociati).

Le porte hanno una capacità MDIX automatica che rileva automaticamente la direzione della trasmissione.

Selezionare tra i seguenti cavi Ethernet per il collegamento alle porte Ethernet:

- TCSECN3M3M••••: cavo schermato Cat 5E Ethernet diretto, certificato per uso industriale, conforme a CE o UL
- TCSECE3M3M••••: cavo schermato Cat 5E Ethernet diretto, certificato per uso industriale, conforme a CE
- TCSECU3M3M••••: cavo schermato Cat 5E Ethernet diretto, certificato per uso industriale, conforme a UL

La lunghezza massima per un cavo in rame è 100 m. Per distanze superiori a 100 m, usare un cavo in fibra ottica. La CPU non dispone di porte in fibra ottica. È possibile utilizzare switch a doppio anello o moduli convertitori per fibra ottica BMX NRP •••• (vedi Modicon M580 Indipendente, Guida di pianificazione del sistema per, architetture di utilizzo frequente) per gestire la conversione rame-fibra ottica.

Porte Ethernet su CPU standalone

Su CPU standalone, il LED **ACTIVE** è verde. Il LED **LNK** è verde o giallo, a seconda dello stato:

LED	Stato dei LED	Descrizione
ACTIVE	Spento	Nessuna attività è indicata sulla connessione Ethernet.
	Acceso/ lampeggiante	I dati sono trasmessi e ricevuti sul collegamento Ethernet.
LNK	Spento	Nessun collegamento stabilito su questa connessione.
	Acceso verde	Collegamento a 100 Mbps* stabilito su questa connessione.
	Acceso giallo	Collegamento a 10 Mbps* stabilito su questa connessione.
* Il collegamento 10/100 Mbps supporta il trasferimento half-duplex e full-duplex e la negoziazione automatica.		

Porta Service

La porta per manutenzione è quella situata più alto tra le tre porte Ethernet che si trovano sul pannello frontale della CPU. Questa porta può essere utilizzata:

- Per fornire un punto di accesso utilizzabile da altri sistemi o dispositivi per eseguire il monitoraggio o comunicare con la M580 CPU.
- Come porta DIO standalone in grado di supportare una topologia a stella o a margherita di apparecchiature distribuite.
- Per eseguire il mirroring delle porte CPU per diagnostica Ethernet. Lo strumento di assistenza che visualizza l'attività sulla porta replicata può essere un PC o un HMI.

  NOTA: non utilizzare la porta service per collegarsi alla rete del dispositivo, se non in alcune condizioni specifiche descritte in *Modicon M580, Open Ethernet Network, System Planning Guide*.

  La porta service potrebbe non offrire tutte le prestazioni e le funzionalità delle porte di **rete di dispositivi** della CPU.

  Se si collega la porta service, direttamente o tramite switch/hub, alla rete di dispositivi si potrebbe influire sulle prestazioni del sistema.

Doppie porte di rete dispositivi

Si può utilizzare una porta **Device Network** per supportare una topologia a stella, a margherita dell'apparecchiatura distribuita. Si possono utilizzare entrambe le porte **Device Network** per supportare una topologia ad anello.

Se vengono utilizzate come porte RIO, entrambe le porte collegano la CPU all'anello principale in un loop daisy-chain o anello Ethernet.

Per ulteriori informazioni sulle architetture RIO/DIO, consultare il capitolo *Sistema Modicon M580* (vedi Modicon M580 Indipendente, Guida di pianificazione del sistema per, architetture di utilizzo frequente).

Considerazioni sulla messa a terra

Rispettare la regolamentazione e tutte le norme locali e nazionali sulla sicurezza.

⚠⚠PERICOLO

PERICOLO DI SCOSSA ELETTRICA

Se non è possibile provare che il capo di un cavo schermato è collegato alla terra locale, il cavo deve essere considerato pericoloso e occorre indossare dispositivi di protezione individuale (DPI).

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

Porta USB

Introduzione

La porta USB è un connettore USB mini-B ad alta velocità, versione 2.0 (480 Mbps), utilizzabile per un programma Control Expert o un pannello per interfaccia uomo-macchina (HMI). La porta USB può essere collegata a un'altra porta USB, versione 1.1 o successiva.

NOTA: Installare i driver M580 USB prima di collegare il cavo USB tra la CPU e il PC.

Trasparenza

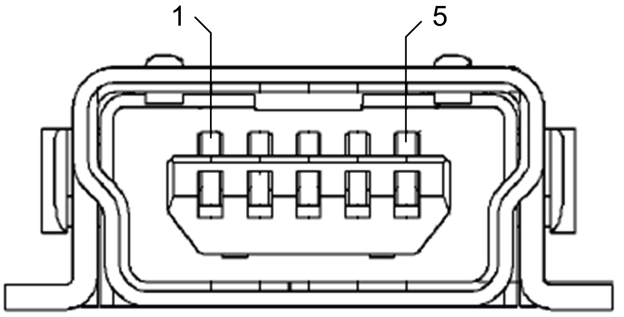
Se il sistema richiede trasparenza tra il dispositivo collegato alla porta USB e la M580rete di dispositivi , aggiungere un percorso statico persistente alla tabella di routing del dispositivo.

Esempio di comando di indirizzamento di una rete di dispositivi con indirizzo IP `X.X.0.0` (per un PC Windows): `route add X.X.0.0 mask 255.255.0.0 90.0.0.1 -p`

(In questo caso, `X.X.0.0` è l'indirizzo di rete utilizzato dalla rete di dispositivi M580, e `255.255.0.0` è la maschera di sottorete corrispondente.)

Assegnazione dei pin

La porta USB ha le seguenti posizioni dei pin e dei pin di uscita:



Legenda:

Pin	Descrizione
1	VBus
2	D-
3	D+
4	Non collegato
5	terra
involucro	terra chassis

Cavi

Usare un cavo BMX XCA USB H018 (1,8 m/5,91 ft) o BMX XCA USB H045 (4,5 m/14,764 ft) per connettere il pannello alla CPU. Questi cavi sono dotati di un connettore di tipo A ad un'estremità e di USB mini-B all'altra.

In un gruppo fisso con una console di tipo XBT collegata alla CPU, collegare il cavo USB a una barra di protezione (vedi Modicon X80, Alimentatori e rack , Manuale di riferimento hardware). Usare la parte esposta della schermatura o il capocorda del cavo metallico BMX XCA per effettuare il collegamento.

Socket SFP

Connettore porta collegamento ridondante

Ogni modulo CPU Hot Standby include un socket SFP a cui è possibile collegare un ricetrasmettitore in fibra ottica o in rame:

Consultare *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente* per informazioni su installazione e rimozione di un socket SFP e un elenco dei ricetrasmettitori SFP disponibili.

Scheda di memoria SD

Scheda di memoria SD BMXRMS004GPF

La scheda di memoria BMXRMS004GPF è da 4 GB, classe 6 per uso industriale. Lo slot della scheda di memoria SD si trova dietro lo sportello sulla parte anteriore del controller.

È possibile utilizzare una scheda di memoria BMXRMS004GPF per archiviazione dati e applicazione.

È possibile utilizzare una scheda di memoria BMXRMS004GPF per l'archiviazione di:

- applicazione progetto M580 Safety.
- dati per task non sicuri (MAST, FAST, AUX0, AUX1).

NOTA:

- Non è possibile memorizzare i dati sulla scheda di memoria SD per il task SAFE.
- La scheda di memoria SD non è inclusa nel loop di sicurezza.

È possibile inserire ed estrarre la scheda con alimentazione inserita e il controller in modalità RUN. Tuttavia, per evitare perdite di dati, utilizzare il bit di sistema %S65 per eseguire una richiesta al sistema di arresto dell'accesso dati alla scheda prima di estrarla dal controller.

NOTA: Altre schede di memoria, incluse quelle utilizzate nei controller M340, non sono compatibili con i controller M580. Se si inserisce un scheda di memoria SD non compatibile nel controller:

- Il controller rimane nello stato NOCONF (vedere Modicon M580, Hardware, Manuale di riferimento).
- Il LED **BKP** del controller si illumina.
- Il LED di accesso alla scheda di memoria lampeggia.

La scheda di memoria BMXRMS004GPF è formattata specificamente per il controller M580. Se si utilizza questa scheda con un altro controller o strumento, la scheda potrebbe non essere riconosciuta.

Caratteristiche della scheda di memoria

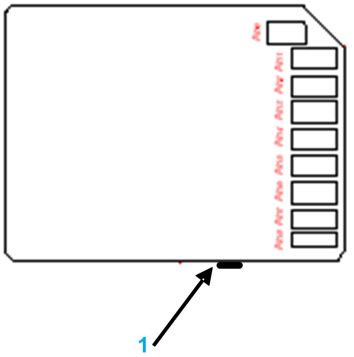
La scheda di memoria BMXRMS004GPF presenta le seguenti caratteristiche:

Caratteristica	**Valore**
dimensioni totali della memoria	4 GB
dimensioni per il backup dell'applicazione	200 MB
dimensioni per i dati	3,8 GB
cicli di scrittura/cancellazione (standard)	100.000
intervallo di temperatura di esercizio	-40...+85 °C (-40...+185 °F)
tempo di conservazione file	10 anni
area di memoria per l'accesso all'FTP	solo directory di memorizzazione dati

NOTA: A causa di formattazione, usura e altri meccanismi interni, la capacità effettivamente disponibile della scheda di memoria è leggermente inferiore alle sue dimensioni globali.

Selettore di lettura/scrittura della scheda

La scheda di memoria BMXRMS004GPF dispone di un selettore di accesso a lettura/scrittura lungo il lato senza smusso, utilizzabile per proteggere la scheda dall'accesso in scrittura non consentito:



1 Selettore di accesso lettura/scrittura

Formattazione della scheda di memoria

La procedura di formattazione è descritta nella sezione *Formattazione della scheda di memoria* in *EcoStruxure™ Control Expert Libreria dei blocchi di sistema*.

Sigilli anti-manomissione e sportello della scheda SD bloccabile

Sigilli anti-manomissione

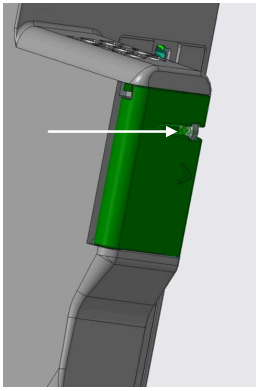
Sul lato destro delle CPU M580 standalone e Hot Standby sono presenti due sigilli anti-manomissione, dove il pannello frontale (ossia la sezione anteriore del contenitore del modulo) si collega all'alloggiamento (ossia la sezione posteriore del contenitore del modulo). Questi sigilli indicano se il modulo è stato aperto ed eventualmente manomesso.

Il contenitore del modulo non è stato aperto se i sigilli anti-manomissione hanno l'aspetto seguente:

Il contenitore del modulo è stato aperto se i sigilli anti-manomissione hanno l'aspetto seguente:

Sportello della scheda SD bloccabile

Lo sportello che copre lo slot della scheda SD può essere bloccato o sigillato.



Per questo scopo:

1. Chiudere lo sportello della scheda SD.

2. Inserire l'estremità di un sigillo in piombo (o il cavo di un lucchetto) attraverso il foro nella parte sporgente attraverso lo sportello della scheda SD.

   NOTA: è possibile utilizzare un filo o un cavo con un diametro massimo di 1,50 mm (0.06 in.).

3. Chiudere il sigillo in piombo (o chiudere il lucchetto).

NOTA: il sigillo o il lucchetto non sono forniti con il modulo.

Caratteristiche della prestazioni di coprocessore e CPU M580 Safety

Introduzione

Questa sezione descrive le caratteristiche delle prestazioni della CPU BMEP584040S e del coprocessore BMEP58CPROS3 (Copro).

Caratteristiche delle prestazioni di coprocessore e CPU M580

CPU e copro Safety

La CPU BME•58•040S e il coprocessore (copro) BMEP58CPROS3 presentano le seguenti caratteristiche delle prestazioni in una soluzione di sicurezza SIL3 M580:

Caratteristica prestazioni		**BME**					
		P582040S	**P584040S**	**P586040S**	**H582040S**	**H584040S**	**H586040S**
Rack locali		4 (1 rack principale + fino a 3 rack di estensione)	8 (1 rack principale + fino a 7 rack di estensione)	8 (1 rack principale + fino a 7 rack di estensione)	1	1	1
Derivazioni RIO (max 2 rack/ derivazione: rack principale + rack di estensione)		8 derivazioni (fino a 2 rack per derivazione)	16 derivazioni (fino a 2 rack per derivazione)	31 derivazioni (fino a 2 rack per derivazione)	8 derivazioni (fino a 2 rack per derivazione)	16 derivazioni (fino a 2 rack per derivazione)	31 derivazioni (fino a 2 rack per derivazione)
Canali I/O	I/O digitali	2048	4096	6144	0[1]	0[1]	0[1]
	I/O analogici	512	1024	1536	0[1]	0[1]	0[1]
	Expert	72	144	216	0[1]	0[1]	0[1]
Porte Ethernet	Backplane	1	1	1	1	1	1
	Service	1	1	1	1	1	1
	RIO	2	2	2	2	2	2
Rete di controllo	Max n. di moduli/ dispositivi	64	128	128	64	128	128

Caratteristica prestazioni		BME					
		P582040S	P584040S	P586040S	H582040S	H584040S	H586040S
	Max capacità ingresso	16 KB	24 KB	24 KB	16 KB	24 KB	24 KB
	Max capacità uscita	16 KB	24 KB	24 KB	16 KB	24 KB	24 KB
	Max capacità ingresso FAST	3 KB	5 KB	5 KB	3 KB	5 KB	5 KB
	Max capacità uscita FAST	3 KB	5 KB	5 KB	3 KB	5 KB	5 KB
Rete apparecchiatura distribuita	Max n. di moduli/ dispositivi	61	61	61	61	61	61
	Max capacità ingresso	2 KB	8 KB	8 KB	2 KB	2 KB	2 KB
	Max capacità uscita	2 KB	8 KB	8 KB	2 KB	2 KB	2 KB
	Max dispositivi CIP Safety	16	64	128	–	–	–
	Max connessioni CIP Safety	32	128	256	–	–	–
Moduli com Ethernet su rack locale	Max moduli com Eth	2	4	4	2	4	4
	Max BMENOC0301/ 0311	2	3	3	2	3	3
	Max BMENOC0321	2	2	2	2	2	2
Allocazione memoria (max)	Programma applicazione non sicuro	8 MB	16 MB	64 MB[4]	8 MB	16 MB	64 MB[4]
	Programma applicazione sicuro	2 MB	4 MB	16 MB[4]	2 MB	4 MB	16 MB[4]
	Dati non sicuri	768 KB	2048 KB	fino a 65536 KB[4]	768 KB	2048 KB	fino a 65536 KB[4]
	Max dati ritenuti configurabili	768 KB	2048 KB	4096 KB	768 KB	2048 KB	4096 KB
	Max dati trasferimento ridondanti configurabili	–	–	–	768 KB	2048 KB	4096 KB[5]
	Dati sicuri (dati non ritenuti)	512 KB	1024 KB	1024 KB[4]	512 KB	1024 KB	1024 KB[4]
	Max dati trasferimento ridondanti sicuri configurabili	–	–	–	512 KB	1024 KB	1024 KB[5]
	Condiviso: Globale -> Sicuro	16 KB	16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]

Caratteristica prestazioni		BME					
		P582040S	P584040S	P586040S	H582040S	H584040S	H586040S
	Condiviso: Sicuro -> Globale	16 KB	16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Condiviso: Globale -> Processo	16 KB	16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Condiviso: Processo -> Globale	16 KB	16 KB	16 KB	16 KB[2]	16 KB[2]	16 KB[2]
	Archiviazione dati totale	4 GB[6]	4 GB[6]	4 GB[6]	4 GB[6]	4 GB[6]	4 GB[6]
Velocità di esecuzione istruzioni	Task MAST e FAST:						
	Booleano	40K istruzioni / ms	40K istruzioni / ms	50K istruzioni / ms	40K istruzioni / ms	40K istruzioni / ms	50K istruzioni / ms
	Specificato	30K istruzioni / ms	30K istruzioni / ms	40K istruzioni / ms	30K istruzioni / ms	30K istruzioni / ms	40K istruzioni / ms
	Task SAFE:						
	Booleano	40K istruzioni / ms	40K istruzioni / ms	40K istruzioni / ms	40K istruzioni / ms[3]	40K istruzioni / ms[3]	40K istruzioni / ms[3]
	Specificato	30K istruzioni / ms	30K istruzioni / ms	30K istruzioni / ms	30K istruzioni / ms[3]	30K istruzioni / ms[3]	30K istruzioni / ms[3]

1. Per i PAC Hot Standby M580 di sicurezza, nel rack locale non sono supportati moduli di I/O.

2. Questi dati sono inclusi nelle aree dati sicure e non sicure.

3. Poiché il task SAFE scambia dati attraverso il backplane, c'è un impatto negativo sulle prestazioni. Ci vuole 1 ms per trasferire 10 KB per BMEH584040S e BMEH586040S e 2 ms per BMEH582040S.

4. Programma applicativo (non sicuro) + Dati applicazione (solo dati non sicuri non ritentivi) + Programma applicativo (sicuro) + Dati applicazione (sicuri) è inferiore a 64MB. Vi è una memoria globale di 64 Mbyte sulla CPU BME•586040S per il programma applicativo e i dati dell'applicazione.

5. Max per trasferimento dati (non sicuri + sicuri) per dati ridondanti è 4MB.

6. 2 GB senza scheda di memoria esterna.

Alimentatori M580 Safety

Introduzione

Questo capitolo descrive gli alimentatori del modulo M580 Safety.

Descrizione fisica degli alimentatori M580 Safety

Utilizzare in un loop M580 Safety

Utilizzare solo l'alimentatore di sicurezza BMXCPS4002S, BMXCPS4022S o BMXCPS3522S in un rack contenente moduli di sicurezza. È possibile utilizzare l'alimentatore di sicurezza in un rack X Bus o Ethernet che sia:

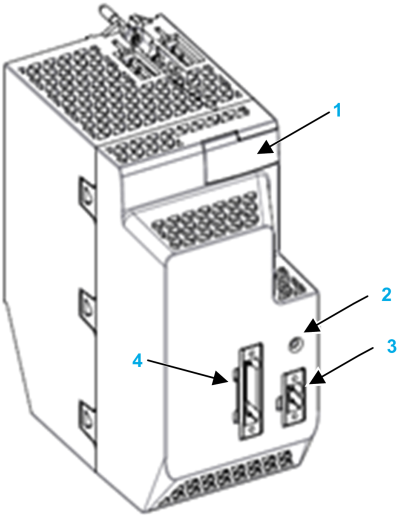
- un rack locale principale
- un rack locale di estensione
- un rack remoto principale
- un rack remoto di estensione

È possibile utilizzare due moduli di alimentazione di sicurezza nei rack Ethernet che supportano la ridondanza. L'alimentatore di sicurezza richiede due slot del modulo ed è posizionato all'estrema sinistra nel rack.

NOTA: Per una descrizione dei rack M580 disponibili, consultare l'argomento *Rack locali e remoti* nel *Modicon M580 - Manuale di riferimento Hardware*.

Pannello frontale alimentatore

Gli alimentatori M580 Safety presentano il seguente pannello frontale:



1 Pannello di visualizzazione a LED

2 Pulsante RESET

3 Contatto relé allarme

4 Connettore 5 pin alimentazione ingresso principale

Array LED

I moduli di alimentazione M580 Safety presentano il seguente pannello LED:

Il pannello LED include i seguenti indicatori LED:

- **OK**: stato di funzionamento
- **ACT**: attività
- **RD**: ridondanza

Ogni LED ha due stati: Acceso (verde) e spento.

Vedere la sezione *Diagnostica LED alimentatore* (vedere Modicon M580, Manuale di sicurezza) nel *Manuale M580 Safety* per informazioni su come utilizzare questi LED per diagnosticare lo stato dell'alimentatore.

RESET

La pressione del pulsante **RESET** sull'alimentatore determina la reinizializzazione di tutti i moduli nello stesso rack dell'alimentatore. Se il modulo di alimentazione M580 Safety è nel rack locale principale, premendo il pulsante **RESET** si reinizializza la CPU.

NOTA: In un design ridondante, con due moduli di alimentazione M580 Safety, è possibile premere il pulsante RESET su uno o entrambi i moduli di alimentazione per eseguire la funzione di reset.

Collegamenti alimentazione ingresso

Per ciascun alimentatore M580 Safety, sono valide le caratteristiche seguenti:

- 5 punti

- Tipo spina rimovibile:
  - sul modulo: testa con flangia filettata
  - morsettiera con flangia per vite
- Passo: 5,08 mm
- Capacita min filo: 0,5 mm^2...2,0 mm^2

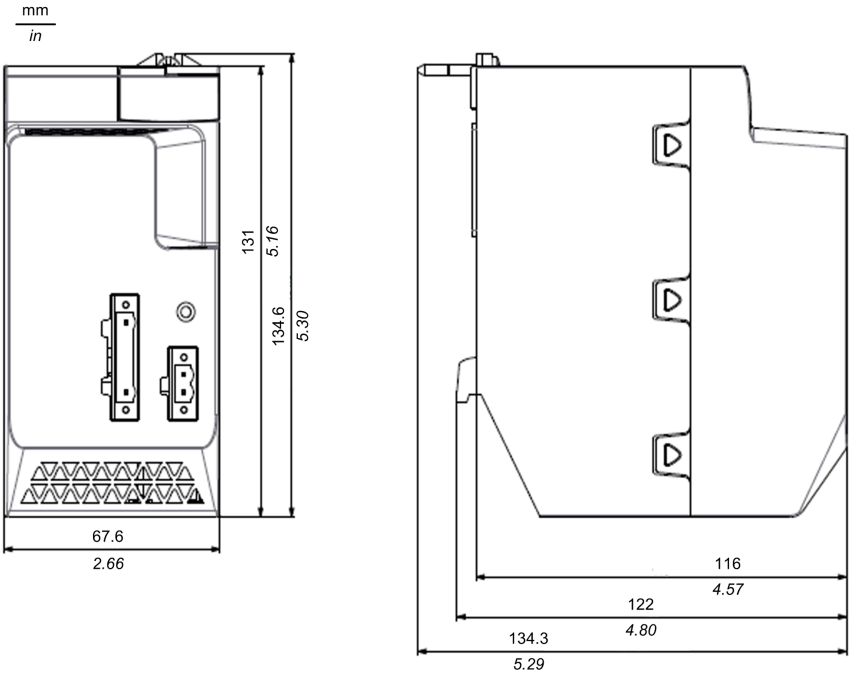
Le assegnazioni dei pin e l'alimentazione di ingresso per ciascun alimentatore M580 Safety sono le seguenti:

Descrizione	**BMXCPS4002S**	**BMXCPS4022S**	**BMXCPS3522S**
Alimentazione ingresso principale	100...240 Vca	24...48 Vcc	125 Vcc
Pin 1	NC	Linea CC	NC
Pin2	NC	Linea CC	NC
Pin3	PE	Neutro CC	PE
Pin4	Neutro CA	Neutro CC	Neutro CC
Pin5	Linea CA	Terra	Linea CC

NOTA: Una morsettiera è fornita con il modulo nei materiali di spedizione.

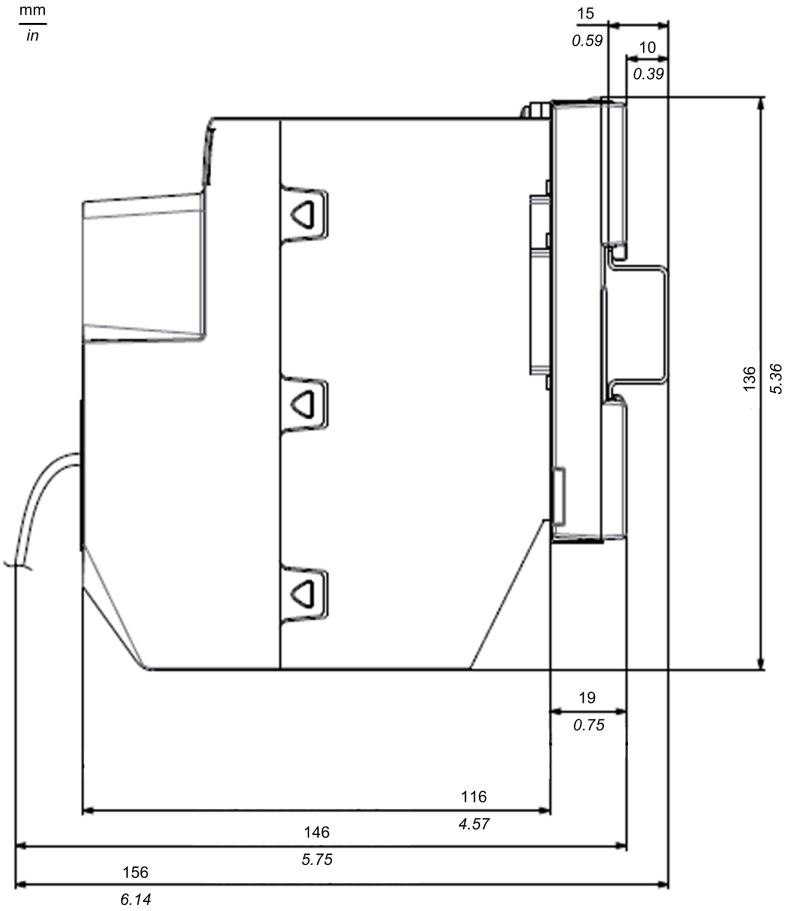
Dimensioni alimentatore

Gli alimentatori M580 Safety presentano le dimensioni seguenti:



Dimensioni cablaggio alimentatore

L'alimentatore di sicurezza M580 presenta le seguenti dimensioni tenendo in considerazione il cablaggio:



Caratteristiche prestazionali dell'alimentatore M580 Safety

Alimentatore BMXCPS4002S Safety

L'alimentatore BMXCPS4002S Safety presenta le seguenti caratteristiche delle prestazioni:

Caratteristiche degli ingressi		
Tensione nominale		100...240Vrms
Campo di tensione		85...132Vrms 170...264Vrms
Campo di frequenza		47...63 Hz
Assenza di tensione di ingresso mascherata		Max 10ms a 100Vrms-15% e a 200Vrms-15%
Potenza apparente di ingresso tipica		130 VA
Corrente di ingresso tipica		1,1Arms a 115Vrms 0,55Arms a 230Vrms
Corrente di spunto a 25° al 1° avvio a 25°C	Picco	≤ 60 A a 24 Vcc ≤ 60 A a 48 Vcc
	I^2t (per valutazione fusibile esterno)	≤ X A^2s a 24 Vcc ≤ X A^2s a 48 Vcc
	It (per valutazione disgiuntore esterno)	≤ X As a 24 Vcc ≤ X As a 48 Vcc
Protezione integrata		Fusibile interno inaccessibile posto all'ingresso L

Caratteristiche delle uscite		
Corrente di uscita MAX 3V3_BAC		5,5A (18,2W)
Corrente di uscita MAX 24V_BAC		1,67A (40W)
Potenza di uscita totale MAX		40 W
Rilevamento	Sovraccarico	Sì - Disgiunzione
	Cortocircuito	Sì - Disgiunzione
	Sovratensione	Sì - Disgiunzione

Altre caratteristiche		
Dielettrico	Primario/Tutti i secondari	SELV/PELV
Intensità	Primario/Messa a terra	SELV/PELV
Resistenza d'isolamento	Primario/Tutti i secondari	100 MΩ
	Primario/Messa a terra	100 MΩ

Alimentatore BMXCPS4022S Safety

Caratteristiche degli ingressi		
Tipo tensione nominale		24...48 Vcc
Campo della tensione di ingresso		18...62,4 Vcc
Efficienza		max perdite ≤7W (efficienza ≥84,8%) a carico massimo continuo, sull'intero campo di tensione di ingresso e intervallo di temperatura
Corrente di ingresso nominale		1,9 A a 24 Vcc
		1,0 A a 48 Vcc
Corrente di spunto al primo avvio a 25°C	Corrente di picco	≤ 60 A a 24 Vcc
		≤ 60 A a 48 Vcc
	I^2t (per valore fusibile esterno)	≤ X A^2s a 24 Vcc
		≤ X A^2s a 48 Vcc
	It (per valore interruttore esterno)	≤ X As a 24 Vcc
		≤ X As a 48 Vcc
Assenza di tensione di ingresso mascherata		Qualsiasi mancanza di alimentazione di ingresso che dura al max:
		• 1 ms a pieno carico e tensione min di linea (ossia 19,2 Vcc)
		• 10 ms a pieno carico e tensione nominale di linea (ossia 24 o 48 Vcc)
		Non deve indurre alcun cambiamento nelle caratteristiche di uscita. Periodo tra interruzioni 1 sec.
Protezione ingressi		• Protezione dal rischio di incendio: da fusibile montato sulla scheda, non accessibile e non sostituibile dall'utente e posizionato su ingresso DC+. Il suo valore è selezionato in conformità con gli standard di sicurezza. Non si deve danneggiare durante i test di resistenza ai disturbi di linea, in nessuna circostanza.

Caratteristiche degli ingressi	
	• Protezione da polarità inversa di ingresso: un circuito integrato deve proteggere il modulo. I fusibili interni (e al limite esterni) non devono bruciare. L'alimentazione deve avviarsi correttamente al ripristino della polarità.

Caratteristiche delle uscite:	
Tensione nominale di uscita	24,35 V
Campo di tensione a stato fisso di uscita	23,3...24,7 V sull'intero campo di tensione di ingresso, sull'intervallo totale del carico di uscita e nell'intervallo globale di temperatura.
Disturbo e ondulazione di uscita	240 mV da picco a picco (misurata con un'ampiezza di banda ≥100 MHz, sui pin del connettore del modulo.
Campo corrente di uscita continua	• Massimo 1,63 A
	• Minimo 0 A
Capacità di corrente di uscita transitoria	1,9 A max per 500 ms, periodo min 20 sec.
Impedenza rispetto a frequenza di uscita	180 mΩ
Risposta tensione di uscita a carico transitorio a 24V_BAC	Per il seguente carico di uscita transitorio a 24V_BAC:
	• Variazione di carico I da limite corrente di uscita continua min a limite corrente di uscita transitoria max (e viceversa).
	• Tempo di transizione 4 µs – ampiezza impulso 500ms – periodo 20 sec.
	• La tensione di uscita transitoria a 24V_BAC deve rimanere nei limiti 23,0...25,0V e il tempo di risposta deve essere ≤ 50 ms.
	• Qualsiasi valore del carico capacitivo a 24V_BAC nei limiti specificati.
Protezione da sovraccarico uscita/corto circuito	• In caso di condizioni di sovraccarico o corto circuito a 24V_BAC (ossia, qualsiasi caso di livello, durata, temperatura, tensione di ingresso), la scheda deve essere protetta dai danni.
	• Il valore massimo globale della soglia di rilevamento sovraccarico (ossia, comprese tutte le tolleranze, deviazioni, ecc.) deve essere inferiore a Imax
	• Imax = 2 A.
Protezione da sovratensione	Disgiunzione dell'alimentazione per un aumento dell'uscita fino a raggiungere 30,0 Vcc ± 0,8 V.
Capacità di carico capacitivo esterno	Tutte le caratteristiche precedenti devono essere rispettate con il valore di carico capacitivo esterno seguente. Questa funzionalità deve essere considerata in particolare per rampe, stabilità del loop di regolazione e protezione/rilevamento sovraccarico.
	Valore capacitivo 11500 µF.

Alimentatore BMXCPS3522S Safety

Caratteristiche degli ingressi:		
Tipo tensione nominale		125 Vcc
Campo della tensione di ingresso		100...150 Vcc
Rendimento		max perdite ≤7W (efficienza ≥84,8%) a carico massimo continuo, sull'intero campo di tensione di ingresso e intervallo di temperatura
Corrente di ingresso nominale		0,6 A a 125 Vcc
Corrente di spunto al primo avvio a 25°C	Corrente di picco	≤ 60 A a 125 Vcc
	I^2t (per valore fusibile esterno)	≤ 0,15 A^2s a 125 Vcc
	It (per valore interruttore esterno)	≤ 0,025 As a 4 Vcc
Assenza di tensione di ingresso mascherata		Qualsiasi mancanza di alimentazione di ingresso che dura al max:
		• 1 ms a pieno carico e tensione min di linea (ossia 100 Vcc)
		• 10 ms a pieno carico e tensione nominale di linea (ossia 125 Vcc)
		Non deve indurre alcun cambiamento nelle caratteristiche di uscita. Periodo tra interruzioni 1 sec.
Protezione ingressi		• Protezione dal rischio di incendio: da fusibile montato sulla scheda, non accessibile e non sostituibile dall'utente e posizionato su ingresso DC +. Il suo valore è selezionato in conformità con gli standard di sicurezza. Non si deve danneggiare durante i test di resistenza ai disturbi di linea, in nessuna circostanza.
		• Protezione da polarità inversa di ingresso: un circuito integrato deve proteggere il modulo. I fusibili interni (e al limite esterni) non devono bruciare. L'alimentazione deve avviarsi correttamente al ripristino della polarità.

	BMXCPS3522 /S Alta potenza
Tensione nominale di uscita	24,35 V
Campo di tensione a stato fisso di uscita	23,3...24,7 V sull'intero campo di tensione di ingresso, sul campo totale del carico di uscita e nell'intervallo globale di temperatura.
Disturbo e ondulazione di uscita	240 mV da picco a picco (misurata con un'ampiezza di banda ≥100 MHz, sui pin del connettore del modulo.

	BMXCPS3522 /S Alta potenza
Campo corrente di uscita continua	• Massimo 1,63 A
	• Minimo 0 A
Capacità di corrente di uscita transitoria	1,9 A max per 500 ms, periodo min 20 sec.
Impedenza rispetto a frequenza di uscita	180 mΩ
Risposta tensione di uscita a carico transitorio a 24V_BAC	Per il seguente carico di uscita transitorio a 24V_BAC:
	• Variazione di carico I da limite corrente di uscita continua min a limite corrente di uscita transitoria max (e viceversa).
	• Tempo di transizione 4 µs – ampiezza impulso 500ms – periodo 20 sec.
	• La tensione di uscita transitoria a 24V_BAC deve rimanere nei limiti 23,0...25,0V e il tempo di risposta deve essere ≤ 50 ms.
	• Qualsiasi valore del carico capacitivo a 24V_BAC nei limiti specificati.
Protezione da sovraccarico uscita/corto circuito	• In caso di condizioni di sovraccarico o corto circuito a 24V_ BAC (ossia, qualsiasi caso di livello, durata, temperatura, tensione di ingresso), la scheda deve essere protetta dai danni.
	• Il valore massimo globale della soglia di rilevamento sovraccarico (ossia, comprese tutte le tolleranze, deviazioni, ecc.) deve essere inferiore a Imax
	• Imax = 2 A.
Protezione da sovratensione	Disgiunzione dell'alimentazione per un aumento dell'uscita fino a raggiungere 30,0 Vcc ± 0,8 V.
Capacità di carico capacitivo esterno	Tutte le caratteristiche precedenti devono essere rispettate con il valore di carico capacitivo esterno seguente. Questa funzionalità deve essere considerata in particolare per rampe, stabilità del loop di regolazione e protezione/rilevamento sovraccarico.
	Valore capacitivo 11500 µF.

Relé allarme alimentatore M580 Safety

Caratteristiche delle prestazioni

La morsettiera del relé allarme sugli alimentatori M580 Safety presenta le seguenti caratteristiche delle prestazioni:

Caratteristiche	
Corrente/Tensione di commutazione nominale	24 Vcc 2A (carico resistivo)
	240 Vca 2A (cos φ =1) punto
Carico di commutazione minimo	5 Vcc 1 mA
Tensione di commutazione massima	62,4 Vcc
	264 Vca
Tipo contatto	Normalmente aperto
Tempo contatto	
• OFF → ON	10 ms o meno
• ON → OFF	12 ms o meno
Protezione integrata	Contro sovraccarico/ corto circuiti: nessuna, occorre inserire un fusibile ad azione veloce.
	Da sovratensione induttiva in CA: nessuna, utilizzare un circuito RC o un soppressore MOV [ZNO] (appropriato per la tensione) in parallelo ai morsetti di ciascun preattuatore.
	Da sovratensione induttiva in CC: nessuna, applicare un diodo di scaricamento ai morsetti di ciascun preattuatore.
Forza dielettrica	Contatto rispetto a terra: 2000 Vrms, 50 Hz, 1 min.(Altitudine 0...2000 m)
Resistenza d'isolamento	10MΩ o più al di sotto di 500 Vcc

Moduli I/O M580 Safety

Introduzione

Questo capitolo descrive i moduli I/O M580 Safety.

Descrizione fisica dei moduli I/O M580 Safety

Introduzione

Questa sezione contiene la descrizione fisica comune dei moduli I/O di sicurezza M580.

Descrizione fisica dei moduli I/O M580

Posizionamento dei moduli I/O di sicurezza

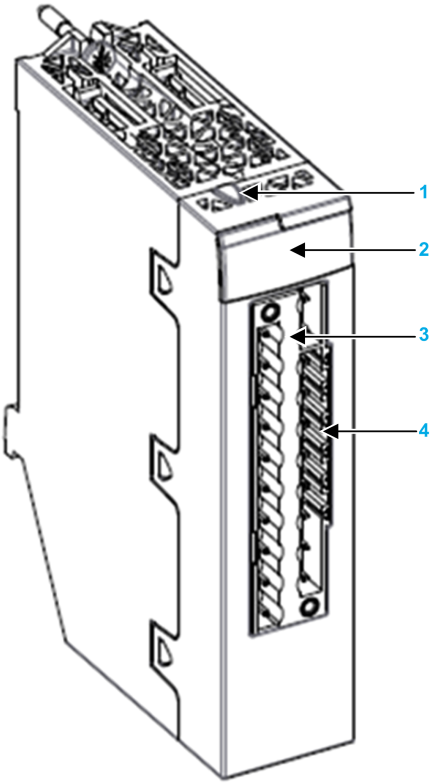
È possibile installare un modulo I/O M580 di sicurezza:

- nel rack locale, in qualsiasi slot non riservato per alimentatore o CPU.
- in un rack remoto, in qualsiasi slot non riservato per alimentatore o adattatore remoto.

NOTA: È possibile installare un modulo I/O di sicurezza in un rack X Bus BMXXBP•••• o in un rack Ethernet BMEXBP••••. Per una descrizione dei rack M580 disponibili, consultare l'argomento *Rack locali e remoti* nel *Modicon M580 - Manuale di riferimento Hardware*.

Pannello frontale del modulo I/O di sicurezza

Il pannello frontale di ciascun modulo I/O di sicurezza presenta le seguenti caratteristiche:



1 Pulsante di blocco/sblocco configurazione

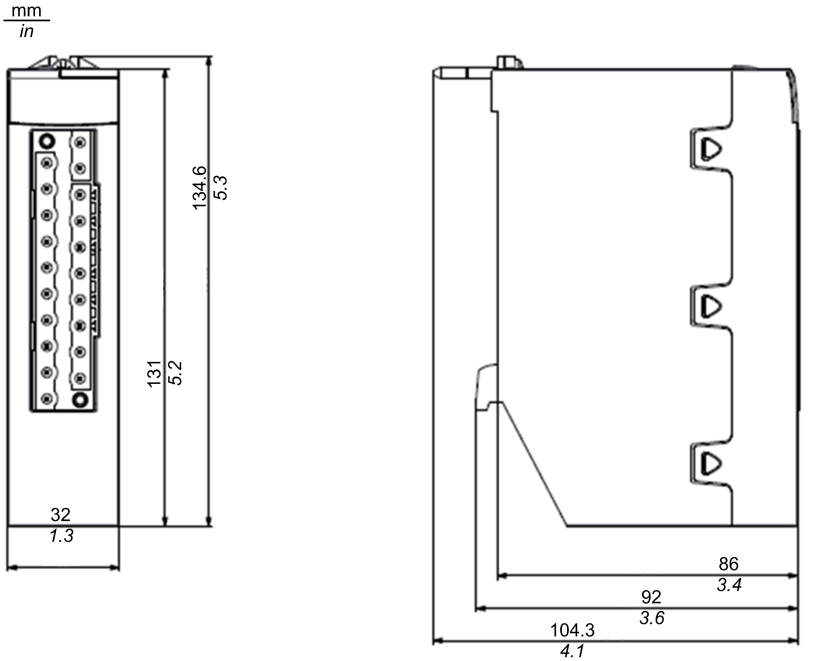
2 Pannello LED

3 Connettore a 20 pin

4 Slot pin codificati

Dimensioni del modulo I/O di sicurezza

Ciascun modulo I/O di sicurezza presenta le seguenti dimensioni fisiche:

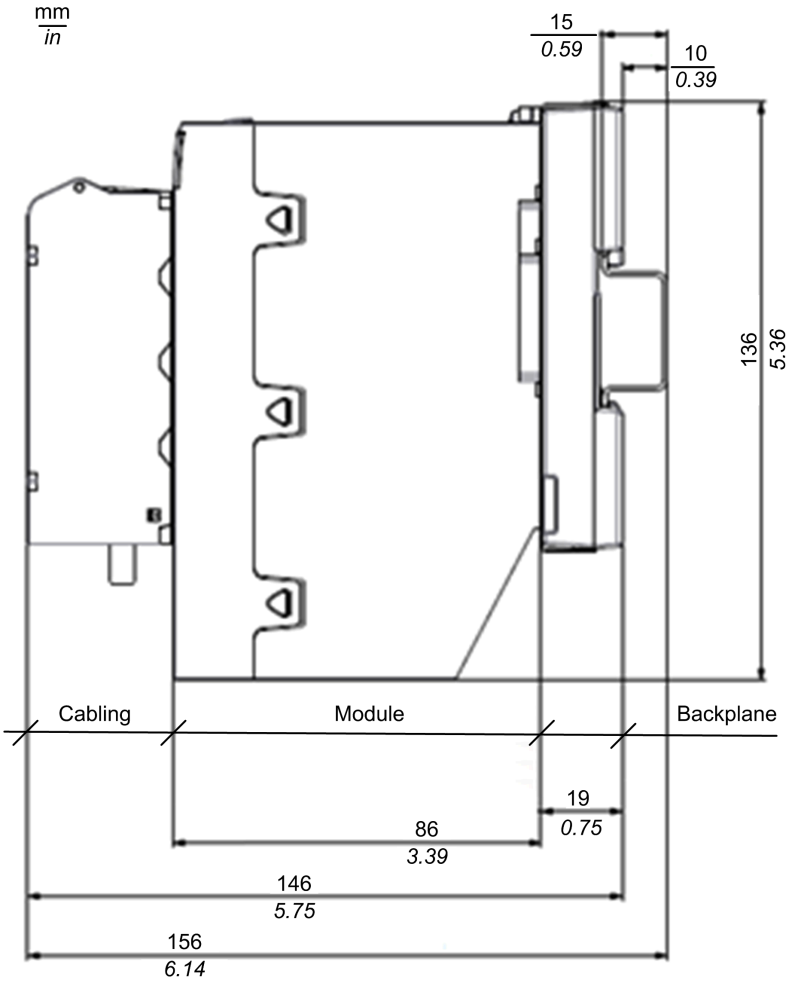


NOTA: Tenere presente l'altezza dei moduli I/O di sicurezza quando si pianifica l'installazione di un rack. Ogni modulo I/O di sicurezza si estende sotto il bordo inferiore del rack di:

- 29,49 mm (1,161 pollici) per un rack Ethernet
- 30,9 mm (1,217 pollici) per un rack X Bus

Dimensioni cablaggio I/O di sicurezza

Ciascun modulo I/O di sicurezza presenta le seguenti dimensioni di cablaggio:



LED

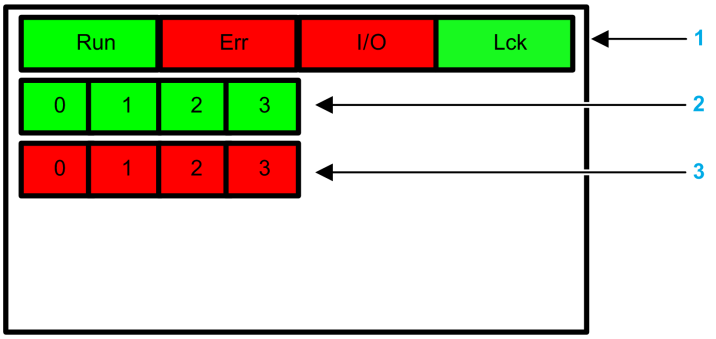
Ciascun modulo I/O di sicurezza fornisce diagnostica LED di modulo e canale sul lato anteriore del modulo:

- I quattro LED superiori (**Run**, **Err**, **I/O** e **Lck**) descrivono insieme lo stato del modulo.

- Le righe inferiori di LED si combinano con i quattro LED in alto per descrivere lo stato e la condizione di ciascun canale di ingresso e uscita.

  NOTA: Per informazioni su come utilizzare i LED del modulo per la diagnostica delle condizioni dei moduli M580 Safety, consultare il capitolo *Diagnostica* di *Manuale M580 Safety*.

LED del modulo di ingresso analogico BMXSAI0410 Safety e del modulo di uscita relé digitale BMXSRA0405 Safety:

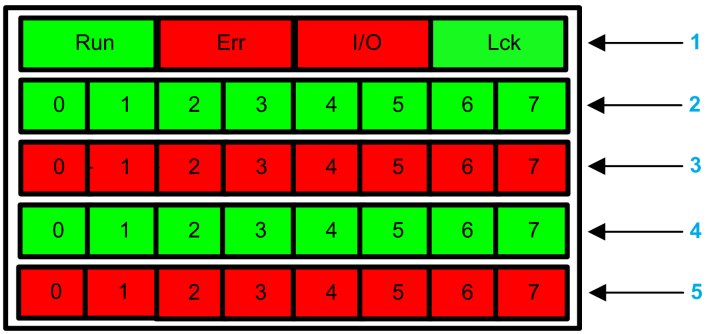


1 LED di stato del modulo

2 LED di stato canale

3 LED errore rilevato sul canale

LED del modulo di ingresso digitale BMXSDI1602 Safety:



1 LED di stato del modulo

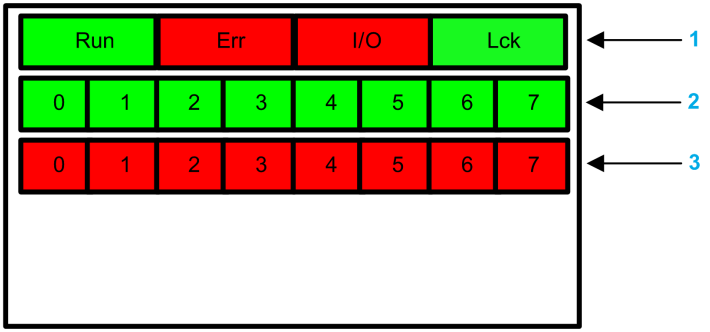
2 LED di stato canale Rango A

3 LED errore rilevato sul canale per Rango A

2 LED di stato canale Rango B

3 LED errore rilevato sul canale per Rango B

LED del modulo di uscita digitale BMXSDO0802 Safety:



1 LED di stato del modulo

2 LED di stato canale

3 LED errore rilevato sul canale

Caratteristiche delle prestazioni I/O M580 Safety

Introduzione

Questa sezione contiene descrive le caratteristiche delle prestazioni dei moduli I/O di sicurezza M580.

Caratteristiche prestazionali del modulo di ingresso analogico BMXSAI0410 Safety

Caratteristiche del modulo di ingresso analogico

Il modulo di ingresso analogico BMXSAI0410 Safety presenta le seguenti caratteristiche delle prestazioni:

Caratteristiche statiche		**Valore**
Impedenza di ingresso nel campo di segnale		286 Ω
Errore ingresso analogico	Errore max scala piena a 25°C	0,30%
Errore ingresso analogico (=tolleranza di sicurezza)	Campo di temperatura completo errore scala piena max da -25°C a 70°C	0,35%
Affidabilità	MTTF a 25°C	54,2 anni
Campo misurazione lineare		0 - 25 mA e 12.500 operazioni (500 ct/mA)
Rilevamento valori al di fuori dell'intervallo		< 3,75 mA e > 20,75 mA
Risoluzione digitale	Risoluzione	16 bit
	Numero di canali convertiti contemporaneamente	4
Formato dati restituito del programma applicativo		binario
Valore di un LSB		0,191 µA
Sovraccarico massimo permanente consentito		25 mA
Valore uscita digitale in condizione di sovraccarico	il sovraccarico viene segnalato all'applicazione client	I = 25 mA

Caratteristiche statiche		Valore
Tipo di ingresso	tipo	4 - 20 mA
	tipo	ingressi isolati mobili
	Campo massimo per ingresso	0-25 mA
Caratteristiche modalità comune	rifiuto modalità comune	da misurare

Caratteristiche dinamiche		Valore
caratteristiche filtro ingresso	ordine	secondo
	Taglio frequenza a -3dB	10,47 Hz

Caratteristiche generali		Valore
Metodo di conversione		approssimazione successiva
Tipo di protezione		diodo di protezione
Potenziale di isolamento nella normale operazione	Isolamento tra canali	500 VCA eff per 1 min.
	Isolamento da canale a backplane	1500 VCA eff per 1 min.
Dati alimentazione esterna - se richiesto		non richiesto
Tipo e lunghezza del cavo - regole di installazione per fornire immunità dalle interferenze		cavo schermato
Taratura o verifica per il mantenimento della precisione nominale		Nessuna taratura
Esempi tipici di connessioni esterne		sensore di temperatura e sensore di pressione

Caratteristiche diverse		Valore
Monotonicità con codice non mancante		si
Crosstalk tra c.c. e c.a. 50 Hz e CA 60Hz		–
Non linearità	+/-	0,006% (LSB)
Ripetibilità a temperatura fissa dopo il tempo di stabilizzazione specificato		–
Consumo 3,3 V	Tipico	223 mA
	Max.	256 mA
Consumo 24V	Tipico	92 mA
	Max.	115 mA
Dissipazione di potenza	Max.	3,98 W

Caratteristiche prestazionali del modulo di ingresso digitale BMXSDI1602 Safety

Caratteristiche del modulo di ingresso digitale

Il modulo di ingresso BMXSDI1602 Safety presenta le seguenti caratteristiche delle prestazioni:

Caratteristica		**Valore**
Ingresso nominale	Tensione	24 V CC
Tipo alimentazione sensore esterno	SELV/PELV, sovratensione II	(Max 60 V)
Corrente di ingresso tipica	Corrente	3,2 mA
Valori limite ingresso	Tensione allo stato 1	≥ 11 V
	Tensione allo stato 0	≤ 5 V
	Corrente allo stato 1	> 2 mA per U ≥ 11 V
	Corrente allo stato 0	< 1,5 mA
	Alimentazione sensore (Oscillazione inclusa)	Da 19 a 30 V (Possibile fino a 33. Limitata 1 ora al giorno)
Impedenza di ingresso	A Unom	7,5 KΩ
Tempo di risposta	Tipico//Massimo	100 µs/ 250 µs
Affidabilità	MTTF a Tamb = 25 °C	31,5 anni
Polarità inversa		Protetto
IEC61131-2 - Edizione 3.0 (2007)		Tipo 3
Compatibilità	(2 fili, 3 fili pross. Sensori)	IEC 947-5-2
Rigidità dielettrica	Primari/secondario	1500 VRMS (a 4000 m) 50/60 Hz per 1 min
Resistenza d'isolamento		> 10 Mµ (a 500 VCC)
Tipo di ingresso		Sink di corrente
Messa in parallelo ingressi(1)		Sì
Tensione sensore Soglia di monitoraggio	OK	> 18,6 VCC < 32 VCC
	Fuori campo operativo	< 18,6 VCC > 33 VCC

Caratteristica		Valore
Tempo di risposta di monitoraggio tensione sensore	Alla scomparsa	4,4 ms < T < 30 ms
	Alla comparsa	0,18 ms < T < 0,3 ms
Capacità esterna massima quando si utilizza VS per corto circuito per rilevamento 24 V	Max.	80 nF
Consumo 3,3 V	Tipico	200 mA
	Max.	256 mA
Consumo 24V	Tipico	63 mA
	Max.	100 mA
Potenza dissipata max.		3,57 W
(1) Questa caratteristica consente di collegare diversi ingressi sullo stesso modulo o su moduli diversi se sono richiesti ingressi ridondanti.		

Caratteristiche prestazionali del modulo di uscita digitale BMXSDO0802 Safety

Caratteristiche del modulo di uscita digitale

Il modulo di uscita digitale BMXSDO0802 Safety presenta le seguenti caratteristiche delle prestazioni:

Caratteristica		Valore
Valori nominali	Tensione	24 VCC
	Corrente	0,5 A
Valori limite	Tensione	19...30 V(1)
	Corrente/Canale	0,625 A
	Corrente/Modulo	5 A
Tipo di alimentazione attuatore esterno		SELV/PELV (max 60 V), Categoria sovratensione II
Potenza lampada a filamento di tungsteno	max.	6 W
Corrente di dispersione	Allo stato 0	< 0.5 mA
Tensione residua	Allo stato 1	< 1,2 V

Caratteristica		**Valore**
Protezioni	Tensione transitoria	si
	Corrente di disgiunzione sovraccarico	> 0,625 A
	Cortocircuito	si
	Polarità errata	si
	Temperatura eccessiva	si
Carico minimo. Valore resistenza (per preattuatore)		48 Ω
Rilevamento completo di TAGLIO filo: valore di capacità di carico cavo max (compresa capacità preattuatore) tra uscita e preattuatore		10 nF
Tempo di risposta(2)		1,2 ms
Affidabilità: MTTF		45,8 anni a 25 °C
Frequenza di commutazione su carico induttivo		0,5 / LI²Hz con Fmax =2 Hz
Messa in parallelo delle uscite		Sì (2 max)
Compatibilità con ingressi DC		Sì (solo tipo sink 3 o sink non IEC)
Protezione integrata	Contro sovratensione	Sì - con TVS interno
	Contro l'inversione di polarità	Sì - con diodo inverso Fornire un fusibile al preattuatore 24 V.
	Contro cortocircuiti e sovraccarichi	Sì - con limitatore di corrente e disgiuntore elettronico 1,5 In < Id < 2 In
Tensione preattuatore 24 V Soglia di monitoraggio	OK	> 19,0 V e < 31,8 V
	Fuori campo operativo	< 18,0 V e > 31,8 V
Tempo di risposta di monitoraggio tensione preattuatore	Alla scomparsa	2 ms < T < 5,6 ms
	Alla comparsa	10 ms < T < 15,6 ms
Consumo 3,3 V	Tipico	240 mA
	Max.	264 mA
Consumo 24 V backplane	Tipico	80 mA
	Max.	90 mA
Consumo 24 V preattuatore (senza corrente di carico)	Tipico	5 mA
	Max.	15 mA
Dissipazione energia		4,4 W max

Caratteristica	Valore
Forza dielettrica (uscita/terra o logica interna)	1500 V rms e 50/60 Hz per 1 min
Resistenza d'isolamento	> 10 MΩ a 500 VCC
(1) 33 V consentiti per 1 ora ogni 24h. **(2)** Tutte le uscite sono dotate di circuiti di smagnetizzazione veloci per gli elettromagneti. Tempo di scarica elettromagnete < L/R.	

Modulo di uscita relé digitale BMXSRA0405 Safety

Caratteristiche del modulo di uscita relé digitale

Il modulo di uscita relé digitale di sicurezza BMXSRA0405 presenta le seguenti caratteristiche delle prestazioni:

Caratteristica		Valore
Commutazione nominale		24 VDC 5A (carico resistivo)
Tensione / Corrente		240 VCA 5A (cos Φ =1)
Corrente max. per contatti su carico resistivo		5A (CC12 e CA12)
Corrente max. per contatti su carico induttivo		4A DC13 e 3A AC15
Temperatura di funzionamento		Da -0 ° a + 60 °C
Tipo di alimentazione attuatore esterno		Categoria sovratensione II
Carico commutazione min		5 VDC 10 mA
Carico commutazione max		264 VAC 30 VDC
Tempo di commutazione	OFF→ ON (operazione)	12 ms tipico
	ON →OFF (rilascio)	6 ms tipico
Durata (in base a relé Elesta SIF3)	Specifiche meccaniche	10 milioni di cicli o più
	Specifiche elettriche	DC12 24Vdc / 5A → 300.000 cicli
		DC12 24Vdc / 2A →500.000 cicli
		DC12 24Vdc / 1A→1.000.000 cicli
	L/R = 40 ms	DC13 24Vdc (0.1Hz) / 4A→30.000 ciclic
		DC13 24Vdc (0.1Hz) / 2A→50.000 cicli
		DC13 24Vdc (0.1Hz) / 1A→80.000 cicli

Caratteristica		**Valore**
	–	AC12 250Vac / 5A→70.000 cicli
		AC12 250Vac / 2A→30.000 cicli
		AC12 250Vac / 1A→250.000 cicli
	–	AC15 250Vac / 3A→40.000 cicli
		AC15 250Vac / 2A→80.000 cicli
		AC15 250Vac / 1A→80.000 cicli
Protezione integrata	Da sovraccarichi e cortocircuiti	Nessuna - un fusibile ad azione veloce deve essere inserito in ciascun canale o gruppo di canali.
	Da sovratensioni induttive in ~	Nessuna - un circuito RC o limitatore di picco MOV (ZNO) idoneo per la tensione deve essere inserito in parallelo tra i terminali di ogni preattuatore.
	Da sovratensioni induttive in =	Nessuna - un diodo a scarica deve essere inserito tra i terminali di ciascun preattuatore.
Frequenza di commutazione max		5 cicli al secondo
Tensione dielettrica max tra canali		3000 V rms 50/60Hz per 1 min
Tensione dielettrica max tra canali e backplane		3000 V rms 50/60Hz per 1 min
Standard di isolamento rinforzato		Isolamento 3000 Vca tra lato processo (contatto relé) e il backplane
Resistenza d'isolamento		>10MW o più per tester di resistenza di isolamento
Affidabilità: MTTF a Tamb = 25°C		36,9 anni
Grado di protezione		IP20
Consumo 3,3V	Tipico	215 mA
	Massimo	240 mA
Consumo corrente interna relé 24V	Tipico	95 mA
	Massimo	130 mA
Dissipazione energia	4 relé alimentati	3 W tipica, 3,9 W massima

Installazione del PAC M580 Safety

Panoramica

Questo capitolo spiega come installare il PAC M580 Safety.

NOTA: Per ulteriori informazioni su come installare i PAC M580, consultare l'argomento *Installazione di un rackl locale* nel *Modicon M580 - Manuale di riferimento hardware*.

Installazione di moduli di estensione e rack M580

Introduzione

Questa sezione descrive come installare un rack M580 e moduli di estensione per un PAC di sicurezza M580.

Pianificazione dell'installazione del rack locale

Introduzione

Le dimensioni, il numero di rack e i tipi di moduli installati sono aspetti importanti da prendere in considerazione quando si pianifica un'installazione. L'installazione può avvenire in un cabinet o fuori da un cabinet. Devono essere note l'altezza, la larghezza e la profondità del modulo di testa del sistema installato nonché la distanza tra il rack locale e il rack di estensione.

⚠ AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Installare i rack nel senso della lunghezza e in orizzontale per facilitare la ventilazione.

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

I moduli come l'alimentatore, la CPU e i moduli di I/O vengono raffreddati per convezione naturale. Montarli su un rack installato in orizzontale, come illustrato in questo manuale per garantire il raffreddamento termico necessario. In posizioni diverse da quelle indicate si può verificare surriscaldamento e funzionamento anomalo delle apparecchiature.

Uso del rack

I rack disponibili in Control Expert e il loro utilizzo consentito sono descritti di seguito:

Codice prodotto	Slot	Bus	Uso			
			Rack principale locale	Rack di estensione locale	Rack principale remoto	Rack di estensione remoto
Rack BME:						
BME XBP 0400	4	XBus ed Ethernet	x	x	x	x
BME XBP 0800	8	XBus ed Ethernet	x	x	x	x
BME XBP 1200	12	XBus ed Ethernet	x	x	x	x
BME XBP 1600	16	XBus ed Ethernet	x	x	x	x
BME XBP 0602	6	XBus ed Ethernet	x	x	x	x
BME XBP 1002	10	XBus ed Ethernet	x	x	x	x
BME XBP 1402	14	XBus ed Ethernet	x	x	x	x
Rack BMX:						
BMX XBP 0400	4	Bus X	–	x	x	x
BMX XBP 0600	6	Bus X	–	x	x	x
BMX XBP 0800	8	Bus X	–	x	x	x
BMX XBP 1200	12	Bus X	–	x	x	x
BMX XBP 1600	16	Bus X	–	x	x	x
Rack Premium:						
NOTA: I rack Premium non sono supportati dai PAC di sicurezza M580.						
Rack Quantum:						
140 XBP 002 00	2	Quantum	–	–	x	x
140 XBP 003 00	3	Quantum	–	–	x	x
140 XBP 004 00	4	Quantum	–	–	x	x
140 XBP 006 00	6	Quantum	–	–	x	x
140 XBP 010 00	10	Quantum	–	–	x	x
140 XBP 016 00	16	Quantum	–	–	x	x
X: consentito – : non consentito						

Distanza intorno ai rack

Lasciare uno spazio minimo di 12 mm (0.472 in.) sul lato destro di ogni rack per consentire il raffreddamento.

Se sono necessari rack di estensione, lasciare uno spazio minimo di 35 mm (1,378 in.) davanti ai moduli. Il modulo di estensione del rack BMX XBE 1000 richiede uno spazio per il connettore e la terminazione del bus locale.

Requisiti di spazio per una CPU M580 in un rack principale locale

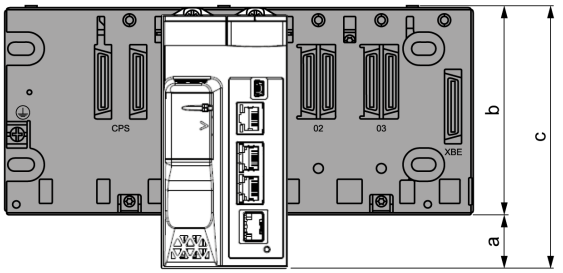
⚠AVVERTIMENTO

SURRISCALDAMENTO E FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

Rispettare le distanze adeguate per consentire il raffreddamento quando si installano i rack.

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

Nel rack locale principale, lasciare spazio aggiuntivo nella parte inferiore del rack per la CPU. L'illustrazione mostra le dimensioni di montaggio quando si utilizza un rack X Bus o un rack Ethernet. L'altezza totale del rack locale principale in entrambi i casi è di 134,6 mm (5,299 pollici).



a: spazio aggiuntivo sotto il rack adeguato all'altezza della CPU. Per un rack X Bus, il valore è 32,0 mm (1.260 in.); per un rack Ethernet, il valore è 30,59 mm (1.204 in.).

b L'altezza del rack. Per un rack X Bus, l'altezza è 103,7 mm (4.083 in.); per un rack Ethernet, l'altezza è 105,11 mm (4.138 in.).

c L'altezza del rack locale principale, 135,7 mm (5.343 in.).

Considerazioni sulla temperatura all'interno di un cabinet

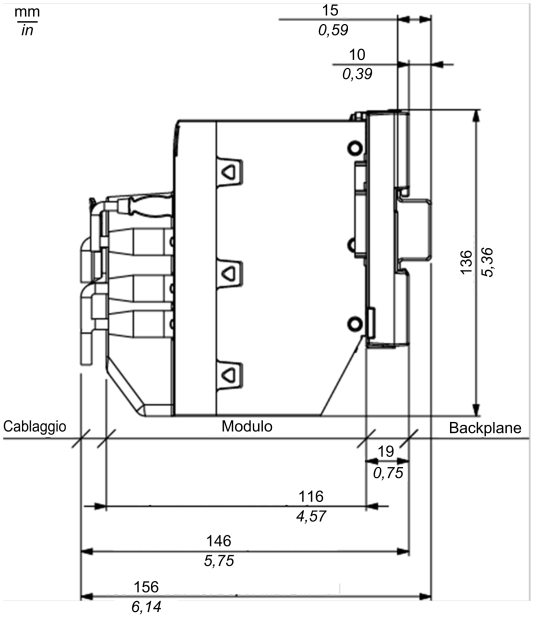
Se i rack sono installati in un cabinet, è necessario facilitare la circolazione dell'aria. Utilizzare un cabinet che consenta le seguenti distanze minime:

- 80 mm (3.15 in.) al di sopra dei moduli nel rack
- 60 mm (2.36 in.) al di sotto dei moduli sul rack
- 60 mm (2.36 in.) tra i moduli e le canaline passacavi

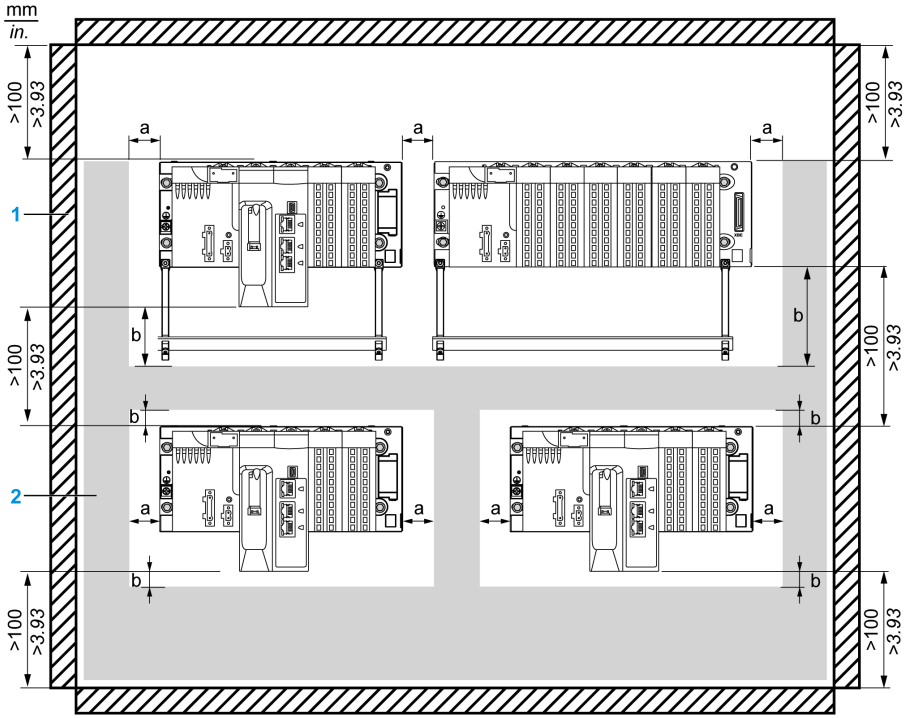
La profondità minima del cabinet è:

- 150 mm (5.91 in.) se il rack è fissato a una piastra
- 160 mm (6.30 in.) se il rack è montato su una guida DIN da 15 mm (0.59 in.)
- se i moduli di estensione del rack BMX XBE 1000 sono collegati, utilizzare cavi BMX XBC •••K con connettori angolati a 45°.

L'illustrazione mostra la vista laterale di un rack su una guida DIN con i moduli e i cavi montati in un cabinet:



La seguente illustrazione mostra le regole di un'installazione tipica in un cabinet con canaline:



1 installazione o intelaiatura

2 canalina di cablaggio o guida di instradamento cavi

a distanza laterale: > 40 mm (1.57 in.)

b distanza dall'alto e dal basso con oggetti circostanti: > 20 mm (0.79 in.)

NOTA: Per incrementare la densità, è accettabile una minore spaziatura fra i rack se:

- Non sono presenti barre di schermatura o canaline fra i rack.
- La spaziatura fra i rack non è inferiore a 40 mm (1,57 pollici)
- Si applica un declassamento di 5 °C (9 °F) alla massima temperatura ambiente consentita. Vale a dire, 55 °C (131 °F) per i moduli in versione standard e rivestiti e 65 °C (149 °F) per i moduli hardened (rinforzati).

Montaggio dei rack

Introduzione

I rack Ethernet e X Bus possono essere montati su:

- guide DIN
- pareti
- griglia di montaggio Telequick

NOTA: Montare i rack su una superficie metallica adeguatamente messa a terra per consentire al PAC di funzionare correttamente in presenza di interferenze elettromagnetiche.

NOTA: Le viti di montaggio situate sul lato sinistro del backplane sono accessibili senza disinserire il modulo di alimentazione. Montare il backplane utilizzando il foro di fissaggio più a sinistra sul pannello.

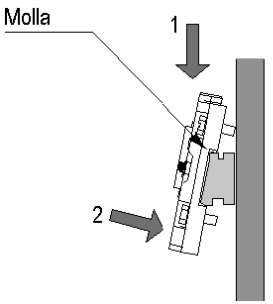
Montaggio su una guida DIN

La maggior parte dei rack può essere montata su guide DIN larghe 35 mm (1,38 pollici) e profonde 15 mm (0,59 pollici) .

NOTA: I rack più lunghi di 400 mm (15,75 pollici) che supportano più di 8 slot per moduli non possono essere montati su una guida DIN. Non montare un rack BMXXBP1200 (PV:02 o successiva)(H), BMEXBP1002(H) o BMEXBP1200(H) su una guida DIN.

NOTA: Se viene montato su una guida DIN, il sistema è maggiormente soggetto a sollecitazioni meccaniche.

Montaggio di un rack su una guida DIN:

Passo	Azione	Illustrazione
1	Posizionare il rack sopra la guida DIN ed esercitare pressione sulla parte superiore in modo da comprimere le molle che sono in contatto con la guida DIN.	
2	Inclinare il rack all'indietro per portarlo a contatto con la guida DIN.	
3	Rilasciare il rack per bloccarlo.	

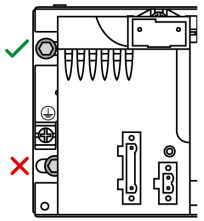
Per rimuovere un rack da una guida DIN:

Passo	Azione
1	Esercitare pressione sulla parte superiore in modo da comprimere le molle che sono in contatto con la guida DIN.
2	Inclinare il rack in avanti per sganciarlo dalla guida DIN.
3	Rimuovere il rack.

Montaggio su una parete

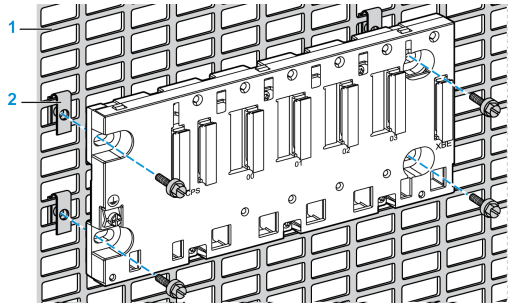
Il rack può essere montato su una parete all'interno o all'esterno di un cabinet inserendo delle viti M4M5, M6 o UNC #6 nei fori di fissaggio.

Collocare le 2 viti sul lato sinistro (accanto all'alimentatore) il più vicino possibile al bordo sinistro del rack. In questo modo, le viti restano accessibili dopo aver montato l'alimentatore.



Montaggio su griglia Telequick AM1-PA e griglie di montaggio AM3-PA

Un rack può essere montato su una griglia di montaggio TelequickAM1-PA o AM3-PA mediante delle viti M4M5, M6 o UNC #6.



Estensione di un rack

Introduzione

Quando l'installazione include più di un rack nel rack locale in una derivazione remota, installare un modulo di estensione rack BMXXBE1000 sul rack principale e sui rack estesi. I moduli di estensione del rack sono collegati tra di loro mediante cavi di estensione X Bus.

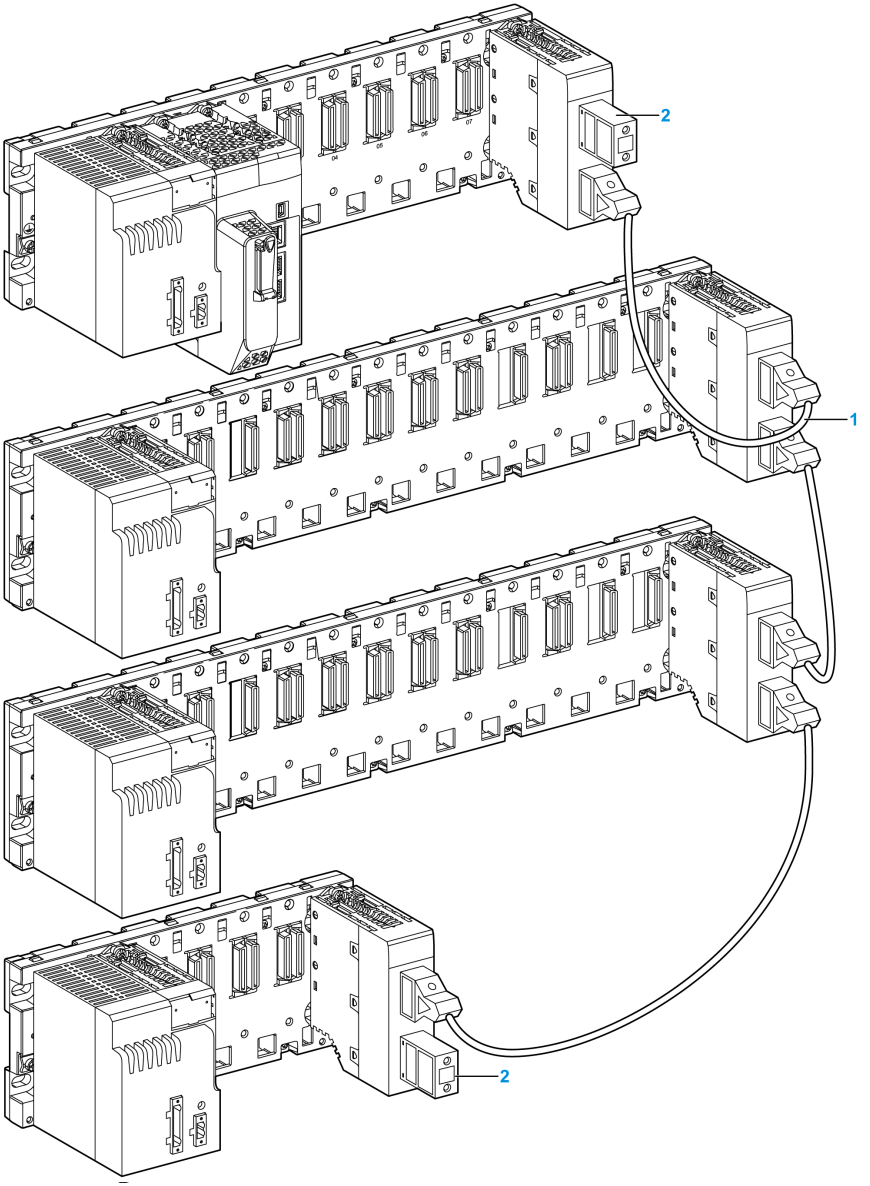
NOTA: Per informazioni su come installare e collegare moduli di estensione del rack, consultare l'argomento *Installazione dei moduli diestensione rack Modicon X80* nel *Modicon M580 - Manuale di riferimento hardware*.

Creazione di un sistema di sicurezza M580 mediante rack di estensione locali

Con cavi e moduli di estensione BMXXBE1000, è possibile aggiungere al PAC di sicurezza M580:

- fino a sette rack di estensine al rack principale locale.
- un rack di estensione a un rack principale remoto.

Esempio di rack principale locale Ethernet con rack di estensione e cavi e moduli di estensione:



1 Una stessa stazione può contenere rack di dimensioni diverse, che possono essere interconnessi mediante cavi di estensione.

2 I moduli di estensione situati alle estremità dei cavi interconnessi hanno una terminazione.

Installazione di CPU M580, copro, alimentatore e I/O

Introduzione

Questa sezione descrive come installare una CPU M580 Safety, coprocessore, alimentatore e moduli I/O.

Installazione di CPU e coprocessore

Introduzione

È possibile installare la CPU BME•58•040S e il coprocessore BMEP58CPROS3 solo in un rack BMEXBP••00 o BMEXBP••02 Ethernet.

Precauzioni per l'installazione

Una CPU M580 è alimentata dal bus del rack. Assicurarsi che l'alimentatore del rack sia spento prima di installare la CPU.

⚠⚠PERICOLO

RISCHIO DI SCOSSA ELETTRICA, ESPLOSIONE O ARCO ELETTRICO

- Mettere fuori tensione tutte le apparecchiature, inclusi i dispositivi collegati, prima di rimuovere qualunque coperchio o sportello, o prima di installare/disinstallare accessori, hardware, cavi o fili, tranne che per le condizioni specificate nell'apposta Guida hardware per questa apparecchiatura.
- Per verificare che l'alimentazione sia isolata, usare sempre un rilevatore di tensione correttamente tarato.
- Prima di riattivare l'alimentazione dell'unità rimontare e fissare tutti i coperchi, i componenti hardware e i cavi e verificare la presenza di un buon collegamento di terra.
- Quando si utilizza questa apparecchiatura e qualunque prodotto associato, usare esclusivamente la tensione specificata.

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

Rimuovere la copertura di protezione dai connettori dello slot del rack prima di inserire il modulo nel rack.

⚠ AVVERTIMENTO
FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA Verificare che il controller non contenga una scheda di memoria SD non supportata prima di accendere il controller. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

NOTA:

- Verificare che lo sportello dello slot della scheda di memoria sia chiuso dopo aver inserito una scheda di memoria nel controller.
- Fare riferimento a `%SW97` per controllare lo stato della scheda SD.

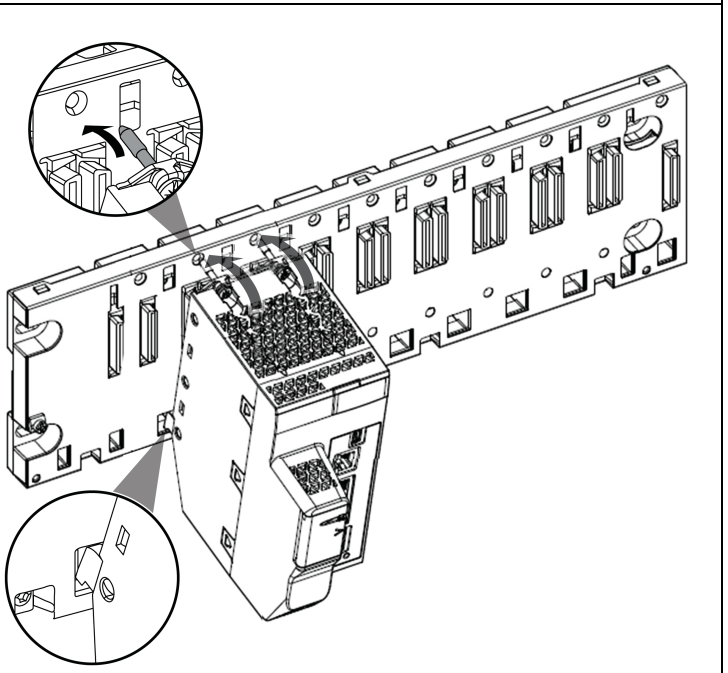
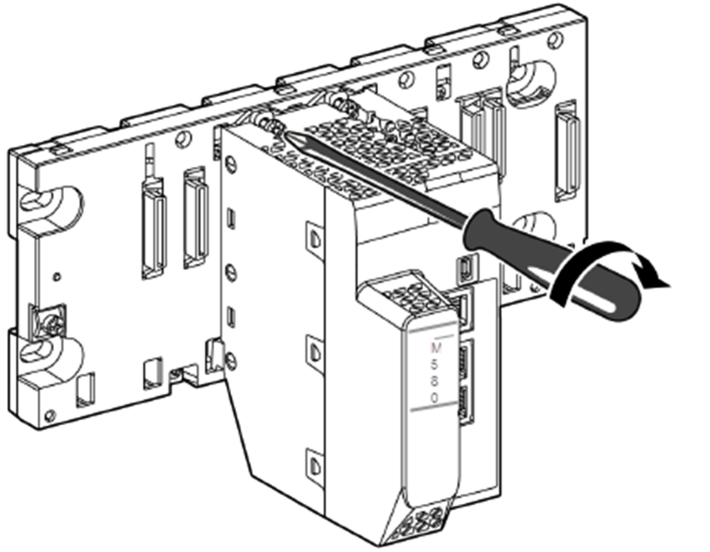
Installazione di CPU e coprocessore nel rack

Installare CPU e coprocessore nel rack nelle seguenti posizioni degli slot:

- CPU: slot **00** e **01**.
- Coprocessore: slot **02** e **03**

Seguire questi passaggi per installare una CPU e Coprocessore in un rack:

Passo	Azione
1	Assicurarsi che l'alimentatore sia spento.
2	Verificare quanto segue: • se si utilizza una scheda di memoria SD, che sia supportata dalla CPU. • che le coperture di protezione dei connettori siano state rimosse. • che la CPU sia collocata negli slot con marcatura **00** e **01**.

Passo	Azione	
3	Posizionare i pin di individuazione posti in basso nel retro del modulo negli slot corrispondenti sul rack.	
4	Ruotare il modulo verso la parte superiore del rack in modo che sia allineato alla parte posteriore del rack. A questo punto il modulo è in posizione.	
5	Serrare le 2 viti situate sulla parte superiore della CPU per mantenere il modulo in posizione nel rack. coppia di serraggio: 0,4...1,5 N m (0.30...1.10 lbf-ft).	
6	Per installare il modulo Copro, posizionarlo negli slot **02** e **03** e seguire i passaggi 3, 4 e 5 precedenti.	

Messa a terra

Rispettare la regolamentazione e tutte le norme locali e nazionali sulla sicurezza.

⚠⚠PERICOLO

PERICOLO DI SCOSSA ELETTRICA

Se non è possibile provare che il capo di un cavo schermato è collegato alla terra locale, il cavo deve essere considerato pericoloso e occorre indossare dispositivi di protezione individuale (DPI).

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

Per informazioni sulla messa a terra di CPU e coprocessore, vedere la sezione *Considerazioni sulla messa a terra* in *Modicon M580 - Manuale di riferimento hardware*.

Installazione di un modulo di alimentazione

Introduzione

Installare il modulo di alimentazione di sicurezza M580 in qualsiasi rack X Bus o Ethernet contenente altri moduli di sicurezza M580. Il modulo di alimentazione di sicurezza può essere utilizzato in rack che richiedono un alimentatore singolo o alimentatori ridondanti doppi.

⚠AVVERTIMENTO

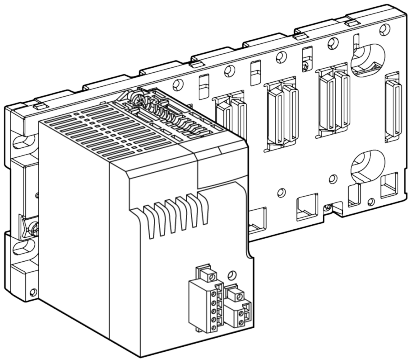
IMPOSSIBILE ESEGUIRE LA FUNZIONE DI SICUREZZA

Utilizzare solo l'alimentatore di sicurezza BMXCPS4002S, BMXCPS4022S o BMXCPS3522S su rack che comprendano almeno un modulo di sicurezza.

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

Per un rack che richiede solo un singolo alimentatore di sicurezza, posizionare un modulo di alimentazione M580 Safety nel rack nei due slot contrassegnati **CPS**. Per un rack alimentatore doppio BMEXBP••02 (vedere Modicon M580, Manuale di riferimento hardware), posizionare due moduli di alimentazione M580 Safety affiancati nei quattro slot contrassegnati **CPS**.

Esempio di singolo modulo di alimentazione installato in un rack BMEXBP0400:



NOTA: Il design del modulo di alimentazione permette di posizionarlo solo negli slot dedicati contrassegnati **CPS**.

Precauzioni per l'installazione

Il modulo di alimentazione di sicurezza M580 non supporta hot swap. Confermare che il modulo sia spento quando viene inserito nel backplane o estratto dal backplane.

Non collegare o scollegare la morsettiera rimovibile quando è presente tensione sul modulo di alimentazione M580 Safety. Confermare che l'alimentazione al modulo dal sezionatore a monte sia disattivata prima di eseguire una di queste operazioni.

Non collegare o scollegare la morsettiera rimovibile del relé di allarme quando il modulo di alimentazione M580 Safety è in funzione. Confermare che il modulo non sia alimentato prima di eseguire una di queste operazioni.

⚠⚠PERICOLO

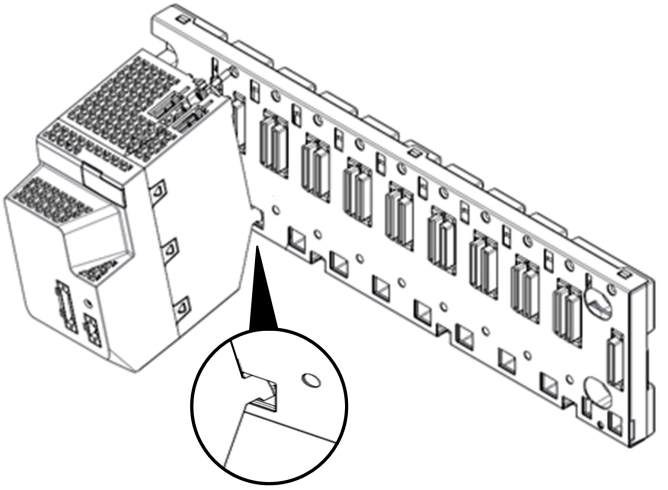
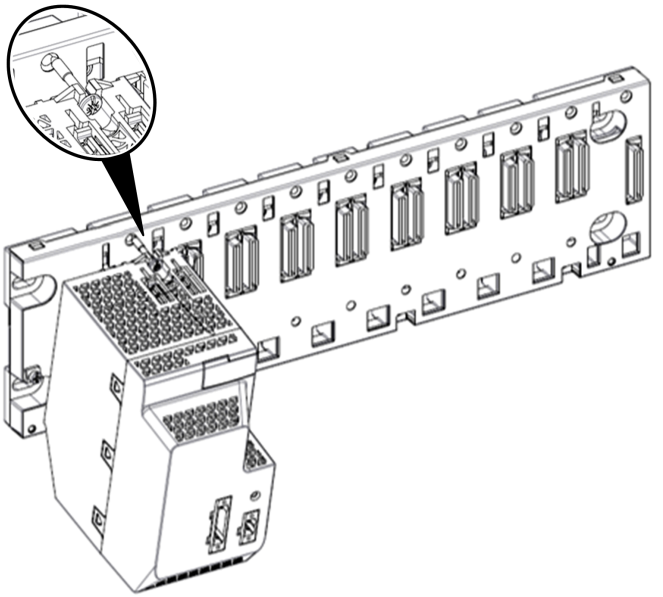
RISCHIO DI SCOSSA ELETTRICA, ESPLOSIONE O ARCO ELETTRICO

- Mettere fuori tensione tutte le apparecchiature, inclusi i dispositivi collegati, prima di rimuovere qualunque coperchio o sportello, o prima di installare/disinstallare accessori, hardware, cavi o fili, tranne che per le condizioni specificate nell'apposta Guida hardware per questa apparecchiatura.
- Per verificare che l'alimentazione sia isolata, usare sempre un rilevatore di tensione correttamente tarato.
- Prima di riattivare l'alimentazione dell'unità rimontare e fissare tutti i coperchi, i componenti hardware e i cavi e verificare la presenza di un buon collegamento di terra.
- Quando si utilizza questa apparecchiatura e qualunque prodotto associato, usare esclusivamente la tensione specificata.

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

Installazione del modulo di alimentazione nel rack

Seguire questa procedura per installare il modulo di alimentazione di sicurezza negli slot del rack contrassegnati da **CPS**:

Passo	Azione	
1	Verificare che il modulo di alimentazione sia posizionato negli slot contrassegnati **CPS**.	
2	Posizionare i pin di individuazione posti in basso nel retro del modulo negli slot corrispondenti sul rack.	
3	Ruotare il modulo verso la parte superiore del rack in modo che sia allineato alla parte posteriore del rack. A questo punto il modulo è in posizione.	
4	Serrare la singola vite di montaggio sul modulo di alimentazione per tenere il modulo in posizione nel rack. coppia di serraggio: 0,4...1,5 N m (0.30...1.10 lbf-ft).	
5	Per i rack che richiedono alimentatori doppi, ripetere i passi 2, 3 e 4 per il secondo alimentatore.	

Messa a terra del modulo di alimentazione

Rispettare la regolamentazione e tutte le norme locali e nazionali sulla sicurezza.

⚠⚠PERICOLO

PERICOLO DI SCOSSA ELETTRICA

Se non è possibile provare che il capo di un cavo schermato è collegato alla terra locale, il cavo deve essere considerato pericoloso e occorre indossare dispositivi di protezione individuale (DPI).

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

Per informazioni sulla messa a terra dell'alimentatore, vedere l'argomento *Messa a terra del rack e del modulo di alimentazione*.

Installazione I/O M580 Safety

Introduzione

È possibile installare un modulo I/O di sicurezza M580 in qualsiasi rack X Bus o Ethernet posizionandolo in qualsiasi slot non riservato per l'alimentatore di sicurezza o la CPU (nel caso di un rack principale locale).

NOTA: Utilizzare solo un alimentatore di sicurezza BMXCPS4002S, BMXCPS4022S o BMXCPS3522S per i rack contenenti moduli I/O di sicurezza.

Gli I/O di sicurezza M580 supportano hot swap.

Precauzioni generali sul cablaggio

Per limitare l'interferenza di un carico CC con una sorgente CA, separare i cavi del circuito di alimentazione (ad esempio, cavi che portano all'alimentatore) dai cavi di ingresso dai sensori e cavi di uscita che portano agli attuatori.

Posizionare i cavi che collegano la CPU ai moduli I/O in una guaina racchiusa da un condotto metallico. Tenere la guaina dei cavi I/O separata dai cavi di alimentazione posti nella propria guaina. Posizionare i cavi di alimentazione nella guaina in condotti separati dai cavi I/O. I cavi di alimentazione e i cavi di I/O devono essere separati da una distanza minima di 100 mm.

Precauzioni sulla messa a terra

Ciascun modulo I/O M580 Safety è dotato di contatti di collegamento a terra.

Utilizzare una barra BMXXSP•••• per proteggere il rack dai disturbi elettromagnetici.

Per il modulo di ingresso analogico BMXSAI0410 Safety, utilizzare una barra BMXXSP••••. Collegare il rivestimento del cavo alla barra di messa a terra fissandolo alla barra lato modulo.

⚠⚠PERICOLO

RISCHIO DI SCOSSA ELETTRICA, ESPLOSIONE O ARCO ELETTRICO

- Verificare che ogni morsettiera resti collegata alla barra di messa a terra BMXXSP•••• durante il montaggio o la rimozione dei moduli I/O di sicurezza.
- Scollegare la tensione di alimentazione da sensori o attuatori.

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

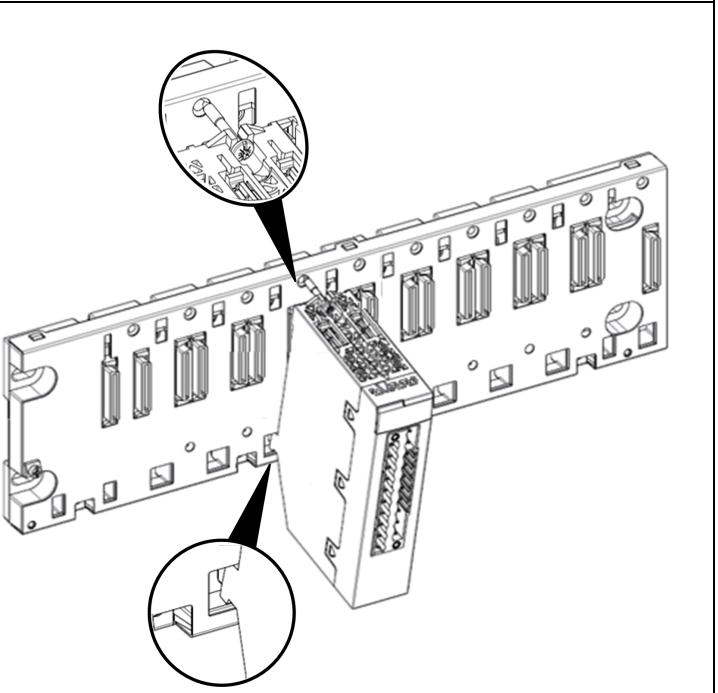
Posizionamento sensore modulo di ingresso (In relazione alla terra)

Quando si posizionano i sensori nel sistema:

- Posizionare i sensori vicini tra loro, separati da non più di pochi metri.
- I sensori devono fare riferimento a un singolo punto collegato alla terra del PAC.

Installazione di un modulo I/O di sicurezza nel rack

Un modulo I/O di sicurezza M580 richiede un singolo slot del rack. È possibile installare un modulo I/O di sicurezza in qualsiasi slot non riservato per alimentatore o CPU. Per installare un modulo I/O di sicurezza in un rack, procedere come segue:

Passo	Azione	
1	Posizionare i pin di individuazione posti in basso nel retro del modulo negli slot corrispondenti sul rack.	
2	Ruotare il modulo verso la parte superiore del rack in modo che sia allineato alla parte posteriore del rack. A questo punto il modulo è in posizione.	
3	Serrare la singola vite di montaggio sul modulo per tenere il modulo in posizione nel rack. Coppia di serraggio: 0,4...1,5 N m (0.30...1.10 lbf-ft).	
4	Per ciascun modulo aggiuntivo, ripetere i passi 1, 2 e 3 finché tutti i moduli sono installati sul rack.	

Messa a terra dei moduli I/O

Per informazioni sulla messa a terra, vedere *Messa a terra del rack e del modulo di alimentazione*.

NOTA: Per il modulo di ingresso analogico BMXSAI0410 Safety, utilizzare una barra di messa a terra BMXXSP••••. Per informazioni su come installare questa apparecchiatura, vedere *Kit di connessione di schermatura*.

Installazione di una scheda di memoria SD in una CPU

Introduzione

La CPU BME•58•040S supporta l'uso della scheda di memoria SD da BMXRMS004GPF 4GB.

Manutenzione della scheda di memoria

Affinché la scheda di memoria continui a funzionare correttamente, adottare le seguenti precauzioni:

- Evitare di rimuovere la scheda di memoria dallo slot mentre la CPU sta accedendo alla scheda (accesso alla scheda di memoria - LED verde acceso o lampeggiante).
- Evitare di toccare i connettori della scheda di memoria.
- Tenere la scheda di memoria lontano da fonti elettrostatiche ed elettromagnetiche quali calore, raggi solari, acqua e umidità.
- Fare attenzione che la scheda di memoria non subisca urti.
- Prima di spedire una scheda di memoria per posta ordinaria, verificare la regolamentazione sulla sicurezza del servizio postale. Per motivi di sicurezza, in alcuni paesi la posta viene esposta a livelli di radiazione elevati. Questa esposizione potrebbe causare la cancellazione del contenuto della scheda di memoria, rendendola quindi inutilizzabile.
- Se una scheda viene estratta senza generare un fronte di salita del bit %S65 e senza controllare che il LED verde che indica l'accesso alla scheda di memoria sia spento, i dati (file, applicazione, ecc.) possono andare persi o presentare delle anomalie.

Procedura di inserimento della scheda di memoria

Procedura per l'inserimento della scheda di memoria in una CPU BME•58•040S:

Passo	Descrizione
1	Aprire il coperchio di protezione della scheda di memoria SD.
2	Inserire la scheda nel relativo slot.
3	Spingere la scheda di memoria fino a udire uno scatto. **Risultato:** la scheda viene agganciata nello slot. **Nota:** l'inserimento della scheda di memoria non forza il ripristino dell'applicazione.
4	Chiudere il coperchio di protezione della scheda di memoria.

Procedura di rimozione della scheda di memoria

NOTA: Prima di rimuovere una scheda di memoria, è necessario generare un fronte di salita sul bit %S65. Se una scheda viene estratta senza generare un fronte di salita del bit `%S65` e senza controllare che il LED verde che indica l'accesso alla scheda di memoria sia spento, i dati possono andare persi.

Procedura per la rimozione della scheda di memoria da una CPU BME•58•040S:

Passo	Descrizione
1	Generare un fronte di salita sul bit %S65.
2	Verificare che il LED verde di accesso alla scheda di memoria sia spento.
3	Aprire il coperchio di protezione della scheda di memoria SD.
4	Spingere la scheda di memoria fino a udire un clic, quindi rilasciarla. **Risultato:** la scheda viene sganciata dallo slot.
5	Rimuovere la scheda dallo slot. **Nota:** il LEDdi accesso alla scheda di memoria è acceso quando si rimuove la scheda dalla CPU.
6	Chiudere il coperchio di protezione della scheda di memoria.

Aggiornamento del firmware del controller M580 Safety

La procedura varia in base alla versione iniziale e della versione di destinazione del controller. Nella versione 4.x è stato introdotto un nuovo boot loader. Pertanto, l'aggiornamento da una versione precedente (V3.22 o precedente) alla versione V4.x o il downgrade da una versione V4.x a una versione precedente richiede procedure specifiche.

Per le procedure dettagliate per l'aggiornamento del firmware, consultare *Controller Modicon M580 - Guida all'installazione del firmware*.

Aggiornamento del firmware alla versione 4.21

È possibile aggiornare il firmware dei controller di sicurezza alla versione 4.21 dalle seguenti versioni precedenti:

- 3.30.06 per i controller BMEP586040S
- 3.20.05 o precedente per gli altri controller di sicurezza M580

La procedura è descritta nella sezione *Aggiornamento firmware da v3.x a v4.x* di Controller Modicon M580 - Guida all'installazione del firmware.

Versioni del firmware di fallback

Se l'aggiornamento del firmware non riesce, il controller di sicurezza applica la seguente versione del firmware di fallback:

- 3.30.06 per il controller BME58P6040S
- 3.20.05 per gli altri controller di sicurezza M580

Livello di applicazione e stato operativo del controller dopo il completamento dell'aggiornamento

Se l'aggiornamento riesce, il controller di sicurezza riavvia l'applicazione precedentemente caricata nel controller e funziona in stato STOP.

NOTA: In questo caso, il controller funziona in stato STOP anche quando è selezionata l'impostazione *Avvio automatico in RUN*.

Se l'aggiornamento non riesce e se l'applicazione caricata in precedenza nel controller è:

- non compatibile con la versione del firmware di fallback, il controller si riavvia nello stato operativo NOCONF.
- compatibile con la versione del firmware di fallback, il controller riavvia l'applicazione precedentemente caricata nel controller e funziona in stato STOP.

Downgrade del firmware dalla versione 4.21 o successiva

È possibile eseguire il downgrade del firmware dei controller di sicurezza dalla versione 4.21 o successiva alle seguenti versioni precedenti:

- Versione 3.30.06 per BMEP586040S
- Versione 3.20.05 per gli altri controller M580 Safety

La procedura è descritta in *Controller Modicon M580 - Guida all'installazione del firmware* sezione *Procedura di declassamento del firmware*.

Versioni del firmware di fallback

Se il downgrade del firmware non riesce, occorre utilizzare lo strumento EcoStruxure Automation Device Maintenance (EADM) per riattivare il controller installando una versione firmware 4.21 o successiva.

Livello di applicazione e stato operativo del controller dopo il completamento del downgrade

Se il downgrade avviene correttamente e se l'applicazione caricata in precedenza sul controller è:

- non compatibile con la versione del firmware di fallback, il controller si riavvia nello stato operativo NOCONF.
- compatibile con la versione del firmware di fallback, il controller si riavvia con l'applicazione caricata in precedenza nel controller e funziona in stato STOP anche quando è selezionata l'impostazione *Avvio automatico in RUN*.

Se il downgrade non riesce, il controller mantiene il firmware originale.

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

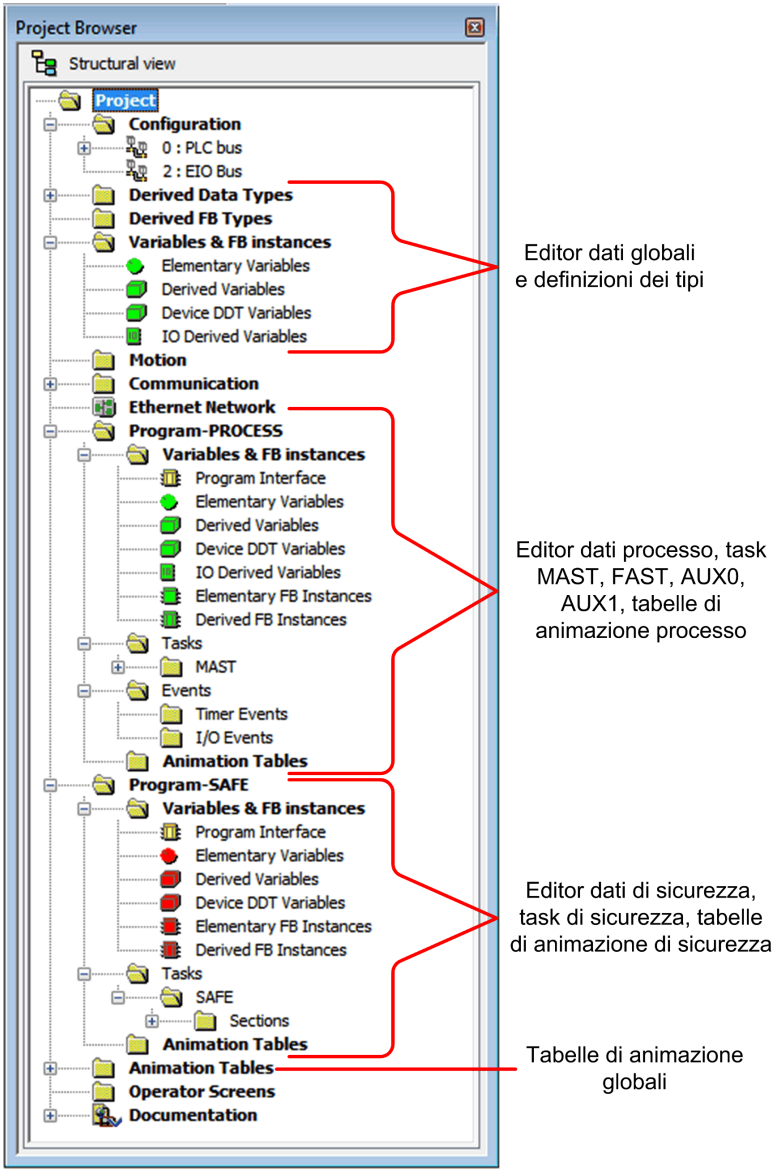
Introduzione

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:



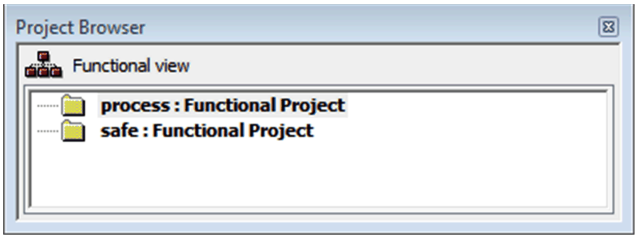
Osservando il **Browser di progetto** si potrà notare che:

- 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 PAC M580 Safety

Due modalità operative

Il PAC M580 Safety presenta 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 XL Safety è uno strumento esclusivo che consente di gestire le transizioni tra le modalità operative.

NOTA: l'impostazione della modalità operativa di un PAC di sicurezza Hot Standby, in modalità di sicurezza o di manutenzione, non è inclusa nel trasferimento di un'applicazione dal PAC primario al PAC di standby. Durante lo switchover, quando un PAC di sicurezza passa da PAC di standby a PAC primario, viene impostata automaticamente la modalità operativa di sicurezza.

Modalità di sicurezza e relative limitazioni

La modalità di sicurezza è la modalità predefinita del PAC di sicurezza. Quando si accende il PAC di sicurezza con una valida applicazione presente, il PAC entra nella 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 PAC M580 Safety opera in modalità di sicurezza, le seguenti funzioni **non** sono disponibili:

- Download di una configurazione modificata da Control Expert al PAC.
- 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 una CPU 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 PAC di sicurezza entra automaticamente in modalità di sicurezza se la comunicazione tra Control Expert e il PAC viene persa, oppure viene eseguito un comando di scollegamento. 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 PAC M580 Safety opera in modalità di manutenzione, sono disponibili le seguenti funzioni:

- Download di una configurazione modificata da Control Expert al PAC.
- 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 PLC Safety non viene mantenuto.

⚠AVVERTIMENTO

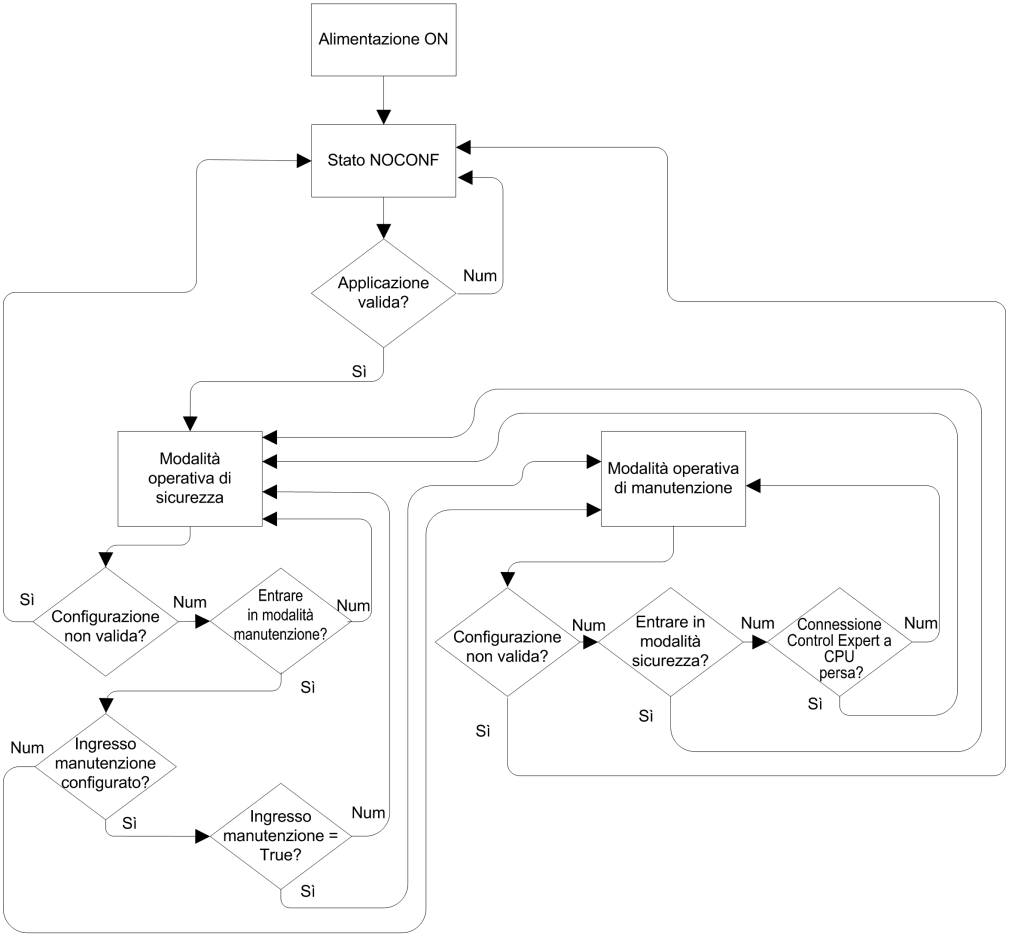
PERDITA DEL LIVELLO DI INTEGRITÀ DI SICUREZZA

Adottare le misure appropriate per garantire lo stato di sicurezza 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.

Transizioni tra le modalità operative

Lo schema seguente mostra come il PAC M580 di sicurezza 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 PAC di sicurezza, quando la comunicazione tra Control Expert e il PAC viene perso 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 di ingresso di manutenzione è configurata in Control Expert nella scheda **Configurazione** della CPU:
  - 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 PAC 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 PAC di sicurezza dalla modalità di manutenzione alla modalità di sicurezza non è possibile se:

- Il PAC 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 nella modalità di sicurezza sono registrati nel server SYSLOG nella CPU.

Determinazione della modalità operativa

È possibile determinare la modalità di funzionamento corrente di un PAC M580 Safety che utilizza i LED **SMOD** della CPU e del coprocessore oppure Control Expert.

Quando i LED **SMOD** della CPU e del coprocessore sono:

- Accesi *lampeggianti*, il PAC è in modalità di manutenzione.
- Accesi *fissi*, il PAC è in modalità di sicurezza.

Control Expert, quando è collegato al PAC, identifica la modalità operativa del PAC M580 Safety in diverse posizioni:

- Le parole di sistema %SW12 (coprocessore) e %SW13 (CPU), pagina 221 insieme indicano la modalità operativa del PAC, come indicato di seguito:
  - se %SW12 è impostata a 16#A501 (esa) e %SW13 è impostata a 16#501A (esa), il PAC è in modalità di manutenzione.
  - Se una o entrambe le parole di sistema sono impostate a 16#5AFE (esa), il PAC è in modalità di sicurezza.
- Le schede secondarie **Task** e **Informazioni** della scheda **Animazione** della CPU visualizzano la modalità operativa del PAC.
- La barra delle applicazioni, al fondo della finestra principale di Control Expert, indica la modalità operativa come MANUTENZIONE o SICUREZZA.

Stati operativi del PAC M580 Safety

Stati operativi

Gli stati operativi del PAC di sicurezza M580 sono descritti di seguito.

NOTA: Per una descrizione della relazione tra gli stati operativi del PAC di sicurezza M580 e quelli del PAC di Hot Standby M580, consultare il documento *Modicon M580 Hot Standby, Guida di pianificazione del sistema per architetture di utilizzo frequente* e gli argomenti *Stati del sistema Hot Standby* e *Transizioni e assegnazioni dello stato Hot Standby*.

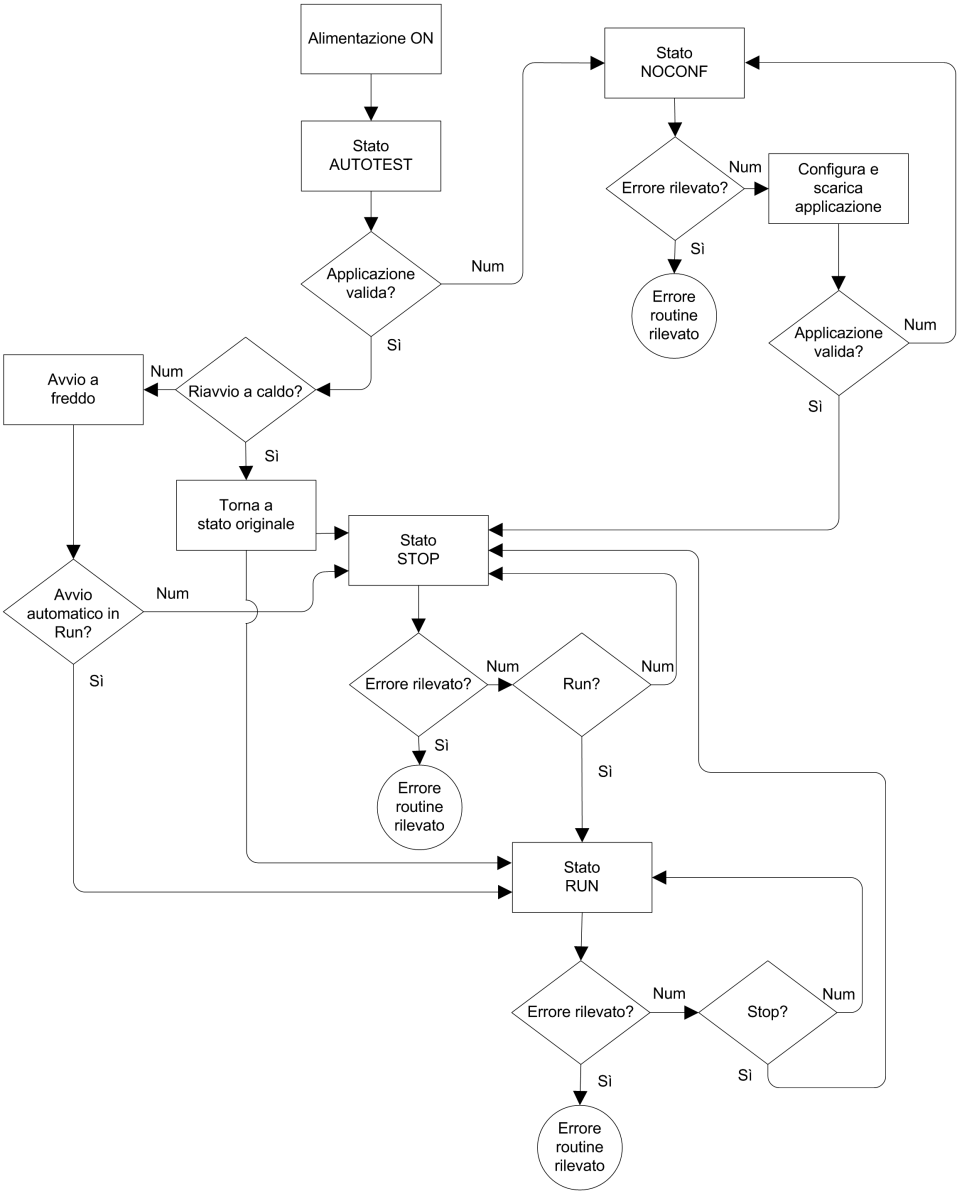
Stato operativo	Si applica a...	Descrizione
AUTOTEST	PAC	La CPU sta eseguendo test automatici interni. **NOTA:** Se al rack locale principale sono collegate estensioni rack e ai connettori non utilizzati del modulo di estensione rack non sono state applicate le terminazioni di linea, la CPU rimane in AUTOTEST dopo il completamento dei test automatici.
NOCONF	PAC	Il programma applicativo non è valido.
STOP	PAC o Task	Il PAC 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 119). • L'esecuzione è arrestata dall'esecuzione di un comando STOP (modalità di sicurezza, pagina 119 o manutenzione, pagina 120). • Sono stati impostati punti di interruzione in modalità di manutenzione, quindi la connessione tra Control Expert e la CPU è stata persa per oltre 50 secondi. La CPU legge gli ingressi associati a ciascun task, ma non aggiorna le uscite, che entrano nel rispettivo stato di posizionamento di sicurezza. La CPU può essere riavviata 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 della CPU.
HALT	Task	Il PAC di sicurezza M580 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 ciascun caso, le operazioni del task vengono arrestate in quanto è stata rilevata una condizione di blocco imprevista, determinando una condizione ripristinabile (vedi Modicon M580, Manuale di sicurezza). La CPU legge gli ingressi associati a ciascun task arrestato, ma non aggiorna le uscite, che entrano in stato di posizionamento di sicurezza.
RUN	PAC o Task	Con una applicazione valida e nessun errore rilevato, la CPU legge gli ingressi associati a ciascun task, esegue il codice associato a ciascun task e aggiorna le uscite associate. • in modalità di sicurezza, pagina 119: la funzione di sicurezza viene eseguita e tutte le limitazioni applicate. • in modalità di manutenzione, pagina 120: il PAC funziona come qualsiasi CPU non di sicurezza. Avviene la doppia esecuzione del codice del task SAFE, ma i risultati non vengono confrontati. **NOTA:** l'emissione di un comando RUN in Control Expert avvia tutti i task. L'evento RUN viene registrato nel server SYSLOG della CPU.

Stato operativo	Si applica a...	Descrizione
WAIT	PAC	La CPU si trova in stato transitorio durante il backup dei dati quando viene rilevata una condizione di disinserzione. La CPU si riavvia solo quando viene ripristinata l'alimentazione e viene rifornita la riserva di energia. Poiché WAIT è uno stato transitorio, potrebbe non essere visibile. La CPU esegue un riavvio a caldo, pagina 132 per uscire dallo stato WAIT.
ERROR	PAC	La CPU viene arrestata perché è stato rilevato un errore non ripristinabile (vedi Modicon M580, Manuale di sicurezza) hardware o del sistema. Lo stato ERROR attiva la funzione di sicurezza (vedi Modicon M580, Manuale di sicurezza). Quando il sistema è pronto per il riavvio, eseguire un avvio a freddo, pagina 132 della CPU per uscire dallo stato ERROR, facendo clic per spegnere e riaccendere o eseguendo un RESET.
OS DOWNLOAD	PAC	Download del firmware della CPU o del COPRO in corso.

Consultare gli argomenti *Diagnostica LED CPU M580 CPU* (vedi Modicon M580, Manuale di sicurezza) e *Diagnostica LED coprocessore M580 Safety* (vedi Modicon M580, Manuale di sicurezza) per informazioni sugli stati operativi del PAC.

Transizioni dello stato operativo

Le transizioni tra diversi stati in un PAC di sicurezza M580 sono descritte di seguito:



Per informazioni su come vengono gestiti gli errori rilevati dal sistema di sicurezza, consultare *Elaborazione degli errori rilevati*, pagina 128.

Elaborazione degli errori rilevati

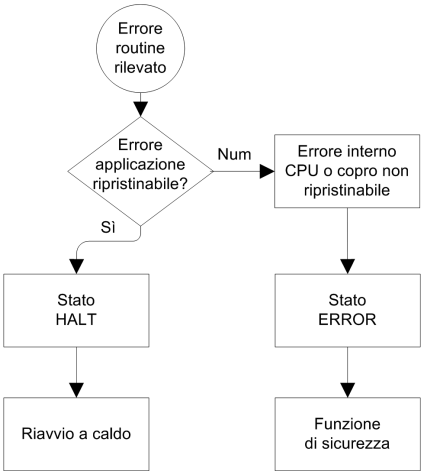
Il PAC di sicurezza M580 gestisce i seguenti tipi di errori rilevati della CPU:

- 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 di CPU o coprocessore: questi eventi provocano l'ingresso del PAC 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:

Tipo di errore rilevato	Stato del task			
	FAST	**SAFE**	**MAST**	**AUX**
Errori 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 rilevato di esecuzione codice doppio CPU	RUN	HALT[2]	RUN	RUN

Tipo di errore rilevato	Stato del task			
	FAST	**SAFE**	**MAST**	**AUX**
Overrun watchdog di sicurezza[3]	ERROR	ERROR[2]	ERROR	ERROR
Errore interno rilevato CPU	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 nel relativo stato configurabile dall'utente (posizione di sicurezza o mantieni).

3. Il watchdog di sicurezza viene impostato a un valore uguale a 1,5 volte il watchdog del task SAFE.

Visualizzatore di stato di sicurezza della barra dei task

Quando Control Expert è collegato al PAC di sicurezza M580, 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 PAC 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 di alimentazione, il PAC M580 Safety può eseguire un avvio a freddo, pagina 132 o un avvio a caldo, pagina 132 al ripristino dell'alimentazione.

Avvio iniziale

All'avvio iniziale, il PAC M580 Safety esegue un avvio a freddo. Tutti i task, compresi il task SAFE e i task non sicuri (MAST, FAST, AUX0, AUX1), entrano nello stato STOP a meno che **Avvio automatico in RUN** sia attivato, in questo 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 alimentazione si esaurisce, il PAC M580 Safety esegue un ciclo di spegnimento e riaccensione completo.

Prima di spegnere il sistema, la CPU di sicurezza memorizza i seguenti dati che definiscono il contesto operativo al momento dello 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).

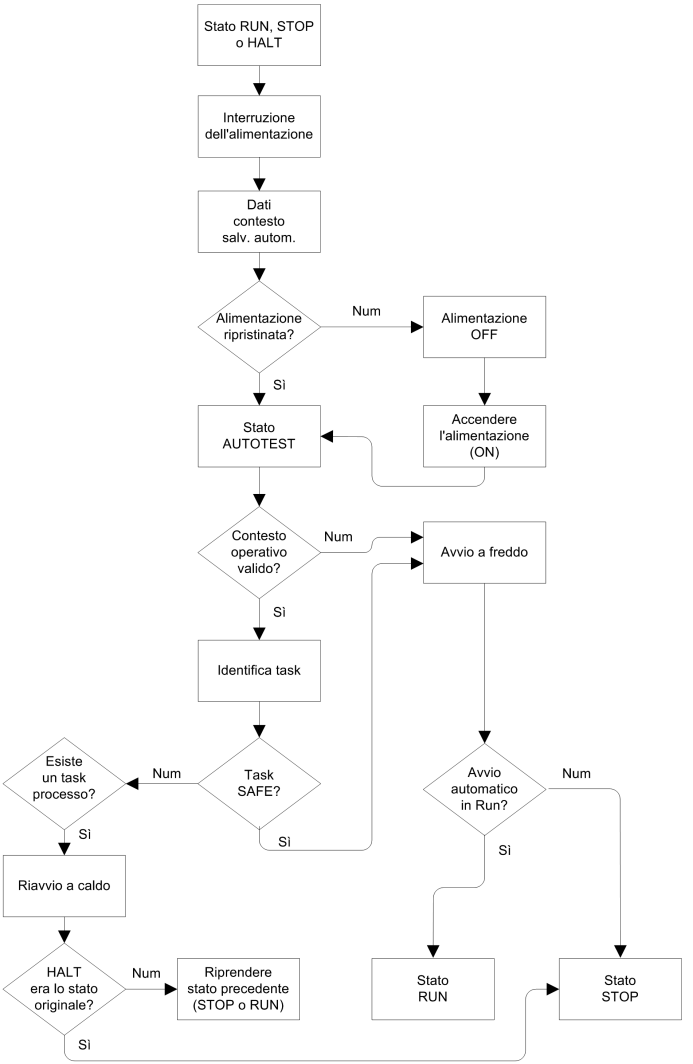
Quindi, il PAC di sicurezza M580 esegue test automatici e controlla la validità dei dati del contesto operativo salvati al momento dell'interruzione di alimentazione, come indicato di seguito:

- 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 148 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 PAC e la CPU vengono reimpostate.
- 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

Confermare che la selezione **Avvio automatico in RUN** sia compatibile con il comportamento corretto del sistema; in caso contrario, disattivare questa funzione.

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

Task del PAC M580 Safety

Introduzione

Un PAC M580 Safety può eseguire applicazioni che comprendono uno o 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 PAC M580 Safety supporta i seguenti task:

- FAST
- SAFE
- MAST
- AUX0
- AUX1

Caratteristiche dei task

I task supportati dal PAC di sicurezza M580 presentano le seguenti caratteristiche:

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 della CPU), l'impostazione **Watchdog** minima è 64 ms.

3. Supportato dai PAC standalone BMEP58•040S Safety. Non supportato dai PAC Hot Standby BMEH58•040S Safety.

4. I PAC standalone BMEP58•040S Safety supportano modelli di tempo ciclici e periodici. I PAC BMEH58•040S Safety Hot Standby supportano solo il modello di tempo periodico.

Priorità task

I PAC M580 Safety eseguono i task in attesa 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 il valore uguale a una volta e una volta e mezza dell'impostazione del watchdog del task SAFE), la CPU e il Copro 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. Utilizzare un valore del watchdog del task FAST non molto maggiore del periodo FAST.

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

Il menu **Crea** di Control Expert Safety presenta tre diversi comandi di creazione e un comando Firma Safe, come segue:

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 145. • 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 137 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 PAC M580 Safety, standalone e Hot Standby, includono un meccanismo di produzione di un'impronta algoritmica SHA256 dell'applicazione sicura: la firma di origini SAFE. Quando si trasferisce l'applicazione dal PC al PAC, Control Expert confronta la firma di origini SAFE nel PC con la firma di origini SAFE nel PAC per determinare se l'applicazione sicura nel PC è la stessa o diversa dall'applicazione sicura nel PAC.

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 sia 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**
CPU di sicurezza	Modificare il codice prodotto della CPU tramite **Sostituisci processore...**
	Modificare la versione della CPU tramite **Sostituisci processore...**
	Modificare qualsiasi parametro sulle schede **Configurazione** o **Hot Standby** della CPU.
	Modificare un parametro su una scheda dell'intestazione di comunicatore Ethernet della CPU (**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 del modulo tramite il comando **Rinnova ID e Ricrea tutto**.
	Modifica del nome istanza DDT del dispositivo.
Modulo CIP Safety	**Aggiungere**/**Eliminare** un modulo.
	Modifica di un parametro del modulo CIP Safety nell'editor DTM del dispositivo CIP Safety, oppure nell'**Elenco dispositivi** dell'editor DTM master della CPU.

Dispositivo	Azione
	Modifica del nome istanza DDT del dispositivo.
Alimentatore di sicurezza	**Aggiungere**/**Eliminare** un alimentatore di sicurezza.
Altre apparecchiature correlate alla 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 • Consenti procedure • Consenti commenti annidati

Tipo	Componenti
	• 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 singola per EBOOL
	Generale > Tempo[1] • Fuso orario personalizzato • Fuso orario • Offset ora • Passa automaticamente all'ora legale ◦ Tutte le impostazioni START ed 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 SAFE 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 da PC al PLC

Quando si scarica un'applicazione dal PC al PAC, Control Expert confronta la firma di origini SAFE nell'applicazione scaricata con una presente nel controller. Control Expert si comporta come segue:

Nuova Firma Safe	Firma Safe PAC	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 PAC (YYYY) sono UGUALI. 3. L’applicazione sicura nel PC (XXXX) e l’applicazione sicura nel PAC (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 **Proprietà del progetto > Identificazione**: Nel **Browser di progetto**, fare clic con il pulsante destro del mouse su **Progetto** e selezionare **Proprietà**.
- (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 **Trasferimento del progetto al PLC**: Selezionare questo comando dal menu **PLC** (o nella finestra di dialogo **PC < - - > Confronto PLC**.

Confronto tra la firma di origini SAFE e SAId

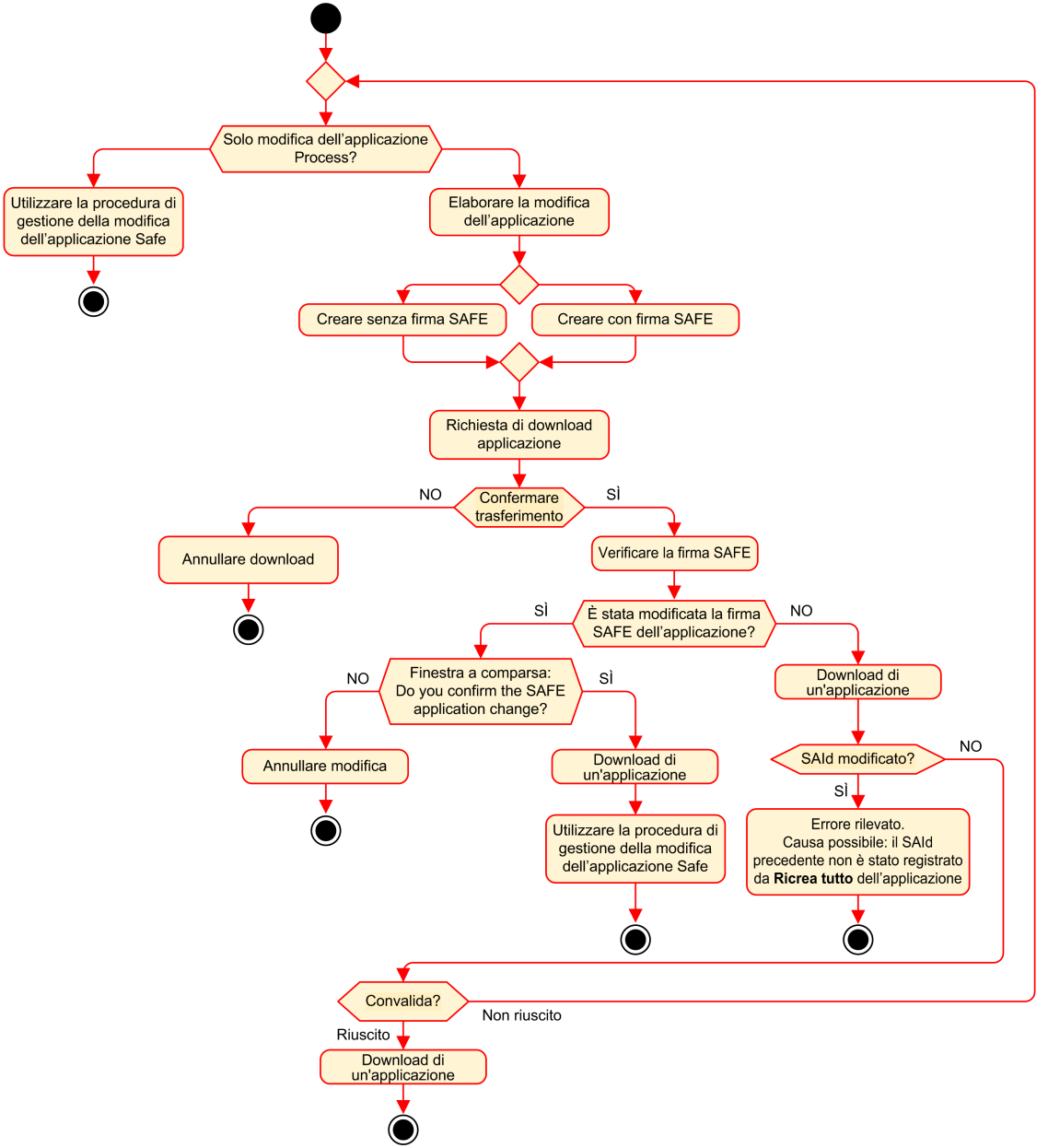
La firma di origini SAFE è stata creata per fornire una verifica *a priori* che l’applicazione non sia stata modificata. Utilizzare questa funzione ogni volta che l'applicazione di processo viene modificata, pagina 143 per evitare modifiche involontarie dell'applicazione sicura.

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.

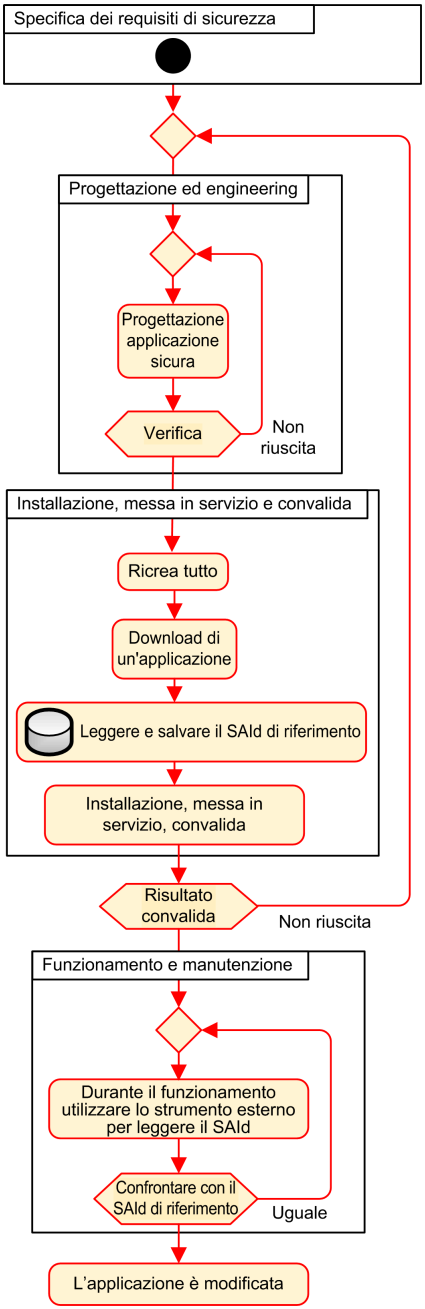
SAId può essere valutato solo in fase di runtime. Viene calcolato due volte e confrontato da CPU e da COPRO, sulla base di un codice binario eseguito dall'applicazione sicura. Poiché SAId è sensibile a tutte le modifiche, incluse quelle che possono essere introdotte da un comando **Ricrea tutto** dopo una modifica di creazione, utilizzare un comando **Ricrea tutto** per generare una versione di riferimento dell'applicazione sicura. Questo processo, pagina 144 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 best practice utilizzato per confermare che l'applicazione sicura sia quella convalidata. Il valore SAId non viene verificato automaticamente dall'applicazione. Per questo motivo, verificare regolarmente SAId con qualsiasi mezzo appropriato (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 221.

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, pagina 75, che si trova in alto nella parte frontale 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 di I/O può impedire il tentativo di assegnare al modulo una configurazione non corretta o proteggere il modulo 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	Connettere Control Expert al PAC M580 Safety.
2	Utilizzare il comando **Trasferimento progetto dal PLC** per caricare il progetto dal PAC 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, pagina 75 per oltre 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 PAC M580 Safety in modalità operativa di manutenzione, pagina 120.
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, pagina 75 per oltre 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 PAC M580 Safety in modalità operativa di manutenzione, pagina 120.
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**.

Passo	Azione
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, pagina 75 per oltre 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 PAC di entrare in modalità di sicurezza, pagina 119.

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 132

Lavorare con le tabelle di animazione in Control Expert

Tabelle di animazione e schermate operatore

Introduzione

Un PAC 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 sicurezza da un PAC di sicurezza M580 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 PAC M580 Safety.

Quando Control Expert è collegato al PAC 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 PAC M580 Safety opera in modalità sicura o in modalità di manutenzione.
- L'aggiunta o l'eliminazione di variabili dello spazio dei nomi a una tabella di animazione di sicurezza è supportata mentre il PAC di sicurezza M580 opera in modalità di manutenzione.
- L'aggiunta o l'eliminazione di variabili dello spazio dei nomi sicuro a una tabella di animazione sicura è supportata mentre il PAC M580 Safety opera in modalità di sicurezza solo se le impostazioni di progetto non comprendono 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 PAC di sicurezza M580, 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: 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.

⚠ AVVERTIMENTO
FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA • Verificare che l'applicazione presenti le corrette impostazioni di progetto. • Verificare la sinstassi per accedere alle variabili nei diversi spazi dei nomi. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Per evitare 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 sicuro, per impostazione predefinita Control Expert include il task MAST. 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 periodica del task (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 BME•584040S, e BME•586040S)
  - (0,273 x Dimensione_dati_sicuri) + 2 ms (per BME•582040S)

  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 $Size_{kbyte}$ e Dimensione_dati_sicuri siano uguali.					

NOTA: Configurare il watchdog del task SAFE con un valore maggiore del **Periodo** del task SAFE.

Per informazioni su come la configurazione del task SAFE influisce sul tempo, vedere l'argomento *Tempo di sicurezza del processo* (vedere Modicon M580, Manuale di sicurezza),.

Consultare l'argomento *Task PAC M580 Safety*, pagina 133 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 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:

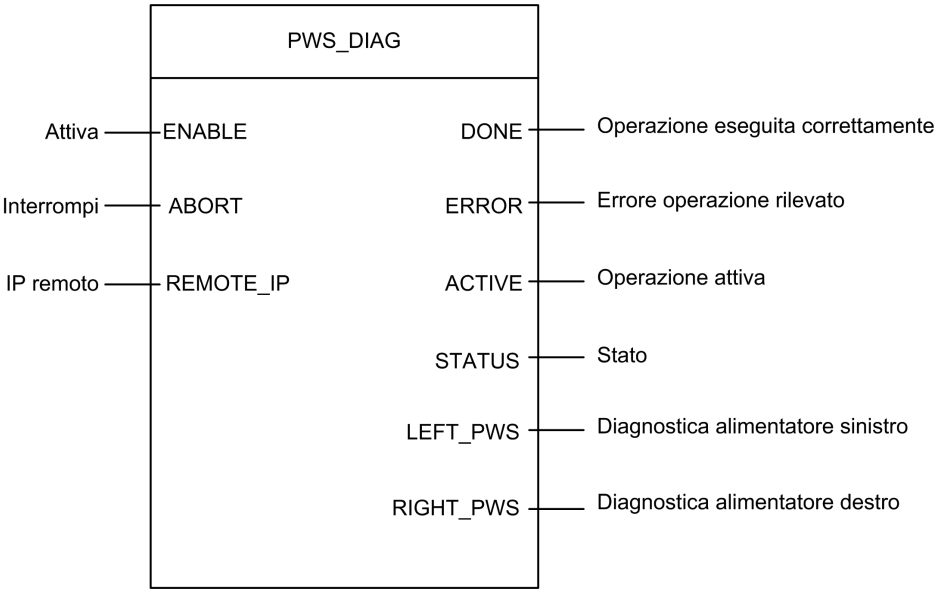
- Temperatura ambiente dell'alimentatore.
- Tensione e corrente sulla linea backplane 3,3V.
- Tensione e corrente sulla linea backplane 24V.
- Energia cumulata totale dell'alimentatore dalla data di fabbricazione sulle linee backplane 3,3V e 24V.
- Tempo operativo come master dall'ultima accensione e 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

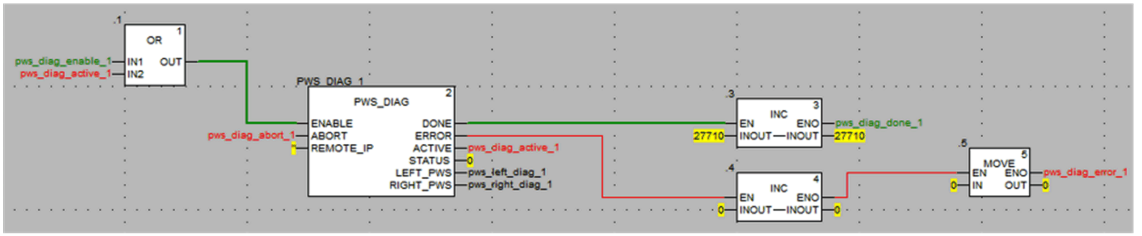
Parametri di ingresso:

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 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

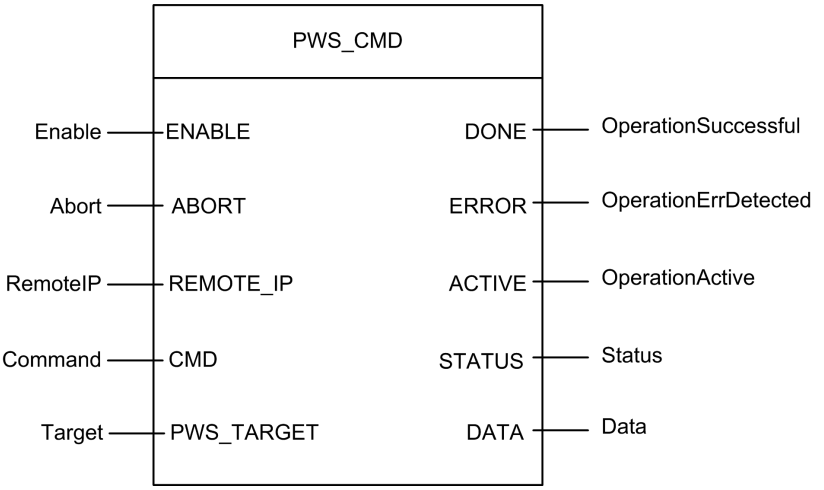
Il blocco funzione PWS_CMD può essere utilizzato per emettere due comandi:

- 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:

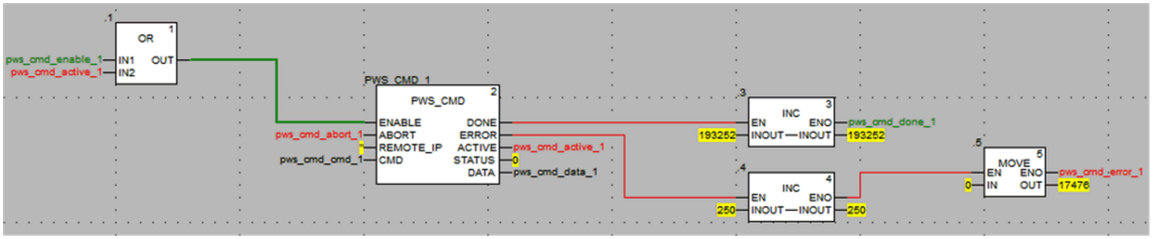
Nome parametro	Tipo di dati	Descrizione
ENABLE	BOOL	Quando è ON, l'operazione è attivata.
ABORT	BOOL	Quando è ON, l'operazione corrente viene interrotta.
REMOTE_IP	STRING	Indirizzo IP ("ip1.ip2.ip3.ip4") della derivazione che contiene il modulo alimentatore. Lasciare in questo campo una stringa vuota ("") 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:

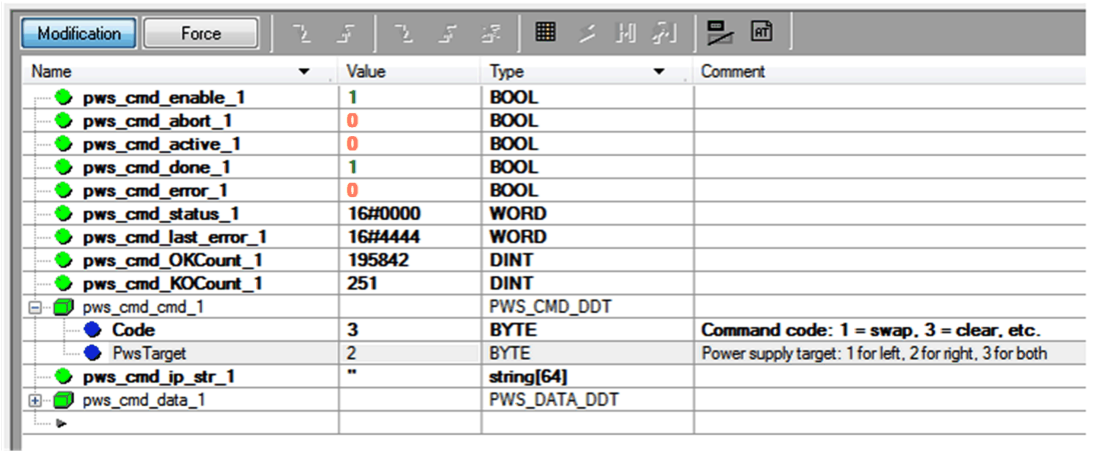
Nome parametro	Tipo di dati	Descrizione
DONE	BOOL	ON quando l'operazione viene conclusa correttamente.
ERROR	BOOL	ON quando l'operazione non è eseguita correttamente e viene interrotta.
ACTIVE	BOOL	ON quando l'operazione è attiva.
STATUS	WORD	Identificatore errore rilevato.
DATA	ANY	Dati di risposta (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 183.

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 183.

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 EcoStruxure Control Expert. Questa sezione descrive le funzionalità di questo strumento correlato esclusivamente ai progetti M580 Safety.

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 Control Expert installato su una workstation. L'utilizzo dello strumento di configurazione *Editor di sicurezza* per gestire l'accesso al software Control Expert è opzionale.

NOTA: la gestione dell'accesso si riferisce all'hardware, in genere workstation, su cui è installato il software EcoStruxure Control Expert e non al progetto, che ha il 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 crea o modifica un profilo utente, occorre confermare che tutte le modifiche necessarie sono state effettuate.

Categorie di utenti

L'**Editor di sicurezza** supporta due categorie di utenti:

- **SecurityAdmin:** l'amministratore della sicurezza (*SecurityAdmin*) è l'unico utente in grado di gestire la sicurezza di accesso per il software. Il *SecurityAdmin* specifica chi può accedere al software e i relativi diritti di accesso. Durante l'installazione di EcoStruxure Control Expert sulla workstation, solo il *SecurityAdmin* può accedere alla configurazione di sicurezza senza alcuna limitazione dei diritti (senza una password).

  NOTA: il nome utente riservato all'amministratore della sicurezza è *SecurityAdmin*. Questo utente esegue il ruolo amministrativo che era gestito dal *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* se 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

Il profilo utente comprende tutte le autorizzazioni di accesso per un utente. Il profilo utente può essere definito dall'utente *SecurityAdmin* o può essere creato applicando un profilo preconfigurato fornito con lo strumento **Editor di sicurezza**.

Profili utente preconfigurati

L'**Editor sicurezza** offre i seguenti 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, eccetto: • 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, eccetto: • 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, eccetto: • 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 consentita. • 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 **Program**, ma rispetto al programma di sicurezza, eccetto: • 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 consentita. • Il comando del programma di sicurezza per entrare in modalità di manutenzione è consentito.
Disattivato	✓	✓	L'utente non può 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 di utente preconfigurato:

- Regolazione_utente_sicurezza

- Debug_utente_sicurezza
- Operativo_utente_sicurezza
- Programma_utente_sicurezza
- Regolazione_utente
- Debug_utente
- Operativo_utente
- Programma_utente

Vedere l'argomento *Funzioni utente* (vedere EcoStruxure™ EcoStruxure Control Expert, Editor sicurezza, Guida al funzionamento) per ulteriori informazioni su come l'utente *SecurityAdmin* può assegnare un profilo preconfigurato a un utente.

Diritti di accesso

Introduzione

Questo argomento 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 PLC*	✓	–	✓	–	–	–	✓	✓
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	–	–	–	–	–	–	–	✓

✓ : 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 la 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 la configurazione degli I/O di sicurezza	–	–	–	–	–	–	–	✓
Regola I/O	✓	–	✓	–	✓	–	✓	✓
Regola gli 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

Impostazioni del progetto di sicurezza M580

Introduzione

Questa sezione descrive le impostazioni esclusive del progetto di sicurezza M580 Control Expert

Impostazioni progetto per un progetto M580 Safety in Control Expert

Impostazioni di progetto specifiche dell'ambito

Selezionare **Strumenti > Impostazioni progetto...** nel menu principale di Control Expert per aprire una finestra in cui è possibile configurare e visualizzare le impostazioni di un progetto M580 Safety. Le impostazioni del progetto sono suddivise in tre gruppi, in base all'**Ambito** delle impostazioni, come segue:

- **comune**: queste impostazioni si applicano all'intera applicazione e possono influire sulle aree globale, processo e sicura del progetto.
- **processo**: queste impostazioni si applicano solo all'area PROCESS del progetto.
- **sicuro**: queste impostazioni si applicano solo all'area SAFE del progetto.

In questo argomento vengono descritte solo le parti della finestra **Impostazioni progetto** che variano da un progetto M580 non di sicurezza. Vedere la sezione *Impostazioni progetto* del manuale *EcoStruxure™ Control Expert - Modalità operative* per informazioni sulle funzionalità comuni ai progetti M580 Safety e non di sicurezza.

Impostazioni progetto comuni

Le seguenti impostazioni **Ambito > comune** si applicano alle aree di progetto globale, sicura e processo, ma in modo diverso dalle stesse impostazioni in un progetto M580 non di sicurezza:

Gruppo	Impostazione	Descrizione
Impostazioni **Generali**:		
Impostazioni Creazione	Memoria dati libera (in kbyte)	Questa impostazione è disattivata. **NOTA:** in un sistema M580 Safety, i dati vengono allocati dinamicamente e non è necessario riservare un blocco dati di dimensioni fisse.

Gruppo	Impostazione	Descrizione
	Modalità collegata virtuale	La modalità collegata virtuale è possibile e disattivata per impostazione predefinita per i controller M580 Safety. Quando è attivata la modalità Collegato virtuale, le modifiche che non richiedono una ricostruzione del progetto sono consentite nelle aree Comune, Processo e SICURA del programma. Per impedire modifiche nell'area SICURA del programma con la modalità collegato virtuale attivata, impostare una password di sicurezza per attivare la protezione. **NOTA:** • La modalità collegata virtuale è attivata e deselezionata per impostazione predefinita per processori M580 Safety. • La modalità collegata virtuale può essere controllata dall'utente. Quando è attivata la modalità Collegato virtuale, le modifiche che non richiedono una ricostruzione del progetto sono consentite nelle aree Comune, Processo e SICURA del programma. Se si desidera impedire le modifiche nella parte SICURA del programma con la modalità Collegato virtuale attivata, impostare una password di sicurezza e attivare la protezione nelle proprietà del progetto.
Dati integrati del PLC	Dizionario dati • Uso dello spazio dei nomi di processo	Determina come una schermata operatore può accedere e leggere le variabili dello spazio dei nomi di processo: • Se selezionato, la schermata operatore può leggere le variabili dell'area di processo solo mediante il formato "PROCESS.<nome variabile>". • Se deselezionata, la schermata operatore può leggere le variabili dell'area di processo solo mediante il formato “<nome variabile>” senza il prefisso PROCESS. **NOTA:** è possibile accedere a tutte le variabili nell'area sicura mediante il formato "SAFE.<nome variabile>".
	Ottimizza modifica dati online	Si applica a: • Programma di processo nelle modalità di funzionamento di sicurezza e manutenzione. • Programma di sicurezza solo nella modalità di funzionamento di manutenzione.
Diagnostica del PLC	Informazioni di diagnostica del visualizzatore rack • Nomi delle variabili del Visualizzatore rack	Entrambe queste impostazioni sono disponibili per entrambe le variabili di processo e sicurezza.

Gruppo	Impostazione	Descrizione
	Informazioni sul Visualizzatore programmi	Questa impostazione è disponibile per le sezioni di codice di processo e sicurezza.
Ora	Modalità oro-datario	Questa impostazione è disponibile per programmi di processo e sicurezza, ad eccezione del mancato supporto del timestamp per le variabili di sicurezza.
Impostazioni **Schermata operatore**:		
Schermata controllata	Visualizzazione schermate controllate con il PLC	Questa impostazione è disponibile nel PAC di sicurezza M580 per la variabile selezionata.

Impostazioni di progetto comuni che non influiscono sull'area di sicurezza del progetto

Le seguenti impostazioni **Ambito > comune** si applicano al programma di processo, ma non al programma di sicurezza in un progetto M580 Safety:

Gruppo	Impostazione	Descrizione
Impostazioni **Generali**:		
Comportamento PLC	Reimposta %M su transizione Stop -> Run	Le sezioni codice LL984 non sono supportate nel programma di sicurezza.
Configurazione	Tipo di dati di I/O preferito M580 (I/O locale)	Solo il tipo dati DDDT del dispositivo è disponibile per i moduli I/O di sicurezza.
Impostazioni delle **Variabili**:		
–	Variabili array rappresentate direttamente	L'accesso %MW non è supportato nel programma di sicurezza.
	Attiva analisi veloce per il trending	Lo strumento di trending non è supportato nel programma di sicurezza. È supportato solo nel task MAST del programma di processo.
	Forza inizializzazione riferimenti	I riferimenti non sono consentiti nel programma di sicurezza.
Impostazioni del **Programma**:		
Linguaggi • Comune	Consenti commenti annidati	Supportato solo per task non di sicurezza (MAST, FAST, AUX0 e AUX1).
	Consenti assegnazioni multiple (a:=b:=c) (ST/LD)	• Il linguaggio ST, che comprende il blocco Operativo, non è supportato dal programma di sicurezza. • Il linguaggio LD nel programma di sicurezza non supporta

Gruppo	Impostazione	Descrizione
	Consenti parametri vuoti in chiamata non formale (ST/IL)	I linguaggi ST e IL non sono supportati nel programma di sicurezza.
Linguaggi • ST	Consenti salto ed etichetta	Il linguaggio ST non è supportato nel programma di sicurezza.

Impostazioni di progetto che influiscono sulle aree di processo e progetto sicuro in modo diverso

Ambito > sicuro e **Ambito > processo** presentano la stessa raccolta di impostazioni di programma. Tuttavia, le seguenti impostazioni sono trattate in modo diverso in ciascun ambito nel progetto M580 Safety

Gruppo	Impostazione	Descrizione
Impostazioni **Generali**:		
Impostazioni creazione	Codice ottimizzato	• Attivato per l'ambito di processo. • Disattivato e deselezionato per l'ambito sicuro.
	Gestione firma sicura	• Disattivata per l'ambito di processo. • Attivato e impostato su **Automatico** per impostazione predefinita, per l'ambito sicuro.
Diagnostica del PLC	Diagnostica dell'applicazione • Livello diagnostica dell'applicazione	• Attivato per l'ambito di processo. • Disattivato e deselezionato per l'ambito sicuro.
Impostazioni delle **Variabili**:		
–	Consenti array dinamici	Queste impostazioni sono: • Attivato per l'ambito di processo. • Disattivato e deselezionato per l'ambito sicuro. **NOTA:** Gli array dinamici non sono supportati per le variabili del programma di sicurezza.
	Disattiva controllo compatibilità dimensione array	
Impostazioni del **Programma**:		
Linguaggi	Diagramma a blocchi funzione (FBD)	Attivato per ambiti sicuro e di processo.
	Ladder (LD)	
	Grafico di funzione sequenziale (SFC)	• Attivato per l'ambito di processo. • Disattivato e deselezionato per l'ambito sicuro.
	List (IL)	

Gruppo	Impostazione	Descrizione
	Testo strutturato (ST)	
	Logica Ladder 984 (LL984)	
Linguaggi • Comune	Consenti subroutine	• Attivato per l'ambito di processo. • Disattivato e deselezionato per l'ambito sicuro. **NOTA:** Le subroutine non sono supportate nel programma di sicurezza.
	Uso di espressioni ST (LD/FBD)	• Attivato per l'ambito di processo. • Disattivato e deselezionato per l'ambito sicuro. **NOTA:** Le espressioni ST non sono supportate nel programma di sicurezza.
	Abilita conversione di tipo implicito	• Attivato per l'ambito di processo. • Disattivato e deselezionato per l'ambito sicuro. **NOTA:** Le conversioni di tipo implicito non sono supportate nel programma di sicurezza.

Appendici

Contenuto della sezione

IEC 61508 210
Oggetti di sistema 218
Riferimenti SRAC 225

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

Informazioni generali su IEC 61508 211
Policy SIL 213

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.

Policy 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. La IEC 61508 specifica 4 livelli di prestazioni di sicurezza che dipendono dal rischio o impatti causati dal processo per cui si utilizza il sistema correlato alla sicurezza. Più pericolosi sono i possibili impatti su comunità e ambiente, maggiori sono i requisiti di sicurezza per ridurre il rischio.

Descrizione valore SIL

Livello discreto (1 su 4) per la specifica dei requisiti di integrità di sicurezza delle funzioni di sicurezza che deve essere assegnato ai sistemi, dove il livello di integrità di sicurezza 4 è il più alto e il livello 1 il più basso, vedere SIL per bassa richiesta, pagina 215.

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 di esecuzione delle funzioni di sicurezza

I requisiti della funzione di sicurezza derivano 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
- Frequenza di guasto
- Copertura diagnostica
- Frazione di guasti di sicurezza
- Tolleranza di errore hardware

In base al 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 IEC 61508, il valore SIL è limitato dalla Frazione di guasti sicurezza (SFF) e dalla Tolleranza di errore hardware (HFT) del sottosistema che esegue la funzione di sicurezza. Un HFT pari a n significa che n+1 errori possono provocare una perdita della funzione di sicurezza, non è possibile accedere allo stato di sicurezza. SFF dipende dalla frequenza guasti e dalla copertura diagnostica.

La tabella seguente mostra la relazione tra SFF, HFT e SIL per sottosistemi correlati alla sicurezza complessi in base a IEC 61508-2, in cui le modalità di guasto di tutti i componenti non possono essere completamente definite:

SFF	**HFT = 0**	**HFT = 1**	**HFT = 2**
SFF ≤ 60%	-	SIL 1	SIL 2
60% < SFF ≤ 90%	SIL 1	SIL 2	SIL 3
90% < SFF ≤ 99%	SIL 2	SIL 3	SIL 4
SFF > 99%	SIL 3	SIL 4	SIL 4

Vi sono due modi per raggiungere un determinato livello di integrità di sicurezza:

- aumentando HFT fornendo ulteriori percorsi di arresto indipendenti
- aumentando SFF tramite ulteriore diagnostica

Descrizione della relazione a richiesta SIL

La IEC 61508 distingue tra modalità a bassa richiesta e modalità ad alta richiesta (o continua) di funzionamento.

Nella modalità a bassa richiesta, la frequenza della richiesta per il funzionamento fatta su un sistema correlato alla sicurezza non è maggiore di 1 all'anno e non maggiore del doppio della frequenza di 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 di richiesta di operatività fatta su un sistema correlato alla sicurezza è maggiore di 1 all'anno e maggiore del doppio della frequenza di test di tenuta. Il valore SIL per un sistema correlato alla sicurezza ad alta

richiesta è direttamente legato alla probabilità che si verifichi un guasto pericoloso all'ora oppure, 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 della sicurezza	Probabilità di guasto su richiesta
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 della sicurezza	Probabilità di guasto/ora
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

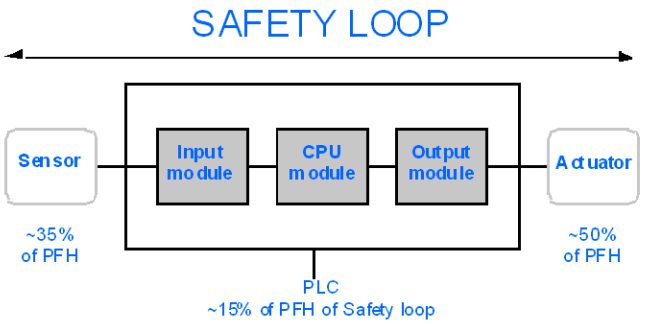
Il loop di sicurezza con il PAC M580 Safety è composto dalle seguenti 3 parti:

- Sensori

- PAC M580 Safety con alimentatore di sicurezza, CPU 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 canale nero. Questo significa che lo scambio di dati tra gli I/O e il PAC non può danneggiarsi senza alcun rilevamento da parte del ricevente.

La seguente figura mostra un loop di sicurezza tipico:



Come mostrato nella figura precedente, il contributo del PAC è solo del 10-20% in quanto la probabilità di guasto di sensori e attuatori è in genere più alta.

Un presupposto conservativo del 10% per la contribuzione del PAC di sicurezza sulla probabilità globale lascia maggiore margine per l'utente e determina le seguenti probabilità richieste di guasto per il PAC di sicurezza:

- PFD ≥ 10^{-5} - < 10^{-4} per bassa richiesta
- PFH ≥ 10^{-9} - < 10^{-8} per alta richiesta

Descrizione dell'equazione PFD

La IEC 61508 presume che metà dei guasti finisca in uno stato di sicurezza. 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 2 test di tenuta.

La probabilità di guasto/ora implica un intervallo di tempo di 1 ora. Quindi, l'equazione PFD si riduce a quella seguente:

$PFH = \lambda_{DU}$

Oggetti di sistema

Contenuto del capitolo

Bit di sistema M580 Safety 219
Parole di sistema M580 Safety 221

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 PAC M580 Safety

Le seguenti parole di sistema si applicano al PAC M580 Safety. Per una descrizione delle parole di sistema valide per PAC M580 Safety e PAC M580 non di sicurezza, vedere 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.

Parola	Funzione	Tipo
%SW4	Periodo del task SAFE definito nella configurazione. Il periodo non è modificabile dall'operatore.	L
%SW12	Indica la modalità operativa del modulo Copro: • 16#A501 = modalità di manutenzione • 16#5AFE = modalità di sicurezza Qualsiasi altro valore è interpretato come errore rilevato.	L
%SW13	Indica la modalità operativa della CPU: • 16#501A = modalità di manutenzione • 16#5AFE = modalità di sicurezza Qualsiasi altro valore è interpretato come errore rilevato.	L
%SW42	Ora corrente task SAFE. Indica il tempo di esecuzione dell'ultimo ciclo del task SAFE (in ms).	L
%SW43	Durata max. task SAFE. Indica il tempo di esecuzione del task SAFE più lungo dall'ultimo avvio a freddo (in ms).	L
%SW44	Durata min. task SAFE. Indica il tempo di esecuzione del task SAFE più breve dall'ultimo avvio a freddo (in ms).	L
%SW110	Percentuale del carico della CPU di sistema utilizzato dal sistema per servizi interni.	L
%SW111	Percentuale del carico della CPU di sistema utilizzato dal task MAST.	L
%SW112	Percentuale del carico della CPU di sistema utilizzato dal task FAST.	L
%SW113	Percentuale del carico della CPU di sistema utilizzato dal task SAFE.	L
%SW114	Percentuale del carico della CPU di sistema utilizzato dal task AUX0.	L
%SW115	Percentuale del carico della CPU di sistema utilizzato dal task AUX1.	L
%SW116	Carico totale della CPU di sistema.	L

Parola	Funzione	Tipo
%SW124	Contiene la causa dell'errore irreversibile rilevato quando il PAC 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 watchdog di sicurezza rilevato sulla CPU. • 0x5AFF: Errore di overrun watchdog di sicurezza rilevato sul coprocessore. • 0x5B01: Coprocessore non rilevato all'avvio. • 0x5AC03: Errore irreversibile CIP Safety rilevato dalla CPU. • 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*.	L
%SW125	Contiene la causa dell'errore reversibile rilevato nel PAC M580 Safety: • 0x5AC0: La configurazione CIP Safety non è corretta (rilevata dalla CPU). • 0x5AC1: La configurazione CIP Safety non è corretta (rilevata dal coprocessore). • 0x5AF3: Errore di confronto rilevato dalla CPU principale. • 0x5AFC: Errore di confronto rilevato dal coprocessore. • 0x5AFD: Errore interno rilevato dal coprocessore. • 0x5AFE: Errore di sincronizzazione rilevato tra CPU 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*.	L
%SW126 %SW127	Queste due parole di sistema contengono informazioni per uso interno Schneider Electric per consentire di analizzare nei dettagli un errore rilevato.	L
%SW128	Con firmware della CPU 3.10 o precedenti, forzare la sincronizzazione dell'ora tra ora NTP e ora Safe negli stessi moduli IO di sicurezza e il task CPU Safe: • Il cambiamento di valore da 16#1AE5 a 16#E51A forza la sincronizzazione. Consultare l'argomento *Procedura per la sincronizzazione delle impostazioni dell'ora NTP* (vedere Modicon M580, Manuale di sicurezza). • Altre sequenze e valori non forzano la sincronizzazione.	L/S
%SW142	Contiene la versione del firmware COPRO di sicurezza in 4 cifre BCD: ad esempio la versione firmware 21.42 corrisponde a %SW142 = 16#2142.	L
%SW148	Conteggio degli errori ECC (codice correzione errore) rilevati dalla CPU.	L
%SW152	Con il firmware della CPU 3.10 o precedente, stato dell'ora della CPU NTP aggiornato dal modulo di comunicazione Ethernet (ad esempio BMENOC0301/11) sul backplane dell'X Bus tramite la funzione di sincronizzazione dell'ora forzata opzionale: • 0: l'ora della CPU non è aggiornata dal modulo di comunicazione Ethernet. • 1: l'ora della CPU è aggiornata dal modulo di comunicazione Ethernet.	L

Parola	Funzione	Tipo
%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 quindi l'ID applicazione di sicurezza), l'esecuzione di un comando **Ricrea tutto** può modificare di nuovo l'ID dell'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`.	L
%SW171	Stato dei task FAST: • 0: Non esistono task FAST • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	L
%SW172	Stato del task SAFE: • 0: Non esiste alcun task SAFE • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	L
%SW173	Stato del task MAST: • 0: Non esiste alcun task MAST • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	L
%SW174	Stato del task AUX0: • 0: Nessun task AUX0 esistente • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	L

Parola	Funzione	Tipo
%SW175	Stato del task AUX1: • 0: Non esiste alcun task AUX1 • 1: Stop • 2: Run • 3: Punto di interruzione • 4: Pausa	L
%SW176	Stato di conteggio bit forzato per le variabili SAFE del programma: • Incrementa ogni volta che viene forzato un bit digitale. • Diminuisce ogni volta che viene annullata la forzatura di un bit digitale.	L

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 - Guida alla pianificazione del sistema di sicurezza* sono elencate come requisiti.

Nella tabella seguente è riportato il titolo del paragrafo in cui è possibile trovare il requisito:

Requisito del messaggio informativo di sicurezza	
Id	**In questa posizione**
PG #1	Prima di iniziare, pagina 8
PG #2	Avvio e test, pagina 9
PG #3	Definizione di un modulo non interferente, pagina 20
PG #4	Considerazioni sulla messa a terra, pagina 50
PG #5	Pianificazione dell'installazione del rack locale, Introduzione, pagina 88
PG #6	Requisiti di spazio per una CPU M580 in un rack locale principale, pagina 90
PG #7	Precauzioni per l'installazione, pagina 98
PG #8	Precauzioni per l'installazione, pagina 98
PG #9	Messa a terra, pagina 101
PG #10	Installazione di un modulo di alimentazione, Introduzione, pagina 101
PG #11	Precauzioni per l'installazione, pagina 102
PG #12	Precauzioni per l'installazione, pagina 102
PG #13	Precauzioni per l'installazione, pagina 102
PG #14	Messa a terra del modulo di alimentazione, pagina 105
PG #15	Precauzioni sulla messa a terra, pagina 106

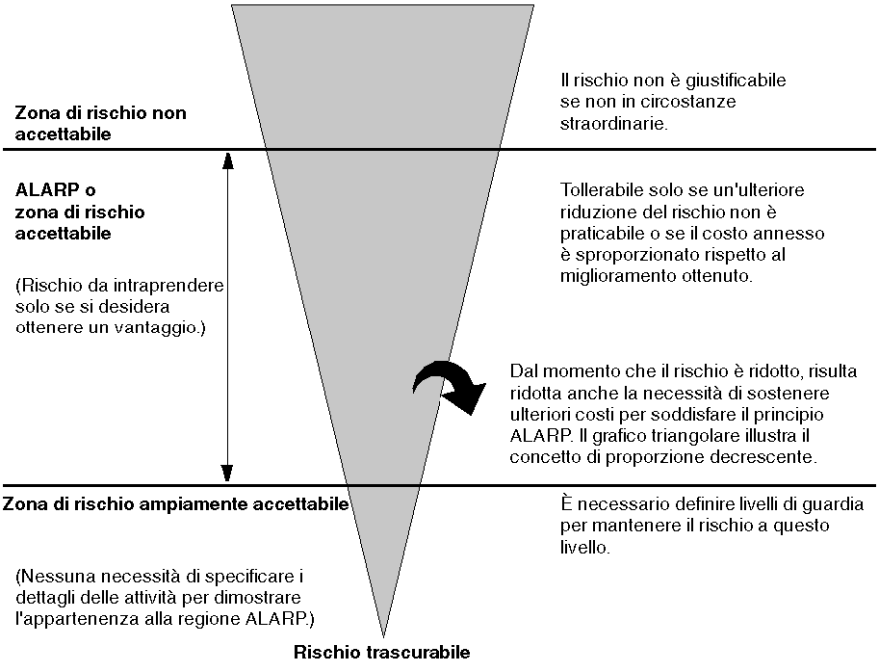
Requisito del messaggio informativo di sicurezza	
Id	**In questa posizione**
PG #16	Funzionalità della modalità manutenzione, pagina 120
PG #17	Riavvio a caldo, pagina 132
PG #18	Blocco della configurazione del modulo I/O di sicurezza, pagina 145
PG #19	Visualizzazione dei dati sulle schermate operatore, pagina 152

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.

D

DIO:

(*I/O distribuiti*) Noto anche come apparecchiatura distribuita. I DRSs utilizzano le porte DIO per collegare l'apparecchiatura distribuita.

F

FTP:

(*File Transfer Protocol*, protocollo di trasferimento file): protocollo che copia un file da un host a un altro su una rete basata su TCP/IP, ad esempio Internet. FTP utilizza un'architettura client-server e connessioni di controllo e di dati separate tra client e server.

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.)

S

SFF:

(*Safe Failure Fraction, frazione di guasti di sicurezza*)

SRAC:

(*Safety Related Application Condition*, condizione dell'applicazione di sicurezza)

Indice

61508
IEC 211
61511
IEC 211

A

alimentatore
caratteristiche prestazioni 67
alimentazione
installare 101
Allarme, morsettiera relé 72
anti-manomissione, sigillo 54
applicazione 183
protezione 164
area relativa alla sicurezza
password 172
avvio 129
avvio a caldo 132
avvio a freddo 132
dopo interruzione alimentazione 130
iniziale 130
avvio a caldo 132
avvio a freddo 132

B

blocco configurazione I/O 145
BME•58•040S, CPU
caratteristiche delle prestazioni 57
BMEP58CPROS3, coprocessore
caratteristiche delle prestazioni 57
BMXRMS004GPF 52
BMXSAI0410
caratteristiche prestazioni 80
BMXSDI1602
caratteristiche prestazioni 82
BMXSDO0802
caratteristiche prestazioni 83
BMXSRA0405
caratteristiche delle prestazioni 85

C

caratteristiche delle prestazioni
CPU e coprocessore 57
caratteristiche prestazioni
alimentatore 67
BMXSAI0410 80
BMXSDI1602 82
BMXSDO0802 83
Cavi USB BMXXCAUSB018 50
Cavi USB BMXXCAUSB045 50
Configurazione di I/O
blocco 145
Control Expert
editor sicurezza 193
gestione accesso a 190
impostazioni progetto 204
profili utente predefiniti 193
separazione dati 115
coprocessore
dimensioni 39
pannello frontale 41
CPU
dimensioni 39
installare 98
pannello frontale 39
Crea, comando
Crea modifiche 137
Ricrea tutto il progetto 137
Rinnova ID e Ricrea tutto 137
crittografia
file 164

D

Dati, comando inizializzazione
Init 148
Init Safety 148
dati, memorizzazione
protezione 181
Dati, separazione in Control Expert 115
dimensione
coprocessore 39
CPU 39
M580 Safety, alimentatore 61
Dimensioni
modulo I/O di sicurezza 74
dimenticare

password 183
Doppie, porte di rete 49

E

editor sicurezza 190
Ethernet, porte 47
  doppie porte di rete 49
  LED 49
  pin 48
  porta service 49

F

file
  crittografia 164
firma di origini SAFE 137
firma safe 137
firmware 183
  protezione 179
Frazione di guasti sicurezza (SFF) 214
Frontale, pannello
  modulo I/O di sicurezza 75
FTP
  SD, scheda di memoria 52

G

Guasto, frequenza 216

H

HFT (Tolleranza di errore hardware) 214
HMI 152

I

IEC 61508
  sicurezza funzionale 211
IEC 61511
  sicurezza funzionale per l'industria di processo 211
impostazioni progetto 204
ingresso manutenzione 123
Inizializzazione dati 148
installare
  alimentazione 101
  CPU 98
  modulo I/O 105
  rack locale 88
Installazione
  scheda di memoria 107

L

LED
  coprocessore 45
  CPU 45
  modulo I/O di sicurezza 77
LED coprocessore 45
LED della CPU 45
LED, pannello
  alimentatore 63
Livello di integrità di sicurezza (SIL) 213

M

M580 Safety, alimentatore
  dimensioni 61
  pannello frontale 62
  pannello LED 63
  RESET, funzione 63
manutenzione, modalità operativa 120
massimo dispositivi
  topologia CIP Safety 28
memorizzazione dati 183
modalità operativa di sicurezza 119
modo operativo 119
moduli
  certificato 18
  non interferenti 20
  tipo 1 non interferente 20
  tipo 2 non interferente 23
modulo I/O
  installare 105
MTBF (tempo medio tra guasti) 216

O

Operativi, stati 124

P

pannello frontale
  alimentatore 62
  coprocessor 41
  CPU 39
parole di sistema di sicurezza 221
password
  dimenticare 183
  perdita 183
  sezione 172
perdita
  password 183
PFD (Probabilità di guasto su richiesta)..... 214
PFH (Probabilità di guasto all'ora) 214
Prestazioni, caratteristiche
  BMXSRA0405 85
Probabilità di guasto all'ora (PFH) 214
Probabilità di guasto su richiesta (PFD)..... 214
Programma, unità
  protezione 177
protezione
  applicazione 164
  firmware 179
  memorizzazione dati 181
Protezione
  sezione 177
  Unità programma 177

R

Rack
  montaggio 93
rack locale
  installare 88
Rack, modulo estensione 95
RESET 63
Ridondante, porta collegamento 52

S

Safety, bit di sistema 219
scheda di memoria
  FTP 52
Scheda di memoria
  installazione 107
scheda di memoria SD
  FTP 52
scheda SD
  sportello bloccabile 55
Service, porta 49
Sezione
  protezione 177
SFF (Frazione di guasti sicurezza) 214
SFP, socket 52
Sicurezza, loop 215
Sicurezza, modulo I/O
  dimensioni 74
  LED 77
  pannello frontale 75
SIL (Livello di integrità di sicurezza 213
sistema
  parole 221
Sistema
  bit 219
spazio dei nomi di processo
  uso di 204
  utilizzo dalla schermata operatore 204

T

tabelle di animazione 149
task 133, 154
  configurazione 134
Task SAFE
  configurazione 154
Tempo medio tra guasti (MTBF) 216
Tolleranza di errore hardware (HFT) 214
topologia
  alta disponibilità 32
  apparecchiatura distribuita 35
  designazione 26
  peer-to-peer 34
  rack principale locale più estensione 31
trending, strumento 153

U

USB
  assegnazione dei pin 50
  cavi 50
  trasparenza 50
uso dello spazio dei nomi di processo 204

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.

QGH60286.08