Sistemi di controller Modicon

Sicurezza informatica

Guida utente

Traduzione delle istruzioni originali

11/2024

EIO0000002002.10

www.se.com

Informazioni di carattere legale

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

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

Sommario

Informazioni di sicurezza

Informazioni importanti

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

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

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

⚠ PERICOLO

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

⚠ AVVERTIMENTO

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

⚠ ATTENZIONE

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

AVVISO

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

Nota

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

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

Prima di iniziare

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

⚠AVVERTIMENTO

APPARECCHIATURA NON PROTETTA

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

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

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

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

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

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

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

Avviamento e verifica

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

⚠ AVVERTIMENTO

RISCHI RELATIVI AL FUNZIONAMENTO DELL'APPARECCHIATURA

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

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

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

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

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

Prima di mettere sotto tensione l'apparecchiatura:

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

Funzionamento e regolazioni

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

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

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

Informazioni sul manuale

Scopo del documento

Questa guida definisce gli elementi di sicurezza informatica che consentono di configurare un sistema meno suscettibile agli attacchi informatici.

NOTA: I termini sicurezza, sicurezza, protezione e protezione sono utilizzati in tutto il presente documento in riferimento agli argomenti relativi alla sicurezza informatica.

Nota di validità

Questo documento è stato aggiornato per EcoStruxure™ Control Expert V16.0.

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/.

Lingue disponibili per il documento

Il documento è disponibile nelle seguenti lingue:

- Cinese (EIO0000002004)
- Inglese (EIO0000001999)
- Francese (EIO0000002001)
- Tedesco (EIO0000002000)
- Italiano (EIO0000002002)
- Spagnolo (EIO0000002003)

Informazioni relative alle Sicurezza informatica

Le informazioni sulla sicurezza informatica sono disponibili sul sito Web di Schneider Electric: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

Documenti disponibili per il download nella sezione di supporto della sicurezza informatica:

Titolo della documentazione	Indirizzo pagina Web
How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations	www.se.com/ww/en/download/document/STN v2

Documenti correlati

Titolo della documentazione	Numero di codice prodotto
Modicon M580 - Guida di pianificazione del sistema	HRB65322 (CHS) HRB62666 (ENG) HRB65318 (FRE) HRB65319 (GER) RB65320 (ITA) HRB65321 (SPA)
Modicon M580 - Guida di riferimento hardware	EIO0000001583 (CHS) EIO0000001578 (ENG) EIO0000001579 (FRE) EIO0000001580 (GER) EIO0000001582 (ITA) EIO0000001581 (SPA)
Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Modulo di comunicazione, Guida di installazione e configurazione	HRB65316 (CHS) HRB62665 (ENG) HRB65311 (FRE) HRB65313 (GER) HRB65314 (ITA) HRB65315 (SPA)
Modicon M340 per Ethernet, Moduli di comunicazione e processori, Manuale utente	31007493 (CHS) 31007131 (ENG) 31007132 (FRE) 31007133 (GER) 31007494 (ITA) 31007134 (SPA)
Quantum con EcoStruxure™ Control Expert, Configurazione TCP/IP, Manuale dell'utente	31007110 (CHS) 33002467 (ENG) 33002468 (FRE) 33002469 (GER) 31008078 (ITA) 33002470 (SPA)
Premium e Atrium con EcoStruxure™ Control Expert, Moduli di rete Ethernet, Manuale dell'utente	31007102 (CHS) 35006192 (ENG) 35006193 (FRE) 35006194 (GER) 31007214 (ITA) 35006195 (SPA)
EcoStruxure™ Control Expert, Modalità operative	33003697 (CHS) 33003101 (ENG)

Titolo della documentazione	Numero di codice prodotto
	33003102 (FRE) 33003103 (GER) 33003696 (ITA) 33003104 (SPA)
Quantum con EcoStruxure™ Control Expert, Manuale di riferimento hardware	35012184 (CHS) 35010529 (ENG) 35010530 (FRE) 35010531 (GER) 35013975 (ITA) 35010532 (SPA)
Quantum con EcoStruxure™ Control Expert, 140NOC77101, Ethernet Modulo di comunicazione, Manuale dell'utente	S1A33993 (CHS) S1A33985 (ENG) S1A33986 (FRE) S1A33987 (GER) S1A33989 (ITA) S1A33988 (SPA)
Premium con EcoStruxure™ Control Expert, TSXETC101, Ethernet Modulo di comunicazione, Manuale dell'utente	S1A34008 (CHS) S1A34003 (ENG) S1A34004 (FRE) S1A34005 (GER) S1A34007 (ITA) S1A34006 (SPA)
Modicon M340, BMXNOC0401 Modulo di comunicazione Ethernet, Manuale dell'utente	S1A34014 (CHS) S1A34009 (ENG) S1A34010 (FRE) S1A34011 (GER) S1A34013 (ITA) S1A34012 (SPA)
Quantum EIO, Rete di controllo, Guida di installazione e configurazione	S1A48999 (CHS) S1A48993 (ENG) S1A48994 (FRE) S1A48995 (GER) S1A48997 (ITA) S1A48998 (SPA)
EcoStruxure™ Control Expert, Comunicazione, Libreria dei blocchi	33003683 (CHS) 33002527 (ENG) 33002528 (FRE) 33002529 (GER) 33003682 (ITA) 33002530 (SPA)
Quantum con EcoStruxure™ Control Expert, Ethernet Moduli di rete, Manuale dell'utente	31007112 (CHS) 33002479 (ENG) 33002480 (FRE) 33002481 (GER) 31007213 (ITA) 33002482 (SPA)
Modicon M580 BMECXM CANopen Moduli, Manuale dell'utente	EIO0000002134 (CHS) EIO0000002129 (ENG) EIO0000002130 (FRE) EIO0000002131 (GER)

Titolo della documentazione	Numero di codice prodotto
	EIO0000002132 (ITA) EIO0000002133 (SPA)
EcoStruxure Automation Device Maintenance, Strumento di aggiornamento firmware, Guida online	EIO0000004050 (CHS) EIO0000004033 (ENG) EIO0000004046 (GER) EIO0000004048 (FRE) EIO0000004049 (ITA) EIO0000004047 (SPA)
Momentum for EcoStruxure™ Control Expert 171CBU78090, 171CBU98090, 171CBU98091 Processors User Guide	HRB44124 (ENG)
Modicon MC80 Program Logic Controller (PLC) User Manual	EIO0000002071 (ENG)

Informazioni relative al prodotto

⚠⚠PERICOLO

PERICOLO DI SCOSSE ELETTRICHE, ESPLOSIONE O ARCO ELETTRICO

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

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

⚠AVVERTIMENTO

PERDITA DI CONTROLLO

- Eseguire un’analisi FMEA (Failure Mode and Effects Analysis) o un'analisi dei rischi equivalente dell'applicazione e applicare 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, fare riferimento a NEMA ICS 1.1 (ultima edizione), *Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control* e a NEMA ICS 7.1 (ultima edizione), *Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems* o alla pubblicazione equivalente valida nel proprio paese.

⚠AVVERTIMENTO

FUNZIONAMENTO IMPREVISTO DELL'APPARECCHIATURA

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

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

⚠ AVVERTIMENTO
FUNZIONAMENTO ANOMALO DELL'APPARECCHIATURA, PERDITA DEL CONTROLLO, PERDITA DEI DATI L'utente, e chiunque sia proprietario, progettista, utilizzatore e/o responsabile della manutenzione delle apparecchiature che utilizzi EcoStruxure Control Expert deve leggere, comprendere e seguire le istruzioni descritte nel presente documento. **Il mancato rispetto di queste istruzioni può provocare morte, gravi infortuni o danni alle apparecchiature.**

Marchi commerciali

Terminologia derivata dagli standard

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

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

Queste norme comprendono, tra le altre:

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

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

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

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

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

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

Informazioni sulla terminologia non inclusiva o non sensibile

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

Presentazione

Introduzione

Lo scopo di questo manuale è presentare soluzioni di sicurezza informatica implementate nei controller Modicon e nelle applicazioni software associate. Oltre alle soluzioni presentate in questo manuale, attenersi alle linee guida fornite nelle note tecniche di Schneider Electric sicurezza informatica disponibili sul Schneider Electric website.

Linee guida Schneider Electric

Introduzione

Il sistema PC può eseguire varie applicazioni per migliorare la sicurezza nell'ambiente di controllo. Il sistema dispone di impostazioni predefinite che richiedono una riconfigurazione per l'allineamento con le linee guida Schneider Electric per il rafforzamento dei dispositivi previsto dalla strategia protezione approfondita.

Un argomento dedicato alla sicurezza informatica è disponibile nell'area di supporto del sito Web Schneider Electric.

Approccio Defense-In-Depth

Oltre alle soluzioni presentate nel presente documento, seguire la stratregia di protezione approfondita Schneider Electric descritta nei seguenti documenti:

- **Titolo del manuale:** How can I ... Reduce Vulnerability to Cyber Attacks? System Technical Note, Cybersecurity Recommendations
- **Descrizione del collegamento al sito Web (descrizione del manuale):** How Can I Reduce Vulnerability to Cyber Attacks in PlantStruxure Architectures?

Gestione delle vulnerabilità

Le vulnerabilità segnalate dai dispositivi Schneider Electric sono documentatr nella pagina Web **Cybersecurity support** all'indirizzo http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page.

È possibile accedere a un elenco di notifiche di sicurezza facendo clic su **Security Notifications** per visualizzare: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp.

Se si verifica un incidente di sicurezza informatica o una vulnerabilità non menzionata nell'elenco fornito da Schneider Electric, è possibile segnalare questo incidente o vulnerabilità facendo clic su **Report a Vulnerability** nella pagina Web **Cybersecurity support** per aprire: https://www.se.com/ww/en/work/support/cybersecurity/report-a-vulnerability.jsp

Come proteggere l'architettura

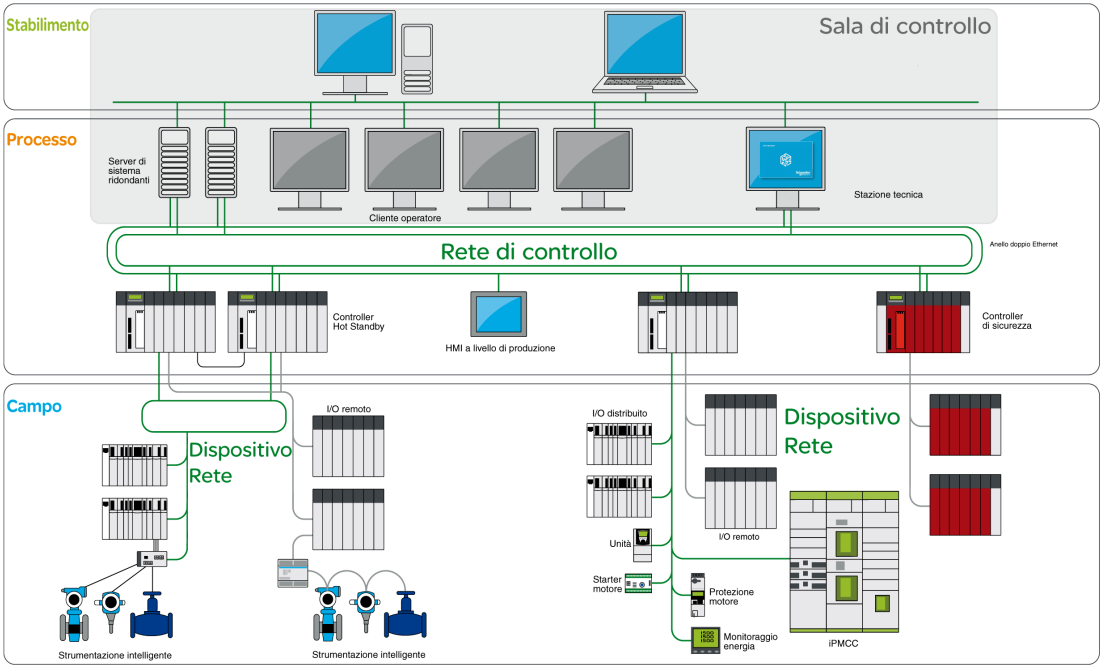
Introduzione

Questo capitolo descrive come contribuire a creare controller Modicon più sicuri.

Vista del sistema

Architettura del sistema

La seguente architettura evidenzia la necessità di disporre di un'architettura a più livelli (con una rete di controllo e una rete di dispositivi) che possa essere più protetta. Un'architettura flat (tutte le apparecchiature collegate alla stessa rete) non può essere protetta in maniera appropriata.



Comunicazione più sicura

L'apparecchiatura nella sala di controllo è più esposta agli attacchi rispetto all'apparecchiatura collegata alle rete dei dispositivi. Pertanto, implementare una comunicazione più sicura tra la sala di controllo e il controller e i dispositivi. Isolare la rete dei dispositivi dagli altri livelli di rete (come le reti di controllo e le reti remote).

Nell'architettura di sistema precedente, l'area della sala di controllo è in grigio per distinguerla dalcontroller e altri dispositivi.

Accesso più protetto alle porte USB

L'accesso fisico alle porte USB deve essere controllato.

NOTA: È possibile proteggere le porte USB solo mediante mezzi fisici (ad esempio cabinet o chiave fisica).

Accesso più protetto al collegamento Hot Standby e alla rete di dispositivi

Controllare l'accesso fisico al collegamento di Hot Standby e alla rete di dispositivi.

Test

Control Expert fornisce un simulatore per testare l'applicazione prima di metterla in servizio come parte del sistema di automazione industriale. Il simulatore è conforme a requisiti di sicurezza informatica:

- Il simulatore può essere utilizzato solo con un'applicazione aperta in Control Expert.
- L'applicazione aperta nel simulatore non può essere caricata dal simulatore al controller.

Per informazioni su come utilizzare il simulatore, consultare la guida di *EcoStruxure™ Control Expert, Simulatore controller* (https://youtu.be/RrkorSe0G8s).

Impostazione delle password in Control Expert

Utilizzare il software Control Expert per impostare password che consentano di proteggere il progetto. È possibile impostare le password seguenti:

- Password applicazione, con o senza crittografia file
- Password dell'area di sicurezza
- Password aggiornamento firmware
- Password unità programma, sezione e subroutine
- Password Web/memorizzazione dati

Password dell'applicazione

Control Expert fornisce un meccanismo di password che consente di proteggere dall'accesso non autorizzato all'applicazione. Control Expert utilizza la password quando:

- Si apre l'applicazione in Control Expert.
- Collegarsi al controller in Control Expert.

La protezione dell'applicazione tramite password impedisce modifiche, aperture o download indesiderati dei file dell'applicazione. La password è memorizzata nell'applicazione in modo codificato.

Oltre alla protezione tramite password, è possibile crittografare i file .STU, .STA e .ZEF. La funzione di crittografia dei file di Control Expert consente di impedire modifiche non autorizzate da parte di personale non qualificato e rafforza la protezione contro il furto della proprietà intellettuale e altre intenzioni dannose. L'opzione di crittografia file è protetta da un meccanismo di password.

NOTA: quando un controller viene gestito come parte di un progetto di sistema, la password dell'applicazione e la crittografia dei file vengono disattivate nell'editor Control Expert e devono essere gestite tramite Topology Manager.

Per informazioni su come impostare e utilizzare le password dell'applicazione, vedere la sezione *Protezione dell'applicazione* nel manuale *EcoStruxure™ Control Expert, Modalità operative*.

Password dell'area di sicurezza

I controller di sicurezza includono una funzione di protezione tramite password dell'area di sicurezza, accessibile dalla schermata **Proprietà** del progetto. Questa funzione consente di proteggere gli elementi del progetto situati nell'area di sicurezza del progetto di sicurezza funzionale.

Quando la funzione di protezione tramite password dell'area di sicurezza è attiva, le parti di sicurezza dell'applicazione non possono essere modificate

Per informazioni su come impostare e utilizzare le password dell'area di sicurezza, vedere la sezione *Protezione tramite password dell'area sicura* nel manuale *EcoStruxure™ Control Expert, Modalità operative*.

Password di aggiornamento firmware

La protezione del firmware tramite password consente di impedire l'accesso non autorizzato al firmware del modulo.

Per i controller M580, la gestione degli aggiornamenti del firmware dipende dalla versione del firmware del controller utilizzata per creare l'applicazione.

- Per le versioni del firmware del controller precedenti alla 4.01:
  - L'aggiornamento del firmware viene gestito tramite FTP.
  - L'accesso all'aggiornamento del firmware *può* essere protetto da password.
- Per le versioni firmware del controller 4.01 e successive:
  - L'accesso all'aggiornamento del firmware è gestito tramite HTTPS (più sicuro di FTP).
  - L'accesso all'aggiornamento del firmware *deve* essere protetto da password.
  - L'accesso alla memorizzazione dei dati e alle pagine Web sono protetti con la stessa password.

Per informazioni su come impostare e utilizzare le password del firmware, vedere la sezione *Protezione del firmware* nel manuale *EcoStruxure™ Control Expert, Modalità operative*.

Password unità programma, sezione e subroutine

La funzione di protezione subroutine, unità programma e sezione, se attivata, utilizza una password per proteggere questi elementi del programma. Questa funzione è accessibile dalla schermata Proprietà del progetto in modalità offline.

Per informazioni su come impostare e utilizzare le password di unità programma, sezione e subrouting, vedere la sezione *Protezione dell'unità di programma, della sezione e delle subroutine* nel manuale *EcoStruxure™ Control Expert, Modalità operative*.

Password Web/Memorizzazione dati

La protezione tramite password impedisce l'accesso non autorizzato all'area di memorizzazione dati della scheda di memoria SD (se nel controller è inserita una scheda valida).

Per i controller 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.
- Versione 15.1 e successive, è possibile fornire la protezione tramite password per la diagnostica Web e per l'accesso alla memorizzazione dati.

Per i controller M580, la gestione delle interfacce Web e memorizzazione dati dipende dalla versione firmware del controller utilizzata per creare l'applicazione:

- Per le versioni del firmware del controller precedenti alla 4.01:
  - La memorizzazione dei dati è gestita tramite FTP.
  - L'accesso alla memorizzazione *può* essere protetto da password.
  - L'accesso alle pagine Web non può essere protetto da password.
- Per le versioni firmware del controller 4.01 e successive:
  - La memorizzazione dati è gestita tramite HTTPS (più sicuro di FTP).
  - L'accesso alla memorizzazione dati e alle pagine Web *deve* essere protetto da password.
  - L'accesso alla memorizzazione dei dati e alle pagine Web sono protetti con la stessa password.

Per informazioni su come impostare e utilizzare le password di memorizzazione dati/Web, vedere la sezione *Protezione Web/Memorizzazione dati* nel manuale *EcoStruxure™ Control Expert, Modalità operative*.

Rafforzamento del PC

I PC della workstation situati nella sala di controllo sono esposti ad attacchi. I PC che supportano EcoStruxure™ Control Expert o EcoStruxure™ Server Expert devono essere rafforzati.

Poiché tutte queste applicazioni vengono eseguite sul sistema operativo Windows, in questo capitolo vengono fornite istruzioni su come rafforzare un PC concentrandosi sulla protezione per Windows 10.

Rafforzamento della workstation tecnica

Per proteggere la workstation, vengono utilizzate le seguenti funzioni chiave: Fare clic su un elemento per ulteriori informazioni su tale caratteristica:

- Riduzione superficie d'attacco, pagina 24
- Configurazione e controllo dei criteri di sicurezza, pagina 25
- Gestione account utente, pagina 25
- Gestione controllo accesso, pagina 26
- Protezione dei servizi di rete, pagina 27, tra cui:
  - Disabilitazione di Remote Desktop Protocol, pagina 27
  - Disabilitazione di LANMAN e NTLM, pagina 28
  - Disabilitazione delle schede di interfaccia di rete inutilizzate, pagina 28
  - Configurazione della connessione alla rete locale, pagina 29
- Attivare o installare lo strumento di protezione antivirus, pagina 29
- Gestione sistematica delle patch, pagina 30
- Gestione backup, pagina 30
- Gestione della riservatezza, pagina 31
- Gestione controllo, pagina 31

Questo argomento include anche riferimenti a diverse guide di configurazione della sicurezza informatica di Windows 10, pagina 31.

Riduzione superficie attacco

La superficie di attacco del sistema di rete è la raccolta di aree in cui un intruso può tentare di aggiungere o estrarre dati.

Per ridurre la superficie potenziale di attacco:

- Disattivare tutte le applicazioni software, i servizi e le porte di comunicazione non utilizzati.
- Disabilitare o limitare l'accesso ai dispositivi di archiviazione rimovibili (ad esempio, USB).
- Utilizzare la workstation solo per una singola funzione (ad esempio, installare OPC UA Server Expert e Control Expert su PC diversi).

Configurazione e controllo dei criteri di sicurezza

I criteri di protezione di Windows possono essere impostati tramite oggetti Criteri di gruppo.

Un Oggetto Criteri di gruppo (GPO) è un insieme di modifiche di configurazione che è possibile applicare a una workstation PC. Per ulteriori informazioni sull'Editor Criteri di gruppo locali, fare riferimento alle guide per la configurazione della protezione del Centro per la sicurezza Internet (CIS) riportate di seguito., pagina 31

È inoltre possibile definire oggetti Criteri di gruppo di dominio in Windows Active Directory.

Le configurazioni di sicurezza devono essere controllate regolarmente e automaticamente.

Gestione account utente

- **Modifica password predefinite**:

  Prima di distribuire qualsiasi nuovo asset, modificare tutte le password predefinite in valori coerenti con gli account di livello amministrativo.

  Disabilitare l'accesso automatico di Windows.

  Per una descrizione delle impostazioni della password dell'account di Windows, fare riferimento alle guide di configurazione della protezione del Centro per la sicurezza Internet (CIS) riportate di seguito., pagina 31

- **Impostazione account utente**:

  Gli account utente possono essere definiti localmente (gruppo di lavoro) in un computer autonomo o tramite un controller di dominio di Windows Active Directory che consente di centralizzare la gestione di tutti gli utenti in un sistema.

  Seguire queste linee guida quando si configurano gli account utente:

  - Utilizzare un account utente singolo standard (senza privilegi di amministratore) per eseguire le applicazioni software configurate per l'esecuzione come applicazioni autonome (ad esempio Control Expert).
  - Utilizzare un account di sistema locale per le applicazioni software configurate per l'esecuzione come servizio (ad esempio, OFS UA).
  - Utilizzare un account amministrativo dedicato per installare le applicazioni software e configurare IPSec.
  - Impostare un gestore di password per gestire le password (ad esempio, KeyPass).
  - Disabilitare tutti gli account non associati all'attività (ad esempio, gli account di debug). Vedere Controllo CIS 16.8, pagina 31.
  - Disattivare automaticamente gli account inattivi dopo un periodo di inattività impostato. Vedere Controllo CIS 16.9, pagina 31.
  - Bloccare automaticamente le sessioni della workstation dopo un periodo di inattività standard. Vedere Controllo CIS 16.11, pagina 31.

Gestione controllo accesso

È necessario controllare l'accesso a tutte le informazioni memorizzate nei sistemi con file system, condivisione di rete, attestazioni, applicazioni o database. Questi controlli applicano il **principio del privilegio minimo**, per cui solo le persone autorizzate possono accedere alle informazioni e le informazioni a cui possono accedere sono solo le informazioni di cui hanno minimo bisogno, date le loro responsabilità.

Le **autorizzazioni** sono correlate agli oggetti. A seconda degli oggetti, l'autorizzazione può essere implementata in base a:

- Oggetti di Windows Active Directory.
- Accesso ai file NTFS tramite l'elenco di controllo di accesso discrezionale (DACL, Discretionary Access Control List).
- Autorizzazioni cartella condivisa.
- Servizio Registro di sistema remoto (attivazione/disattivazione).

I **privilegi** sono diritti utente non legati a un oggetto, ma specifici del computer. Possono essere gestiti tramite le impostazioni di Criteri di gruppo, ad esempio le impostazioni "Accesso agli archivi rimovibili" nell'editor Criteri gruppo locale possono limitare l'accesso all'archiviazione dei dispositivi USB (lettura o scrittura).

Servizi di rete sicuri

Disinstallare o disattivare i servizi di rete non necessari o inutilizzati.

È possibile disattivare un servizio in diversi modi (Strumento servizi, Modello protezione, Oggetto Criteri di gruppo, PowerShell, SC.exe).

Utilizzare Windows Firewall con una regola di negazione predefinita che riduca tutto il traffico tranne i servizi e le porte esplicitamente consentiti.

- **Utilizzo del firewall**:

  Windows Firewall è necessario per la configurazione IPSEC in Windows 10. Nelle versioni recenti dei sistemi operativi Windows, incluso Windows 10, il firewall è attivato per impostazione predefinita. Per ulteriori informazioni sulle impostazioni di Windows Firewall, consultare le guide per la configurazione della sicurezza del Centro per la sicurezza Internet (CIS) a cui si fa riferimento di seguito.

- **Strumento Server Manager**:

  Server Manager consente di visualizzare tutte le dipendenze di una funzionalità in modo da poter determinare se è consigliabile rimuoverla da un server Windows.

  È possibile selezionare i ruoli del server, ad esempio Server Web (IIS), Server DNS e così via.

  È possibile selezionare le funzionalità server, ad esempio BitLocker, .NET Framework e così via.

- **Internet Information Server (IIS) - Sicurezza server Web**:

  Usare un'installazione minima della versione più recente.

  Configurare il controllo di accesso IIS (TLS e autenticazione utente).

  Abilitare la registrazione e verificare i registri per le firme di hacking.

  Ulteriori dettagli sulle impostazioni IIS sono disponibili nel documento di riferimento CIS (vedere il collegamento seguente)., pagina 31

- **Disabilitazione di SMBv1**:

  Server Message Block versione 1 (SMBv1) è un protocollo utilizzato per la condivisione dei servizi (come stampa, file e comunicazione) tra PC su una rete. È stato dimostrato che SMBv1 presenta una vulnerabilità che consente l'esecuzione del codice remoto sul PC host.

  È possibile disattivare SMBv1 per ridurre al minimo le vulnerabilità.

Disabilitazione di Remote Desktop Protocol

Le linee guida dell'approccio di difesa in profondità (Defense-in-Depth, DiD) di Schneider Electric includono la disattivazione del protocollo RDP (Remote Desktop Protocol) a meno

che l'applicazione non richieda RDP. La procedura seguente descrive come disattivare il protocollo:

Passo	Azione
1	In Windows 10, disabilitare RDP tramite **Computer > Proprietà sistema > Impostazioni di sistema avanzate**.
2	Nella scheda **Remoto**, deselezionare la casella di controllo **Consenti connessioni di Assistenza remota al computer**.
3	Selezionare la casella di controllo **Non consentire la connessione al computer**.

Disabilitazione di LANMAN e NTLM

Disattivare il protocollo Microsoft LAN Manager (LANMAN) e il suo successore NT LAN Manager (NTLM) per ridurre al minimo le vulnerabilità.

La procedura seguente descrive come disattivare LANMAN e NTLM in un sistema Windows 10:

Passo	Azione
1	In una finestra di comando, eseguire `secpol.msc` per aprire la finestra **Criteri di sicurezza locali**.
2	Aprire **Impostazioni di protezione > Criteri locali > Opzioni di sicurezza**.
3	Selezionare **Invia solo risposta NTLMv2. Rifiutare LM e NTLM** nel campo **Sicurezza di rete: livello di autenticazione di LAN Manager**.
4	Selezionare la casella di controllo **Sicurezza di rete: non memorizzare il valore hash di LAN Manager al prossimo cambio di password**.
5	In una finestra di comando, immettere `gpupdate` per confermare il criterio di sicurezza modificato.

Disabilitazione delle schede di interfaccia di rete inutilizzate

Disattivare le schede di interfaccia di rete non richieste dall'applicazione. Ad esempio, se il sistema è dotato di 2 schede e l'applicazione ne utilizza solo una, verificare che l'altra scheda di rete (Connessione alla rete locale, LAN 2) sia disattivata.

Per disattivare una scheda di rete in Windows 10:

Passo	Azione
1	Aprire **Pannello di controllo > Rete e Internet > Centro connessioni di rete e condivisione > Modifica impostazioni scheda**.
2	Fare clic con il pulsante destro del mouse sulla connessione non utilizzata. Selezionare **Disabilita**.

Configurazione della connessione alla rete locale

Diverse impostazioni di rete di Windows forniscono una protezione avanzata in linea con l'approccio di difesa in profondità (DID).

Nei sistemi Windows 10, accedere a queste impostazioni aprendo **Pannello di controllo > Rete e Internet > Centro connessioni di rete e condivisione > Modifica impostazioni scheda > Connessione alla rete locale (x).**

Questo elenco è un esempio delle modifiche alla configurazione che possono essere apportate nel sistema dalla schermata **Proprietà connessione alla rete locale (LAN):**:

- Disattivare tutti gli stack IPv6 sulle rispettive schede di rete.
- Deselezionare tutte le voci delle **Proprietà connessione alla rete locale (LAN)** tranne **Utilità di pianificazione pacchetti QoS** e **Protocollo Internet versione 4**.
- Nella scheda **Wins** nelle **Impostazioni avanzate TCP/IP**, deselezionare le caselle di controllo **Attiva LMHOSTS** e **Disattiva NetBIOS su TCP/IP**.
- Attivare **Condivisione di file e stampanti per rete Microsoft**.

Le linee guida di Schneider Electric per una difesa approfondita includono anche quanto segue:

- Definire solo indirizzi IPv4, maschere di sottorete e gateway statici.
- Non utilizzare DHCP o DNS nella sala di controllo.

Abilitazione o installazione di strumenti di protezione antivirus

È possibile migliorare la risposta del sistema contro virus e codice dannoso utilizzando gli strumenti incorporati in Windows 10. Se necessario, è anche possibile installare un software antivirus aggiuntivo.

Le edizioni Enterprise di Windows 10 includono *Windows Defender Advanced Threat Protection*, una piattaforma di sicurezza che monitora gli endpoint, ad esempio i PC Windows 10 che utilizzano sensori comportamentali. La tecnologia Microsoft *SmartScreen* è un'altra funzionalità integrata che analizza, scarica e blocca l'accesso a siti Web e download noti per essere dannosi.

Ulteriori informazioni sulle impostazioni di *Windows Defender* sono disponibili nel documento Centro per la sicurezza Internet (CIS) a cui si fa riferimento di seguito, tra cui:

- Accertarsi che il software antimalware dell'organizzazione aggiorni regolarmente il motore di scansione e il database delle firme (CIS Control 8.2).
- Configurare la scansione antimalware dei supporti rimovibili: USB (vedere Controllo CIS 8.4)., pagina 31
- Configurare i dispositivi in modo che non eseguano automaticamente il contenuto da un supporto rimovibile: USB (vedere Controllo CIS 8.5)., pagina 31

Gestione sistematica delle patch

Installare sempre la versione stabile più recente di tutti gli aggiornamenti relativi alla sicurezza del sistema operativo, delle applicazioni (inclusi browser Web e client di posta elettronica) e dei driver.

Abilitare l'aggiornamento automatico in Windows 10.

Per ulteriori informazioni, vedere il documento del Centro per la sicurezza Internet (CIS) indicato di seguito., pagina 31

Gestione backup

Assicurarsi che:

- Tutti i dati di sistema vengono salvati automaticamente e regolarmente (vedere Controllo CIS 10.1)., pagina 31
- Il backup dei sistemi chiave dell'organizzazione viene eseguito come un sistema completo, tramite processi quali l'imaging, per consentire il ripristino rapido di un intero sistema. (Vedere Controllo CIS 10.2)., pagina 31
- I backup vengono protetti in modo appropriato tramite la sicurezza fisica o la crittografia quando vengono archiviati e anche quando vengono spostati in rete. Ciò comprende backup remoti e servizi cloud. (Vedere Controllo CIS 10.4)., pagina 31
- Tutti i backup dispongono di almeno una destinazione di backup offline (non accessibile tramite una connessione di rete) (Vedere Controllo CIS 10.5), pagina 31.

È possibile:

- Utilizzare *Cronologia file* e altri strumenti gratuiti disponibili in Windows 10 per creare backup di file.
- Creare un'unità di ripristino per ripristinare il sistema da un backup dell'immagine.
- Utilizzare un servizio di sincronizzazione e condivisione dello storage per inserire i backup nel cloud, ad esempio *OneDrive*, *Dropbox* oppure *Google Drive*.

Ulteriori informazioni sulla cronologia file di Windows, sulle impostazioni di backup/ripristino sono disponibili nel documento CIS a cui si fa riferimento di seguito.

Gestione della riservatezza

Rimuovere dalla rete i dati sensibili o i sistemi a cui l'organizzazione non accede regolarmente. Questi sistemi possono essere utilizzati come sistemi autonomi (scollegati dalla rete) della business unit che occasionalmente deve utilizzarli, oppure possono essere completamente virtualizzati e disattivati fino a quando necessario. Vedere il documento CIS a cui si fa riferimento di seguito.(Vedere Controllo CIS 13.2)., pagina 31

Attivare la crittografia del disco con *Bitlocker*. Ulteriori dettagli sulle impostazioni di *Bitlocker* sono disponibili nel documento CIS a cui si fa riferimento di seguito.

Gestione controllo

Verificare che la registrazione della protezione locale sia stata configurata sugli host Windows. Per informazioni dettagliate sulla configurazione dei criteri di controllo, vedere il documento CIS a cui si fa riferimento di seguito., pagina 31

Guide alla configurazione della Sicurezza informatica di Windows 10

Verificare di utilizzare Windows 10 con le impostazioni di Sicurezza informatica per utilizzare le guide di configurazione di Windows, tra cui:

- Guide alla configurazione della sicurezza dal Centro per la sicurezza Internet - CIS

  https://www.cisecurity.org/press-release/cis-controls-microsoft-windows-10-cyber-hygiene-guide/

  - Livello IG1:

    https://www.cisecurity.org/cis-benchmarks/

    https://www.cisecurity.org/benchmark/microsoft_windows_desktop/

    https://www.cisecurity.org/benchmark/microsoft_iis/

- Linee guida per la configurazione della sicurezza sviluppate dal Dipartimento della Difesa degli Stati Uniti (DISA STIG)

  https://www.stigviewer.com/stig/windows_10/2020-06-15/

Il documento "CIS benchmark" e "STIG Windows 10 Security Technical Implementation Guide" propongono profili opzionali. La scelta di un profilo dipende dalla criticità delle applicazioni eseguite su Windows.

Disattivazione dei servizi di comunicazione integrati non utilizzati

Servizi di comunicazione integrati

I servizi di comunicazione integrati sono servizi basati su IP utilizzati in modalità server su un prodotto integrato (ad esempio HTTP o FTP).

Disattivare servizi inutilizzati

Per ridurre i rischi di attacco, disattivare qualsiasi servizio integrato inutilizzato, ad esempio HTTP e FTP, per chiudere le potenziali porte di comunicazione.

Disattivare i servizi Ethernet in Control Expert

È possibile attivare/disattivare i servizi Ethernet che utilizzano le schede Ethernet in control Expert. La descrizione delle schede è fornita per ciascuno dei seguenti sistemi:

- Modicon M340, pagina 132
- Modicon M580, pagina 133
- Modicon Quantum, pagina 133
- Modicon X80 modules, pagina 135
- Modicon Premium/Atrium, pagina 137
- Modicon Momentum MDI, pagina 139
- Modicon MC80, pagina 139

Impostare i parametri delle schede Ethernet prima di scaricare l'applicazione nel controller.

Le impostazioni predefinite (livello di sicurezza massimo) riducono lle funzionalità di comunicazione. Se è necessario utilizzare i servizi, devono essere riattivate.

NOTA: Su alcuni prodotti, il blocco funzione `ETH_PORT_CTRL (see EcoStruxure™ Control Expert, Communication, Block Library)` consente di disattivare un servizio attivato dopo la configurazione nell'applicazione Control Expert. Il servizio può essere riattivato utilizzando lo stesso blocco funzione.

Limitazione del flusso di dati dalla rete di controllo (controllo di accesso)

Flusso di dati dalla rete di controllo

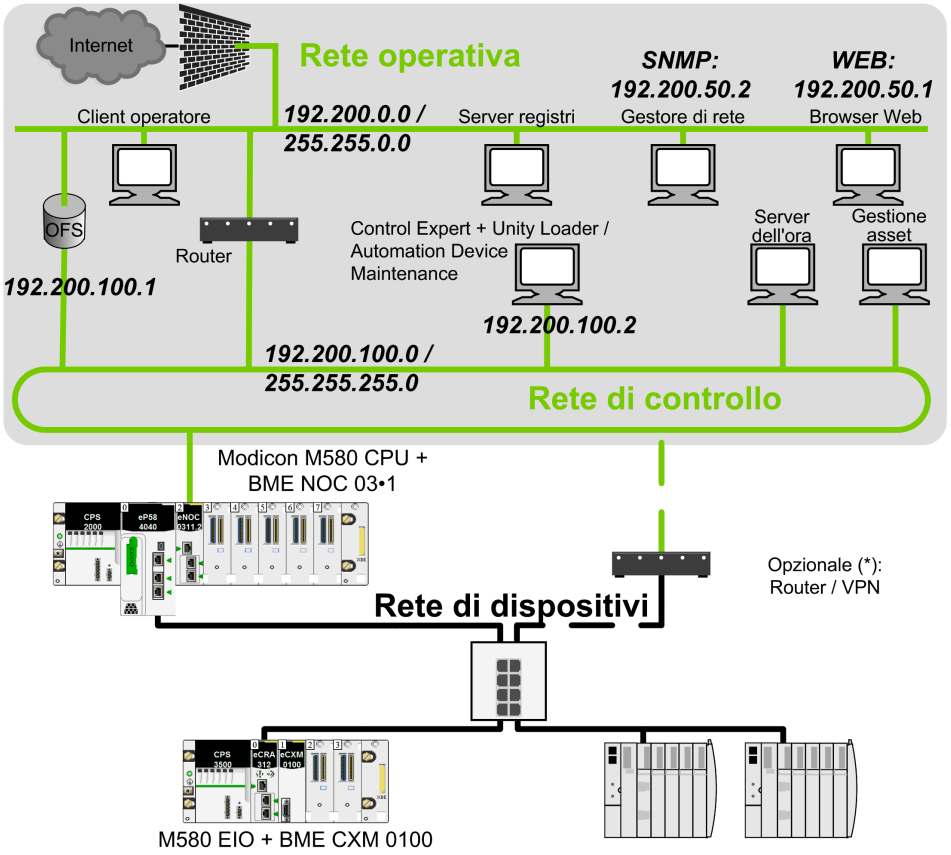
Il flusso di dati dalla rete di controllo è un flusso dati basato su IP inizializzato sulla rete di controllo.

Descrizione

Per controllare l'accesso ai server di comunicazione in un prodotto integrato, la gestione del controllo di accesso limita il flusso di dati basato su IP dalla rete di controllo a una sorgente autorizzata o a un sottogruppo di indirizzi IP .

Esempio di architettura

La seguente figura mostra il ruolo e l'impatto delle impostazioni del controllo di accesso. Il controllo di accesso gestisce il flusso dati Ethernet dai dispositivi che comunicano sul funzionamento e le reti di controllo (posizionate nell'area in grigio).



(*) Alcuni servizi richiedono l'accesso alla rete di dispositivi (ad esempio: aggiornamento del firmware, all'indicazione dell'ora di origine). In tali casi, un router/VPN opzionale consente di proteggere il controllo di accesso.

Impostazione degli indirizzi autorizzati nell'esempio di architettura.

Obiettivi del controllo d'accesso:

- Qualsiasi apparecchiatura collegata alla rete operativa (indirizzo IP = 192.200.x.x) può accedere al server Web del controller.
- Qualsiasi apparecchiatura collegata alla rete di controllo (indirizzo IP = 192.200.100.x) può comunicare con il controller con Modbus TCP e può accedere al server Web.

Per limitare il flusso di dati, nell'esempio precedente di architettura il servizio e l'indirizzo autorizzati sono impostati come segue nella tabella di controllo di accesso EcoStruxure Control Expert:

Sorgente	**Indirizzo IP**	**Subnet**	**Subnet mask**	**FTP**	**TFTP**	**HTTP / HTTPS**	**Port502**	**EIP**	**SNMP**
Gestore di rete	192.200.50.2	No	–	–	–	–	–	–	+
Rete operativa	192.200.0.0	Sì	255.255.0.0	–	–	+	–	–	–
Automation Device Maintenance	192.200.100-.2	No	–	+ [1]	–	– [2]	+	–	–
Rete di controllo	192.200.100-.0	Sì	255.255.255-.0	–	–	–	+	–	–

+ Selezionato

- Non selezionato o nessun contenuto

[1] Per versioni firmware M580 uguali o superiori a v4.10, FTP non è selezionato.

[2] Per versioni firmware M580 uguali o superiori a v4.10, è selezionato HTTP/HTTPS.

Descrizione delle impostazioni

Viene impostato un indirizzo autorizzato per i dispositivi autorizzati a comunicare con il controller tramite Modbus TCP o EtherNet/IP.

Spiegazione delle impostazioni dei servizi per ogni indirizzo IP nell'esempio precedente:

192.200.50.2 (SNMP)	Impostazione per autorizzare l'accesso dal gestore di rete utilizzando SNMP.
192.200.0.0 (HTTP/HTTPS)	La subnet della rete operativa è impostata per autorizzare tutti i browser Web collegati alla rete operativa ad accedere al browser Web del controller.
192.200.100.2 (FTP) 1)	Impostato per autorizzare l'accesso da Automation Device Maintenance con FTP.
192.200.100.0 (Port502)	La subnet della rete di controllo è impostata per autorizzare tutte le apparecchiature collegate alla rete di controllo (OFS, Control Expert, Automation Device Maintenance) per accedere al controller tramite Port502 Modbus.
1) Per versioni firmware M580 uguali o superiori a v4.10, FTP non è utilizzato. Utilizzare invece HTTP/HTTPS.	

NOTA: L'analisi dell'elenco di accesso esamina ogni voce dell'elenco del controllo di accesso. Se viene trovata una corrispondenza corretta (indirizzo IP + servizio autorizzato), tutte le altre voci verranno ignorate.

Nella schermata **Sicurezza** di EcoStruxure Control Expert per una sottorete dedicata, immettere le regole specifiche prima della regola della sottorete. Ad esempio: Per assegnare una specifica autorizzazione SNMP al dispositivo 192.200.50.2, immettere la regola prima della regola di sottorete globale 192.200.0.0/255.255.0.0 che consente l'accesso HTTP a tutti i dispositivi della sottorete.

Configurazione della comunicazione crittografata

Introduzione

L'obiettivo della comunicazione crittografata è proteggere i canali di comunicazione che consentono l'accesso remoto alle risorse critiche del sistema (ad esempio applicazione Modicon M580 PAC integrata, firmware). IPsec (Internet Protocol Security) è uno standard aperto definito da IETF per consentire comunicazioni protette e private su reti IP fornite mediante una combinazione di meccanismi di crittografia e di sicurezza del protocollo. L'implementazione della protezione IPsec include l'anti-replay, il controllo di integrità dei messaggi e l'autenticazione dell'origine dei messaggi.

IPsec è supportato su Microsoft Windows versioni 7 e 10. È avviato dal sistema operativo del PC.

Descrizione

La funzione IPsec consente di proteggere:

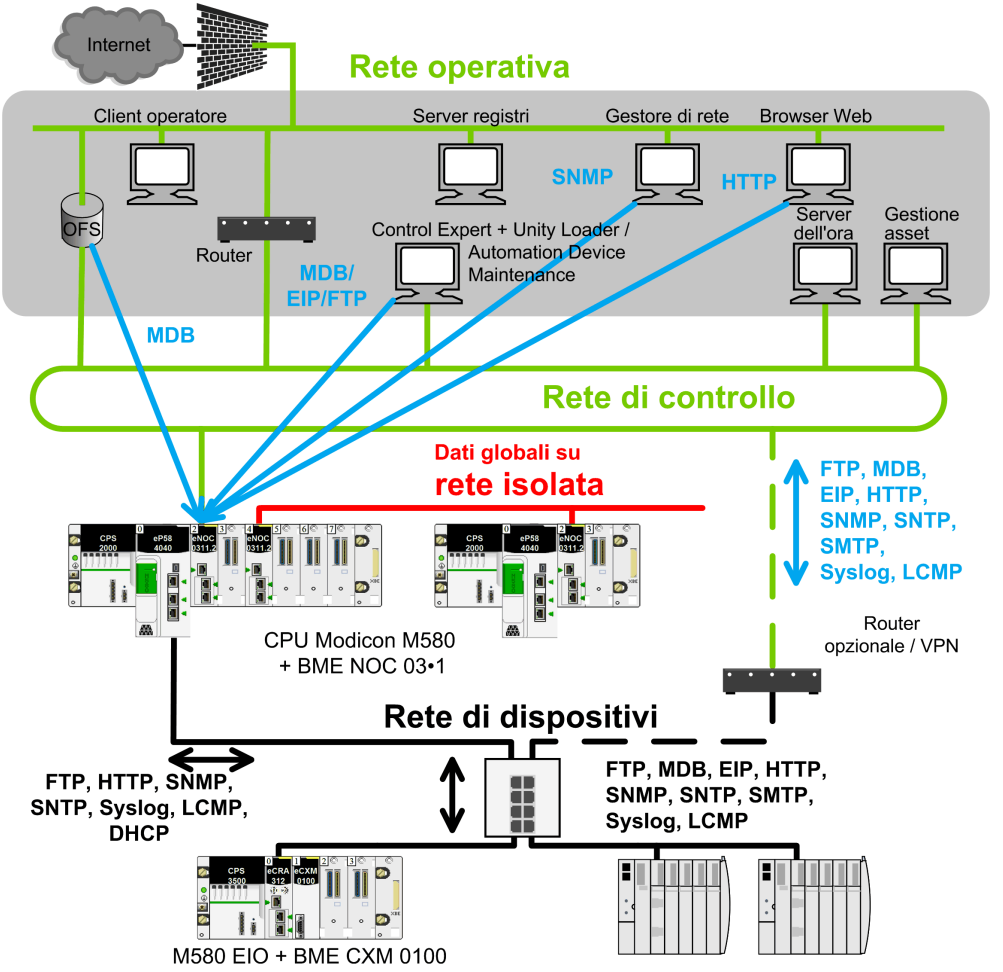
- L’accesso Modbus della sala di controllo al controller tramite moduli BMENOC0301 and BMENOC0311.
- L'accesso della sala di controllo ai servizi di comunicazione in esecuzione all'interno dei moduli BMENOC0301 and BMENOC0311 in modalità server (Modbus, EtherNet/IP, HTTP, FTP, SNMP).

  NOTA: IPsec consente di proteggere i servizi in esecuzione in modalità server nel controller. I servizi client sicuri avviati dal PAC Modicon M580 non rientrano nell'ambito di questo manuale.

Connessione wireless: se si utilizza un modulo wireless PMXNOW0300 per configurare una connessione wireless, configurare tale modulo con le impostazioni di sicurezza massime disponibili (WPA2-PSK).

Esempio di architettura

La figura seguente illustra, attraverso un esempio, i vari protocolli o servizi messi in atto in una comunicazione crittografata dalla sala di controllo a un controller Modicon M580.



Comunicazione crittografata (IPsec).

Comunicazione non IPsec.

Flusso di dati con funzionalità di comunicazione crittografata

Per facilitare le comunicazioni quando IPsec è attivato, usare le seguenti funzioni:

Funzione Ethernet	Sicurezza del flusso dati
Server EIP classe 3	Questi servizi sono supportati tramite connessioni crittografate.
Server FTP, server TFTP	
HTTP	
ICMP	
Server Modbus (porta 502)	
ARP	Questi servizi sono supportati tramite connessioni crittografate e non crittografate. **NOTA:** Questo traffico bypassa la gestione del protocollo IPsec nel BMENOC e pertanto non utilizza IPsec.
LLDP	
Protocollo di controllo loop	
Scanner Modbus	
RSTP	
DHCP, BootP client	Questi servizi non sono supportati quando è abilitato IPSec. **NOTA:** Prima dell'avvio di IKE/IPsec dal peer (PC), questo traffico non è protetto da IPSec. Dopo aver stabilito IKE/IPSec, questo traffico è crittografato da IPsec. Il protocollo potrebbe essere supportato, ma solo se il destinatario del pacchetto è un PC con IPSec configurato e abilitato.
DHCP, BootP server	
EIP classe 1, TCP (inoltro aperto)	
EIP classe 1, UDP (scambio dati)	
Client Modbus	
Client NTP	
Agente SNMP	
Trap SNMP	
Client Syslog (UDP)	

NOTA:

- IPsec è una protezione OSI di livello 3. I protocolli OSI di livello 2 (ARP, RSTP, LLDP, protocollo di controllo loop) non sono protetti da IPsec.
- Il flusso di comunicazione dei **Dati globali** (quando si usano i moduli BMXNGD0100) non può essere protetto da IPsec. Usare una configurazione di questo tipo su una rete isolata.

Limitazioni

Limitazioni IPsec nell'architettura: i moduli BMENOC0301 and BMENOC0311 non supportano l'inoltro IP alla rete di dispositivi.

Se è necessaria la trasparenza tra la rete di controllo e la rete dei dispositivi, è necessario un router esterno/vpn per assicurare una comunicazione crittografata tra la rete di controllo e la rete dei dispositivi (come mostrato nella figura di esempio d'architettura, pagina 38 precedente).

Per eseguire le seguenti operazioni dalla rete di controllo, è richiesta la trasparenza:

- Aggiornare il firmware di un controller M580 da Automation Device Maintenance tramite il servizio HTTPS.
- Eseguire una diagnostica di rete di un controller M580 da uno strumento di gestione della rete tramite servizio SNMP.
- Diagnostica di un controller M580 da un DTM tramite servizio EIP.
- Diagnostica di un controller M580 da un browser Web tramite servizio HTTP.
- Registrare gli eventi di sicurezza informatica del controller M580 in un server syslog tramite servizio syslog.
- Sincronizzare l'ora del controller M580 ottenuta da un server dell'ora globale tramite il servizio NTP.

Impostazione della comunicazione IPsec nell'architettura di sistema

Per impostare la comunicazione IPsec procedere come segue:

- Nella sala di controllo, identificare le applicazioni client autorizzate che devono comunicare con il sistema Modicon M580 PAC che utilizza Modbus (Control Expert, Automation Device Maintenance, OFS, applicazioni per i clienti come SGBackup, ...).

  Configurare IPsec su tutti i PC che supportano queste applicazioni autorizzate.
- Nella sala di controllo, identificare le applicazioni client autorizzate che devono comunicare con moduli BMENOC0301 and BMENOC0311 configurati nel rack locale (Control Expert DTM, Automation Device Maintenance, gestore SNMP, browser Web, designer Web per moduli FactoryCast BMENOC0301 and BMENOC0311).

  Configurare IPsec su tutti i PC che supportano queste applicazioni autorizzate.

- Incorporare i moduli BMENOC0301 and BMENOC0311 con funzione IPsec sul backplane di ogni sistema Modicon M580 PAC collegato alla rete di controllo.

  Per configurare la funzione IPsec sui moduli BMENOC0301 and BMENOC0311, procedere in 2 fasi:

  - Attivare la funzione IPsec.
  - Configurare una chiave precondivisa. Una chiave precondivisa è un codice segreto che consente a due dispositivi di effettuare un'autenticazione reciproca.

    NOTA: poiché IPsec è basato sul codice segreto condiviso, questo codice assume un ruolo fondamentale nelle procedure di sicurezza e deve essere gestito dall'amministratore della sicurezza. Per aumentare la sicurezza della chiave precondivisa, utilizzare uno strumento esterno come KeePass, pagina 41 per generare una stringa di caratteri appropriata.

La configurazione dei moduli BMENOC0301 and BMENOC0311 viene eseguita con Control Expert. Per proteggere questa configurazione, il primo download può essere effettuato in modo ottimale tramite una connessione punto a punto, ad esempio la porta USB. Successivamente, i download futuri possono essere eseguiti tramite Ethernet con una funzione IPsec, supponendo che IPsec sia attivato.

Ogni PC che supporta IPsec deve soddisfare i seguenti requisiti per la configurazione IPsec:

- Utilizzare il SO Microsoft Windows 10.
- Acquisire i diritti amministratore per configurare IPsec.

  Una volta eggettuata la configurazione IPsec, impostare l'account Windows come account utente normale senza privilegi di amministratore.
- **Rafforzare la protezione del PC come spiegato nella *sezione* Rafforzamento della protezione PC**, pagina 23.

Per ulteriori informazioni sulla configurazione, vedere la sezione sezione *Configurazione delle comunicazioni di sicurezza IP* (vedere Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Modulo di comunicazione, Guida di installazione e configurazione).

Generare chiavi precondivise con la protezione più elevata

La sicurezza delle comunicazioni IPsec dipende dalla complessità del codice condiviso. Utilizzare strumenti specifici per generare chiavi precondivise della massima sicurezza.

Uno di questi strumenti è KeePass, che si può scaricare come freeware da the Internet. Scaricare e installare KeePass nel PC e avviarlo.

Configurare e utilizzare KeePass v2.34 per generare password che possono essere utilizzate come codici precondivisi:

Passo	Azione
1	Creare una nuova cartella del database delle chiavi (**File > New**),
2	Nella finestra di dialogo **Create New Password Database** specificare un nome di cartella nella casella **File Name** e salvare le modifiche.
3	Nella finestra di dialogo **Create Composite Master Key**, immettere una **Master password**. Immettere nuovamente la password nel campo della password **Repeat**.
4	Premere **OK** per aprire **Step 2** e premere di nuovo **OK**.
5	Nella nuova finestra di dialogo del database, espandere **New database**.
6	Selezionare **Network** e aggiungere una voce (**Edit > Add Entry**).
7	Nel campo **Title**, specificare un nome per il modulo (ad esempio, eNOC).
8	Nel campo **User name**, specificare un nome utente.
9	Fare clic sull'icona **Generate a password**.
10	Selezionare **Open password generator**.
11	Premere **OK** per completare i campi **Password** e **Repeat**.
12	Aprire la finestra di dialogo **Password Generation Options** (**Tools > Generate Password**).
13	Effettuare queste selezioni in **Generate using character set**: • Upper-case (A, B, C, …) • Lower-case (a, b, c, …) • Digits (0, 1, 2, …) • Minus (-) • Underline (_) • Special (!, $, %, &, …) • Brackets ([,], [, (,), <, >) **NOTA:** Questi caratteri non sono accettati per l'uso nella chiave precondivisa: • { • } • ; • #
14	Premere **OK**.
15	Fare clic con il pulsante destro del mouse sul dispositivo nella casella **Database** e scorrere fino a **Copy Password**.
16	Aprire la schermata di configurazione della protezione in Control Expert.
17	Incollare il codice nella schermata di configurazione IPsec.

Diagnosticare la comunicazione IPsec nell'architettura di sistema

Le informazioni sulla diagnostica IPsec nell'architettura di sistema sono contenute nella sezione *Configurazione delle comunicazioni crittografate IP* (vedere Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Modulo di comunicazione, Guida di installazione e configurazione).

Destinazione sicurezza CSPN

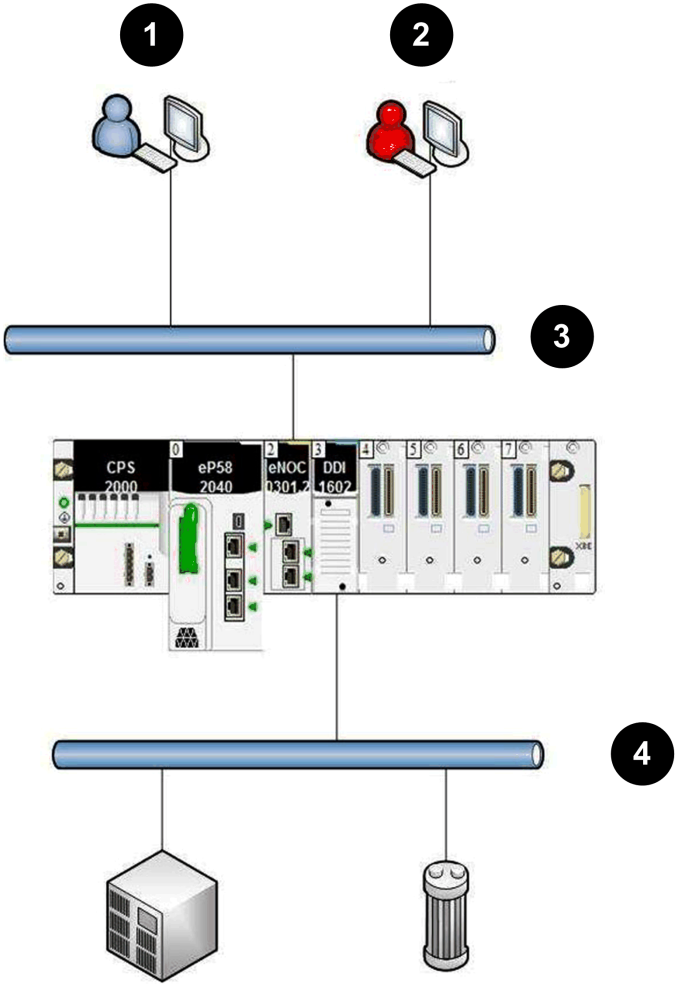
Introduzione a CSPN

CSPN (Certification de Sécurité de Premier Niveau) è una certificazione di sicurezza informatica attualmente utilizzata in Francia. Un prodotto con certificazione CSPN deve resistere a un attacco informatico condotto da due mesi/uomo di hacker esperti. Il sistema M580 è certificato CSPN. Questa sezione descrive l'ambiente, le configurazioni del PAC (controller di automazione programmabile) e i parametri che soddisfano i requisiti CSPN per garantire il massimo livello di sicurezza.

Introduzione a Modicon M580

Il sistema PAC Modicon M580 è progettato per controllare e comandare un processo industriale continuamente senza intervento umano. Per ciascun passaggio, il controller elabora i dati ricevuti attraverso gli ingressi e i sensori e invia comandi alle uscite e agli attuatori. Gli scambi con la supervisione (HMI, SCADA) vengono eseguiti con moduli di comunicazione Ethernet BMENOC0301 and BMENOC0311 sul rack locale con il controller.

L'illustrazione seguente descrive una tipica architettura di sistema M580 che può essere vulnerabile a un attacco di sicurezza:



1 operatore che utilizza EcoStruxure Control Expert

2 aggressore

3 rete di supervisione

4 rete di campo senza aggressori

Caratteristiche di M580

Il controller M580 offre le seguenti funzionalità:

Funzionalità	Descrizione
Esecuzione programma utente	Un controller M580 esegue un programma utente che elabora gli ingressi e aggiorna le uscite.
Gestione ingresso/uscita	Un controller M580 può leggere gli ingressi locali e scrivere le uscite locali. Questi ingressi/uscite possono essere digitali o analogici e consentono al controller M580 di controllare e comandare il processo industriale.
Comunicazione con la supervisione	Un controller M580 può comunicare con SCADA per ricevere comandi e trasmettere dati di processo utilizzando il protocollo Modbus.
Funzioni amministrative	Un controller M580 include funzioni amministrative fornite in EcoStruxure Control Expert, per la configurazione e la programmazione.
Funzione di registrazione remota	Un controller M580 supporta la definizione di criteri di registrazione remota; può registrare eventi amministrativi e di sicurezza.

Configurazione di M580

Una configurazione di un M580 con certificazione CSPN include i seguenti componenti:

Modulo	Firmware	Descrizione
BMEP58•0•0	versione 2.20	Il controller è conforme alle regole di sicurezza descritte nei documenti di sicurezza (vedere i presupposti).
BMENOC0301 and BMENOC0311	versione 2.11	Questo modulo Ethernet gestisce le comunicazioni crittografate con il livello superiore (software di supervisione ed engineering EcoStruxure Control Expert).

NOTA: software di programmazione EcoStruxure Control Expert, PC, altri moduli controller e componenti backplane non sono inclusi nell'ambito della certificazione.

Profili utente

Gli utenti che interagiscono con il controller per un'implementazione migliorata hanno le seguenti profili predefiniti dell'Editor di sicurezza EcoStruxure Control Expert:

Profilo utente	Descrizione
ReadOnly	Non è autorizzata alcuna modifica all'applicazione.
Operate	Sono abilitate solo l'esecuzione dell'applicazione e la modifica dei parametri.
Program	Sono abilitate tutte le funzioni.

Implementazione migliorata

Questi elementi contribuiscono a creare un ambiente sicuro per una migliore implementazione:

Elemento	Considerazioni sulla sicurezza
Documentazione di sicurezza	Tutte le istruzioni contenute nella documentazione (ad esempio, guide utente, white paper) vengono applicate prima della valutazione.
Amministratori	Gli amministratori del sistema devono essere competenti, adeguatamente formati ed affidabili.
Locali	L'accesso alla posizione del controller è limitato a persone fidate. In particolare, un aggressore non ha accesso alle porte fisiche dei controller. Dato che è possibile ottenere gratuitamente prodotti identici, l'aggressore può procurarsene uno per studiarne le vulnerabilità in qualsiasi modo.
Servizi non analizzati disabilitati	Qualsiasi servizio non coperto dalla protezione deve essere disabilitato nella configurazione o da un programma utente (come descritto nella documentazione relativa alla sicurezza).
Verifica dell'applicazione utente	L'integrità dell'applicazione EcoStruxure Control Expert è controllata dall'amministratore prima di essere caricata nel controller.
Funzione di registrazione attiva	La funzione di registrazione (logging) è attiva e i registri non sono danneggiati.
Controllo registri	Gli amministratori di sistema devono controllare con regolarità i registri locali e remoti.
Prima configurazione	La configurazione iniziale viene caricata nel controller tramite l'interfaccia USB e il controller è scollegato dalla rete.
Aggiornamento firmware	L'aggiornamento del firmware viene eseguito tramite l'interfaccia USB e il controller è scollegato dalla rete.
Password robuste	Gli amministratori di sistema devono utilizzare password robuste formate da una combinazione di lettere maiuscole, lettere minuscole, numeri e caratteri speciali

Modalità operative

Le seguenti modalità di funzionamento sono conformi con i requisiti CSPN:

- Durante la fase di messa in servizio, la configurazione iniziale del controller può essere eseguita con una stazione di engineering Control Expert collegata punto a punto **o** alla porta Ethernet **o** alla porta USB locale del controller.
- In condizioni operative normali (modalità di funzionamento, SCADA connesso alla rete controllo Ethernet), confermare che Control Expert è disconnesso.
- Apportare ulteriori modifiche alla configurazione o al programma applicativo con Control Expert collegato alla porta USB del controller.

Parametri di Sicurezza informatica

Questa tabella descrive i parametri di sicurezza informatica:

Parametro	Sezione	Guida utente
ACL attivato.	Configurazione dei servizi di sicurezza	Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Modulo di comunicazione, Guida di installazione e configurazione
IPsec attivato su BMENOC0301/0311 con sicurezza massima.	Configurazione dei servizi di sicurezza	
Applicazione sicurezza selezionata (protocolli FTP, TFTP, HTTP, DHCP/BOOTP, SNMP, EIP, NTP disattivati).	Configurazione dei servizi di sicurezza	
Registro attivato.	Registrazione dei DTM e degli eventi modulo nel server Syslog	
RUN/STOP da solo ingresso attivato.	Gestione dell'ingresso Run/Stop	Guida di riferimento hardware M580
Protezione della memoria attivata.	Protezione della memoria	
Protezione di un progetto: • Applicazione bloccata con login e password. • Protezione della sezione attivata.	Come proteggere un progetto in Control Expert	
Nessuna informazione di caricamento memorizzata nel controller.	Dati integrati nel controller	EcoStruxure™ Control Expert, Modalità operative
Password predefinita per il servizio FTP modificata.	Protezione del firmware	
Le sezioni dell'applicazione sono impostate senza l'accesso in lettura/scrittura.	Protezione delle sezioni e delle subroutine	

Asset importanti

Ambiente: Questa tabella mostra gli asset importanti per l'ambiente:

Asset	Uso appropriato
Controllo-comando del processo industriale	Il controller controlla e comanda un processo industriale mediante la lettura degli ingressi e l'invio di comandi agli attuatori. La disponibilità di queste azioni è protetta.
Flussi della workstation di engineering	I flussi tra il controller e la workstation di engineering devono essere protetti in termini di integrità, riservatezza e autenticità.

Requisiti di sicurezza per le risorse critiche per l'ambiente:

Asset	Disponibilità	Confidenzialità	Integrità	Autenticità
Controllo-comando del processo industriale	X			
Flussi della workstation di engineering		X	X	X

controller: Questa tabella mostra gli asset critici per i controller:

Asset	Descrizione di uso appropriato
Firmware	Il firmware è protetto a livello di integrità e di autenticità.
Memoria controller	La memoria del controller contiene la configurazione del controller e un programma caricato dall'utente. La sua integrità e la sua autenticità devono essere protette durante il funzionamento.
Modalità di esecuzione	L'integrità e l'autenticità della modalità di esecuzione del controller sono protette.
Confidenzialità dell'utente	Tutte le password utilizzate per eseguire l'autenticazione sono conservate con la massima confidenzialità dagli utenti appropriati.

Requisiti di sicurezza per le risorse critiche del controller:

Asset	Disponibilità	Confidenzialità	Integrità	Autenticità
Firmware			X	X
Memoria controller			X	X
Modalità di esecuzione			X	X
Confidenzialità dell'utente		X	X	

Minacce alla sicurezza

Minacce considerate dagli attacchi che controllano un dispositivo collegato alla rete di supervisione:

Tipo di minaccia	Controllo-comando del processo industriale	Flussi della workstation di engineering	Firmware	Memoria controller	Modalità di esecuzio-ne	Confi-denziali-tà dell'uten-te
Denial of Service	Di					
Alterazione firmware		I, Au				
Alterazione modalità di esecuzione					Au, I	
Alterazione del programma in memoria				I, Au		
Alterazione flusso	Di	Au, C, I				C, I

Di: disponibilità

I: integrità

C: confidenzialità

Au: autenticità

Tipo di minaccia	Descrizione
Denial of Service	L'aggressore riesce a generare un attacco Denial of Service sul controller eseguendo un'azione imprevista o esplorando una vulnerabilità (inviando una richiesta non corretta, utilizzando un file di configurazione danneggiato e così via). Il Denial of Service influisce sull'intero controller o solo su alcune funzioni.
Alterazione firmware	L'aggressore riesce a iniettare ed eseguire un firmware danneggiato sul controller. L'iniezione del codice può essere temporanea o permanente e non include esecuzioni impreviste o non autorizzate del codice. Un utente può tentare di installare tale aggiornamento sul controller con mezzi legittimi. Infine, l'aggressore riesce a modificare la versione del firmware installato sul controller senza possedere la relativa autorizzazione.
Alterazione modalità di esecuzione	L'aggressore riesce a modificare la modalità di esecuzione del controller senza essere autorizzato (ad esempio, un comando di arresto).
Alterazione della memoria	L'aggressore riesce a modificare, temporaneamente o permanentemente, il programma utente o la configurazione in esecuzione nella memoria del controller.
Alterazione flusso	L'aggressore riesce a danneggiare gli scambi fra il controller e un componente esterno senza essere scoperto. L'aggressore può eseguire attacchi come furto di credenziali, violazione del controllo di accesso o controllo-comando della mitigazione del processo industriale.

Tipo di minaccia	Denial of Service persistente	Alterazione firmware	Alterazione modalità di esecuzione	Alterazione della memoria	Alterazione flusso
Gestione ingressi non valida	X				
Archiviazione dei dati riservati				X	
Autenticazione su interfaccia amministrativa					X
Politica di controllo accessi					X
Firma firmware		X			
Integrità e autenticità della memoria del controller				X	
integrità della modalità di esecuzione del controller			X		
Comunicazioni più sicure					X

Tipo di minaccia	Descrizione
Gestione ingressi non valida	Il controller è stato sviluppato per gestire correttamente ingressi non validi, in particolare traffico di rete non valido.
Forza dei dati riservati	Il controller è stato sviluppato per gestire correttamente ingressi non validi, in particolare traffico di rete non valido. • La PSK utilizzata per creare il tunnel IPsec • La password dell'applicazione utilizzata per leggere il file .STU di Control Expert e collegare il file al controller • Password di altri servizi (come FTP)
autenticazione sull'interfaccia amministrativa	I token di sessione sono protetti da hijack e replay in quanto hanno una vita breve. L'identità e le autorizzazioni dell'account utente vengono controllate sistematicamente prima di qualsiasi azione privilegiata. In ogni configurazione è impostata una password dell'applicazione che impedisce qualsiasi modifica del controller da parte di un utente non autentico.
Criteri di controllo accesso	I criteri di controllo accesso consentono di controllare l'autenticità delle operazioni privilegiate, ovvero operazioni che possono alterare gli asset critici identificati. L'elenco di controllo accesso (ACL) viene attivato in ogni configurazione e solo gli indirizzi IP identificati possono collegarsi al controller.
Firma firmware	Durante ciascun aggiornamento del firmware, l'integrità e l'autenticità del nuovo firmware vene verificata prima dell'aggiornamento.

Tipo di minaccia	Descrizione
Integrità e autenticità della memoria del controller	La funzione di protezione della memoria è attivata in ciascuna configurazione: ciò consente di prevenire la modifica del programma in esecuzione senza un'azione in ingressi o uscite specifici. Se non è installato alcun modulo di I/O, l'interfaccia di programmazione è bloccata. Il controller garantisce l'integrità e l'autenticità del programma utente, consentendo agli utenti autorizzati di modificare il programma. La protezione della memoria consente inoltre di garantire la protezione della configurazione, che comprende vari parametri di sicurezza: • Politica di controllo accessi • RUN/STOP da solo ingresso attivato. • Protezione della memoria attivata. • Servizi attivati/disattivati (FTP, TFTP, HTTP, DHCP, SNMP, EIP, NTP). • Parametri IPsec. • Parametri Syslog.
Integrità della modalità di esecuzione del controller	Il controller garantisce che la modalità di esecuzione possa essere modificata da utenti autorizzati e autenticati. La funzione RUN/STOP da solo ingresso è attivata, in modo da impedire la possibilità di modificare lo stato di RUN/STOP tramite l'interfaccia Ethernet.
Comunicazione crittografata	Il controller supporta la comunicazione crittografata, protetta in integrità, confidenzialità e autenticità (IPsec crittografato con ESP). Il protocollo FTP è disabilitato e IPsec consente di proteggere la comunicazione Modbus tramite i moduli BMENOC0301 and BMENOC0311.

Configurare l’audit di Sicurezza informatica (Registrazione eventi)

La registrazione degli eventi e l'analisi della registrazione sono essenziali. L'analisi delle azioni esamina le azioni dell'utente a scopo di manutenzione e per individuare possibili eventi anomali che possono indicare un attacco potenziale.

Il sistema completo necessita di un sistema di registrazione robusto e affidabile distribuito su tutti i dispositivi. Gli eventi relativi alla sicurezza informatica vengono registrati localmente e inviati a un server remoto tramite il protocollo Syslog.

Nell'architettura di sistema, la registrazione degli eventi comporta due parti:

- Un server di registrazione che riceve tutti gli eventi di sicurezza informatica del sistema tramite protocollo Syslog.
- Client di registro (punti di connessione Ethernet dove gli eventi di sicurezza informatica sono monitorati: dispositivo, Control Expert).

Descrizione del servizio di registro eventi

Il ruolo di ogni client di registro evento è di:

- Rilevare e orodatare gli eventi.

  Un singolo riferimento NTP deve essere configurato nel sistema per orodatare gli eventi di sicurezza informatica.

- Inviare gli eventi rilevati a un server di registrazione eventi.

  Gli eventi sono scambiati tra il client e il server utilizzando il protocollo Syslog (specifiche RFC 5424).

  I messaggi Syslog rispettano il formato descritto nelle specifiche RFC 5424.

  Gli scambi Syslog vengono effettuati con il protocollo TCP.

  Sui dispositivi, gli eventi non vanno persi nel caso di un'interruzione temporanea della rete. Gli eventi vanno persi in caso di reset del dispositivo (tranne che per firmware controller Modicon M580 ≥ 4.0).

Valori della struttura per i tipi di evento

Valori del servizio del messaggio Syslog come indicato dalla specifica RFC 5424 associata ai tipi di evento:

Valore del servizio:	**Descrizione**
0	Messaggi Kernel
1	Messaggi a livello utente.
2	Sistema di posta elettronica.
3	Daemon di sistema.
4	Messaggi di Sicurezza / autorizzazione
5	Messaggi generati internamente da Syslog.
6	Sottosistema di stampa.
7	Nuovi sottosistemi di rete.
8	Sottosistema UUCP
9	Daemon di clock.
10	Messaggi di sicurezza / autorizzazione
11	Daemon FTP.
12	Sottosistema NTP.
13	Verifica registro.

Valore del servizio:	Descrizione
14	Avviso registro.
15	Daemon di clock.
16...23	Uso locale da 0 a 7.

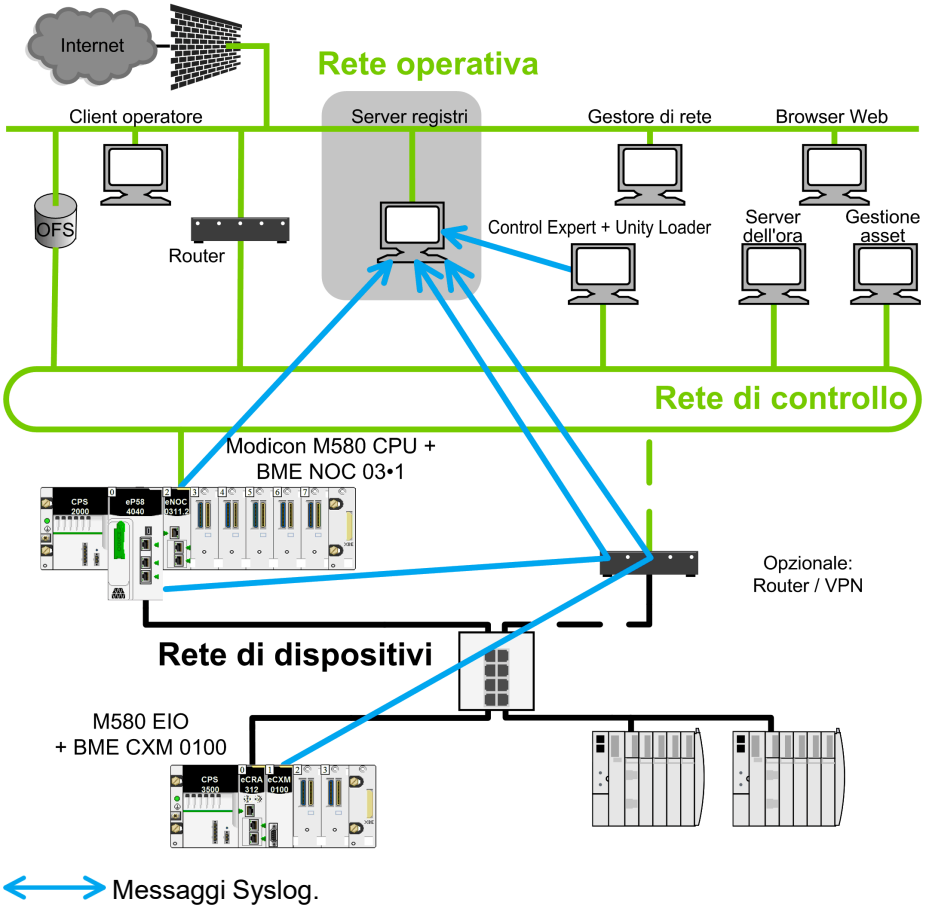
Valori di gravità per i tipi di evento

Valori di gravità del messaggio Syslog come indicato dalla specifica RFC 5424 associata ai tipi di evento:

Valore di gravità	Parola chiave	Descrizione
0	Emergency	Sistema non utilizzabile.
1	Alert	Occorre agire immediatamente.
2	Critical	Condizioni critiche.
3	Error	Condizioni di errore.
4	Warning	Condizioni di avviso.
5	Notice	Normale ma condizione significativa.
6	Informational	Messaggi informativi.
7	Debug	Messaggi di livello debug.

Esempio di architettura

La seguente figura mostra la posizione del server di registrazione in un'architettura di sistema.



Struttura messaggio evento registrato per controller Modicon M580 (versione firmware 4.10) e BMENOR2200H (versione firmware 3.01)

Campi	Descrizione
PRI	Informazioni su struttura e gravità: "FACILTY" = 10 per eventi di sicurezza informatica
VERSION	Versione della specifica del protocollo Syslog (Versione = 1 per RFC 5424).
TIMESTAMP	Il formato orodatario è emesso da RFC 3339 che raccomanda il seguente formato di data e ora Internet ISO8601: YYY-MM-DD**T**hh:mm:ss.nnn**Z** **NOTA: -**, **T**, **:**, **.**, **Z** sono caratteri obbligatori e fanno parte del campo orodatario. **T** e **Z** devono essere scritti in maiuscolo. **Z** specifica che l'ora è UTC. Descrizione del contenuto del campo dell'ora: • YYY: Anno • MM: Mese • DD: Giorno • hh: Ora • mm: Minuti • ss: Secondi • nnn: Frazione di secondo in millisecondi (0 se non disponibile)
HOSTNAME	Identifica il computer che ha inviato originariamente il messaggio Syslog: nome di dominio completo (FQDN) o indirizzo IP statico sorgente se FQDN non è supportato. Indirizzo @IP di origine = Indirizzo @IP A OPPURE Indirizzo @IP B nel caso del controller HSBY
APP-NAME	Identifica l'applicazione che ha inizializzato il messaggio Syslog. Contiene informazioni che identificano l'entità che invia il messaggio (ad esempio, sottoinsieme del riferimento commerciale).
PROCID	Nome del processo o del protocollo che ha originato il messaggio (ad esempio, Modbus, HTTPS, LocalHMI)
MSGID	Identificatore del tipo di evento. (ad esempio, CONNECTION_FAILURE_AND_BLOCK).
Informazioni evento	<ac:structured-macro ac:name="unmigrated-wiki-markup" ac:schema-version="1" ac:macro-id="30296255-e8b7-4cf1-982e-2c45b17b1f06"><ac:plain-text-body><![CDATA[**[authn@3833]**, **[authz@3833]**, **[config@3833]**, **[cred@3833], [backup@3833], [plc@3833] [system@3833]** Vedere la descrizione STRUCTURED-DATA più avanti.
MSG	Messaggio contenente il risultato specifico dell'evento (vedere Descrizioni dei messaggi del registro eventi per Control Expert, pagina 62)

- Descrizione **STRUCTURED-DATA**: informazioni obbligatorie sull'evento.
  - **[meta]**: dati strutturati obbligatori per fornire meta-informazioni sul messaggio. Dove parametro è:
    - **sequenceId**: l'identificativo dell'evento (rollover a 1 quando viene raggiunto il valore massimo 2147483647).
    - **sysUpTime**: questo valore deve essere incluso quando il componente non è in grado di ottenere l'ora di sistema (numero intero contenente il tempo in 1/100 di secondo dall'ultima reinizializzazione del sistema).

- Descrizione **STRUCTURED-DATA**: informazioni sull'evento in base alla categoria dell'evento.
  - **[authn@3833]**: dati strutturati utilizzati per gli eventi di autenticazione. Dove si trovano i parametri:
    - **itf**: l'interfaccia a cui è collegato l'utente, una porta di rete o un'interfaccia locale (hmi, usb , ...).
    - **peer**: l'FQDN o l'indirizzo IP del componente da cui l'utente è connesso, più la relativa porta (ipAddress:port), opzionale in caso di interfaccia locale
    - **user**: il nome utente (componente o umano), facoltativo se il nome utente è sconosciuto.
  - **[authz@3833]**: dati strutturati utilizzati per gli eventi di autorizzazione. Dove si trovano i parametri:
    - **user**: il nome utente (componente o umano)
    - **object**: l'accesso all'oggetto da parte dell'utente dipende dal prodotto.
    - **action**: azione eseguita sull'oggetto: Crea, Leggi, Aggiorna, Elimina (CRUD)
  - **[config@3833]**: dati strutturati utilizzati per gli eventi di configurazione. Dove si trovano i parametri:
    - **object**: il nome dell'oggetto di sicurezza da configurare (Firmware, RBAC, Criteri di sicurezza, Impostazione dispositivo, Trust Anchor, oggetti dipendenti dal prodotto)
    - **value**: versione o valore opzionale del nuovo oggetto
  - **[cred@3833]**: dati strutturati utilizzati per gli eventi di gestione delle credenziali. Dove si trovano i parametri:
    - **name**: il nome comune del certificato o il nome di accesso utente
  - **[system@3833]** dati strutturati per eventi di sistema. Dove si trovano i parametri:
    - **object**: il nome dell'oggetto di sistema che cambia (controller, modulo, selettore a rotazione, scheda SD, oggetto dipendente dal prodotto)
  - **[backup@3833]**: dati strutturati utilizzati per il backup. Dove si trovano i parametri:
    - **object**: la parte del componente di cui è stato eseguito il backup/ripristino, l'oggetto dipende dal prodotto.
  - I dati strutturati possono anche essere definiti da ogni applicazione per eventi specifici.

Struttura messaggio evento registrato per controller Modicon M580 (firmware precedente alla versione 4.10), BMENUA0100 (versioni firmware 1.10 e 2.0) e BMENOR2200H (firmware precedente alla versione 3.01)

Struttura messaggio Syslog per firmware controller Modicon M580 e BMENUA0100:

Campo	Descrizione
PRI	Informazioni sul servizio e sulla gravità (descrizione nelle tabelle seguenti).
VERSION	Versione della specifica del protocollo Syslog (Version = 1 per RFC 5424).
TIMESTAMP	Il formato orodatario è emesso da RFC 3339 che raccomanda il seguente formato di data e ora Internet ISO8601: YYY**-**MM**-**DD**T**hh**:**mm**:**ss**.**nnn**Z** **NOTA: -**, **T**, **:**, **.**, **Z** sono caratteri obbligatori e fanno parte del campo orodatario. **T** e **Z** devono essere scritti in maiuscolo. **Z** specifica che l'ora è UTC. Descrizione del contenuto del campo dell'ora: • YYY: Anno • MM: Mese • DD: Giorno • hh: Ora • mm: Minuti • ss: Secondi • nnn: Frazione di secondo in millisecondi (0 se non disponibile)
HOSTNAME	Identifica il computer che ha inviato il messaggio Syslog in origine. Nome di dominio completo (FQDN) o indirizzo IP statico di origine se FQDN non è supportato.
APP-NAME	Identifica l'applicazione che ha inizializzato il messaggio Syslog. Contiene informazioni che identificano l'entità che invia il messaggio (ad esempio, sottoinsieme del riferimento commerciale).
PROCID	Nome del processo o del protocollo che ha originato il messaggio (ad esempio, Modbus, HTTPS, LocalHMI, …) Riceve NILVALUE se non utilizzato.

Campo	Descrizione
MSGID	Identifica il tipo di messaggio a cui è associato l'evento, ad esempio HTTP, FTP, Modbus. Riceve NILVALUE se non utilizzato.
MESSAGE TEXT	Il campo include: • Indirizzo emittente: indirizzo IP dell'entità che genera il registro. • ID peer: ID peer se un peer è coinvolto nell'operazione (ad esempio, il nome utente per un'operazione di registrazione). Riceve Null se non utilizzato. • Indirizzo peer: indirizzo IP peer se un peer è coinvolto nell'operazione. Non utilizzato (null). • Tipo: Numero univoco per identificare un messaggio (vedere Descrizioni dei messaggi del registro eventi per Control Expert, pagina 62). • Commento: Stringa che descrive il messaggio (vedere Descrizione dei messaggi del registro eventi per i controller M580 (versione firmware V4.10) e BMENOR2200H (versione firmware 3.01), pagina 68).

Impostazione di un server Syslog nell'architettura di sistema.

Vari server Syslog sono disponibili per vari sistemi operativi.

NOTA: I server Syslog devono essere conformi a RFC 5424.

Esempi di provider di server Syslog:

- WinSyslog: per sistema operativo Windows.

  Collegamento: www.winsyslog.com/en/.
- Kiwi Syslog: per sistema operativo Windows.

  Collegamento: www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx.
- Splunk: Per sistemi operativi Windows e Unix.

  Collegamento: www.splunk.com/.
- Rsyslog: per sistema operativo Unix.

  Collegamento: www.rsyslog.com/.
- Syslog-ng: open source per sistema operativo Unix.

  Collegamento: www.balabit.com/network-security/syslog-ng/opensource-logging-system.
- Syslog Server: open source per sistema operativo Windows.

  Collegamento: sourceforge.net/projects/syslog-server/.

Impostazione dei client Syslog nell'architettura di sistema

La registrazione degli eventi è gestita in Control Expert per tutti i dispositivi e i Device Type Manager (DTM).

La funzione di registrazione degli eventi, indirizzo del server e numero di porta sono configurati in Control Expert come segue e questi parametri vengono inviati a ciascun client nel sistema dopo l'azione **Crea**:

Passo	Azione
1	Fare clic su **Strumenti** > **Impostazioni progetto**.
2	Fare clic su **Impostazioni progetto** > **Generale** > **Diagnostica PLC**.
3	Selezionare **Registrazione eventi** (deselezionata per impostazione predefinita). **NOTA:** un progetto con questa impostazione selezionata può essere aperto solo a partire da Unity Pro 10.0. Unity Pro è il nome precedente di Control Expert per versione 13.1 o precedenti.
4	Immettere un **Indirizzo server SYSLOG** valido e il **Numero di porta del server SYSLOG**.
5	Eseguire un'azione **Crea** dopo aver configurato questa impostazione (non è necessario selezionare **Analizza progetto**).

Diagnostica della registrazione di eventi

La tabella seguente mostra il tipo di diagnostica di registrazione eventi disponibile per vari dispositivi:

Dispositivi	Informazioni di diagnostica
Control Expert	Se si verifica un errore di comunicazione con il server Syslog, l'errore rilevato è registrato nel visualizzatore di eventi. Per attivare il visualizzatore eventi in Control Expert, selezionare la casella di controllo **Audit** nella scheda **Criteri** dell'Editor sicurezza (vedere EcoStruxure™ Control Expert, Editor sicurezza, Guida al funzionamento).
DDT dispositivo BMENOC0301 and BMENOC0311 (parametro *SERVICE_STATUS2*) DDT dispositivo controller Modicon M580 DDT dispositivo BMECXM	Sono disponibili due informazioni di diagnostica: • EVENT_LOG_STATUS: valore = 1 se il servizio di registro eventi è operativo. Valore = 0 se il servizio di registrazione eventi non è operativo. • LOG_SERVER_NOT_REACHABLE: valore = 1 se il client Syslog non riceve il riconoscimento dei messaggi TCP dal server Syslog. Valore = 0 se viene ricevuta la conferma.

Descrizioni dei messaggi del registro eventi per Control Expert

Evento registrato: Azione applicazione

La tabella seguente presenta le descrizioni dei messaggi quando l'evento registrato è: Azione applicazione.

MSG(1)	Servizio	Gravità	Descrizione
creare un nuovo progetto	10	6	Creazione di una nuova applicazione Control Expert
aprire un progetto esistente	10	6	Apertura di un'applicazione Control Expert esistente
salvare un progetto	10	6	Salvataggio dell'applicazione correntemente aperta
salvare come progetto	10	6	Salvataggio dell'applicazione correntemente aperta tramite un file diverso
importare un progetto	10	6	Importazione di un'applicazione
creare offline	10	6	Creazione applicazione in modalità offline
creare arresto online	10	6	Creazione applicazione in modalità online con controller in Stop
creare esecuzione online	10	6	Creazione dell'applicazione in modalità online controller in RUN
avviare arrestare o inizializzare il PAC	10	6	Avviare / arrestare / inizializzare il controller
Aggiornare valori di inizializzazione con i valori correnti	10	6	Aggiornare valori iniziali con i valori correnti
trasferire progetto da PAC	10	6	Caricare l'applicazione dal controller
trasferire progetto al PAC	10	6	Scaricare l'applicazione nel controller
trasferire valori dati da file a PAC	10	6	Trasferire valori dati da file a controller
ripristinare backup progetto in PAC	10	6	Ripristinare backup progetto nel controller
salvare nel backup progetto in PAC	10	6	Salvare backup progetto in controller
Imposta indirizzo	10	6	Modificare indirizzo connessione controller
Modifica opzioni	10	6	Modifiche opzioni di Control Expert
Modifica valori variabili	10	6	Modifica valore della variabile all'interno del controller

MSG(1)	Servizio	Gravità	Descrizione
Forza bit interni	10	6	Modifica valore di forzatura della variabile all'interno del controller: bit interni
Forza uscite	10	6	Modifica valore di forzatura della variabile all'interno del controller: uscite
Forza ingressi	10	6	Modifica valore di forzatura della variabile nel controller: ingressi
Gestione task	10	6	Gestione task
Modifica del periodo di ciclo del task	10	6	Modifica del periodo di ciclo del task
Eliminare messaggio nel visualizzatore diagnostica	10	6	Eliminare messaggio nel visualizzatore diagnostica
Debug eseguibile	10	6	Debug eseguibile
Sostituire variabile progetto	10	6	Sostituire variabile progetto
Creare librerie o famiglie	10	6	Creare librerie o famiglie all'interno della libreria
Eliminare librerie o famiglie	10	6	Eliminare librerie o famiglie all'interno della libreria
Inserire oggetto nella libreria	10	6	Copiare elemento (DFB/DDT) dall'applicazione nella libreria
Eliminare oggetto dalla libreria	10	6	Eliminare elemento (DFB/DDT) nella libreria
Recuperare oggetto dalla libreria	10	6	Copiare elemento (DFB/DDT/EF/EFB) dalla libreria nell'applicazione
Modificare documentazione	10	6	Modificare documentazione (stampa applicazione)
Modificare vista funzionale	10	6	Modificare vista funzionale
Modificare tabelle di animazione	10	6	Modificare tabelle di animazione
Modificare valori costanti	10	6	Modificare valori costanti
Modificare struttura programma	10	6	Modificare struttura programma
Modificare sezioni programma	10	6	Modificare sezioni programma
Modificare impostazioni progetto	10	6	Modificare impostazioni progetto
Aggiunta Rimozione variabile	10	6	Variabile creata/rimossa nell'editor dati
Modifica attributi principali variabile	10	6	Attributo variabile modificato
Modifica attributi secondari variabile	10	6	Attributo variabile modificato
Aggiunta Rimozione DDT	10	6	DDT creato/rimosso nell'Editor dati
Modifica DDT	10	6	DDT modificato nell'Editor dati

MSG(1)	Servizio	Gravità	Descrizione
Aggiunta Rimozione Tipo DFB	10	6	DFB creato/rimosso nell'Editor dati
Modifica struttura tipo DFB	10	6	Struttura DFB modificata nell'Editor dati
Modifica sezioni tipo DFB	10	6	Sezioni DFB modificate
Modifica istanza DFB	10	6	Modifica istanza DFB nell'editor dati
Modifica attributi secondari istanza DFB	10	6	Modifica attributi secondari dell'istanza DFB nell'Editor dati
Modificare configurazione	10	6	Modifica configurazione controller
Analisi IO	10	6	Sniffing I/O controller
Modificare la configurazione I/O	10	6	Modifica configurazione I/O controller
Regolare gli I/O	10	6	Regolazione configurazione I/O controller
Salvare parametro	10	6	Salvare param configurazione I/O controller dalla schermata I/O
Ripristinare parametro	10	6	Salvare param configurazione I/O controller dalla schermata I/O
Modificare schermate	10	6	Modifica schermate operatore
Modificare messaggi	10	6	Modificare messaggi
Aggiungi/Rimuovi schermate o famiglie	10	6	Schermate operatore: Famiglia/schermata aggiunta/rimossa
Spostare componente	13	6	Sposta blocco FFB
Spostare componente	13	6	Sposta contatto/bobina
Inserire componente	13	6	Inserisci blocco FFB
Inserire componente	13	6	Inserisci contatto/bobina
Eliminare componente	13	6	Elimina blocco FFB
Eliminare componente	13	6	Elimina contatto/bobina
Aggiungere variabile	13	6	Impostare parametro effettivo su blocco FFB
Aggiungere variabile	13	6	Impostare parametro effettivo su contatto/bobina
Eliminare variabile	13	6	Rimuovere parametro effettivo su blocco FFB
Eliminare variabile	13	6	Rimuovere parametro effettivo su contatto/bobina
Modificare variabile	13	6	Modificare parametro effettivo su blocco FFB

MSG(1)	Servizio	Gravità	Descrizione
Modificare variabile	13	6	Modificare parametro effettivo su contatto/ bobina
Pin collegamento	13	6	Creare un collegamento tra due pin
Scalare componente	13	6	Modificare dimensioni blocco FFB estensibile
Scalare componente	13	6	Modificare dimensioni del collegamento verticale/orizzontale
Rinominare variabile	13	6	Rinominare parametro effettivo
Eliminare riga	13	6	Eliminare una singola riga
Eliminare righe da	13	6	Eliminare più righe
Eliminare colonna	13	6	Eliminare una singola colonna
Eliminare colonne da	13	6	Eliminare più colonne
Inserire riga	13	6	Inserire una singola riga
Inserire righe da	13	6	Inserire più righe
Inserire colonna	13	6	Inserire una singola colonna
Inserire colonne da	13	6	Inserire più colonne
(1) Il contenuto MSG include la concatenazione del nome utente, il PID di Control Expert e il messaggio.			

NOTA: I campi HOSTNAME, APP-NAME, PROCID, MSGID e STRUCTURED-DATA non si applicano ai messaggi di Control Expert.

Evento registrato: Azione DTM

La tabella seguente presenta le descrizioni dei messaggi quando l'evento registrato è: Azione DTM.

MSG(1)	Servizio	Gravità	Descrizione
Download parametri nel servizio dispositivo terminato con errore	9	6	Download parametro DTM terminato con errore
Download parametri nel servizio dispositivo terminato senza errori	9	6	Download parametro DTM terminato senza errori
Caricamento parametri dal servizio dispositivo terminato con errore	9	6	Caricamento parametro DTM terminato con errore
Caricamento parametri da servizio dispositivo terminato senza errori	9	6	Caricamento parametro DTM terminato senza errori
Servizio vai online non riuscito	9	6	Connessione al DTM non stabilita

MSG(1)	Servizio	Gravità	Descrizione
Servizio vai online attivato	9	6	Connessione al DTM riuscita
Errore servizio vai offline	9	6	La connessione al DTM non è chiusa
Servizio vai offline riuscito	9	6	Connessione al DTM chiusa correttamente
Servizio FDR download parametri non riuscito	9	6	Il servizio FDR download parametri DTM non è eseguito
Servizio FDR download parametri riuscito	9	6	Servizio FDR download parametri DTM riuscito
Servizio FDR caricamento parametri non riuscito	9	6	Servizio FDR caricamento parametri DTM non eseguito
Servizio FDR caricamento parametri riuscito	9	6	Servizio FDR caricamento parametri DTM completato
Servizio download parametri in dispositivo non riuscito	9	6	Servizio download parametri in dispositivo non eseguito
Servizio download parametri in dispositivo riuscito	9	6	Servizio download parametri in dispositivo riuscito
Servizio caricamento parametri dal dispositivo non riuscito	9	6	Servizio caricamento parametri dal dispositivo non eseguito
Servizio caricamento parametri dal dispositivo riuscito	9	6	Servizio caricamento parametri dal dispositivo riuscito
Evento funzione Audit Trail	9	6	Evento funzione Audit Trail
Evento stato dispositivo Audit Trail	9	6	Evento stato dispositivo Audit Trail
Nessun messaggio di stato dispositivo	9	6	Nessun messaggio di stato dispositivo
Informazioni di stato	9	6	Informazioni di stato
Diritto di accesso: Lettura/Scrittura	9	6	Diritto di accesso: Lettura/Scrittura
Voce enumeratore	9	6	Voce enumeratore
(1) Il contenuto MSG include la concatenazione del nome utente, il PID di Control Expert e il messaggio.			

Evento registrato: Azione password

La tabella seguente presenta le descrizioni dei messaggi quando l'evento registrato è: Azione password.

MSG(1)	Servizio	Gravità	Descrizione
Sicurezza informatica - Modifica della password > Password errata	2	6	Problema durante la modifica della password dell'applicazione
Sicurezza informatica - Verifica della password > Password errata	2	6	Problema durante la verifica della password dell'applicazione
Sicurezza informatica - Verifica password sezione > Password errata	2	6	Problema durante la verifica della password della sezione
Sicurezza informatica - Password memorizzazione dati modificata	2	6	Password di "Memorizzazione dati" modificata
Sicurezza informatica - Password del firmware modificata	2	6	Password di "Download FW" modificata
Sicurezza informatica - Verifica della password > Password errata	2	6	Problema durante la verifica della password dell'applicazione
(1) Il contenuto MSG include la concatenazione del nome utente, il PID di Control Expert e il messaggio.			

Evento registrato: Configurazione SYSLOG modificata

La tabella seguente presenta le descrizioni dei messaggi quando l'evento registrato è: Configurazione SYSLOG modificata.

MSG(1)	Servizio	Gravità	Descrizione
Indirizzo SYSLOG modificato	-	-	Sicurezza informatica - Impostazione progetto Registrazione eventi modificata - Registrazione eventi, indirizzo server SYSLOG, porta o protocollo
(1) Il contenuto MSG include la concatenazione del nome utente, il PID di Control Expert e il messaggio.			

Evento registrato: Azione file

La tabella seguente presenta le descrizioni dei messaggi quando l'evento registrato è: Azione file.

MSG(1)	Servizio	Gravità	Descrizione
Il file XXXXX è stato aperto	0	6	File XXXXX aperto
Scollegamento da PAC @=XXXXXX driver= YYYYY	0	6	Controller scollegato = @XXXXXX driver = YYYYY
Chiudi applicazione XXXXXX	0	6	Chiusura applicazione XXXXXX

MSG(1)	Servizio	Gravità	Descrizione
Il progetto è stato trasferito dal PAC al PC	0	6	Trasferimento da controller a PC
(1) Il contenuto MSG include la concatenazione del nome utente, il PID di Control Expert e il messaggio.			

Descrizione dei messaggi del registro eventi per i controller M580 (versione firmware V4.10) e BMENOR2200H (versione firmware 3.01)

Questa sezione presenta le descrizioni dei messaggi del registro eventi per:

- Controller M580 con versione firmware 4.10 (abbreviato **CPU** nella colonna **Dispositivi**)
- Moduli RTU BMENOR2200H con versione firmware 3.01 (abbreviato "eNOR" nella colonna **Dispositivi**)

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
Connessione riuscita	Tutte le connessioni riuscite da un utente (umano o componente) a un componente, tramite un protocollo crittografato o un protocollo non crittografato, se consentito dalla politica di sicurezza del cliente	Accesso riuscito (server Web tramite HTTPS)	6	HTTPS	CONNECTION_SUCCESS	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*nomeutente*]"	Logon	CPU eNOR
		Accesso riuscito (aggiornamento firmware tramite HTTPS)	6	HTTPS	CONNECTION_SUCCESS	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*nomeutente*]"	Logon	CPU eNOR

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
		Accesso riuscito (OPC-UA)	6	OPC-UA	CONNECTION_SUCCESS	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfaceIP*peer=*peerFQDN:peerPort* user=*nomeutente*]"	Connessione socket	CPU
		Accesso riuscito (password applicazione Unity tramite Modbus-Umas)**Solo modalità standard**	6	MODBUS-UMAS	CONNECTION_SUCCESS	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfaceIP*peer=*peerFQDN:peerPort* user=*nomeutente*]"	Logon	CPU
		Connessione Modbus TCP riuscita (nessun utente)	6	MODBUS	CONNECTION_SUCCESS	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfaceIP*peer=*peerFQDN:peerPort* user=*nomeutente*]"	Connessione socket	CPU eNOR
		Connessione HTTP/DPWS riuscita	6	HTTP	CONNECTION_SUCCESS	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfaceIP*peer=*peerFQDN:peerPort*	Connessione socket	CPU

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
						user=*nomeutente*]"		
		Connessione TCP esplicita EIP riuscita (nessun utente)	6	EIP	CONNECTION_SUCCESS	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*nomeutente*]"	Connessione socket	CPU
		Connessione DNP3 riuscita (nessun utente)	6	DNP3	CONNECTION_SUCCESS	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer=peerFQDN:peerPort user=nomeutente]	Connessione socket	eNOR
		Connessione IEC 60870 riuscita (nessun utente)	6	IEC60870	CONNECTION_SUCCESS	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer=peerFQDN:peerPort user=nomeutente]	Connessione socket	eNOR
Problema di connessione	Tutte le connessioni non riuscite da un utente (umano o	Problema di accesso (password applicazione Unity tramite	5	MODBUSUMAS	CONNECTION_FAILURE	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* |	Password non valida	CPU

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
	componente) a un componente tramite un protocollo crittografato o un protocollo non crittografato se consentito dai criteri di sicurezza del cliente	Modbus-Umas)				*localInterfacepeer=peerFQDN:peerPort* user=*nomeutente*]"		
		Problema di connessione Modbus TCP (nessun utente)	5	MODBUS	CONNECTION_FAILURE	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer=peerFQDN:peerPort* user=*nomeutente*]"	Max connessioni raggiunte". "Flusso dati filtrato	CPU eNOR
		Problema di connessione TCP esplicita EIP (nessun utente)	5	EIP	CONNECTION_FAILURE	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer=peerFQDN:peerPort* user=*nomeutente*]"	Max connessioni raggiunte, flusso dati filtrato	CPU
		Problema di connessione DNP3 (nessun utente)	5	DNP3	CONNECTION_FAILURE	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer=peerFQDN:peerPort user=nomeutente]	Max connessioni raggiunte"	eNOR
		Problema di connessione	5	IEC60870	CON-	[meta sequenceId=num]	Max connessioni raggiunte	eNOR

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
		IEC60870 (nessun utente)			NECTION_FAILURE	[authn@3833 itf=localPort | localInterface peer=peerFQDN:peerPort user=nomeutente]		
Blocco account utente umano a causa di troppi problemi durante i tentativi di autenticazione	I criteri di sicurezza possono richiedere di bloccare un account utente umano dopo un numero configurabile di tentativi. Questo evento informa l'amministratore di potenziali attacchi e che l'account utente umano deve essere bloccato.	Problema di accesso (server Web tramite HTTPS). Blocco account utente umano a causa di troppi problemi durante i tentativi di autenticazione	1	HTTPS	CONNECTION_FAILURE_AND_BLOCK	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*nomeutente*]"	Certificato non valido, password non valida	CPU eNOR
		Problema di accesso (aggiornamento firmware tramite HTTPS). Blocco account utente umano a causa di troppi tentativi di autenticazione non riusciti	1	HTTPS	CONNECTION_FAILURE_AND_BLOCK	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*nomeutente*]"	Certificato non valido" "Password non valida	CPU eNOR
		Problema di accesso (OPC-UA). Blocco account utente umano a causa di troppi	1	OPC-UA	CONNECTION_FAILURE_AND_BLOCK	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=	Certificato non valido, password non valida	—

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
		problemi durante i tentativi di autenticazione				*peerFQDN:peerPort* user=*nomeutente*]"		
Accesso negato (account bloccato)	Un utente umano tenta di connettersi a un account già bloccato.	Problema di accesso (server Web tramite HTTPS). Accesso negato (account bloccato)	1	HTTPS	CONNECTION_FAILURE_ON_BLOCKED	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*nomeutente*]"		CPU eNOR
		Problema di accesso (aggiornamento firmware tramite HTTPS). Accesso negato (account bloccato)	1	HTTPS	CONNECTION_FAILURE_ON_BLOCKED	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*nomeutente*]"		CPU
		Problema di accesso (OPC-UA). Accesso negato (account bloccato)	1	OPC-UA	CONNECTION_FAILURE_ON_BLOCKED	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*nomeutente*]"		—
Disconnessione	Un operatore o un componente si	Disconnessione HTTPS (server Web)	6	HTTPS	DISCONNECTION	"[meta sequenceId=*num*] [authn@3833	Logout manuale	CPU eNOR

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
	scollegano manualmente dopo un timeout a causa di inattività.					itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*nomeutente*]"		
		Disconnessione HTTPS (aggiornamento firmware)	6	HTTPS	DISCONNECTION	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*nomeutente*]"	Logout manuale	CPU eNOR
		Disconnessione OPC-UA	6	OPC-UA	DISCONNECTION	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*nomeutente*]"	Disconnessione socket	CPU
		Disconnessione Modbus	6	MODBUS	DISCONNECTION	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterfacepeer*=*peerFQDN:peerPort* user=*nomeutente*]"	Disconnessione socket	CPU

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
		Disconnessione esplicita EIP	6	EIP	DISCONNECTION	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*nomeutente*]"	Disconnessione socket	CPU
		Disconnessione HTTP (DPWS)	6	HTTP	DISCONNECTION	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*nomeutente*]"	Disconnessione socket	CPU
		Disconnessione HTTPS attivata da un timeout	6	HTTPS	DISCONNECTION	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort* user=*nomeutente*]"	Logout timeout	CPU eNOR
		Disconnessione OPC-UA attivata da un timeout	6	OPC-UA	DISCONNECTION	"[meta sequenceId=*num*] [authn@3833 itf=*localPort* | *localInterface*peer=*peerFQDN:peerPort*	Logout timeout	—

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
						user=*nomeutente*]"		
		Disconnessione DNP3	6	DNP3	DISCONNECTION	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer=peerFQDN:peerPort user=nomeutente]	Disconnessione socket	eNOR
		Disconnessione IEC 60870	6	IEC60870	DISCONNECTION	[meta sequenceId=num] [authn@3833 itf=localPort | localInterface peer=peerFQDN:peerPort user=nomeutente]	Disconnessione socket	eNOR
Modifica parametro principale al runtime	Modifica runtime parametri principale che può causare un impatto significativo sul sistema	Modifica parametri applicazione controller: tempo di ciclo	6	Configurazione	PARAMETER_SET	[meta sequenceId=*num*] [config@3833 object="PLC application" value=*valore*]	Tempo di scansione	CPU
Operazione di backup	Backup di parte o tutto il componente	Download applicazione dal controller	6	Backup	BACKUP	[meta sequenceId=*num*] [backup@3833 object="Applicazione PLC"]		CPU
		Esportazione della	6	Backup	BACKUP	[meta		eNOR

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
		configurazione di Sicurezza informatica dalle pagine Web BME NUA o BME NOR				sequenceId=*num*] [backup@3833 object= "Configurazione Sicurezza informatica"]		
Operazione di ripristino	Ripristino di parte o tutto il componente	Caricamento applicazione/ configurazione del controller nel controller	6	Configurazione	CONFIGURATION_CHANGE	[meta sequenceId=*num*] [config@3833 object= *Oggetto Oggetto* = "Applicazione PLC" or "Configurazione PLC		CPU
		Ripristino applicazione del controller nel controller	6	Backup	RESTORE	[meta sequenceId=*num*] [backup@3833 object= "Applicazione PLC"]		CPU
		Importazione della configurazione di Sicurezza informatica dalle pagine Web BME NUA o BME NOR	6	Backup	RESTORE	[meta sequenceId=*num*] [backup@3833 object= "Configurazione Sicurezza informatica"]		eNOR
Aggiornamento del firmware	Un nuovo firmware è stato verificato e installato correttamente.	Caricamento di un nuovo firmware nel controller dispositivo, nel coprocessore, pagine Web	6	Configurazione	FIRMWARE_UPDATE	[meta sequenceId=*num*] [config@3833 object= *Oggetto* value= *versione*]"Oggetto =		CPU eNOR

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
						"Firmware", "Copro Safety", "Pagine Web		
Aggiornamento firmware non valido	Un nuovo firmware non è stato installato a causa di un errore.	Un nuovo firmware non è stato installato a causa di una versione incompatibile o di una firma non valida	1	Configurazione	FIRMWARE_INVALID	[meta sequenceId=*num*] [config@3833 object= *Oggetto* value= *versione*]"Oggetto = "Firmware", "Copro Safety", "Pagine Web"	Versione incompatibile, firma non valida	CPU eNOR
Modifica dell'ora del dispositivo	Richiesta di modifica dell'ora e della data da parte di un utente.	—	5	Configurazione	TIME_CHANGE	[meta sequenceId=*num*] [config@3833 object= *"Ora"* value= *datetime*]		CPU
Segnale orario fuori tolleranza	Il componente deve convalidare i messaggi di sincronizzazione dell'ora ricevuti attraverso i canali di sincronizzazione dell'ora e l'allarme se il messaggio di sincronizzazione	—	1	Configurazione	TIME_UNEXPECTED	[meta sequenceId=*num*] [config@3833 object= "Ora" value= *datetime*]	Segnale orario fuori tolleranza	

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
	dell'ora non rientra nelle tolleranze dell'orologio interno/ locale del componente (orario trascorso, lontano, ...)							
Modifica hardware	Modifica rilevata nella topologia di rete	Modifica porta fisica di rete: collegamento porta attivo/ inattivo	6	Sistema	HARDWARE_CHANGE	[system@3833 object= *Object*] Object = "eth" seguito da un numero decimale	Collegamento porta attivo, Collegamento porta inattivo	CPU
		Qualsiasi modifica della topologia rilevata da RSTP/HSR/ PRP	6	Sistema	HARDWARE_CHANGE	[system@3833 object= *Object*] Object = "eth" seguito da un numero decimale	Abilitazione Porta Disabilitazione Porta Apprendimento Porta Inoltro Porta Blocco Porta	CPU
	Modifica rilevata nell'hardware	Inserimento/ estrazione scheda SD M580	6	Sistema	HARDWARE_CHANGE	[system@3833 object= "SDCard"]	Inserimento, estrazione	CPU
Cambio modalità di funzionamento	Modifica modalità di funzionamento del programma (Run, Stop, Init, halt) Modalità	—	5	Sistema	OPERATING_MODE_CHANGE	[system@3833 object= Object] Object = "PLC" o "Task PLC safe" o "Modulo"	"Init" "Run" "Stop" "Halt" "Modalità manutenzione" "Modalità sicurezza" "Hsby primario" "Hsby	CPU

Evento registrato	Descrizione	Descrizione aggiuntiva	Gravità	PROCID	MSGID	STRUCTURED-DATA	MSG	Dispositivi
	manutenzione / SafeRun / Stop task SAFE						secondario" "Hsby in attesa" "Master" "Non master"	
Configurazione non valida (Sicurezza informatica esterna)	Una nuova configurazione (non di Sicurezza informatica) non è stata installata a causa di un errore.	Errore di integrità dati (applicazione controller, ...)	1	Configurazione	CONFIGURATION_INVALID	[meta sequenceId=*num*] [config@3833 object=*Oggetto* value=*versione*]"*Oggetto*= "Applicazione PLC" o "Configurazione modulo"	Formato non valido, versione incompatibile	
Riavvia	Reset hardware o automatico dopo caricamento firmware	—	1	Sistema	REBOOT	—	Aggiornamento firmware, Pulsante Reset	CPU
Modifica del certificato del prodotto (e/o delle chiavi)	Gestione certificato: Creazione certificato autofirmato prodottoSL1	—	6	Credenziale	CERTIFICATE_CHANGE	[meta sequenceId=*num*] [cred@3833 name=*NomeComune*]	Creazione certificato	CPU

NOTA: Oltre alla struttura descritta in precedenza, ogni messaggio conterrà anche i seguenti campi e valori:

- Struttura = 10
- HOSTNAME = Nome di dominio completo (FQDN) o indirizzo IP locale
- APPNAME = nome di riferimento commerciale, ad esempio, BMEP584040

Esempio di messaggi del server Syslog

Date	Time	Priority	Hostname	Message
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="331"][authn@3833 if="eth" peer="192.168.11.50:52470"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="330"][authn@3833 if="eth" peer="192.168.11.50:52468"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="329"][authn@3833 if="eth" peer="192.168.11.50:52466"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="328"][authn@3833 if="eth" peer="192.168.11.50:52464"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="327"][authn@3833 if="eth" peer="192.168.11.50:52462"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="326"][authn@3833 if="eth" peer="192.168.11.50:52460"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="325"][authn@3833 if="eth" peer="192.168.11.50:52458"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="324"][authn@3833 if="eth" peer="192.168.11.50:52456"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="323"][authn@3833 if="eth" peer="192.168.11.50:52454"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="322"][authn@3833 if="eth" peer="192.168.11.50:52452"] Socket connection
11-08-2021	11:55:03	System0.Info	192.168.11.1	1 2021-08-26T11:22:41.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="321"][authn@3833 if="eth" peer="192.168.11.50:52450"] Socket connection
11-08-2021	11:54:33	System0.Info	192.168.11.1	1 2021-08-26T11:22:12.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="320"][authn@3833 if="eth" peer="192.168.11.50:52442"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:07.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="319"][authn@3833 if="eth" peer="192.168.1.100:34246"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="318"][authn@3833 if="eth" peer="192.168.11.50:52440"] Socket connection
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:06.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="317"][config@3833 object="Module"]
11-08-2021	11:54:28	System0.Info	192.168.11.1	1 2021-08-26T11:22:04.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="316"][config@3833 object="Module"]
11-08-2021	11:54:24	System0.Notice	192.168.11.1	1 2021-08-26T11:22:03.000Z 192.168.11.1 BMEP585040 System OPERATING_MODE_CHANGE [meta sequenceId="315"][system@3833 object="PLC"] Init
11-08-2021	11:54:13	System0.Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Configuration CONFIGURATION_CHANGE [meta sequenceId="314"][config@3833 object="PLC application"]
11-08-2021	11:54:13	System0.Info	192.168.11.1	1 2021-08-26T11:21:51.000Z 192.168.11.1 BMEP585040 Backup RESTORE [meta sequenceId="313"][backup@3833 object="PLC application"]
11-08-2021	11:54:07	System0.Info	192.168.11.1	1 2021-08-26T11:21:46.000Z 192.168.11.1 BMEP585040 MODBUS CONNECTION_SUCCESS [meta sequenceId="312"][authn@3833 if="eth" peer="192.168.1.100:34235"] Socket connection
11-08-2021	11:53:20	System0.Info	192.168.11.1	1 2021-08-26T11:20:59.000Z 192.168.11.1 BMEP585040 Backup BACKUP [meta sequenceId="311"][backup@3833 object="PLC application"]

Descrizioni dei messaggi del registro eventi per i controller M580 (firmware precedente alla versione 4.10), BMENUA0100 e BMENOR2200H (firmware precedente alla versione 3.01)

Questa sezione presenta le descrizioni dei messaggi del registro eventi per:

- Controller M580 con firmware precedente alla versione 4.10 (abbreviato "CPU" nella colonna **Dispositivi**)
- Moduli di comunicazione BMENUA0100 OPC UA (abbreviato "NUA" nella colonna **Dispositivi**)
- Unità terminale remota BMENOR2200H (abbreviazione "eNOR" nella colonna **Dispositivi**)

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
Connessione riuscita a o da uno strumento o un dispositivo: * Accesso riuscito * Connessione TCP riuscita	Accesso riuscito (Memorizzazione dati tramite FTP, Server FDR con FTP, Caricamento firmware con FTP)	10	6	FTP	indirizzo IP remoto	Li1: connessione riuscita (MNT_ENG_MSG_TYP_CNCTN_SUCCESS)	"Accesso riuscito"	CPU
	Accesso riuscito (server Web tramite HTTPS)			HTTPS	"(null)"		"Accesso riuscito"	NUA
	Accesso riuscito (aggiornamento firmware tramite HTTPS)			HTTPS	"(null)"		"Accesso riuscito"	NUA
	Accesso riuscito (OPC-UA)			OPC-UA	"(null)"		"Accesso riuscito"	NUA
	Accesso riuscito (password applicazione Unity tramite Modbus-Umas)			DEVICE_MANAGER	"(null)"		"Accesso riuscito"	CPU
	Accesso riuscito (server Web tramite HTTPS)			HTTP	"(null)"		"Accesso riuscito" OPPURE "Connessione riuscita" (se non sono disponibili pagine Web M580 per l'accesso utente)	CPU

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
	Connessione TCP riuscita (nessun utente).			MODBUS	indirizzo IP remoto		"Connessione riuscita"	CPU
	Connessione TCP riuscita (nessun utente).			EIP	"(null)"		"Connessione riuscita"	CPU
	Connessione riuscita sul protocollo di comunicazione DNP3 (per master e stazione esterna DNP3)			DNP3	indirizzo IP remoto		"Connessione riuscita"	eNOR
	Connessione riuscita sul protocollo di comunicazione IEC60870 (per client e server IEC60870)			IEC60870	indirizzo IP remoto		"Connessione riuscita"	eNOR
Problema di connessione da o verso uno strumento o un dispositivo: *Problema di connessione TCP dovuto al controllo ACL (indirizzo IP	Problema di accesso (Memorizzazione dati con FTP, Server FDR con FTP, Caricamento firmware con FTP)	10	4	FTP	indirizzo IP remoto	Li2: Connessione non riuscita (credenziali errate) (MNT_ENG_MSG_TYP_CNCTN_FAILURE)	"Accesso non riuscito"	CPU
	Problema di accesso (server Web			HTTPS	"(null)"		"Accesso non riuscito"	NUA

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
sorgente/ filtraggio porta TCP) * Problema di accesso	tramite HTTPS)							
	Problema di accesso (aggiornamento firmware tramite HTTPS)			HTTPS	"(null)"		"Accesso non riuscito"	NUA
	Problema di accesso (OPC-UA)			OPC-UA	"(null)"		"Accesso non riuscito"	NUA
	Problema di accesso (server Web tramite HTTP)			HTTP	indirizzo IP remoto		"Accesso non riuscito" OPPURE "Connessione non riuscita" (se non è presente alcun accesso utente)	CPU
	Problema di accesso (password dell'applicazione Unity tramite Modbus-Umas)			DEVICE_MANAGER	indirizzo IP remoto		"Accesso non riuscito"	CPU
	Problema di connessione TCP (nessun utente)			MODBUS	indirizzo IP remoto		"Connessione non riuscita"	CPU
	Problema di connessione TCP (nessun utente)			EIP	indirizzo IP remoto		"Connessione non riuscita"	CPU
	Problema di connessione sul protocollo			DNP3	indirizzo IP remoto		"Connessione non riuscita"	eNOR

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
	di comunicazione DNP3 (per master e stazione esterna DNP3)							
	Problema di connessione sul protocollo di comunicazione IEC60870 (per client e server IEC60870)			IEC60870	indirizzo IP remoto		"Connessione non riuscita"	eNOR
Disconnessione attivata da locale o peer: * Disconnessione TCP * Logout su richiesta	Disconnessione attivata da peer/utente/locale	10	6	FTP	"(null)"	Li5: disconnessione attivata da peer/user (MNT_ENG_MSG_TYP_DISCONNECTION)	"Disconnessione"	—
	Disconnessione attivata da peer/utente/locale			HTTPS	"(null)"		"Disconnessione"	NUA
	Disconnessione attivata da peer/utente/locale			OPC-UA	"(null)"		"Disconnessione"	NUA
	Disconnessione attivata da peer/utente/locale			MODBUS	indirizzo IP remoto		"Disconnessione"	CPU

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
	—			DNP3	"(null)" o indirizzo ip remoto		"Disconnessione"	eNOR
	—			IEC60870	"(null)" o indirizzo ip remoto		"Disconnessione"	eNOR
Logout automatico (timeout inattività) HTTPS OPC-UA	Disconnessione attivata da un timeout	10	6	HTTPS	"(null)"	Li6: Disconnessione attivata da un timeout (MNT_ ENG_ MSG_ TYP_ DSCNCT_ TIMEOUT)	"Logout automatico"	NUA
	Disconnessione attivata da un timeout			OPC-UA			"Logout automatico"	NUA
Cambiamenti principali nel sistema: Modifica del tempo di esecuzione dei parametri fuori configurazione	Modifica principale del tempo di ciclo o modifica dei parametri dell'applicazione controller del watchdog (tempo di ciclo, watchdog)	13	5	DEVICE_ MANAGER	"(null)"	Li87: Aggiornamento parametro di sistema (MNT_ ENG_ MSG_ TYP_ PARAMETER_ UPDATE)	"Aggiornamento parametro XXXX" (con XXXX che identifica il parametro)XXXX = "Tempo di ciclo" Esempio: aggiornamento parametro tempo di ciclo	CPU
Modifiche principali nel sistema: * Download dell'applicazione o della configurazione dal dispositivo	Download di un file di configurazione dal dispositivo	13	6	MODBUS	"(null)"	Li8: Download di un file di configurazione dal dispositivo (MNT_ ENG_ MSG_ TYP_ CONF_ DL)	"Download applicazione" o "Download configurazione"	CPU

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
* Esportazione (registrazione) file di configurazione di sicurezza informatica dal dispositivo				HTTPS			"Backup configurazione Sicurezza informatica"	NUA
Cambiamenti principali nel sistema	Caricamento dell'applicazione/ configurazione o della configurazione solo nel dispositivo (incluso CCOTF)	13	6	MODBUS	"(null)"	Li9: Caricamento di un file di configurazione nel dispositivo (MNT_ ENG_ MSG_ TYP_ CONF_ UL)	"Caricamento applicazione" o "Caricamento configurazione"	CPU NUA
	Importazione (ripristino) file di configurazione di sicurezza informatica nel dispositivo			HTTPS			"Ripristino configurazione Sicurezza informatica"	NUA
Modifiche principali nel sistema	Caricamento delle pagine Web nel dispositivo	13	6	FTP	"(null)"	Li10: Caricamento di un nuovo firmware nel dispositivo (MNT_ ENG_ MSG_ TYP_ FIRMWARE_ UPDATE)	"Caricamento pagine Web"	CPU
	Caricamento del nuovo			FTP			"Caricamento del firmware	CPU

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
	firmware del coprocessore di sicurezza						del coprocessore di sicurezza"	
	Caricamento di un nuovo firmware nel dispositivo			FTP			"Caricamento firmware"	CPU
	Caricamento di un nuovo firmware nel dispositivo			HTTPS			"Caricamento firmware"	NUA
Modifiche principali nel sistema	Modifica dell'ora del dispositivo	13	6	DEVICE_MANAGER	"(null)"	LI15: Modifica dell'ora dello IED	"Aggiornamento importante ora"	NUA
Parametri di comunicazione runtime Modifica riuscita al di fuori della configurazione	Attivazione/ disattivazione dei servizi di comunicazione	10	4	DEVICE_MANAGER	"(null)"	Li18: Attivazione/ disattivazione di qualsiasi porta fisica (seriale, USB) o logica (telnet, FTP) (MNT_ENG_MSG_TYP_PORT_MANAGEMENT)	"Aggiornamento parametro di comunicazione principale: XXXX YYYY"XXXX = "EIP" o "DHCP" o "FTP" o "MODBUS" o "SNMP" o "HTTP" o "SECURITY" o "NTP" o "IPSEC" o "DEVICE_MANAGER" Solo per NUA: XXXX = "Flussi dati Control Expert solo a	CPU NUA eNOR

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
							controller" o "Flussi dati Control Expert a rete dispositivi" o "Flussi dati da CPU a CPU". Solo per NOR: XXXX = "DNP3 su canale TLS ["*nome canale*"]" o "IEC60870 su TLS"YYYY= "attiva" o "disattiva" Esempio: "Aggiornamento parametri di comunicazione principali: attivazione FTP"	
Modifica porta fisica di rete: collegamento porta attivo/ inattivo	Qualsiasi modifica dello stato della porta fisica di rete. Può essere lo stato semplice di una porta Ethernet o le informazioni raccolte dall'algoritmo RSTP/ HSR/PRP per	10	4	DEVICE_MANAGER	"(null)"	LI19: Qualsiasi modifica dello stato della porta fisica di rete. Può essere lo stato semplice di una porta Ethernet o le informazioni raccolte dall'algoritmo RSTP / HSR /	"Modifica principale dello stato della porta fisica di rete: XXXX collegamento YYYY" XXXX = "ETH" seguito dal numero decimale per la porta o "Porta	CPU NUA

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
	sistemi ridondanti					PRP per sistemi ridondanti (MNT_ ENG_ MSG_ TYP_ NETWK_ PORT_ CHG)	FRONTALE" YYY = "collegamento attivo" o "collegamento inattivo" Esempio: "Modifica principale dello stato della porta fisica di rete: collegamento ETH1 attivo)	
Qualsiasi modifica della topologia rilevata:	Qualsiasi modifica della topologia rilevata da RSTP/ HSR/PRP	10	4	RSTP	"(null)"	LI20: Qualsiasi modifica della topologia rilevata dagli algoritmi RSTP/ HSR/PRP per sistemi ridondanti (MNT_ ENG_ MSG_ TYP_ NTWK_ TPLGY_ CHG)	"Rilevata modifica topologia" o "Rilevata modifica topologia: XXXX YYYY" XXXX = "ETH" seguito dal numero decimale per la porta o "Porta FRONTALE" YYYY = "attiva", "disattiva", "apprendimento", "inoltro", "blocco"	CPU NUA
Errore del controllo integrità: * Errore firma digitale, * Solo integrità	Errore integrità firmware	10	6	DEVICE_ MANAGER	"(null)"	LI84: Errore integrità dati MNT_ ENG_ MSG_ DATA_ INTEGRITY_ ERROR	"Errore integrità firmware"	CPU NUA
	Errore integrità dati: CS Conf, cert, whitelist o RBAC)			DEVICE_ MANAGER			"Errore integrità dati"	NUA

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
(hash mac)								
Modifiche principali nel sistema: Riavvia	Riavvio dopo il caricamento del firmware	13	4	DEVICE_MANAGER	"(null)"	LI14: MNT_ENG_MSG_TYP_REBOOT_ORDER	"Riavvio"	CPU NUA
Modifiche principali nel sistema	Modifica modalità operativa del controller (Run, Stop, Init, halt) Modalità di manutenzione Modifica delle modalità operative di sicurezza (task SafeRun, Stop Safe)	13	5	DEVICE_MANAGER	"(null)"	LI85: Modifica della modalità operativa MNT_ENG_MSG_OPERATING_MODE_CHANGE	"Aggiornamento stato XXXX: YYYY" (dove XXXX identifica l'oggetto che cambia stato e YYYY che identifica il nuovo stato) XXXX = "PLC" o "task PLC safe" o "Dispositivo" YYY = "INIT" o "STOP" o "RUN" o "HALT" o "Modalità manutenzione" o "Modalità sicura" ESEMPI: "Aggiornamento stato PLC: RUN" "Aggiornamento stato PLC: modalità manutenzione"	CPU

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
Modifiche principali nel sistema: Modifica hardware	Funzionamento su scheda SD	13	6	DEVICE_ MANAGER	"(null)"	LI26: Modifica hardware MNT_ ENG_ MSG_ HARDWARE_ CHANGE	"Aggiornamento hardware: XXXX" (dove XXXX descrive l'aggiornamento) XXXX = "Inserimento scheda SD" o "Estrazione scheda SD"	CPU
	Modifica posizione selettore a rotazione: Reset, Advanced			DEVICE_ MANAGER			"Aggiornamento hardware: XXXX" (dove XXXX descrive l'aggiornamento) XXXX = "torna alla modalità di fabbrica" o "modalità protetta"	NUA
Modifica principale in RBAC Sicurezza informatica (eseguita tramite le pagine Web di configurazione della Sicurezza informatica).	Crea account utente Elimina account utente Aggiorna account utente			HTTPS	"(null)"	Li11: MNT_ ENG_ MSG_ TYP_ RBAC_ UPDATE	"Aggiorna RBAC"	NUA
Modifica principale nei criteri di Sicurezza	Servizi di rete Registro eventi	10	4	HTTPS	"(null)"	Li12: MNT_ ENG_ MSG_ TYP_	"Aggiornamento dei principali parametri di sicurezza	NUA

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
informatica (eseguita tramite le pagine Web di configurazione della Sicurezza informatica).	Policy di sicurezza Banner sicurezza					SECURITY_ UPDATE_ UPDATE	informatica: servizi di rete" "Aggiornamento dei principali parametri di sicurezza informatica: registro eventi" "Aggiornamento dei principali parametri di sicurezza informatica: criteri di sicurezza" "Aggiornamento dei principali parametri di sicurezza informatica: banner di sicurezza"	
Modifica principale dei parametri specifici del dispositivo di Sicurezza informatica (eseguiti le pagine Web di configurazione di Sicurezza informatica).	Attiva/ disattiva e configura IPSEC Attiva/ disattiva e configura OPC-UA Attiva/ disattiva e configura DNP3	10	4	HTTPS	"(null)"	Li13: MNT_ ENG_ MSG_ TYP_ DSS_ UPDATE	"Aggiornamento parametro di sicurezza informatica principale: IPSEC" "Aggiornamento parametro di sicurezza informatica principale: OPC-UA"	NUA
Problema di	Un'azione su una risorsa di	10	4	HTTPS	"(null)"	Li21: MNT_ ENG_	"Autorizzazione	—

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
autorizzazione	un utente o di un computer non è autorizzata					MSG_TYP_AUTH_REQ	non riuscita"	
Gestione certificato	Aggiungi/rimuovi certificato client	10	4	HTTPS	"(null)"	Li89: Gestione certificati (MNT_ENG_MSG_TYP_CERT_MGT)	"Aggiungi certificato client" "Rimuovi certificato client"	NUA
Gestione certificati: * Certificato scaduto	Rilevamento scadenza certificato server al riavvio	10	3	DEVICE_MANAGER	"(null)"	Li29: Gestione certificati (MNT_ENG_MSG_TYP_CERT_EXPIRE)	"Certificato scaduto"	NUA
Specifico per il progetto eNOR:								
Problema di autenticazione	—	10	4	"DNP3_Master" o "DNP3_Stazione esterna"	indirizzo IP remoto	Li100: MNT_ENG_MSG_TYPE_AUTHENTICATION_FAILURE	"autenticazione canale ["*nome canale*"] non riuscita"	eNOR
risposta imprevista	—	10	4	"DNP3_Master" o "DNP3_Stazione esterna"	indirizzo IP remoto	Li101: MNT_ENG_MSG_TYPE_UNEXPECTED_RESPONSE	"risposta imprevista canale ["*nome canale*"]"	eNOR
Nessuna risposta	—	10	4	"DNP3_Master" o "DNP3_Stazione esterna"	indirizzo IP remoto	Li102: MNT_ENG_MSG_TYPE_NO_RESPONSE	"nessuna risposta canale ["*nome canale*"]"	eNOR

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
Modalità aggressiva non supportata	—	10	4	"DNP3_ Master" o "DNP3_ Stazione esterna"	indirizzo IP remoto	Li103: MNT_ ENG_ MSG_ TYPE_ AGGRESSIVE_ MODE_ NOT_ SUPPORTED	"modalità aggressiva canale ["*nome canale*"] non supportata"	eNOR
Algoritmo MAC non supportato	—	10	4	"DNP3_ Master" o "DNP3_ Stazione esterna"	indirizzo IP remoto	Li104: MNT_ ENG_ MSG_ TYPE_ MAC_ ALGORITHM_ NOT_ SUPPORTED	"canale ["*nome canale*"] Algoritmo MAC non supportato"	eNOR
Algoritmo di incapsulamento chiave non supportato	—	10	4	"DNP3_ Master" o "DNP3_ Stazione esterna"	indirizzo IP remoto	Li105: MNT_ ENG_ MSG_ TYPE_ KEYWRAP_ ALGORITHM_ NOT_ SUPPORTED	"algoritmo di wrapping della chiave canale ["*nome canale*"] non supportato"	eNOR
Problema di autorizzazione	—	10	4	"DNP3_ Master" o "DNP3_ Stazione esterna"	indirizzo IP remoto	Li86: MNT_ ENG_ MSG_ TYP_ AUTHORIZATION_ FAILURE)	"autorizzazione canale ["*nome canale*"] non riuscita"	eNOR
Metodo di modifica aggiornamento chiave non consentito	—	10	4	"DNP3_ Master" o "DNP3_ Stazione esterna"	indirizzo IP remoto	Li106: MNT_ ENG_ MSG_ TYPE_ UPDATE_ KEY_ CHANGE_	"metodo di modifica della chiave di aggiornamento canale ["*nome canale*"] non	eNOR

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
						METHOD_NOT_PERMITTED	consentito"	
Firma non valida	—	10	4	"DNP3_Master" o "DNP3_Stazione esterna"	indirizzo IP remoto	Li107: MNT_ENG_MSG_TYPE_INVALID_SIGNATURE	"firma non valida canale ["*nome canale*"]"	eNOR
Dati di certificazione non validi	—	10	4	"DNP3_Master" o "DNP3_Stazione esterna"	indirizzo IP remoto	Li108: MNT_ENG_MSG_TYPE_INVALID_CERTIFICATION_DATA	"dati di certificazione non validi canale ["*nome canale*"]"	eNOR
Utente sconosciuto	—	10	4	"DNP3_Master" o "DNP3_Stazione esterna"	indirizzo IP remoto	Li109: MNT_ENG_MSG_TYPE_UNKNOWN_USER	"utente sconosciuto canale ["*nome canale*"]"	eNOR

Evento registrato	Descrizione	Servizio	Gravità	MSGID	MSG: indirPeer	MSG: tipo	MSG: msgApp	Dispositivi
Numero massimo richieste stato chiave sessione superato	—	10	4	"DNP3_ Master" o "DNP3_ Stazione esterna"	indirizzo IP remoto	Li110: MNT_ ENG_ MSG_ TYPE_ MAX_ SESSION_ KEY_ STATUS_ REQ_ EXCEED	"richiesta max stato chiave sessione superata canale ["*nome canale*"]"	eNOR
Modifica chiave sessione riuscita	—	10	6	"DNP3_ Master" o "DNP3_ Stazione esterna"	indirizzo IP remoto	Li111: MNT_ ENG_ MSG_ TYPE_ SESSION_ KEY_ CHANGE_ SUCCESS	"modifica chiave sessione riuscita canale ["*nome canale*"]"	eNOR

NOTA: Oltre alla struttura descritta in precedenza, ogni messaggio conterrà anche i seguenti campi e valori in base al campo Gravità:

- HOSTNAME = indirizzo IP locale o null.
- APPNAME = nome di riferimento commerciale, ad esempio BMEP584040.
- PROCID non utilizzato.
- MSG:IssuerAddress = Indirizzo IP locale.
- MSG:Peer non utilizzato.

Identificazione e autenticazione del controllo

Gestione degli account

Di seguito sono riportate le best practice per la gestione degli account:

- Creare un account utente standard senza privilegi di amministratore.
- Utilizzare l'account utente standard per avviare le applicazioni. Avviare un'applicazione utilizzando account con più privilegi solo se l'applicazione richiede privilegi di livello più elevato per svolgere il ruolo che le è stato assegnato nel sistema.

- Installare le applicazioni utilizzando un account di livello amministrativo.

Gestione dei controlli account utente (UAC) con Windows 10

Per ridurre al minimo le modifiche non autorizzate al sistema operativo del PC, Windows 10 concede alle applicazioni i livelli di autorizzazione di un utente normale senza privilegi amministrativi. Senza privilegi amministrativi, le applicazioni non possono apportare modifiche al sistema. UAC chiede all'utente di concedere o negare ulteriori autorizzazioni a un'applicazione. Impostare UAC al livello massimo. Al livello massimo, UAC informa l'utente prima di consentire a un'applicazione l'esecuzione di modifiche che richiedono l'autorizzazione dell'amministratore di sistema.

Per accedere alle impostazioni in UAC in Windows 10, aprire il **Pannello di controllo > Account utente e protezione per la famiglia > Account utente > Modifica impostazioni di controllo account utente** o immettere **UAC** nel campo di ricerca del **Menu Start** di Windows 10.

Gestione delle password

La gestione delle password è uno degli strumenti fondamentali per il rinforzo della protezione dei dispositivi, ossia per il processo di configurazione di un dispositivo allo scopo di proteggerlo dagli attacchi informatici legati alla comunicazione. È buona norma applicare le seguenti linee guida per la gestione delle password:

- Abilitare l'autenticazione tramite password su tutte le e-mail e server Web, controller e moduli di interfaccia Ethernet.
- Cambiare immediatamente tutte le password predefinite dopo l'installazione, incluse quelle per:
  - account utente e dell'applicazione su Windows, SCADA, HMI e altri sistemi
  - script e codice sorgente
  - dispositivo di controllo di rete
  - dispositivi con account utente
  - Server FTP
  - Dispositivi SNMP e HTTP
  - Control Expert
- Comunicare le password solo alle persone che devono eseguire l'accesso. Vietare la condivisione delle password.

- Non visualizzare le password durante l'immissione delle stesse.
  - Utilizzare password difficili da intuire. Esse devono contenere almeno 8 caratteri, una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali quando ammesso.
- Richiedere la modifica delle password utente e applicazione a intervalli programmati.
- Eliminare gli account di accesso dei dipendenti una volta che è terminato l'uso.
- Richiedere password diverse per diversi account, sistemi e applicazioni.
- Conservare una lista master sicura delle password degli account degli amministratori, in modo che sia possibile accedervi rapidamente in caso di necessità.
- Implementare la gestione delle password in modo che non interferisca con l'abilità dell'operatore di rispondere a eventi come uno spegnimento di emergenza.
- Non trasmettere le password via e-mail o altri modi tramite Internet non protetto.

Gestione HTTP

Hypertext transfer protocol (HTTP) è il protocollo di base utilizzato da Web. Viene utilizzato nei sistemi di controllo per supportare i server Web integrati nei prodotti di controllo. Schneider Electric I server Web utilizzano le comunicazioni HTTP per visualizzare i dati e inviare i comandi tramite le pagine Web.

Se il server HTTP non è necessario, disattivarlo. Altrimenti, se possibile utilizzare il protocollo HTTPS (*hypertext transfer protocol secure*), che è una combinazione di HTTP e un protocollo crittografico, anziché HTTP. Consentire solo il traffico a dispositivi specifici, implementando meccanismi di controllo degli accessi come una regola del firewall che impone restrizioni di accesso da dispositivi specifici a dispositivi specifici.

È possibile configurare HTTPS come server Web predefinito nei prodotti che supportano questa funzionalità.

Importare e considerare attendibili i certificati autofirmati dei controller M580 nei browser Web da una rete attendibile. In questo modo si evita che la notifica venga visualizzata quando ci si collega alle pagine Web dei controller attendibili.

NOTA: Questo processo deve essere ripetuto al rinnovo dei certificati dei controller, ad esempio quando si modificano gli indirizzi IP del controller dall'applicazione.

Gestione FTP

Il protocollo FTP (*File transfer protocol*) fornisce servizi di gestione remota dei file tramite 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.

Considerare il seguente comportamento del servizio FTP fornito da Schneider Electric:

- Il protocollo FTP è disattivato.
- Il protocollo FTP è necessario solo per specifiche attività di manutenzione e configurazione. È opportuno disattivare l'intero insieme di servizi FTP quando non sono richiesti.
- Il protocollo FTP non è sicuro e deve essere utilizzato con cautela per evitare la divulgazione di informazioni riservate e l'accesso non autorizzato ai controller:
  - Se possibile, modificare le password predefinite di tutti i dispositivi che supportano FTP.
  - Utilizzare l'Elenco di controllo di accesso per limitare la comunicazione agli indirizzi IP autorizzati. Vedere "Servizi di Sicurezza informatica per sistema" per informazioni sul modulo interessato.
  - Quando si utilizza il modulo BMENOC, configurare la funzionalità IPSEC (Configurazione della comunicazione crittografata, pagina 36).
  - Bloccare tutto il traffico FTP in ingresso e in uscita sul limite della rete aziendale e della rete operativa della sala di controllo.
  - Filtrare i comandi FTP tra la rete di controllo e la rete operativa per specificare gli host o comunicarli su una rete di gestione crittografata separata.
  - Utilizzare un modulo esterno per configurare una VPN tra i moduli interessati dal controller e la workstation di engineering sulla rete di controllo.
- I moduli BMENOC0301 and BMENOC0311 non supportano l'inoltro IP alla rete di dispositivi.

  Se è richiesta la trasparenza tra le reti di controllo e le reti dei dispositivi, è necessario un router esterno/VPN per fornire una comunicazione crittografata tra le reti di controllo e i dispositivi (vedere la figura in Destinazione sicurezza CSPN, pagina 43).

Nel protocollo FTP, è richiesta la trasparenza per eseguire le seguenti operazioni dalla rete di controllo:

- Aggiornamento del firmware del controller M580 da Automation Device Maintenance.
- Diagnostica di rete del controller M580 eseguita da uno strumento di gestione di rete tramite servizio SNMP.

Gestione SNMP

Il protocollo SNMP (*Simple network management protocol*) offre servizi di gestione di rete tra una console di gestione centrale e dispositivi di rete quali router, stampanti e controller. Il protocollo consiste di tre parti:

- Gestore: un'applicazione che gestisce agenti SNMP su una rete emettendo richieste, ricevendo risposte, ascoltando ed elaborando i segnali trap emessi dagli agenti.

- Agente: un modulo software per la gestione della rete che risiede in un dispositivo gestito. L'agente consente la modifica dei parametri di configurazione da parte dei gestori. I dispositivi gestiti possono essere dispositivi di qualsiasi tipo: router, server di accesso, switch, bridge, hub, controller, dispositivi di connessione.
- Sistema di gestione di rete (NMS): il terminale attraverso cui gli amministratori possono svolgere task amministrativi.

I dispositivi Ethernet di Schneider Electric hanno funzionalità di servizio SNMP per la gestione della rete.

Spesso SNMP viene installato automaticamente con **pubblico** come stringa di lettura e **privato** come stringa di scrittura. Questo tipo di installazione consente all'autore di un attacco di effettuare il riconoscimento su un sistema per creare un Denial of Service.

Per ridurre il rischio di un attacco tramite SNMP:

- Se è richiesto SNMP v1, utilizzare le impostazioni di accesso per limitare i dispositivi (indirizzi IP) che possono accedere allo switch. Assegnare ai dispositivi password diverse di lettura e lettura/scrittura.
- Modificare le password predefinite di tutti i dispositivi che supportano SNMP.
- Bloccare tutto il traffico SNMP in ingresso e in uscita sul limite della rete aziendale e della rete operativa della sala di controllo.
- Filtrare i comandi SNMP v1 tra la rete di controllo e la rete operativa per specificare gli host o comunicarli su una rete di gestione crittografata separata.
- Controllare l'accesso identificando l'indirizzo IP che ha il privilegio di interrogare un dispositivo SNMP.
- Utilizzare un modulo esterno per configurare una VPN tra i moduli interessati dal controller e la workstation di engineering sulla rete di controllo.

Gestione di applicazione, sezione, memorizzazione dati e password del firmware Control Expert

In Control Expert, le password sono applicate ai seguenti elementi (in base al controller):

- **Applicazione**

  Control Expert e la protezione dell'applicazione del controller tramite password impedisce la modifica, il download o l'apertura indesiderati dell'applicazione (file .STU, . STA and .ZEF). La password è memorizzata nell'applicazione in modo codificato.

  Oltre alla protezione tramite password, è possibile crittografare i file .STU, .STA e .ZEF. La funzionalità di crittografia file in Control Expert contribuisce a impedire modifiche non autorizzate da parte di personale non qualificato e rafforza la protezione contro il furto della proprietà intellettuale e altre intenzioni dannose. L'opzione di crittografia file è protetta da un meccanismo di password.

  NOTA: Quando un controller viene gestito come parte di un progetto di sistema, la password dell'applicazione e la crittografia dei file vengono disattivate nell'editor di Control Expert e devono essere gestite mediante Topology Manager.

  Per ulteriori informazioni, vedere la sezione *Protezione dell'applicazione* (vedere EcoStruxure™ Control Expert, Modalità operative).

- **Sezione**

  La funzione di protezione della sezione è accessibile dalla schermata **Proprietà** del progetto in modalità offline. Questa funzione consente di proteggere le sezioni di programma. Per ulteriori informazioni, vedere la sezione *Protezione di sezioni e subroutine* (vedere EcoStruxure™ Control Expert, Modalità operative).

  NOTA: la protezione di sezione non è attiva finché la protezione non viene attivata nel progetto.

- **Memorizzazione dati/Web**

  La protezione della memorizzazione dati con una password consente di impedire l'accesso indesiderato all'area di memorizzazione dati della scheda di memoria SD (se nel controller è inserita una scheda valida). Consente inoltre di impedire l'accesso indesiderato alla diagnostica Web (per firmware controller M580 ≥ 4.0). Per ulteriori informazioni, consultare la sezione *Protezione della memorizzazione dati* (vedere EcoStruxure™ Control Expert, Modalità operative).

- **Firmware**

  La protezione da download del firmware tramite password impedisce il download di firmware dannoso. Per ulteriori informazioni, vedere la sezione *Protezione del firmware* (vedere EcoStruxure™ Control Expert, Modalità operative).

Autorizzazioni di controllo

Editor di sicurezza di Control Expert

Per definire gli utenti del software e le rispettive autorizzazioni viene utilizzato uno strumento di configurazione della sicurezza. La sicurezza di accesso di EcoStruxure Control Expert

riguarda il terminale o i terminali sui quali è installato il software e non il progetto, che dispone di un proprio sistema di protezione.

Per informazioni più dettagliate, vedere *EcoStruxure™ Control Expert, Editor sicurezza, Guida operativa*.

È buona prassi stabilire una password dedicata per l'amministratore di sicurezza (*SecurityAdmin*) e limitare le autorizzazioni degli altri utenti con un profilo restrittivo.

Programmazione e modalità di monitoraggio

Sono disponibili due modalità per accedere al controller in modalità **Online**:

- Modalità di **programmazione**: il programma del controller può essere modificato. Quando si collega un terminale al controller per la prima volta, il controller diventa riservato e non è possibile collegare un altro terminale finché il controller è riservato.
- Modalità di **monitoraggio**: il programma del controller non può essere modificato, ma le variabili possono essere modificate. La modalità di monitoraggio non riserva il controller ed è possibile accedere a un controller già riservato in modalità di monitoraggio.

Per scegliere una modalità in EcoStruxure Control Expert, selezionare: **Strumenti > Opzioni... > Connessione > Modalità di connessione predefinita**.

Per ulteriori informazioni su queste modalità, vedere la sezione *Servizi in modalità online* (vedere EcoStruxure™ Control Expert, Modalità operative).

È buona norma impostare la modalità di accesso del controller **Online** su **Monitoraggio** quando possibile.

Protezione sezioni programma

La funzione di protezione di una sezione è accessibile dalla schermata **Proprietà** del progetto in modalità offline. Questa funzione permette di proteggere le sezioni del programma. Per ulteriori informazioni, vedere la sezione *Protezione di sezioni e subroutine* (vedere EcoStruxure™ Control Expert, Modalità operative).

NOTA: la protezione di sezione non è attiva finché la protezione non viene attivata nel progetto.

È buona prassi attivare la protezione delle sezioni.

Protezione della memoria del controller

La protezione della memoria impedisce il trasferimento di un progetto nel controller e le modifiche in modalità online, indipendentemente dal canale di comunicazione.

NOTA: La protezione della memoria del controller non può essere configurata con i controller Hot Standby. In questi casi, utilizzare la comunicazione crittografata IPsec.

La protezione della memoria è attivata nel modo seguente:

- Controller Modicon M340: Bit di ingresso. Per ulteriori informazioni, vedere la sezione *Configurazione dei processori Modicon M340* sezione (vedere EcoStruxure™ Control Expert, Modalità operative).
- Controller Modicon M580: Bit di ingresso. Per ulteriori informazioni, vedere la sezione *Gestione dell'ingresso Run/Stop* (vedere Modicon M580, Hardware, Manuale di riferimento).
- Controller Modicon Quantum: Interruttore a chiave fisico sul modulo del controller, per controller low end (vedere Quantum con EcoStruxure™ Control Expert, Hardware, Manuale di riferimento) o high end (vedere Quantum con EcoStruxure™ Control Expert, Hardware, Manuale di riferimento).
- Controller Modicon Premium: Bit di ingresso. Per ulteriori informazioni, vedere la sezione *Configurazione dei processori Premium* sezione (vedere EcoStruxure™ Control Expert, Modalità operative).
- Controller Modicon MC80: Bit di ingresso. Per ulteriori informazioni, vedere Modicon MC80 Program Logic Controller (PLC) - Manuale utente.
- Controller Modicon Momentum MDI: Bit di ingresso. Per ulteriori informazioni, vedere EcoStruxure™, Processori Control Expert 171CBU78090, 171CBU98090, 171CBU98091, Guida utente.

È buona norma attivare la protezione della memoria del controller quando possibile.

Accesso Run/Stop remoto del controller

La gestione dell'accesso remoto Run/Stop definisce il modo in cui un controller può essere avviato o arrestato in remoto e dipende dal sistema.

NOTA: non è possibile configurare l'accesso run/stop remoto del controller con i controller Hot Standby. In questi casi, utilizzare la comunicazione crittografata IPsec.

Controller	Accesso
Modicon M580:	L'accesso remoto del controller a run/stop consente una delle operazioni seguenti: • Arrestare o avviare il controller da remoto su richiesta. • Arrestare il controller da remoto su richiesta. Rifiutare le richieste di esecuzione da remoto del controller. Quando è configurato un ingresso valido, è disponibile solo un'esecuzione controllata dall'ingresso. • Rifiutare le richieste di esecuzione o arresto da remoto del controller. Vedere *Gestione dell'ingresso Run/Stop* per le opzioni di configurazione del controller che impediscono ai comandi remoti di accedere alla sezione Modalità Run/Stop (vedere Modicon M580, Hardware, Manuale di riferimento).
Modicon M340:	L'accesso remoto del controller a run/stop consente una delle operazioni seguenti: • Arrestare o avviare il controller da remoto su richiesta. • Arrestare il controller da remoto su richiesta. Rifiutare le richieste di esecuzione da remoto del controller. Quando è configurato un ingresso valido, è disponibile solo un'esecuzione controllata dall'ingresso. Vedere la *sezione Configurazione dei processori Modicon M340* (vedere EcoStruxure™ Control Expert, Modalità operative).
Modicon Premium:	L'accesso remoto del controller a run/stop consente una delle operazioni seguenti: • Arrestare o avviare il controller da remoto su richiesta. • Arrestare il controller da remoto su richiesta. Rifiutare le richieste di esecuzione da remoto del controller. Quando è configurato un ingresso valido, è disponibile solo un'esecuzione controllata dall'ingresso. Vedere la *sezione Configurazione dei processori Premium\Atrium* (vedere EcoStruxure™ Control Expert, Modalità operative).
Modicon Quantum:	L'accesso remoto del controller a run/stop consente di: • Arrestare o avviare il controller da remoto su richiesta.
Modicon MC80:	L'accesso remoto del controller a run/stop consente una delle operazioni seguenti: • Arrestare o avviare il controller da remoto su richiesta. • Arrestare il controller da remoto su richiesta. Rifiutare le richieste di esecuzione da remoto del controller. Quando è configurato un ingresso valido, è disponibile solo un'esecuzione controllata dall'ingresso. • Rifiutare l'esecuzione o l'arresto del controller in remoto su richiesta. Vedere la sezione *Configurazione dei processori Modicon MC80* in Modicon MC80 Program Logic Controller (PLC) - Manuale utente.
Modicon Momentum MDI	L'accesso remoto del controller a run/stop consente una delle operazioni seguenti: • Arrestare o avviare il controller da remoto su richiesta. • Arrestare il controller da remoto su richiesta. Rifiutare le richieste di esecuzione da remoto del controller. Quando è configurato un ingresso valido, è disponibile solo un'esecuzione controllata dall'ingresso. Vedere la sezione *Configurazione dei processori Modicon Momentum MDI* in Modicon Momentum per EcoStruxure™ Control Expert Processori 171CBU78090, 171CBU98090, 171CBU98091 - Guida utente.

È buona prassi rifiutare l'esecuzione o l'arresto del controller da remoto su richiesta.

Accesso alle variabili controller

Per proteggere i dati del controller dall'accesso in lettura o scrittura non autorizzato, utilizzare le migliori prassi seguenti quando possibile:

- Usare dati non identificati
- Configurare EcoStruxure Control Expert per memorizzare solo le variabili HMI: **Strumenti > Impostazioni progetto... > Dati integrati PLC > Dizionario dati > Solo variabili HMI**.

  Solo variabili HMI può essere solo selezionato se il **Dizionario dati** è selezionato.
- Definire come *HMI* le variabili a cui si accede dall'HMI o SCADA. Le variabili non definite come *HMI* non sono accessibili ai client esterni.
- La connessione con SCADA deve basarsi su OFS.

Protezione memoria dati

È possibile attivare la protezione della memoria dati in EcoStruxure Control Expert selezionando **Strumenti > Impostazioni progetto > Dati integrati PLC**, quindi selezionare **Applica**. Questa funzione consente di proteggere sia i dati identificati sia quelli non identificati.

Per ulteriori informazioni sulla funzione di protezione della memoria dati, vedere la sezione Protezione della memoria dati nel documento Modalità operative EcoStruxure Control Expert.

Gestire controlli di integrità dati

Introduzione

La funzionalità di controllo automatico dell'integrità in Control Expert consente di evitare che file e software Control Expert vengano modificati da virus o malware. È inoltre possibile avviare manualmente il controllo integrità.

Controllo automatico dell'integrità

Control Expert con Topology Manager si basa sull'architettura client/server.

I server sono configurati per l'avvio automatico all'accensione o al riavvio del computer. Prima dell'avvio dei server, viene eseguito un controllo di integrità su entrambi.

Il server si avvia solo se il controllo di integrità viene completato senza rilevare danni ai dati. Se il controllo di integrità rileva il danneggiamento dei dati, viene registrato un errore visualizzabile tramite il **Visualizzatore eventi**.

Una finestra di messaggio indica i file danneggiati. Fare clic su **OK**, l'istanza Control Expert si chiude. Per ulteriori informazioni, consultare *EcoStruxure Control Expert, Manuale di installazione* e la sezione *Attivazione della comunicazione con client remoti e rafforzamento della sicurezza*.

Controllo manuale dell'integrità con Control Expert Classic

Per eseguire un controllo di integrità manuale all'avvio di un'istanza di Control Expert Classic, procedere come segue:

Passo	Azione
1	Fare clic su **Guida > Informazioni su Control Expert XXX**.
2	Nel campo **Controllo integrità**, fare clic su **Esegui test automatico**. **Risultato**: il controllo di integrità viene eseguito in background. Control Expert crea un registro del login riuscito e non riuscito del componente. Il file di registro contiene l'indirizzo IP, la data e l'ora e il risultato dell'accesso. **NOTA:** Se un controllo di integrità visualizza un accesso non riuscito al componente, il **Visualizzatore eventi** visualizza un messaggio. Fare clic su **OK**. Correggere manualmente le voci nel registro.

Controllo manuale dell'integrità con Control Expert

Per eseguire un controllo di integrità manuale all'avvio di un'istanza di Control Expert, procedere come segue:

Passo	Azione
1	Fare clic su **Guida > Informazioni su...** nella barra degli strumenti di Gestore topologia.
2	Nella casella **Informazioni su**, fare clic sul collegamento **Esegui test automatico**. **Risultato**: il controllo di integrità viene eseguito in background. Le analisi vengono eseguite sui server client locali (locali o remoti) a cui è collegato il client. Il client e i server continuano a funzionare finché non viene restituito il risultato del controllo di integrità. Per conoscere le conseguenze del controllo di integrità, vedere la tabella seguente.

CONDIZIONE	CONSEGUENZA
Nessun danneggiamento dei dati rilevato	Viene visualizzato il messaggio test automatico completato correttamente. Fare clic su **OK**.
Rilevato danneggiamento dei dati sul client	Una finestra di messaggio indica i file danneggiati. Fare clic su **OK**, si chiude il client Control Expert.
Rilevato danneggiamento dei dati su uno dei server	Il server si arresta. È stato registrato un errore che è possibile visualizzare con il **Visualizzatore eventi**.

Controllo integrità firmware M580

Il controllo dell'integrità del firmware del controller M580 viene eseguito automaticamente dopo un nuovo caricamento del firmware o il riavvio di Modicon M580 PAC.

Gestione della scheda SD

Attivare la firma dell'applicazione per evitare di eseguire un'applicazione errata da una scheda SD.

La firma della scheda SD è gestita tramite le funzioni `SIG_WRITE` e `SIG_CHECK` (vedere *EcoStruxure™ Control Expert, Communication, Block Library*).

Configurazione della protezione della porta della scheda SD

Per i controller con versione firmware 4.30 o successiva è disponibile un meccanismo di protezione della scheda SD.

Questa funzionalità può essere abilitata o disabilitata dalla scheda **Configurazione** nelle pagine Web del controller.

Aprire la pagina **Home**:

Passo	Azione
1	Aprire un browser Internet.
2	Nella barra degli indirizzi, immettere l'indirizzo IP del controller.
3	Immettere il nome utente **modbususer** e la password dell'applicazione.
4	Premere **Invio** e attendere l'apertura della pagina.

Passo	Azione
5	Selezionare **Configurazione > Sicurezza informatica**.
6	Nell'elenco a discesa, selezionare **Porta scheda SD** per configurare questa funzionalità: • **Attivata** (Le schede SD non vengono considerate dal controller). • **Disattivata** (Le schede SD sono considerate dal controller). **NOTA:** se una scheda SD è già inserita nel controller, la protezione viene attivata quando la scheda SD viene rimossa o quando si spegne e riaccende il controller. **NOTA:** quando la Protezione porta della scheda SD è attivata, l'area di memoria del backup del controller è il NAND del controller. Pertanto, l'eliminazione dell'area di backup quando la protezione è attivata comporta la cancellazione di NAND del controller.

Configurare un collegamento tecnico sicuro tra Control Expert e un controller M580 Ethernet

Compatibilità

- M580 PV < 25 (controller bianchi) e PV >= 25 (controller grigi).
- Control Expert Classic e Control Expert Topology Manager versioni V16.0 e successive.
- Firmware M580 V4.20 e successivo.
- Applicazione Control Expert versione V4.20 e successive.

Scopo di una connessione sicura

Mediante le versioni software, hardware e dell'applicazione indicate sopra, è possibile configurare una connessione sicura tra Control Expert e un controller M580 Ethernet. Questa connessione è basata sul protocollo TLS (Transport Layer Security) e fornisce una comunicazione crittografata end-to-end.

Un collegamento tecnico sicuro consente di proteggere il controller M580 dagli attacchi informatici fornendo:

- Autenticazione del controller basata su un certificato M580 autofirmato.
- Crittografia dei flussi di dati tra Control Expert e il controller M580.
- Autenticazione del client Control Expert tramite la richiesta di login/password per stabilire il tunnel HTTPS.

Una connessione sicura consente di proteggere dagli attacchi di rete seguenti:

- Attacchi replay.
- Recupero password (hash).
- Ripristino binariao applicazione.
- Attacchi man-in-the-middle (MITM) che possono modificare i dati o l'applicazione.

Funzionalità di una connessione sicura

Le funzionalità seguenti sono state aggiunte all'**Editor sicurezza**, al firmware del controller M580 e a Control Expert per supportare la creazione di un collegamento tecnico sicuro:

- Driver protocollo di comunicazione, pagina 111 sicuri
- Tre Modalità collegamento tecnico, pagina 111

Driver protocollo di comunicazione

HTTPS e **HTTPS tramite USB** sono nuovi driver che supportano collegamenti tecnici sicuri.

NOTA: Per chiarezza, sono stati rinominati due driver preesistenti:

- **TCPIP** è ora **Modbus TCP**
- **USB** è ora **Modbus TCP tramite USB**

Modalità collegamento tecnico

In base al livello di sicurezza informatica mirata, è possibile selezionare una delle tre seguenti **Modalità collegamento tecnico**:

- **Accesso completo**:

  Il controller si comporta come nelle versioni firmware precedenti. Sono accettate comunicazioni sicure e non sicure.

  - Per la comunicazione Control Expert, il controller accetta i driver non sicuri **Modbus TCP** e **Modbus TCP tramite USB** o i driver sicuri **HTTPS** e **HTTPS tramite USB**.
  - Per la comunicazione SCADA o controller-controller, **Modbus TCP** (porta 502) è accettato.

- **Filtrato** (predefinito)

  Modalità ibrida utilizzabile per applicare la sicurezza informatica sul collegamento tecnico e la connettività non sicura sui collegamenti a SCADA o altri controller.

  - Per la comunicazione Control Expert, il controller accetta i driver sicuri **HTTPS** e **HTTPS tramite USB**.
  - Per la comunicazione SCADA o controller-controller, **Modbus TCP** (porta 502) o **UMAS** (OFS) sono accettati.

    NOTA: in modalità **Filtrato**, il controller accetta i driver non sicuri **Modbus TCP** e **Modbus TCP tramite USB**, ma solo con **Modalità di connessione** impostata su **monitoraggio** nelle opzioni del progetto. La modalità di monitoraggio è di sola lettura e non consente di scaricare un'applicazione nel controller o di arrestarlo.

- **Rinforzato**:

  Questa modalità fornisce il massimo livello di sicurezza. Solo i protocolli sicuri sono accettati dal controller.

  - Per la comunicazione Control Expert, il controller accetta i driver sicuri **HTTPS** e **HTTPS tramite USB**.
  - Per la comunicazione SCADA o controller-controller, **Modbus TCP** (porta 502) o **UMAS** (OFS) sono **NON** sono accettati.

  NOTA: Il tempo di download dell'applicazione potrebbe essere significativamente influenzato se è configurata la modalità **Accesso completo** e vengono utilizzati i driver sicuri **HTTPS** o **HTTPS tramite USB**. Se si intende utilizzare driver sicuri, prendere in considerazione l'utilizzo della modalità **Filtrato** o **Rinforzato** per mantenere le prestazioni.

Riepilogo disponibilità protocollo

Ciascuna opzione della **Modalità collegamento tecnico** supporta le seguenti combinazioni di porte logiche e protocolli di comunicazione:

Scopo del collegamento:		**Collegamento tecnico sicuro**	**Collegamento tecnico non sicuro**		**HMI / SCADA**
Driver:		**HTTPS** o **HTTPS tramite USB**	**Modbus TCP** e **Modbus TCP tramite USB**		Modbus TCPIP o UMAS
Porta logica di comunicazione:		443	502		502
Modalità di connessione:		**Monitoraggio** o **Programmazione**	**Programma-zione**	**Monitorag-gio**	N/D
Modalità collegamento tecnico:	Rinforzato	✓	✗	✗	✗
	Ffiltrato	✓	✗	✓	✓
	Accesso completo	✓	✓	✓	✓

Whitelist certificato Editor di sicurezza

Un **Whitelist certificato** è introdotto nell'**Editor di sicurezza** e include le seguenti caratteristiche:

- **Aggiungi**: utilizzare questo comando per configurare l'indirizzo IP del controller M580 sul quale si desidera creare un collegamento tecnico sicuro.

- **Ottieni certificato**: utilizzare questo comando per recuperare il certificato HTTPS dal dispositivo.
- Una finestra di dialogo che consente di considerare attendibile il certificato e di aggiungerlo all'archivio certificati di Windows.
- **Visualizza certificato**: utilizzare questo comando per visualizzare e verificare il certificato.
- **Rimuovi**: utilizzare questo comando per rimuovere un certificato dall'elenco.

NOTA: In questa release sono supportati solo i certificati autofirmati.

Configurazione di una procedura di connessione sicura

La configurazione del collegamento tecnico sicuro viene eseguita tramite Control Expert e l'Editor di sicurezza e seguendo le operazioni descritte di seguito.

Attività preliminari

1. Aggiornare il controller a:
   a. V4.20 o successiva per controller standard.
   b. V4.21 o successiva per controller di sicurezza.
2. Aggiornare Control Expert a V16.0 o successiva.
3. Aprire un progetto esistente e modificare il livello dell'applicazione a V4.20 o successiva, oppure creare un nuovo progetto con il livello dell'applicazione a V4.20 o successiva.
4. Attivare HTTPS, se disattivato, nella scheda Sicurezza del controller.
5. Selezionare un'impostazione di modalità collegamento tecnico (consultare Modalità collegamento tecnico).
6. Configurare le impostazioni definitive dell'indirizzo IP del controller M580 Ethernet, se non già eseguite.

   NOTA: poiché il certificato di un controller M580 contiene l'indirizzo IP, ogni volta che si modifica l'impostazione dell'indirizzo IP, il controller rinnova il proprio certificato. È necessario considerare sempre attendibile il certificato nell'Editor sicurezza.
7. Creare una password dell'applicazione per il nuovo progetto.
8. Creare il firmware e le password Web per il nuovo progetto.

9. Scaricare l'applicazione nel controller con **Modbus TCP** o **Modbus TCP tramite USB**.

Fase 1: considerare attendibile il certificato M580 nell'Editor di sicurezza

1. Aprire l'Editor di sicurezza.
2. Al primo avvio dell'Editor di sicurezza, configurare una password per SecurityAdmin e attendere l'installazione dell'Editor di sicurezza.
3. Accedere come SecurityAdmin con password configurata.
4. Selezionare la scheda **whitelist certificati**.
5. Fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo **Aggiungi configurazione di connessione**.
6. Selezionare **HTTPS** o **HTTPS su USB** come **Protocollo di comunicazione**. Impostare quindi **Indirizzo IP** all'indirizzo IP configurato del controller.
7. Fare clic su **OK**.
8. Selezionare la riga corrispondente al controller.
9. Fare clic su **Considera attendibile certificato**, quindi su **Sì** per aggiungerlo.

   La colonna Stato certificato viene aggiornata e indica:

   - valido: il certificato è stato aggiunto correttamente.
   - sconosciuto: nessun certificato aggiunto. Utilizzare il suggerimento per visualizzare i dettagli dell'errore rilevato.
10. Se il certificato è valido, fare clic sui puntini di sospensione (...) per visualizzarne nome e dettagli dispositivo.

Fase 2: configurazione di una connessione sicura

1. Selezionare **PLC > Imposta indirizzo...** in Control Expert.
2. Nell'area PLC, immettere l'indirizzo IP del controller M580 o SYS se si sta utilizzando un cavo USB.
3. Nell'area **Protocollo di comunicazione**, selezionare **HTTPS** o **HTTPS tramite USB**.
4. Fare clic su **OK**.
5. In Control Expert, selezionare **PLC > Connetti**.
6. Impostare una password dell'applicazione

Considerazioni sulla modalità operativa

Comunicazione pronta

Quando si avvia per la prima volta un nuovo controller M580 pronto all'uso, vengono applicate le seguenti limitazioni:

- Non è supportata la connessione HTTPS tra Control Expert e il controller M580.
- La comunicazione è possibile solo utilizzando USB o TCPIP.

Ripristino controller M580 a NOCONF

È possibile commutare il controller M580 su NOCONF nei modi seguenti:

- Impostare la rotellina per ripristinare un controller Hot Standby M580.
- Usare una scheda SD nel modo seguente:
  1. Creare un'applicazione senza password.
  2. Caricare l'applicazione in un altro controller M580 dello stesso modello.
  3. Inserire la scheda SD in questo controller.
  4. Impostare %S66 su TRUE per eseguire il backup dell'applicazione sulla scheda SD.
  5. Inserire la scheda SD nel controller M580 originale quindi spegnere e riaccendere il controller.

Reimpostazione della password dell'applicazione

La procedura di ripristino della password dell'applicazione tramite assistenza tecnica è ancora disponibile nella **Modalità collegamento tecnico Filtrato** e **Accesso completo**.

È supportata la modifica della password dell'applicazione online.

Compatibilità e limitazioni della programmazione sicura rinforzata

Compatibilità

Vedere la sezione Configurare un collegamento tecnico sicuro tra Control Expert e un controller M580 Ethernet, pagina 110.

Limitazioni della modalità collegamento tecnico

Per qualsiasi connessione fisica, valgono le seguenti limitazioni per l'opzione **Modalità collegamento tecnico Rinforzata**:

- La funzionalità Dizionario dati non è funzionale.
- BMENUA0100•• non è supportato in modalità collegamento tecnico forzato.
- Eseguire l'aggiornamento a M580 con una versione prodotto (PV) 3 o successiva.
- Il controller non è accessibile mediante i seguenti blocchi funzione:
  - READ_VAR
  - WRITE_VAR
  - DATA_EXCH
  - READ_REMOTE
- Il controller non può essere analizzato da uno scanner Modbus.
- Lo scanner Modbus del controller M580 non è in grado di eseguire la scansione dei dispositivi Modbus.

- In base al protocollo di comunicazione selezionato (Modbus TCP o EtherNet/IP), alcuni servizi di diagnostica DTM non sono disponibili, come indicato di seguito:

Servizi DTM	**Protocollo**	**Disponibilità**
Connessione DTM EtherNet/IP	EtherNet/IP	✓
Disconnessione DTM EtherNet/IP	EtherNet/IP	✓
Connessione DTM Modbus	Modbus TCP	✗
Disconnessione DTM Modbus	Modbus TCP	✗
Diagnostica Ethernet	EtherNet/IP	✓
Diagnostica larghezza di banda	Modbus TCP	✗
Diagnostica RSTP	Modbus TCP	✗
Diagnostica del servizio di sincronizzazione dell'ora	EtherNet/IP	✓

Compatibilità adattatore di comunicazione

La tabella seguente riepiloga i servizi disponibili su un controller o un adattatore di comunicazione, a seconda della modalità di progettazione selezionata.

Le righe corrispondono ai servizi disponibili:

- Collegamento tecnico: Il collegamento tra Control Expert e il controller.
- Comunicazione modalità client: Scanner, Modbus, EtherNet/IP (implicito o esplicito), OPCUA, DNP3, IEC 61850.
- Comunicazione modalità server: Modbus, EtherNet/IP, OPCUA, DNP3, IEC 61850.

Le colonne corrispondono alle diverse configurazioni possibili. Ad esempio:

- Controller solo: un controller viene utilizzato senza alcun adattatore di comunicazione.
- Controller+NOC con backplane On: nel rack principale sono presenti un controller e un BMENOC03••; la porta backplane del BMENOC03•• è abilitata; Control Expert è collegato al BMENOC03••.
- Backplane controller+NOC disattivato: nel rack principale sono presenti un controller e un BMENOC03••; la porta backplane del BMENOC03•• è disattivata; Control Expert è collegato al BMENOC03••.

Quando si utilizza un adattatore di comunicazione, alcuni servizi sono disponibili sull'adattatore stesso o dal controller attraverso l'adattatore di comunicazione. Per distinguere questi due casi, si utilizzano le lettere "C" per il controller e "M" per il modulo. Ad esempio:

- Se la connessione da Control Expert al controller può essere effettuata con l'indirizzo IP del controller, si utilizza la lettera "C".
- Se la connessione da Control Expert viene effettuata utilizzando l'indirizzo IP di BMENUA0100, si utilizza la lettera "M" nella colonna relativa al modulo.

Sistema Modicon M580		Solo controller			Controller + NOC (NOC301, NOC311, NOC321)			Controller + NOC (NOC301, NOC311, NOC321)			Controller + NOC321			Controller + NUA (Modalità sic.)			Controller + BMXNOR			Controller + BMENOR step3			Controller + NOP			Controller + NOP		
Parametro dell'adattatore di comunicazione					Backplane Porta abilitata			Backplane Porta disabilitata			Backplane Porta disabilitata Inoltro IP			Inoltro IP			Backplane Isolato			Backplane Porta disabilitata			Backplane Porta abilitata senza inoltro IP			Backplane Porta disabilitata Inoltro IP		
Topologia																												
Modalità sicurezza																													
Collegamento tecnico	HTTPS	C	C	C	C	C	C	X	X	X	C	C	C	C* M	C* M	X	X	X	X	X	X	X	C	C	C	X	X	X
	Modbus TCP Monitoraggio	C	C	X	C M	C M	X	C	C	X	C	C	X	C* M	C* M	X	M	M	X	M**	M**	X	C M	C M	X	M	M	X
	Modbus TCP Programmazione	C	X	X	C M	X	X	C	X	X	C	X	X	C* M	X	X	M	X	X	M**	X	X	C M	X	X	M	X	X

Sistema Modicon M580		Solo controller			Controller + NOC (NOC301, NOC311, NOC321)			Controller + NOC (NOC301, NOC311, NOC321)			Controller + NOC321			Controller + NUA (Modalità sic.)			Controller + BMXNOR			Controller + BMENOR step3			Controller + NOP			Controller + NOP		
Parametro dell'adattatore di comunicazione					Backplane Porta abilitata			Backplane Porta disabilitata			Backplane Porta disabilitata Inoltro IP			Inoltro IP			Backplane Isolato			Backplane Porta disabilitata			Backplane Porta abilitata senza inoltro IP			Backplane Porta disabilitata Inoltro IP		
Topologia																												
Modalità sicurezza																													
Modalità client	Scanner IO Modbus	C	C	X	C M	C M	M	M	M	M	C M	C M	M	C*	C*	X	-	-	-	-	-	-	C	C	X	-	-	-
	EIP Scanner	C	C	C	C M	C M	C M	M	M	M	C M	C M	C M	C*	C*	C*	-	-	-	-	-	-	C	C	C	-	-	-
	EFB Modbus	C	C	X	C	C	X	C	C	X	C	C	X	C*	C*	X	C	C	X	C	C	X	C	C	X	C	C	X
	EFB EIP	C	C	C	C	C	C	C	C	C	C	C	C	C*	C*	C*	C	C	C	C	C	C	C	C	C	C	C	C
	EFB OPCUA	C	C	C	-	-	-	-	-	-	C	C	C	C*	C*	C*	-	-	-	-	-	-	C	C	C	C	C	C
	DNP3 IEC 60870	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-
	IEC 61850	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X
Modalità server	Modbus Server / UMAS	C	C	X	M	M	X	M	M	X	C	C	X	C* M-*	C* M*	X	M	M	X	M**	M**	X	C M	C M	X	M	M	X

Sistema Modicon M580		**Solo controller**			**Controller + NOC (NOC301, NOC311, NOC321)**			**Controller + NOC (NOC301, NOC311, NOC321)**			**Controller + NOC321**			**Controller + NUA (Modalità sic.)**			**Controller + BMXNOR**			**Controller + BMENOR step3**			**Controller + NOP**			**Controller + NOP**		
Parametro dell'adattatore di comunicazione					**Backplane Porta abilitata**			**Backplane Porta disabilitata**			**Backplane Porta disabilitata Inoltro IP**			**Inoltro IP**			**Backplane Isolato**			**Backplane Porta disabilitata**			**Backplane Porta abilitata senza inoltro IP**			**Backplane Porta disabilitata Inoltro IP**		
Topologia																												
Modalità sicurezza																															
Comunicazione SCADA	Server OPCUA	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	-	-	-	-	-	-	-	-	-	-	-	-
	Adattatore EtherNet/IP (Server locale)	C	C	C	M	M	M	M	M	M	C M	C M	C M	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Server Web HTTPS del controller	C	C	C	C	C	C	-	-	-	C	C	C	C*	C*	C*	-	-	-	-	-	-	-	C	C	C	-	-	-
	DNP3 - IEC 60870	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X	-	-	-	-	-	-	-
	IEC 61850	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	M	M	X	M	M	X

Simbolo	Descrizione
	Modalità collegamento tecnico impostata su **Accesso completo**
	Modalità collegamento tecnico impostata su **Filtrato**
	Modalità collegamento tecnico impostata su **Rinforzato**
C	• In modalità client "C" indica che la comunicazione è avviata dal controller. • In modalità server "C" indica che l'indirizzo IP di destinazione è il controller.
M	• In modalità client "M" indica che la comunicazione è avviata dall'adattatore di comunicazione. • In modalità server "M" indica che l'indirizzo IP di destinazione è l'adattatore di comunicazione. In entrambi i casi il modulo comunica con il controller tramite XBUS.
X	Non supportato
*	In base alle regole di inoltro configurate nel modulo BMENUA0100.
**	Se il server Modbus è attivato nel BMENOR00200
-	Non applicabile

Porte e servizi M580 Ethernet

Questa sezione presenta i servizi Ethernet M580 disponibili e il loro stato predefinito nell'applicazione Control Expert.

"Out of box" indica che la configurazione si applica a un controller nuovo di fabbrica, senza alcuna applicazione installata. Dopo aver installato un'applicazione sul controller, questa configurazione "out of box" non può più essere realizzata.

"Predefinito" indica che la configurazione si applica a un'applicazione Control Expert predefinita.

Controller M580 con versione firmware ≥ 4,10

Servizio	Numero di porta	Out of box	Predefinito	Note
HTTP	80/tcp	Chiuso	Chiuso	Server Web
Modbus TCP	502/tcp	Aperto	Aperto	-
EtherNet/IP	44818/tcp-udp	Chiuso	Chiuso	EtherNet/IP esplicito (Classe 3)
DHCP	67/udp	Chiuso	Chiuso	-
FTP	21/tcp	Aperto	Chiuso	Firmware, memorizzazione dati, FDR
TFTP	69/udp	Chiuso	Chiuso	FDR (X80)
SNMP	161/udp	Chiuso	Chiuso	-
EtherNet/IP	2222/udp	Chiuso	Chiuso	EtherNet/IP implicito (Classe 1)
NTP/SNTP	123/udp	Chiuso	Chiuso	NTPV4 o SNTP

Controller M580 con versione firmware ≥ 4.10

Servizio	Numero di porta	Out of box	Predefinito	Note
HTTPS	443/tcp	Aperto	Aperto	Web, firmware, memorizzazione dati
Modbus TCP	502/tcp	Aperto	Aperto	NOTA(1)
EtherNet/IP	44818/tcp-udp	Chiuso	Chiuso	EtherNet/IP esplicito (Classe 3)
DHCP	67/udp	Chiuso	Chiuso	-

Servizio	Numero di porta	Out of box	Predefinito	Note
FTP	21/tcp	Chiuso	Chiuso	FDR
TFTP	69/udp	Chiuso	Chiuso	FDR (X80)
SNMP	161/udp	Chiuso	Chiuso	-
EtherNet/IP	2222/udp	Chiuso	Chiuso	EtherNet/IP implicito (Classe 1)
NTP/SNTP	123/udp	Chiuso	Chiuso	NTPV4 o SNTP
DPWS	9867/tcp	Aperto	Aperto	Aggiornamento firmware, NOTA(1)
WS-Discovery	3702/udp	Chiuso	Chiuso	Sincronizzazione stato con SNMP
NOTA(1): la porta e il relativo servizio sono di primaria importanza per il cliente, per garantire che le funzioni fondamentali siano operative nell'ambiente industriale desiderato. La porta rimane aperta per motivi di sicurezza e disponibilità. Gli utenti non possono disattivare la porta.				

Servizi per sistema di Sicurezza informatica

Introduzione

Questo capitolo elenca i principali servizi di sicurezza informatica disponibili per ciascun sistema e indica dove reperire informazioni dettagliate nella guida di Control Expert.

Servizi di Sicurezza informatica

Panoramica

Software, DTM o i dispositivi sono elementi che forniscono servizi di sicurezza informatica in un sistema globale. I servizi di sicurezza informatica sono elencati per i seguenti elementi:

- Software Control Expert, pagina 126
- Controller Modicon M340, pagina 126
- Controller Modicon M580, pagina 127
- Controller e moduli di comunicazione Modicon Quantum, pagina 128
- Moduli Modicon X80, pagina 129
- Controller e moduli di comunicazione Modicon Premium/Atrium, pagina 130
- Modicon Momentum MDI, pagina 131
- Modicon MC80, pagina 132

I servizi di sicurezza informatica elencati di seguito sono descritti nel capitolo precedente:

- Disattivare servizi inutilizzati, pagina 32
- Controllo accesso, pagina 33
- Configurare la comunicazione crittografata, pagina 36
- Registrazione eventi, pagina 52
- Autenticazione, pagina 97
- Autorizzazioni, pagina 102
- Controlli di integrità, pagina 106

Servizi di Sicurezza informatica nel software Unity Pro/ Control Expert

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

Disponibilità dei servizi di Sicurezza informatica

Software	**Servizi di Sicurezza informatica**							
Codice prodotto	**Disattivare servizi inutilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Comunicazione crittografata con confidenzialità**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
Unity Pro v8.1	–	N.A.	–	–	–	X	X	X
Unity Pro≥v10.0	–	N.A.	X	–	X	X	X	X
Unity Pro≥v13.0	–	N.A.	X	X	X	X	X	X
Control Expert≥v14.0	X	X	X	X	X	X	X	X

X Disponibile, è implementato almeno un servizio.

- Non disponibile

N.A. Non applicabile

Sono disponibili meccanismi di recupero delle password più affidabili quando si utilizza Control Expert versioni superiori o uguali alla versione v.15.1 destinate alle applicazioni per le versioni firmware M580 superiori o uguali alla versione v4.01.

Servizi di Sicurezza informatica nei controller Modicon M340

Versione firmware minima e servizi di sicurezza informatica disponibilità nei controller Modicon M340:

Controller		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
BMX P34 1000	2.60	–	–	–	–	X	X	–
BMX P34 2000	2.60	–	–	–	–	X	X	–
BMX P34 2010	2.60	–	–	–	–	X	X	–
BMX P34 20102	2.60	–	–	–	–	X	X	–
BMX P34 2020	2.60	X	X	–	–	X	X	–
BMX P34 2030	2.60	X	X	–	–	X	X	–
BMX P34 20302	2.60	X	X	–	–	X	X	–

X Disponibile, è implementato almeno un servizio.

- Non disponibile

Servizi di Sicurezza informatica nei controller Modicon M580

Versione firmware minima e servizi di sicurezza informatica disponibilità nei controller Modicon M580:

Controller		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
BME P58 1020	1.00	X	X	–	X	X	X	X
BME P58 2020	1.00	X	X	–	X	X	X	X
BME P58 2040	1.00	X	X	–	X	X	X	X
BME P58 3020	1.00	X	X	–	X	X	X	X
BME P58 3040	1.00	X	X	–	X	X	X	X
BME P58 4020	1.00	X	X	–	X	X	X	X
BME P58 4040	1.00	X	X	–	X	X	X	X
BME P58 5040	2.10	X	X	–	X	X	X	X
BME P58 6040	2.10	X	X	–	X	X	X	X

Controller		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
BME H58 2040	2.10	X	X	–	X	X	X	X
BME H58 4040	2.10	X	X	–	X	X	X	X
BME H58 6040	2.10	X	X	–	X	X	X	X

X Disponibile, è implementato almeno un servizio.

- Non disponibile

Servizi di Sicurezza informatica nei controller e moduli Modicon Quantum

Versione firmware minima e servizi di sicurezza informatica disponibilità nei controller Modicon Quantum:

Controller		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
140CPU31110	3.20	–	–	–	–	X	X	–
140CPU43412•	3.20	–	–	–	–	X	X	–
140CPU53414•	3.20	–	–	–	–	X	X	–
140CPU651•0	3.20	X	X	–	–	X	X	–
140CPU65260	3.20	X	X	–	–	X	X	–
140CPU65860	3.20	X	X	–	–	X	X	–
140CPU67060	3.20	X	X	–	–	X	X	–
140CPU67160	3.20	X	X	–	–	X	X	–
140CPU6726•	3.20	X	X	–	–	X	X	–
140CPU67861	3.20	X	X	–	–	X	X	–

X Disponibile, è implementato almeno un servizio.

- Non disponibile

Moduli Modicon Quantum che supportano servizi di sicurezza informatica:

Modulo		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
140NOC7710•	1.00	–	X	–	–	X	–	–
140NOC78000	2.00	X	X	–	–	X	–	–
140NOC78100	2.00	X	X	–	–	X	–	–
140NOE771••	X	X	–	–	–	X	–	–
140NWM10000	–	X	–	–	–	–	–	–
X Disponibile, è implementato almeno un servizio. **-** Non disponibile								

Servizi di Sicurezza informatica nei moduli Modicon X80

Moduli Modicon X80 che supportano servizi di sicurezza informatica:

Modulo		Servizi di Sicurezza informatica							
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Comunicazione crittografata con confidenzialità**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
BMECXM0100	1.01	X	X	–	–	X	–	–	X
BMENOC0301	1,01	X	X	X	–	X	X	–	X
BMENOC0311	1,01	X	X	X	–	X	X	–	X
BMXNOC0401.2	2.05	X	X	–	–	–	–	–	–
BMXNOE0100.2	2.90	X	X	–	–	–	–	–	–
BMXNOE0110.2	6.00	X	X	–	–	–	–	–	–
BMXPRA0100	2.60	X	X	–	–	–	X	–	–
BMENOC0301	2.11	X	X	X	X	X	X	–	X

Modulo		Servizi di Sicurezza informatica							
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Comunicazione crittografata con confidenzialità**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
BMENOC0311	2.11	X	X	X	X	X	X	–	X
X Disponibile, è implementato almeno un servizio. **-** Non disponibile									

Servizi di Sicurezza informatica nei controller e moduli Modicon Premium/Atrium

Versione firmware minima e servizi di sicurezza informatica disponibilità nei controller Modicon Premium/Atrium:

Controller		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
TSXH57•4M	3.10	–	–	–	–	X	X	–
TSXP570244M	3.10	–	–	–	–	X	X	–
TSXP57•04M	3.10	–	–	–	–	X	X	–
TSXP57•54M	3.10	–	–	–	–	X	X	–
TSXP571634M TSXP572634M TSXP573634M (tramite la porta ETY)	3.10	X	X	–	–	X	X	–

Controller		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
TSXP574634M TSXP575634M TSXP576634M (porta Ethernet integrata)	3.10	X	X	–	–	X	X	–
X Disponibile, è implementato almeno un servizio. **-** Non disponibile								

Moduli Modicon Premium/Atrium che supportano servizi di sicurezza informatica:

Modulo		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
TSXETC101.2	2.04	X	X	–	–	–	–	–
TSXETY4103	5.70	X	X	–	–	–	–	–
TSXETY5103	5.90	X	X	–	–	–	–	–
X Disponibile, è implementato almeno un servizio. **-** Non disponibile								

Servizi di sicurezza informatica in moduli e controller Modicon Momentum MDI

Versione firmware minima e disponibilità dei servizi di sicurezza informatica in Modicon Momentum MDI:

Controller		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
171CBU78090	1.0	X	X	–	–	X	X	–
171CBU98090	1.0	X	X	–	–	X	X	–
171CBU98091	1.0	X	X	–	–	X	X	–
X Disponibile, è implementato almeno un servizio. **-** Non disponibile								

Servizi di sicurezza informatica in moduli e controller Modicon MC80

Versione firmware minima e disponibilità dei servizi di sicurezza informatica in Modicon MC80:

Controller		Servizi di Sicurezza informatica						
Codice prodotto	**Firmware min.**	**Disattivazione dei servizi non utilizzati**	**Controllo accesso**	**Comunicazione crittografata**	**Registrazione degli eventi**	**Autenticazione**	**Autorizzazioni**	**Controlli di integrità**
BMKC8020301	1.2	X	X	–	–	X	X	–
BMKC8020310	1.0	X	X	–	–	X	X	–
BMKC8030311	1.2	X	X	–	–	X	X	–
X Disponibile, è implementato almeno un servizio. **-** Non disponibile								

Servizi di sicurezza Modicon M340

Panoramica

La descrizione delle impostazioni dei servizi di sicurezza della comunicazione è fornita per controller Modicon M340 in diversi manuali, come descritto nella sezione seguente.

Controller Modicon M340 con porte Ethernet integrate

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza* (vedere Modicon M340 per Ethernet, Moduli di comunicazione e processori, Manuale utente).
Controllo degli accessi:	Vedere la sezione *Parametri di configurazione della messaggistica* (vedere Modicon M340 per Ethernet, Moduli di comunicazione e processori, Manuale utente).

Servizi di sicurezza Modicon M580

Controller Modicon M580

La descrizione dei parametri di comunicazione relativi alla sicurezza informatica è fornita nella sezione che descrive la *Scheda Sicurezza* (vedere Modicon M580, Hardware, Manuale di riferimento).

Servizi di sicurezza Modicon Quantum

Panoramica

La descrizione delle impostazioni dei servizi di sicurezza della comunicazione è fornita per controller Modicon Quantum e moduli Ethernet in diversi manuali, come descritto nelle sezioni seguenti.

Controller Modicon Quantum con porte Ethernet integrate

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza (Attivare / Disattivare HTTP, FTP e TFTP)* (vedere Quantum utilizzo EcoStruxure™ Control Expert, Ethernet Moduli di rete, Manuale dell'utente).
Controllo degli accessi:	Vedere la sezione *Modicon Quantum con configurazione della messaggistica del controller Ethernet Control Expert* (vedere Quantum con EcoStruxure™ Control Expert, Ethernet Moduli di rete, Manuale dell'utente).

Modulo 140 NOC 771 0x

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza (Attivare / Disattivare HTTP, FTP e TFTP)* (vedere Quantum utilizzo EcoStruxure™ Control Expert, Ethernet Moduli di rete, Manuale dell'utente).
Controllo degli accessi:	Vedere la sezione *Configurazione del controllo di accesso* (vedere Quantum con EcoStruxure™ Control Expert, 140 NOC 771 01, Modulo di comunicazione Ethernet, Manuale utente).

Modulo 140 NOC 780 00

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza* (vedere Quantum EIO, Rete di controllo, Guida di installazione e configurazione).
Controllo degli accessi:	Vedere la sezione *Configurazione del controllo di accesso* (vedere Quantum EIO, Rete di controllo, Guida di installazione e configurazione).

Modulo 140 NOC 781 00

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza* (vedere Quantum EIO, Rete di controllo, Guida di installazione e configurazione).
Controllo degli accessi:	Vedere la sezione *Configurazione del controllo di accesso* (vedere Quantum EIO, Rete di controllo, Guida di installazione e configurazione).

Modulo 140 NOE 771 xx

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza (Attivare / Disattivare HTTP, FTP e TFTP)* (vedere Quantum utilizzo EcoStruxure™ Control Expert, Ethernet Moduli di rete, Manuale dell'utente), sezione *Sicurezza* (vedere Quantum utilizzo EcoStruxure™ Control Expert, Ethernet Moduli di rete, Manuale dell'utente) e sezione *Definizione delle password di scrittura e HTTP* (vedere Quantum utilizzo EcoStruxure™ Control Expert, Moduli di rete Ethernet, Manuale dell'utente).

Modulo 140 NWM 100 00

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza (Attivare / Disattivare HTTP, FTP e TFTP)* (vedere Quantum utilizzo EcoStruxure™ Control Expert, Ethernet Moduli di rete, Manuale dell'utente).

Servizi di sicurezza Modicon X80

Panoramica

La descrizione delle impostazioni dei servizi di sicurezza della comunicazione è fornita per moduli Modicon X80 Ethernet in diversi manuali, come descritto nelle seguenti sezioni.

Modulo BMXNOC0401.2

Una descrizione dei parametri di comunicazione relativi alla sicurezza informatica è disponibile nelle seguenti sezioni:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza* (vedere Modicon M340 per Ethernet, Moduli di comunicazione e processori, Manuale utente).
Controllo degli accessi:	Vedere la sezione *Configurazione del controllo di accesso* (vedere Modicon M340, BMX NOC 0401, Modulo di comunicazione Ethernet, Manuale utente).

Modulo BMXNOE0100.2 e BMXNOE0110.2

Una descrizione dei parametri di comunicazione relativi alla sicurezza informatica è disponibile nelle seguenti sezioni:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza* (vedere Modicon M340 per Ethernet, Moduli di comunicazione e processori, Manuale utente).
Controllo degli accessi:	Vedere la sezione *Parametri di configurazione della messaggistica* (vedere Modicon M340 per Ethernet, Moduli di comunicazione e processori, Manuale utente).

Modulo BMXPRA0100

Il modulo BMXPRA0100 è configurato come controller Modicon M340. Una descrizione dei parametri di comunicazione relativi alla sicurezza informatica è disponibile nelle seguenti sezioni:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza* (vedere Modicon M340 per Ethernet, Moduli di comunicazione e processori, Manuale utente).
Controllo degli accessi:	Vedere la sezione *Parametri di configurazione della messaggeria* (vedere Modicon M340 per Ethernet, Moduli di comunicazione e processori, Manuale utente).

Modulo BMXNOR0200H

Una descrizione dei parametri di comunicazione relativi alla sicurezza informatica è disponibile nelle seguenti sezioni:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza* (vedere Modicon X80 , BMXNOR0200H Modulo RTU, Manuale utente).
Controllo degli accessi:	Vedere lasezione *Parametri di configurazione della messaggeria*.

Modulo BMENOR2200H

Una descrizione dei parametri di comunicazione relativi alla sicurezza informatica è disponibile nelle seguenti sezioni:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza*.
Controllo degli accessi:	Vedere lasezione *Parametri di configurazione della messaggeria*.

Modulo BMECXM0100

Una descrizione dei parametri di comunicazione relativi alla sicurezza informatica è fornita nel capitolo *Configurazione dei servizi Ethernet* (vedere Modicon M580, BMECXM CANopen Moduli, Manuale utente).

Moduli BMENOC0301 and BMENOC0311

Una descrizione dei parametri di comunicazione relativi alla sicurezza informatica è fornita nellasezione *Configurazione dei servizi di sicurezza* (vedere Modicon M580 BMENOC0301 / BMENOC0311 Ethernet Modulo di comunicazione, Guida di installazione e configurazione).

Modulo BMENUA0100

Una descrizione dei parametri di comunicazione relativi alla sicurezza informatica è disponibile nelle seguenti sezioni:

Comunicazione **Ethernet**:	Vedere la sezione Impostazioni di Sicurezza informatica (vedere M580, BMENUA0100 Modulo integrato OPC UA, Guida di installazione e configurazione).
Controllo di accesso:	Vedere la sezione *Controllo accesso*.

Servizi di sicurezza Modicon Premium/Atrium

Panoramica

La descrizione delle impostazioni dei servizi di sicurezza della comunicazione è fornita per controller Modicon Premium/Atrium e moduli Ethernet in diversi manuali, come descritto nelle sezioni seguenti.

Controller Modicon Premium/Atrium con porte Ethernet integrate

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Parametri di configurazione del servizio di sicurezza* (vedere Premium e Atrium Utilizzo EcoStruxure™ Control Expert, Moduli di rete Ethernet, Manuale dell'utente).
Controllo degli accessi:	Vedere la sezione *Configurazione della messaggistica TCP/IP (TSX P57 6634/ 5634/4634)* (vedere Premium e Atrium Utilizzo EcoStruxure™ Control Expert, Moduli di rete Ethernet, Manuale dell'utente).

Controller Modicon Premium/Atrium tramite porte ETY

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Parametri di configurazione del servizio di sicurezza* (vedere Premium e Atrium Utilizzo EcoStruxure™ Control Expert, Moduli di rete Ethernet, Manuale dell'utente).
Controllo degli accessi:	Vedere la sezione *Configurazione della messaggistica TCP/IP* (vedere Premium e Atrium Utilizzo EcoStruxure™ Control Expert, Moduli di rete Ethernet, Manuale dell'utente).

Modulo TSX ETC 101.2

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Sicurezza* (vedere Premium con EcoStruxure™ Control Expert, TSX ETC 101 - Modulo di comunicazione Ethernet, Manuale utente).
Controllo degli accessi:	Vedere la sezione *Configurazione del controllo di accesso* (vedere Premium con EcoStruxure™ Control Expert, TSX ETC 101 - Modulo di comunicazione Ethernet, Manuale utente).

Modulo TSX ETY x103

Le sezioni seguenti contengono la descrizione dei parametri di comunicazione relativi alla sicurezza informatica:

Comunicazione Ethernet:	Vedere la sezione *Parametri di configurazione del servizio di sicurezza* (vedere Premium e Atrium Utilizzo EcoStruxure™ Control Expert, Moduli di rete Ethernet, Manuale dell'utente).
Controllo degli accessi:	Vedere la sezione *Configurazione della messaggistica TCP/IP* (vedere Premium e Atrium Utilizzo EcoStruxure™ Control Expert, Moduli di rete Ethernet, Manuale dell'utente).

Servizi di sicurezza Modicon Momentum MDI

La descrizione delle impostazioni dei servizi di sicurezza della comunicazione è fornita per il controller Modicon Momentum MDI descritta in *Momentum per EcoStruxure™ Control Expert - Processori 171CBU78090, 171CBU98090, 171CBU98091 - Guida utente*.

Servizi di sicurezza modicon MC80

La descrizione delle impostazioni dei servizi di sicurezza della comunicazione è fornita per il controller MC80 descritta in *Modicon MC80 Program Logic Controller (PLC) - Manuale dell'utente*.

Come proteggere l'architettura M580, M340, Momentum MDI e MC80 con EAGLE40 tramite VPN

Introduzione

Questo capitolo spiega come aumentare la protezione dei controller dagli attacchi informatici affidandosi a un dispositivo firewall come EAGLE40-07 di Belden, configurato per stabilire connessioni VPN. L'implementazione di tale dispositivo in un'architettura può aiutare a mitigare le vulnerabilità esistenti nei dispositivi e a ridurre la superficie di attacco di diversi prodotti.

È buona norma aumentare la protezione di rete, workstation e dispositivi, come descritto in *Sistemi di controller Modicon - Sicurezza informatica - Guida utente* disponibile per il download all'indirizzo: https://www.se.com/us/en/download/document/EIO0000001999/

Firewall EAGLE40

Perché utilizzare un firewall?

L'utilizzo di un firewall per rafforzare la sicurezza informatica di un'architettura esistente offre i seguenti vantaggi:

- La sicurezza informatica delle reti e dei dispositivi di controllo è rafforzata.
- La sicurezza informatica rafforzata si basa sul protocollo IPSEC.
- L'impatto sull'architettura e sulle prestazioni esistenti può essere ridotto al minimo.

Caratteristiche principali di EAGLE40

Il firewall EAGLE40 è una soluzione per coprire o mitigare i problemi residui di sicurezza informatica.

- Attraverso la potente VPN IPSEC, il firewall EAGLE40 fornisce la riservatezza prevista sul traffico di rete per contribuire a prevenire gli attacchi condotti da *Man in the middle*. Assicura inoltre l'autenticazione del mittente evitando attacchi di tipo "spoofing". L'integrità dei messaggi è rafforzata dai metodi di crittografia e non può essere manomessa.

- Sono inoltre disponibili funzionalità di filtro standard che consentono di controllare il traffico e i protocolli in base all'indirizzo IP, Mac e alla porta dei dispositivi di rete.
- Il firewall EAGLE40 è un prodotto scalabile che può essere incluso nelle architetture multipunto, con prestazioni di velocità e larghezza di banda che garantiscono la trasparenza della rete.

Prerequisiti

Installazione del software

È necessario un software client VPN compatibile per stabilire un tunnel VPN basato sul protocollo IPSEC tra il client e il firewall.

Il firewall EAGLE40 richiede l'uso del client VPN IPSEC/IKEV2.

NOTA: Utilizzare la soluzione client VPN fornita da TheGreenBow.

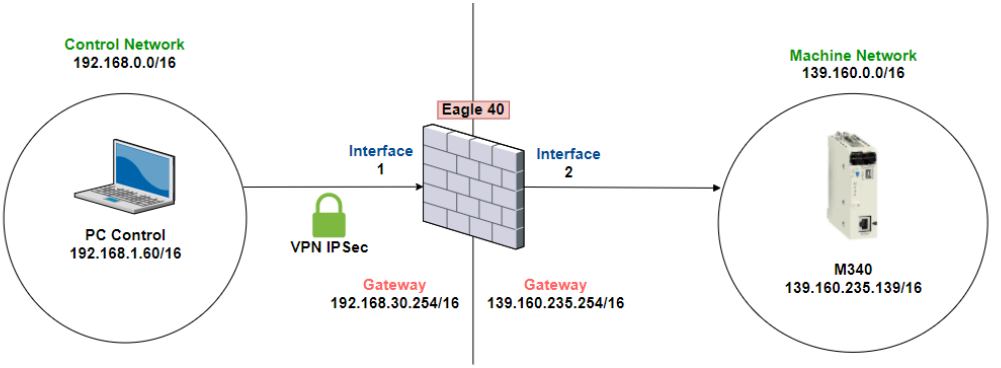
Nelle procedure di configurazione descritte di seguito, si utilizza questo software che è possibile scaricare al seguente URL:

https://www.thegreenbow.com/en/

Macchine e sistemi operativi

Prima di configurare il firewall, è necessario preparare tutti gli indirizzi IP in uso nelle architetture.

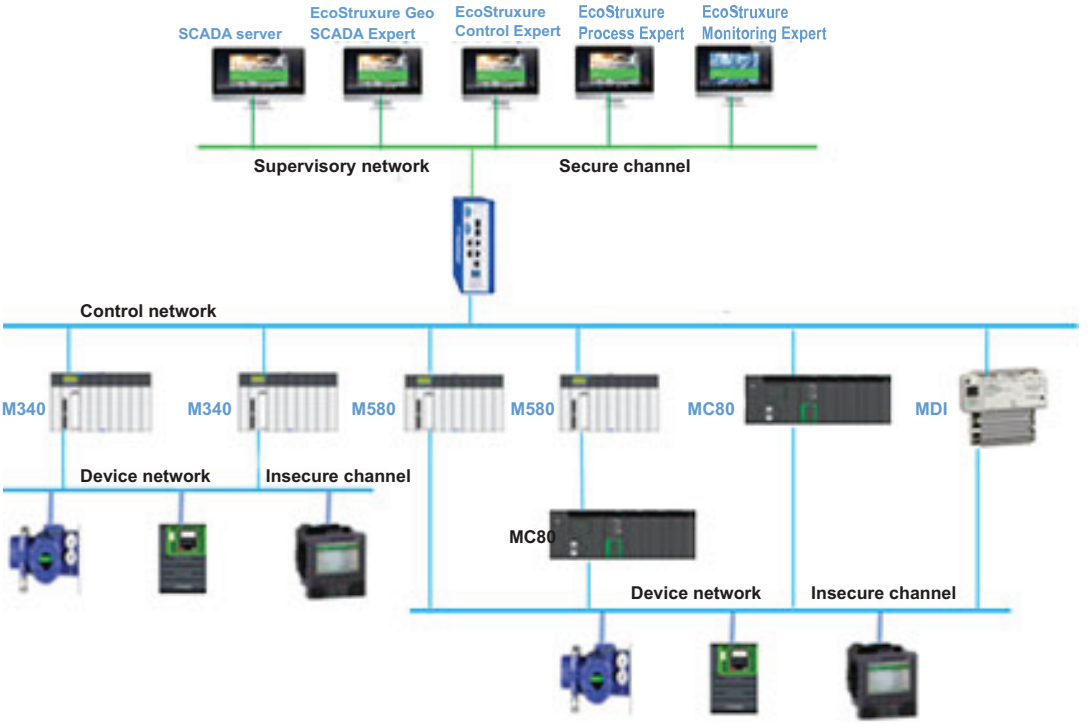
Lo schema seguente è un esempio:



Architettura tipica

Le istruzioni relative all'architettura e alla configurazione contenute nel presente documento sono fornite a titolo di esempio e possono essere adattate alle varie architetture e sistemi.

Ad esempio, l'architettura mista seguente, che combina controller Modicon M340, M580, Momentum MDI e MC80, è un'architettura tipica:



NOTA: Installare il firewall EAGLE40 in prossimità dei controller.

Configurazione del firewall

Configurazione Web

Per configurare il firewall, aprire un browser Internet e immettere il seguente URL:

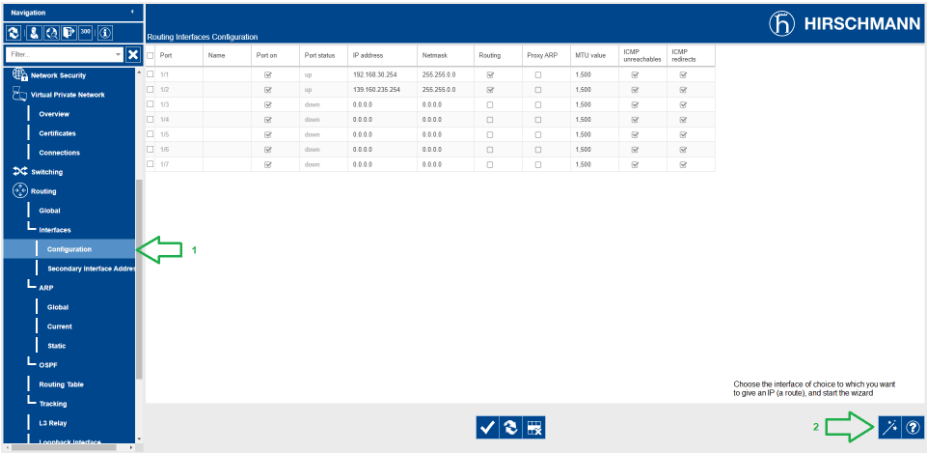
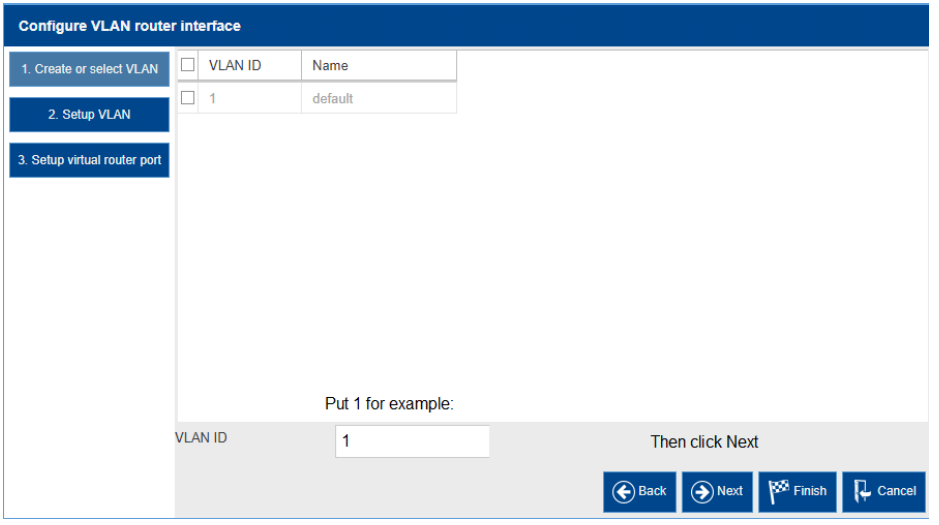
```
https://[IPFirewall]/admin
```

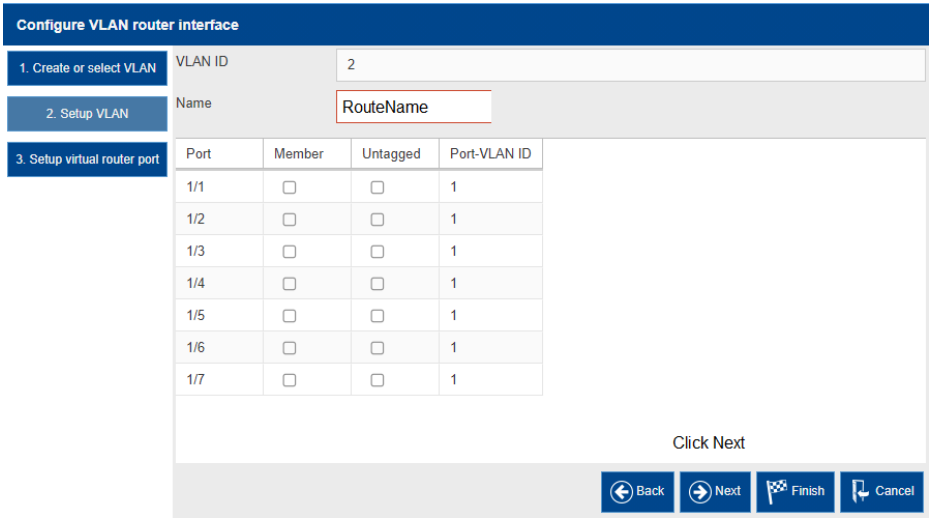
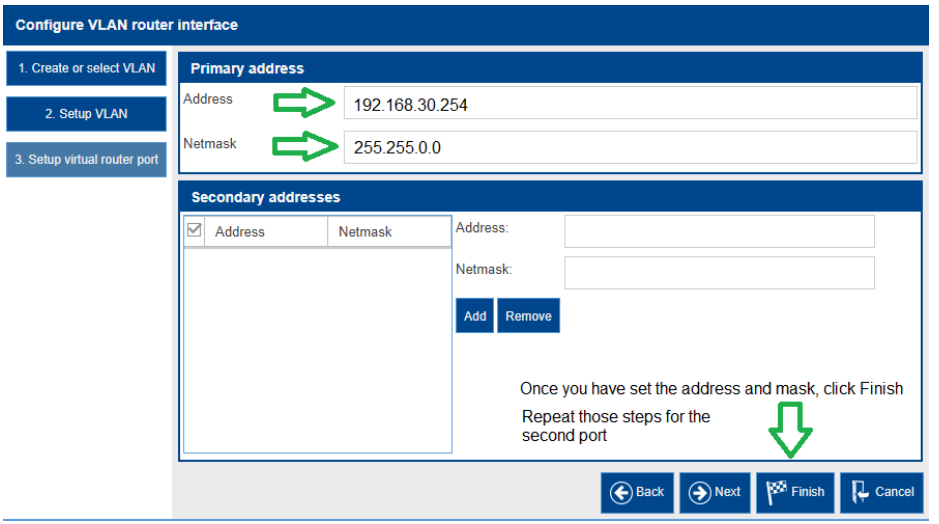
Fare clic su **Invio** e utilizzare la combinazione nome utente/password predefinita `admin/private` per accedere.

NOTA: Al primo accesso, è necessario modificare la password.

Configurazione dei percorsi

Per configurare i percorsi, procedere come segue:

Passo	Azione
1	 **1.** Nel riquadro di sinistra **Navigation** aprire la pagina Web **Routing > Interfaces > Configuration**. Selezionare l'interfaccia Ethernet che si desidera configurare. **2.** Fare clic sull'icona  per avviare la finestra **Configure VLAN Router Interface**.
2	Impostare un numero ID sulla VLAN che si desidera configurare (1 nell'esempio), quindi fare clic su **Next**. 

Passo	Azione
3	Impostare un nome di percorso per la VLAN da configurare (RouteName nell'esempio), quindi fare clic su **Next**. 
4	Impostare l'indirizzo IP della rete di controllo e la relativa maschera (`192.168.30.254/16` nell'esempio), quindi fare clic su **Finish**. 
5	Ripetere i passi da 1 a 4 per la rete di macchine che utilizza la seconda interfaccia Ethernet.

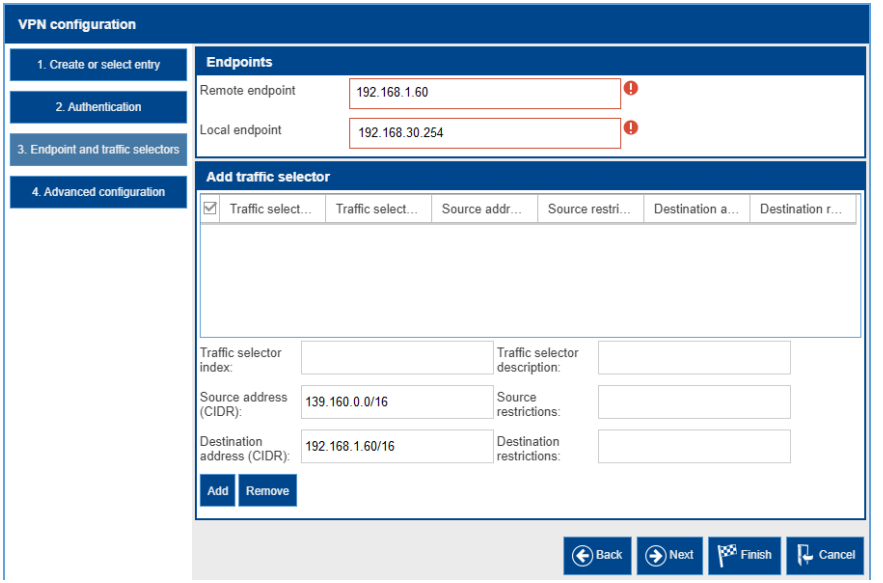
Nell'esempio seguente è stata impostata l'interfaccia gateway della rete di controllo del firewall su `192.168.30.254/16` sulla prima porta fisica e la rete di macchine su `139.160.235.254/16` sulla seconda porta fisica.

Port	Name	Port on	Port status	IP address	Netmask	Routing	Proxy ARP	MTU value	ICMP unreachables	ICMP redirects
1/1		☑	up	192.168.30.254	255.255.0.0	☑	☐	1,500	☑	☑
1/2		☑	up	139.160.235.254	255.255.0.0	☑	☐	1,500	☑	☑
1/3		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/4		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/5		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/6		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑
1/7		☑	down	0.0.0.0	0.0.0.0	☐	☐	1,500	☑	☑

Configurazione della VPN nel firewall

Per configurare la VPN, procedere nel modo seguente:

Passo	Azione
1	Nel riquadro sinistro della pagina Web, fare clic sul menu **Virtual Private Network** > **Connections**. Fare clic sull'icona  .
2	Scegliere un numero di indice e un nome, quindi fare clic su **Next**.
3	Scegliere una password (PSK), quindi fare clic su **Next**.

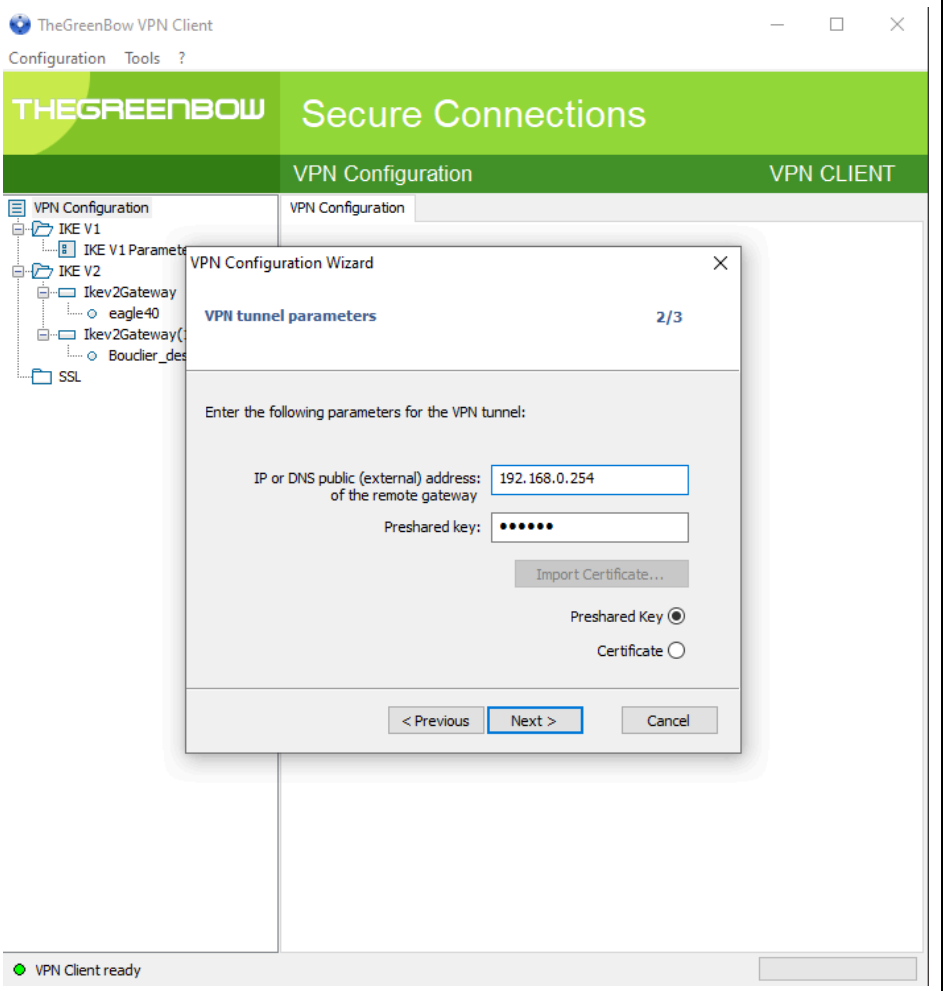
Passo	Azione
4	Compilare gli indirizzi IP e le maschere in base alla rete. • **Remote endpoint**: il computer che si connette al firewall tramite VPN. • **Local endpoint**: il gateway configurato nei percorsi. • **Source address (CIDR)**: la rete di macchine protetta accessibile solo una volta connessa tramite VPN. • **Destination address (CIDR)**: il computer che si connette al firewall tramite VPN.  Fare clic su **Next**.
5	Impostare un tempo margine. Il valore predefinito è 150. Impostare **IKE Version** a ikev2, quindi fare clic su **Finish**.

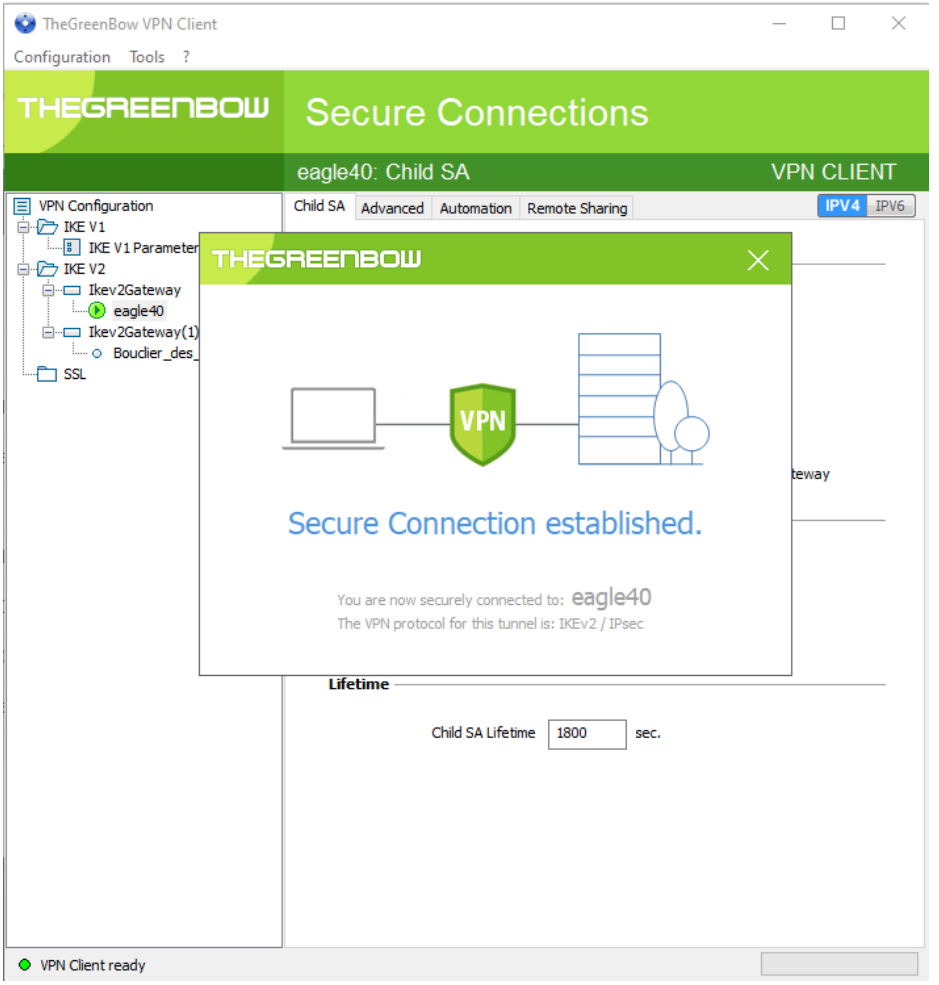
Configurazione del client VPN

NOTA: In questo esempio, si utilizza la soluzione client VPN fornita da TheGreenBow.

Per configurare il client VPN, procedere nel modo seguente:

Passo	Azione
1	Scaricare e installare il software client VPN.
2	Nel riquadro sinistro della finestra Client VPN, fare clic con il pulsante destro del mouse su **VPN Configuration** e scegliere **Wizard**.
3	Selezionare **IKEv2 Tunnel** e fare clic su **Avanti**.

Passo	Azione
4	Impostare l'indirizzo IP del firewall accessibile tramite l'interfaccia di rete di controllo (192.168.0.254 nell'esempio). Immettere il PSK selezionato in precedenza.  Fare clic su **Next**, quindi su **Finish**.
5	Nel riquadro sinistro della finestra Client VPN, fare clic con il pulsante destro del mouse sul tunnel Ikev2 appena creato e rinominarlo.

Passo	Azione
6	Fare clic con il pulsante destro del mouse sul tunnel Ikev2 appena rinominato e selezionare **Open Tunnel**. Una notifica conferma che è stata stabilita la connessione sicura. 

Glossario

802.1Q:

L'identificatore del protocollo IEEE per LAN virtuale (VLAN). Questo standard fornisce livelli di identificazione e qualità di servizio VLAN (QoS).

A

adattatore:

Un adattatore è la destinazione delle richieste di connessione dati di I/O in tempo reale provenienti dagli scanner. Non può inviare o ricevere dati di I/O in tempo reale a meno che non sia specificamente configurato dallo scanner per eseguire queste operazioni; inoltre non memorizza o genera i parametri di comunicazione dati necessari per stabilire la connessione. Un adattatore accetta richieste di messaggi espliciti (con e senza connessione) provenienti da altri dispositivi.

ambiente critico:

Resistenza a idrocarburi, oli industriali, detergenti e residui di saldatura. Umidità relativa fino a 100%, atmosfera salina, variazioni di temperatura significative, temperatura di funzionamento tra - 10°C e + 70°C o in installazioni mobili. Per i dispositivi rinforzati (H), l'umidità relativa arriva fino al 95% e la temperatura di funzionamento è compresa tra -25°C e + 70°C.

Anello principale:

L'anello principale di una rete Ethernet RIO. L'anello contiene moduli RIO e un rack locale (contenente un controller con servizio di scansione I/O Ethernet) e un modulo di alimentazione.

apparecchiatura distribuita:

Qualsiasi dispositivo Ethernet (dispositivo Schneider Electric, PC, server o dispositivi di terze parti) che supporti lo scambio con un controller o altro servizio di scansione I/O Ethernet.

architettura:

L'architettura descrive una struttura per la definizione delle specifiche di una rete che comprende i seguenti componenti:

- componenti fisici, loro organizzazione funzionale e configurazione
- principi e procedure di funzionamento
- formati di dati utilizzati durante il funzionamento

ARRAY:

Un `ARRAY` è una tabella di elementi dello stesso tipo. La sintassi è la seguente: `ARRAY [<limiti>] OF <Tipo>`

Esempio: `ARRAY [1..2] OF BOOL` è una tabella a una dimensione composta da due elementi di tipo `BOOL`.

`ARRAY [1..10, 1..20] OF INT` è una tabella a due dimensioni composta da 10x20 elementi di tipo `INT`.

ART:

(*application response time*) Il tempo impiegato da un'applicazione del controller per reagire a un determinato ingresso. L'ART viene misurato dal momento in cui un segnale fisico viene attivato nel controller, generando un comando di scrittura, fino a quando non si attiva l'uscita remota, a dimostrazione che i dati sono stati ricevuti.

AUX:

Un task (AUX) è un task del processore periodico e facoltativo eseguito attraverso il proprio software di programmazione. Il task AUX viene utilizzato per eseguire una parte dell'applicazione che richiede una priorità bassa. Questo task viene eseguito solo se i task MAST e FAST non hanno nulla da eseguire. Il task AUX ha due sezioni:

- IN: gli ingressi sono copiati nella sezione IN prima dell'esecuzione del task AUX.
- OUT: le uscite sono copiate nella sezione OUT dopo l'esecuzione del task AUX.

B

BCD:

(*Binary-Coded Decimal*, decimale in codice binario) Codifica binaria di numeri decimali.

BOOL:

(*Tipo booleano*) Tipo di dati base utilizzato in informatica. Una variabile `BOOL` può avere uno dei seguenti valori: 0 (`FALSE`) o 1 (`TRUE`).

Un bit estratto di parola è di tipo `BOOL`, ad esempio: `%MW10.4`.

BOOTP:

(*Bootstrap Protocol*). Un protocollo di rete UDP che può essere utilizzato da un client di rete per recuperare automaticamente un indirizzo IP da un server. Il client si identifica sul server utilizzando il proprio indirizzo MAC. Il server, che conserva una tabella preconfigurata degli indirizzi MAC del dispositivo client e gli indirizzi IP associati, invia al client l'indirizzo IP definito. Il servizio BOOTP utilizza le porte UDP 67 e 68.

broadcast:

Un messaggio inviato a tutti i dispositivi in un dominio di trasmissione.

C

CCOTF:

(*Modifica al volo della configurazione*) Una funzionalità di Control Expert che consente una modifica hardware del modulo nella configurazione di sistema mentre il sistema è in funzione. Questa modifica non influisce sulle operazioni attive.

CIP™:

(*Common Industrial Protocol*) Modello completo di messaggi e servizi per la raccolta di applicazioni di automazione destinate ai processi di produzione: controllo, sicurezza, sincronizzazione, movimento, configurazione e informazione). Con il protocollo CIP gli utenti possono integrare queste applicazioni di produzione con reti Ethernet aziendali e Internet. CIP è il protocollo di base di EtherNet/IP.

client di messaggistica esplicita:

(*classe di client di messaggistica esplicita*) Classe di dispositivi definita dall'ODVA per i nodi EtherNet/IP che supporta solo la messaggistica esplicita come client. I sistemi HMI e SCADA sono gli esempi più comuni di questa classe di dispositivi.

Cloud DIO:

Un gruppo di apparecchiature distribuite non richiesto per supportare RSTP. I cloud DIO richiedono solo una connessione unica (non ad anello) in rame. Possono essere collegati ad alcune porte in rame sui DRS, oppure direttamente al controller o ai moduli di comunicazione Ethernet nel *rack locale*. I cloud DIO **non possono** essere collegati a *sotto-anelli*.

connessione di classe 1:

Una connessione di classe di trasporto 1 su protocollo CIP viene utilizzata per la trasmissione dei dati di I/O mediante una funzione di messaggistica implicita tra dispositivi EtherNet/IP.

connessione di classe 3:

Una connessione con classe di trasporto 3 su protocollo CIP viene utilizzata per la messaggistica esplicita tra dispositivi EtherNet/IP.

connessione ottimizzata su rack:

I dati di più moduli di I/O vengono consolidati in un unico pacchetto dati per essere presentati allo scanner in un messaggio implicito su una rete EtherNet/IP.

connessione:

Un circuito virtuale tra due o più dispositivi di rete, creato prima della trasmissione dei dati. Dopo aver stabilito una connessione, una serie di dati viene trasmessa sullo stesso percorso di comunicazione senza bisogno di specificare informazioni di instradamento, compresi l'indirizzo di origine e di destinazione con ciascuna porzione di dati.

convergenza di rete:

Attività di riconfigurazione della rete in situazione di perdita di rete per garantire la disponibilità del sistema.

CPU:

(*Central Processing Unit*, unità di elaborazione centrale) La CPU, nota anche come processore o controller, è il centro di elaborazione di un processo di produzione industriale. A differenza dei sistemi controllati da relè, effettua l'automazione del processo. Le CPU sono computer adatti a resistere alle difficili condizioni di un ambiente industriale.

D

DDT:

(*Derived Data Type*, tipo di dati derivati) Un DDT è un insieme di elementi dello stesso tipo (`ARRAY`) o di tipi diversi (struttura).

destinazione:

In una rete EtherNet/IP un dispositivo è considerato la destinazione quando è il destinatario di una richiesta di collegamento per le comunicazioni di messaggistica implicita o esplicita, oppure di una richiesta di messaggi per una comunicazione di messaggistica esplicita senza connessione.

determinismo:

Per un'applicazione e architettura definite, è possibile prevedere che il ritardo tra un evento (modifica del valore di un ingresso) e il corrispondente cambiamento dell'uscita di un controller è un tempo finito *t*, minore della scadenza necessaria per il processo.

Device DDT (DDDT):

Un DDT di dispositivo è un DDT predefinito dal costruttore e non modificabile dall'utente. Contiene gli elementi di linguaggio di I/O di un modulo di I/O.

DFB:

(*Derived function block*, Blocco funzione derivato) I tipi DFB sono blocchi funzione programmabili dall'utente in linguaggio ST, IL, LD o FBD.

L'uso di questi tipi DFB in un'applicazione consente di:

- semplificare la progettazione e la stesura del programma,
- accrescere la leggibilità del programma,
- facilitare il debug
- diminuire il volume del codice creato

DHCP:

(*Dynamic Host Configuration Protocol*) Un'estensione del protocollo di comunicazione BOOTP che esegue l'assegnazione automatica delle impostazioni di indirizzamento IP, inclusi indirizzo IP, maschera di sottorete, indirizzo IP del gateway e nomi dei server DNS. Il protocollo DHCP non richiede la gestione di una tabella per l'identificazione dei singoli dispositivi di rete. Il client si identifica sul server DHCP utilizzando il proprio indirizzo MAC o un ID del dispositivo assegnato in modo univoco. Il servizio DHCP utilizza le porte UDP 67 e 68.

diagramma blocco funzione:

Vedere FBD.

DIO:

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

dispositivo di classe scanner:

Un dispositivo di classe scanner è definito dall'ODVA come nodo EtherNet/IP in grado di originare scambi di I/O con altri nodi di rete.

Dispositivo di I/O M580 Ethernet:

Un dispositivo Ethernet che fornisce ripristino automatico della rete e prestazioni RIO deterministiche. È possibile calcolare il tempo necessario per la risoluzione di una scansione logica RIO e il sistema può recuperare rapidamente l'operatività dopo un errore di comunicazione. M580 Ethernet I dispositivi di I/O includono:

- rack locale (incluso un controller con servizio di scansione I/O Ethernet)
- Derivazione RIO (incluso un modulo adattatore X80)
- Switch DRS con una configurazione predefinita

dispositivo pronto:

Dispositivo pronto Ethernet che fornisce servizi aggiuntivi al modulo Ethernet/IP o Modbus, come: singola immissione parametro, dichiarazione editor del bus, trasferimento di sistema, capacità di scansione deterministica, messaggio di avviso per modifiche e autorizzazioni utente condivise tra Control Expert e il dispositivo DTM.

DNS:

(*Domain Name Server/Service*) Un servizio che converte un nome di dominio in formato alfanumerico in un indirizzo IP. È l'ID univoco di un dispositivo di rete.

DRS:

(*switch a doppio anello*) Uno switch a gestione estesa ConneXium configurato per il funzionamento su una rete Ethernet. I file di configurazione predefinita sono forniti da Schneider Electric per lo scaricamento su un DRS per supportare funzionalità speciali dell'architettura dell'anello principale / del sotto-anello.

DSCP:

(*Differentiated Service Code Points*) Questo campo a 6 bit è l'intestazione di un pacchetto IP per classificare il traffico e assegnare le priorità.

DST:

(*Daylight Saving Time*, ora legale) La DST è chiamata anche *ora legale* ed è una pratica che consiste nello spostare avanti l'orologio all'approssimarsi della primavera e nel riportarlo indietro quando sta per iniziare l'autunno.

DT:

(*Date and Time*, data e ora) Il tipo `DT`, codificato in BCD in un formato a 64 bit, contiene le seguenti informazioni:

- l'anno codificato in un campo di 16 bit
- il mese codificato in un campo di 8 bit
- il giorno codificato in un campo di 8 bit
- l'ora codificata in un campo di 8 bit
- i minuti codificati in un campo di 8 bit
- i secondi codificati in un campo di 8 bit

NOTA: Gli otto bit meno significativi non sono utilizzati.

Il tipo `DT` viene immesso nel seguente formato:

DT#<Anno>**-**<Mese>**-**<Giorno>**-**<Ora>**:**<Minuti>**:**<Secondi>

Questa tabella mostra il limite inferiore e superiore di ogni campo:

Campo	Limiti	Commento
Anno	[1990,2099]	Anno
Mese	[01,12]	Lo 0 iniziale viene visualizzato; durante l'immissione dei dati può essere omesso.
Giorno	[01,31]	Per i mesi 01/03/05/07/08/10/12
	[01,30]	Per i mesi 04/06/09/11
	[01,29]	Per il mese 02 (anni bisestili)
	[01,28]	Per il mese 02 (anni non bisestili)
Ora	[00,23]	Lo 0 iniziale viene visualizzato; durante l'immissione dei dati può essere omesso.
Minuto	[00,59]	Lo 0 iniziale viene visualizzato; durante l'immissione dei dati può essere omesso.
Secondo	[00,59]	Lo 0 iniziale viene visualizzato; durante l'immissione dei dati può essere omesso.

DTM:

(*Device Type Manager*) Un DTM è un driver del dispositivo eseguito sul PC host. Fornisce una struttura unificata per l'accesso ai parametri, la configurazione e il funzionamento dei dispositivi e la diagnostica dei problemi. I DTM possono essere una semplice interfaccia utente grafica (Graphical User Interface, GUI) per l'impostazione dei parametri dei dispositivi su un'applicazione altamente sofisticata che supporta l'esecuzione di calcoli complessi in tempo reale a scopo di diagnostica e manutenzione. Nel contesto di un DTM, un dispositivo può essere un modulo di comunicazione o un sistema di rete remoto.

Vedere FDT.

E

EDS:

(*Electronic Data Sheet*) Gli EDS sono semplici file di testo che descrivono le capacità di configurazione di un dispositivo. I file EDS sono elaborati e forniti dal costruttore del dispositivo.

EFB:

(*Elementary function block*, Blocco funzione elementare) Si tratta del blocco, utilizzato in un programma, che esercita una funzione logica predefinita.

Gli EFB possiedono stati e parametri interni. Anche se gli ingressi sono identici, i valori delle uscite possono essere diversi. Ad esempio, un contatore possiede un'uscita che indica che il valore di preselezione è stato raggiunto. Questa uscita è impostata a 1 quando il valore è uguale al valore di preselezione.

EF:

(*Elementary function*, Funzione elementare) Si tratta del blocco, utilizzato in un programma, che esegue una funzione logica predefinita.

Una funzione non dispone di informazioni sullo stato interno. Più chiamate della stessa funzione con gli stessi parametri di ingresso forniranno gli stessi valori di uscita. Per informazioni sulla forma grafica della chiamata di funzione, vedere [*blocco funzionale (istanza)*]. A differenza della chiamata di un blocco funzione, le chiamate di funzione comportano solo un'uscita che non è nominata e il cui nome è identico a quello della funzione. In FBD, ogni chiamata è indicata da un [numero] univoco mediante il blocco grafico. Questo numero viene generato automaticamente e non è modificabile.

Per eseguire l'applicazione, è necessario posizionare e configurare queste funzioni nel programma.

È anche possibile sviluppare altre funzioni con il kit di sviluppo SDKC.

EN:

EN corrisponde a **EN**able (attiva) e si tratta di un ingresso di blocco facoltativo. Quando l'ingresso EN è attivato, viene stabilita automaticamente anche un'uscita ENO.

Se EN = 0, il blocco non è attivato, il programma interno non viene eseguito ed ENO viene impostato su 0.

Se EN = 1, il programma interno del blocco viene eseguito ed ENO viene impostato su 1. Nel caso si verifichi un errore di runtime, ENO viene impostato su 0.

Se l'ingresso EN non è collegato, viene automaticamente impostato su 1.

ENO:

ENO corrisponde a **E**rror **NO**tification (notifica di errore) e si tratta dell'uscita associata all'ingresso facoltativo EN.

Se ENO è impostato su 0 (perché EN = 0 o se viene rilevato un errore di runtime):

- Lo stato delle uscite dei blocchi funzione resta identico a quello in cui si trovavano durante l'ultimo ciclo di scansione eseguito correttamente.
- Le uscite delle funzioni e le procedure vengono impostate su "0".

EtherNet/IP™:

Protocollo di comunicazione di rete per applicazioni di automazione industriale che combina i protocolli di trasmissione Internet standard TCP/IP e UDP con il protocollo CIP (Common Industrial Protocol) per il livello delle applicazioni, al fine di supportare sia lo scambio di dati ad alta velocità sia il controllo industriale. EtherNet/IP si avvale di fogli dati elettronici (EDS, Electronic Data Sheets) per la classificazione di ogni dispositivo di rete e delle relative funzionalità.

Ethernet:

LAN basata su frame con protocollo di accesso CSMA/CD che supporta una velocità di trasmissione di 10 Mb/s, 100 Mb/s o 1 Gb/s. La trasmissione dei segnali può avvenire tramite doppino intrecciato, cavo in fibra ottica o essere di tipo wireless. Lo standard IEEE 802.3 definisce le regole di configurazione di una rete Ethernet cablata. Lo standard IEEE 802.11 definisce le regole di configurazione di una rete Ethernet wireless. Le tipologie più comuni includono 10BASE-T, 100BASE-TX e 1000BASE-T, che possono utilizzare doppini intrecciati di categoria 5e e connettori modulari RJ45.

F

FAST:

Un task attivato da eventi (FAST) è un task del processore periodico e facoltativo che identifica richieste di scansione multiple ad alta priorità, eseguito attraverso il proprio software di programmazione. Un task FAST può pianificare moduli di I/O selezionati affinché la loro logica sia risolta più di una volta per scansione. Il task FAST ha due sezioni:

- IN: gli ingressi sono copiati nella sezione IN prima dell'esecuzione del task FAST.
- OUT: le uscite sono copiate nella sezione OUT dopo l'esecuzione del task FAST.

FBD:

(*function block diagram, diagramma blocco funzione*) Un linguaggio di programmazione grafica IEC 61131-3 che funziona come un diagramma di flusso. Aggiungendo blocchi logici semplici (ad esempio, `AND`, `OR`), ogni funzione o blocco funzione del programma è rappresentato in questo formato grafico. Per ogni blocco, gli ingressi si trovano a sinistra e le uscite a destra. È possibile collegare le uscite dei blocchi agli ingressi di altri blocchi per formare espressioni complesse.

FDR:

(*Fast device replacement*, Sostituzione rapida del dispositivo) Un servizio che utilizza il software di configurazione per sostituire un prodotto non funzionante.

FDT:

(*Field device tool*) Tecnologia che armonizza la comunicazione tra i dispositivi di campo e l'host del sistema.

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.

full duplex:

La capacità di due dispositivi collegati in rete di comunicare tra di loro in modo indipendente e simultaneo in entrambe le direzioni.

G

gateway:

Un dispositivo gateway interconnette due reti diverse, a volte attraverso protocolli di rete diversi. Quando collega reti basate su protocolli diversi, un gateway converte un datagramma da uno stack di un protocollo nell'altro. Quando è utilizzato per la connessione di due reti basate su protocollo IP, un gateway (chiamato anche router) ha due indirizzi IP separati, uno su ciascuna rete.

GPS:

(*Global Positioning System*) Lo standard GPS fornisce segnali di posizionamento, navigazione e tempo basati sullo spazio che vengono trasmessi in tutto il mondo per usi civili e militari. Le prestazioni del servizio di posizionamento standard dipendono dai parametri dei segnali di trasmissione satellitari, dal design della costellazione GPS, dal numero di satelliti in vista e da vari parametri ambientali.

H

HART:

(*Highway Addressable Remote Transducer*) Un protocollo di comunicazione bidirezionale per l'invio e la ricezione di informazioni digitali su fili analogici tra un sistema di controllo o monitoraggio e smart device.

HART è lo standard globale per la fornitura di accesso ai dati tra sistemi host e strumenti di campo intelligenti. Un host può essere una qualsiasi applicazione software, da un dispositivo portatile o un laptop di un tecnico a un sistema di controllo dei processi di un impianto o di gestione degli asset, oppure un altro sistema che utilizza un sistema di controllo.

HMI:

(*Human machine interface*, Interfaccia uomo-macchina) Sistema che permette l'interazione tra uomo e macchina.

Hot Standby:

Un sistema Hot Standby utilizza un PAC (PLC) primario e un PAC standby. I due rack PAC hanno configurazioni hardware e software identiche. Il PAC standby monitora lo stato corrente di sistema del PAC primario. Se il PAC primario diventa inutilizzabile, il controllo ad alta disponibilità viene mantenuto quando il PAC standby assume il controllo del sistema.

HTTP:

(*Hypertext transfer protocol*, Protocollo di trasferimento ipertestuale) Protocollo di rete per sistemi informativi distribuiti e collaborativi. HTTP è alla base della comunicazione dati del Web.

I

%I:

Secondo lo standard IEC, `%I` indica un oggetto linguaggio di tipo ingresso digitale.

IEC 61131-3:

Standard internazionale: controller logici programmabili (PLC)

Parte 3: linguaggi di programmazione

IGMP:

(Internet group management protocol, Protocollo di gestione dei gruppi Internet) Questo standard Internet per il multicasting permette a un host di sottoscrivere un particolare gruppo multicast.

IL:

(*Instruction list*, Lista di istruzioni) Linguaggio di programmazione IEC 61131-3 contenente una serie di istruzioni di base. È molto simile al linguaggio di assemblaggio utilizzato per la programmazione dei processori. Ogni istruzione è costituita da un codice istruzione e da un operando.

indirizzo IP:

Identificativo a 32 bit, formato da un indirizzo di rete e da un indirizzo host assegnato a un dispositivo collegato a una rete TCP/IP.

INT:

(*INTeger*) (codificato a 16 bit) I limiti superiore e inferiore sono i seguenti: da -(2 alla potenza di 15) a (2 alla potenza di 15) - 1.

Esempio: `-32768`, `32767`, `2#1111110001001001`, `16#9FA4`.

IODDT:

(*Input/Output Derived Data Type, tipo di dati derivati di ingresso/uscita*) Un tipo di dati strutturato che rappresenta un modulo o un canale di un controller. Ogni modulo esperto dell'applicazione possiede il proprio IODDT.

IPsec:

(*Internet Protocol Security*) Un set aperto di standard di protocollo che rendono le sessioni di comunicazione IP private e crittografate per il traffico tra i moduli che utilizza IPsec, sviluppato dalla task force ideatrice di Internet (IETF). Gli algoritmi di crittografia e autenticazione IPsec richiedono chiavi di crittografia definite dall'utente che elaborano ciascun pacchetto di comunicazione in una sessione IPsec.

%IW:

Secondo lo standard IEC, `%IW` indica un oggetto linguaggio di tipo ingresso analogico.

L

LD:

(*Ladder diagram, diagramma Ladder*) Un linguaggio di programmazione IEC 61131-3 che rappresenta le istruzioni da eseguire sotto forma di diagrammi grafici molto simili a schemi elettrici (ad esempio, contatti, bobine).

loop a margherita ad alta capacità:

Spesso chiamato HCDL, un loop a margherita ad alta capacità utilizza switch a doppio anello (DRSsRIODIO) per collegare sotto-anelli di dispositivi (contenenti derivazioni o apparecchiatura distribuita) e/o cloud sulla rete EthernetRIO.

loop a margherita semplice:

Spesso chiamato SDCL, un loop a margherita semplice contiene solo moduli RIO (nessuna apparecchiatura distribuita). Questa topologia è costituita da un rack locale (contenente un controller con servizio di scansione I/O Ethernet) e una o più derivazioni RIO (ogni derivazione contiene un modulo adattatore RIO).

M

maschera di sottorete:

Valore a 32 bit utilizzato per nascondere (o mascherare) la porzione di rete dell'indirizzo IP e identificare in tal modo l'indirizzo host di un dispositivo di rete con il protocollo IP.

MAST:

Un task master (MAST) è un task del processore deterministico eseguito mediante il proprio software di programmazione. Il task MAST pianifica la logica del modulo RIO affinché sia risolta in ogni scansione I/O. Il task MAST presenta due sezioni:

- IN: gli ingressi sono copiati nella sezione IN prima dell'esecuzione del task MAST.
- OUT: le uscite sono copiate nella sezione OUT dopo l'esecuzione del task MAST.

MB/TCP:

(*Modbus su protocollo TCP*) Una variante Modbus utilizzata per le comunicazioni su reti TCP/IP.

messaggistica con connessione:

In una rete EtherNet/IP, la messaggistica con connessione utilizza per la comunicazione una connessione CIP. Un messaggio con connessione è una relazione logica tra due o più oggetti applicazione su nodi diversi. La connessione stabilisce un circuito virtuale in anticipo per uno scopo particolare, come messaggi espliciti frequenti o trasferimenti di dati di I/O in tempo reale.

messaggistica esplicita:

Messaggistica basata su TCP/IP per Modbus TCP e EtherNet/IP. È utilizzata per i messaggi client/server da punto a punto che includono sia i dati (in genere informazioni non pianificate tra un client e un server) che le informazioni di instradamento. In una rete EtherNet/IP, la messaggistica esplicita è considerata una messaggistica di classe 3 e può essere basata su connessione o senza connessione.

messaggistica implicita:

Messaggistica collegata di classe 1 basata su protocollo UDP/IP per reti EtherNet/IP. La messaggistica implicita gestisce una connessione aperta per il trasferimento pianificato di dati di controllo tra un produttore e un consumatore. Dato che viene utilizzata una connessione aperta, ciascun messaggio contiene principalmente dati (senza informazioni sull'oggetto) e un identificativo di connessione.

mirroring porte:

In questa modalità, il traffico di dati relativo alla porta di origine su uno switch di rete viene copiato su un'altra porta di destinazione. In tal modo è possibile utilizzare uno strumento di gestione delle connessioni per monitorare e analizzare il traffico.

%M:

Secondo lo standard IEC, `%M` indica un oggetto linguaggio di tipo bit memoria.

MIB:

(*Management Information Base*) Database virtuale utilizzato per la gestione degli oggetti in una rete di comunicazione. Vedere SNMP.

modalità avanzata:

In Control Expert, la modalità avanzata è un'opzione che mostra le proprietà di configurazione riservate agli utenti esperti per semplificare la definizione delle connessioni Ethernet. Poiché si tratta di proprietà che possono essere modificate solo da persone con una solida esperienza nei protocolli di comunicazione EtherNet/IP, possono essere nascoste o visualizzate a seconda delle qualifiche dell'utente specifico che effettua l'accesso.

Modbus:

Modbus è un protocollo di messaggistica del livello delle applicazioni. Modbus fornisce le comunicazioni client e server tra dispositivi connessi a diversi tipi di bus o reti. Modbus offre molti servizi specificati dai codici funzione.

multicast:

Particolare tipo di trasmissione nel quale le copie del pacchetto vengono distribuite a un unico sottoinsieme di destinazioni di rete. La messaggistica implicita utilizza generalmente il formato multicast per le comunicazioni su una rete EtherNet/IP.

%MW:

Secondo lo standard IEC, `%MW` indica un oggetto linguaggio di tipo parola memoria.

N

NIM:

(*Network interface module*, Modulo di interfaccia di rete) Un NIM si trova nella prima posizione di un'isola STB (nella posizione più a sinistra della configurazione fisica). Il NIM fornisce l'interfaccia tra i moduli di I/O e il master del bus di campo. Si tratta del solo modulo dell'isola che dipende dal bus di campo; per ciascun bus di campo è disponibile un tipo di NIM diverso.

nome di dominio:

Stringa alfanumerica che identifica in modo univoco un dispositivo su una rete Internet ed è visualizzata come parte principale di un URL (Uniform Resource Locator) di un sito Web. Ad esempio, il nome di dominio *schneider-electric.com* è la parte principale dell'URL *www.se.com*.

Ciascun nome di dominio è assegnato come parte del DNS ed è associato a un indirizzo IP.

È chiamato anche nome host.

NTP:

(*Network time protocol*) Protocollo per la sincronizzazione degli orologi di sistema dei computer. Il protocollo utilizza un buffer di disturbo per resistere agli effetti della latenza variabile.

O

O -> T:

(*Originator to target*, Dall'origine a destinazione) Vedere origine e destinazione.

ODVA:

(*Open DeviceNet Vendors Association*) ODVA supporta le tecnologie di rete basate su CIP.

OFS:

(*OPC Factory Server*) OFS consente comunicazioni SCADA in tempo reale con la famiglia Control Expert di PLC. OFS utilizza il protocollo di accesso dati OPC standard.

OPC DA:

(*OLE per accesso dati di controllo processo*) La Specifica di accesso ai dati è uno degli standard OPC implementato più comunemente e fornisce le specifiche per le comunicazioni in tempo reale tra client e server.

origine connessione:

Nodo di rete EtherNet/IP che invia una richiesta di connessione per il trasferimento dei dati di I/O o la messaggistica esplicita.

origine:

In una rete EtherNet/IP, un dispositivo è considerato l'origine quando avvia una connessione CIP per le comunicazioni di messaggistica implicita o esplicita, oppure quando invia una richiesta di messaggi per una comunicazione di messaggistica esplicita senza connessione.

orodatarzione dell'applicazione:

Utilizzare la soluzione di orodatazione dell'applicazione per accedere ai buffer eventi orodatario con un sistema SCADA che non supporta l'interfaccia OPC DA. In questo caso, i blocchi funzione nell'applicazione Control Expert leggono gli eventi nel buffer e li formattano per inviarli al sistema SCADA.

P

PAC:

Programmable automation controller, Controller di automazione programmabile. Il PAC è il centro di elaborazione di un processo di produzione industriale. A differenza dei sistemi controllati da relè, il processo è automatizzato. I PAC sono computer adatti a resistere alle difficili condizioni di un ambiente industriale.

porta 502:

La porta 502 dello stack TCP/IP è una porta importante riservata alla comunicazioni Modbus TCP.

Porta service:

Una porta Ethernet dedicata sui moduli M580 RIO. A seconda del tipo di modulo, la porta può supportare tre funzioni principali:

- mirroring della porta: per uso diagnostico
- accesso: per collegamento HMI/Control Expert/ConneXview al controller
- estesa: per estendere la rete di dispositivi a un'altra subnet
- disabilitata: che disabilita la porta; in questa modalità il traffico non viene inoltrato

PTP:

(*Precision time protocol*) Utilizzare questo protocollo per sincronizzare gli orologi attraverso una rete di computer. In una rete LAN, PDP consente di ottenere la precisione dell'orologio nell'ordine dei sub-microsecondi, adatto quindi per sistemi di controllo e misurazione.

Q

%Q:

Secondo lo standard IEC, `%Q` indica un oggetto linguaggio di tipo uscita digitale.

QoS:

(*Quality of Service*, Qualità del servizio) La prassi di assegnare diverse priorità ai vari tipi di traffico per regolare il flusso dei dati sulla rete. In una rete industriale la QoS può contribuire a fornire un livello prevedibile di prestazioni di rete.

%QW:

Secondo lo standard IEC, `%QW` indica un oggetto linguaggio di tipo uscita analogica.

R

rack locale:

Un rack M580 contenente il controller e un alimentatore. Un rack locale è costituito da uno o più rack: il rack principale e il rack esteso, che appartiene alla stessa famiglia del rack principale. Il rack esteso è facoltativo.

rete di controllo:

Una rete basata su Ethernet contenente, tra l'altro, PAC, sistemi SCADA, un server NTP, PC, AMS e switch. Sono supportati due tipi di topologie:

- piana: tutti i moduli e i dispositivi di questa rete appartengono alla stessa subnet.
- su due livelli: la rete è suddivisa in una rete operativa e una rete inter-controller. Queste due reti possono essere fisicamente indipendenti, ma sono generalmente collegati da un dispositivo di instradamento.

rete di dispositivi:

Rete Ethernet con una rete di I/O remoti che include dispositivi di I/O sia remoti sia distribuiti. I dispositivi connessi su questa rete devono seguire regole specifiche per consentire il determinismo degli I/O remoti.

rete DIO isolata:

Una rete EthernetRIO contenente apparecchiatura distribuita che non fa parte di una rete

Rete DIO:

Una rete contenente apparecchiature distribuite, nella quale la scansione I/O viene eseguita da un controller con servizio di scansione DIO sul rack locale. Il traffico di rete DIO viene consegnato dopo il traffico RIO, che ha la priorità in una rete RIO.

Rete EIO:

(Ethernet I/O) Una rete basata su Ethernet che contiene tre tipi di dispositivi:

- rack locale
- Derivazione remota X80 (con un modulo adattatore BM•CRA312•0) o un modulo di switch opzionale di rete BMENOS0300
- Switch a doppio anello esteso ConneXium (DRS)

NOTA: L'apparecchiatura distribuita può anche partecipare a una rete Ethernet I/O che utilizza una connessione a DRSs o la porta service dei moduli remoti X80.

rete inter-controller:

Rete Ethernet che fa parte della rete di controllo; fornisce lo scambio dei dati tra controller e strumenti tecnici, come programmazione, sistema AMS (Asset Management System).

rete operativa:

Una rete basata su Ethernet contenente strumenti per gli operatori (SCADA, PC client, stampanti, strumenti batch ed EMS, ecc.). I controller sono connessi direttamente o attraverso l'instradamento della rete inter-controller. Questa rete fa parte della rete di controllo.

Rete RIO:

Una rete basata su Ethernet che contiene tre tipi di dispositivi RIO: un rack locale, una derivazione RIO e uno switch ConneXium a doppio anello esteso (DRS). Anche l'apparecchiatura distribuita può partecipare a una rete RIO attraverso una connessione ai moduli di switch opzionali di rete DRSs o BMENOS0300.

rete:

Può avere due significati:

- In un diagramma Ladder:

  Una rete è una serie di elementi grafici interconnessi. La portata di una rete è locale, rispetto all'unità (sezione) organizzativa del programma in cui è situata.

- Con moduli di comunicazione esperti:

  Una rete è un gruppo di stazioni che comunicano tra loro. Il termine *rete* è utilizzato inoltre per definire un gruppo di elementi grafici interconnessi. Questo gruppo costituisce successivamente una parte di un programma che può essere composta da un gruppo di reti.

RIO derivazione:

Uno dei tre tipi di moduli RIO in una rete EthernetRIO Una derivazione RIO è un rack M580 di moduli di I/O connessi a una rete Ethernet RIO e gestiti da un modulo adattatore Ethernet RIO. Una derivazione può essere un rack singolo o un rack principale con un rack esteso.

RIO S908:

Un sistema RIO Quantum che utilizza morsetti e cablaggio assiale.

RPI:

(Requested packet interval) Periodo di tempo tra le trasmissioni cicliche dei dati richieste dallo scanner. I dispositivi EtherNet/IP pubblicano i dati alla velocità specificata dall'RPI loro assegnato dallo scanner e a ogni RPI ricevono richieste di messaggi dallo scanner.

RSTP:

(*Rapid spanning tree protocol*) Permette di includere in un progetto di rete collegamenti di riserva (ridondanti) per fornire percorsi di backup automatico qualora un collegamento attivo smetta di funzionare, senza bisogno di loop o di attivare e disattivare manualmente i collegamenti di backup.

S

SCADA:

I sistemi SCADA (*Supervisory Control And Data Acquisition*) sono sistemi informatici per il controllo e il monitoraggio dei processi industriali o tipici dell'infrastruttura o dello stabilimento (ad esempio, la trasmissione dell'elettricità, il trasporto del gas e dell'olio nei condotti e la distribuzione dell'acqua).

Scanner I/O:

Un servizio Ethernet che interroga continuamente i moduli di I/O per raccogliere dati, stato, eventi e informazioni di diagnostica. Questo processo monitora gli ingressi e controlla le uscite. Questo servizio supporta la scansione della logica RIO e DIO.

scanner:

Uno scanner funge da origine delle richieste di connessione di I/O per la messaggistica implicita in una rete EtherNet/IP e delle richieste di messaggi per Modbus TCP.

senza connessione:

Descrive la comunicazione tra i due dispositivi di rete, in cui i dati vengono inviati senza che sia stata stabilita una connessione tra i due dispositivi. Ogni porzione di dato trasmesso include anche informazioni di instradamento, tra cui anche l'indirizzo di origine e di destinazione.

Servizio di scansione Ethernet DIO:

Questo servizio di scansione DIO integrato scanner dei controller M580 gestisce l'apparecchiatura distribuita su una rete di dispositivi M580.

Servizio di scansione I/O Ethernet:

Questo servizio di scansione I/O Ethernet integrato di controller M580 gestisce l'apparecchiatura distribuita **e** derivazioni RIO su una rete di dispositivi M580.

servizio ora di rete:

Utilizzare questo servizio per sincronizzare gli orologi dei computer su Internet per registrare eventi (eventi in sequenza), sincronizzare eventi (attivare eventi simultanei) o sincronizzare allarmi e I/O (allarmi orodatario).

SFC:

(*sequential function chart, grafico di funzione sequenziale*) Un linguaggio di programmazione IEC 61131-3 utilizzato per rappresentare graficamente in modo strutturato il funzionamento di un controller sequenziale. Questa descrizione grafica del comportamento sequenziale del controller e delle varie situazioni che ne derivano si basa su semplici simboli grafici.

SFP:

(*Small Form-factor Pluggable*). Il ricetrasmettitore SFP funge da interfaccia tra un modulo e i cavi in fibra ottica.

slave locale:

La funzionalità offerta dai moduli di comunicazione EtherNet/IP di Schneider Electric che consente a uno scanner di assumere il ruolo di adattatore. Con lo slave locale il modulo può pubblicare i dati utilizzando connessioni di messaggistica implicita. Lo slave locale è tipicamente utilizzato negli scambi peer-to-peer tra i PAC.

SMTP:

(*Simple mail transfer protocol*) Un servizio di notifica e-mail che consente ai progetti basati su controller di segnalare allarmi o eventi. Il controller esegue il monitoraggio del sistema e può creare automaticamente un messaggio di posta elettronica di avvertimento con dati, allarmi e/o eventi. I destinatari dell'e-mail possono essere locali o remoti.

SNMP:

(*Simple network management protocol*) Protocollo utilizzato nei sistemi di gestione di rete per monitorare i dispositivi collegati alla rete. Il protocollo fa parte della suite IP definita dall'IETF (Internet Engineering Task Force) ed è costituito da direttive sulla gestione di rete, compreso un protocollo per il livello delle applicazioni, uno schema di database e una serie di oggetti dati.

SNTP:

(*Simple network time protocol*) Vedere NTP.

SOE:

(*sequenza di eventi*) il software SOE consente agli utenti di comprendere una serie di eventi che possono portare a condizioni non sicure del processo e possibili arresti. I SOE possono essere critici per la risoluzione o la prevenzione di tali condizioni.

sottoanello:

Una rete basata su Ethernet con un loop collegato all'anello principale tramite uno switch a doppio anello (DRS) oppure un modulo di switch opzionale di rete BMENOS0300 sull'anello principale. Questa rete contiene apparecchiature distribuite o RIO.

ST:

(*Structured text*, Testo strutturato) Linguaggio di programmazione IEC 61131-3 che presenta un linguaggio letterale strutturato ed è un linguaggio sviluppato simile ai linguaggi di programmazione dei computer. Consente di strutturare serie di istruzioni.

%SW:

Secondo lo standard IEC, `%SW` indica un oggetto linguaggio di tipo parola di sistema.

switch:

Dispositivo multiporta utilizzato per segmentare la rete e ridurre la probabilità di collisioni. I pacchetti vengono filtrati o inoltrati in base ai loro indirizzi di origine e di destinazione. Gli switch supportano il funzionamento full-duplex e forniscono larghezza di rete completa su ciascuna porta. Uno switch può avere diverse velocità di ingresso/uscita (ad esempio 10, 100 o 1000 Mbps). Gli switch sono considerati dispositivi che operano al livello 2 (livello di collegamento dati) del modello OSI.

T

T -> O:

(*Target to originator*, Dalla destinazione all'origine) Vedere destinazione e origine.

TCP/IP:

Noto anche come *suite di protocolli Internet*, TCP/IP è un insieme di protocolli standard per le comunicazioni di rete. La suite prende il nome dai due protocolli comunemente usati: il protocollo Transmission Control Protocol e il protocollo Ethernet. TCP/IP è un protocollo basato su connessione utilizzato da Modbus TCP e EtherNet/IP per la messaggistica esplicita.

TCP:

(*Transmission Control Protocol*) Protocollo chiave della suite di protocolli Internet (IP) che supporta le comunicazioni basate su una connessione, ovvero stabilisce la connessione necessaria a trasmettere una sequenza ordinata di dati sullo stesso percorso di comunicazione.

TFTP:

(*Trivial File Transfer Protocol*) Una versione semplificata del protocollo *File Transfer Protocol* (FTP), TFTP utilizza un'architettura client-server per effettuare il collegamento tra due dispositivi. Da un client TFTP è possibile caricare singoli file sul server o scaricarli dal server utilizzando il protocollo UDP per il trasferimento dei dati.

TIME_OF_DAY:

Vedere `TOD`.

TOD:

(*Time of day*, Ora del giorno) Il tipo `TOD`, codificato in BCD in un formato a 32 bit, contiene le seguenti informazioni:

- l'ora codificata in un campo di 8 bit
- i minuti codificati in un campo di 8 bit
- i secondi codificati in un campo di 8 bit

NOTA: Gli otto bit meno significativi non sono utilizzati.

Il tipo TOD viene immesso nel seguente formato: xxxxxxxx: **`TOD#`**`<Ora>`**`:`**`<Minuti>`**`:`** `<Secondi>`

Questa tabella mostra il limite inferiore e superiore di ogni campo:

Campo	Limiti	Commento
Ora	[00,23]	Lo 0 iniziale viene visualizzato; durante l'immissione dei dati può essere omesso.
Minuto	[00,59]	Lo 0 iniziale viene visualizzato; durante l'immissione dei dati può essere omesso.
Secondo	[00,59]	Lo 0 iniziale viene visualizzato; durante l'immissione dei dati può essere omesso.

Esempio: `TOD#23:59:45`.

trap:

Un trap è un evento generato da un agente SNMP che può indicare uno dei seguenti eventi:

- Una modifica avvenuta nello stato di un agente.
- Un dispositivo di gestione SNMP non autorizzato che ha tentato di recuperare dati da (o di modificare dati di) un agente SNMP.

TR:

(*Transparent Ready*) Apparecchiatura di distribuzione dell'alimentazione su Web che include apparecchiature di manovra a media e bassa tensione, quadri di commutazione, quadri di strumenti, centri di controllo di motori e sottostazioni di unità. Le apparecchiature Transparent Ready permettono di accedere allo stato delle misurazioni e delle apparecchiature da qualsiasi PC in rete, tramite un normale browser Web.

U

UDP:

(*User Datagram Protocol*) L'UDP è un protocollo di livello di trasporto che supporta le comunicazioni senza connessione. Le applicazioni eseguite su nodi di rete possono utilizzare il protocollo UDP per inviarsi reciprocamente dei datagrammi. A differenza del protocollo TCP, l'UDP non include una comunicazione preliminare per stabilire i percorsi dei dati o fornire ordinamento e controllo dei dati. Poiché evita il carico necessario per fornire queste funzionalità, tuttavia, l'UDP è più veloce del TCP. L'UDP può essere il protocollo ideale per le applicazioni con tempi limitati, dove la perdita di datagrammi è preferibile a un ritardo nella loro trasmissione. L'UDP è il principale protocollo di trasporto per la messaggistica implicita sulle reti EtherNet/IP.

UMAS:

(*Unified Messaging Application Services*) Il protocollo UMAS è un protocollo di sistema proprietario che gestisce le comunicazioni tra Control Expert and a controller.

UTC:

(*Universal Time Coordinated*) Tempo standard principale per regolare gli orologi e i fusi orari nel mondo (vicino allo standard dei fusi orari GMT precedente).

V

valore letterale dell'intero:

Il valore letterale dell'intero consente di immettere valori di tipo intero nel sistema decimale. I valori possono essere preceduti dal segno (+/-). I segni di sottolineatura (_) che separano i numeri non sono significativi.

Esempio:

```
-12, 0, 123_456, +986
```

Variabile:

Entità di memoria di tipo `BOOL`, `WORD`, `DWORD` e simili, con contenuto modificabile dal programma in esecuzione.

VLAN:

(*Virtual local area network*, Rete locale virtuale) Una rete locale (LAN) che si stende oltre una singola LAN ad un gruppo di segmenti di LAN. Una VLAN è un'entità logica creata e configurata esclusivamente utilizzando software applicabile.

Indice

A

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

U

V

X

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.

EIO0000002002.10