

## Controllori GuardLogix

Numeri di catalogo 1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP, 1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT



## Informazioni importanti per l'utente

Le apparecchiature a semiconduttore hanno caratteristiche di funzionamento diverse da quelle delle apparecchiature elettromeccaniche. Nella pubblicazione *Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls SGI-1.1*, disponibile presso l'ufficio vendite locale di Rockwell Automation oppure online all'indirizzo <http://www.rockwellautomation.com/literature/>) sono descritte alcune differenze importanti tra le apparecchiature a semiconduttore ed i dispositivi elettromeccanici cablati. A causa di questa differenza e della grande varietà di utilizzo delle apparecchiature a semiconduttore, tutte le persone responsabili dell'applicazione di questa apparecchiatura devono assicurarsi che ogni applicazione sia accettabile.

In nessun caso Rockwell Automation, Inc. sarà responsabile per danni indiretti derivanti dall'utilizzo o dall'applicazione di questa apparecchiatura.

Gli esempi e gli schemi contenuti nel presente manuale sono inclusi solo a scopo illustrativo. Poiché le variabili ed i requisiti associati alle installazioni specifiche sono innumerevoli, Rockwell Automation, Inc. non può essere ritenuta responsabile per l'utilizzo effettivo basato sugli esempi e gli schemi qui riportati.

Rockwell Automation, Inc. declina qualsiasi responsabilità brevettuale in relazione all'utilizzo di informazioni, circuiti, apparecchiatura o software descritti nel presente manuale.

La riproduzione totale o parziale del contenuto del presente manuale è vietata senza il consenso scritto di Rockwell Automation, Inc.

Ove necessario, nel presente manuale sono utilizzate delle note per avvertire l'utente sulle considerazioni relative alla sicurezza.



**AVVISO:** Identifica informazioni sulle pratiche o le circostanze che possono causare un'esplosione in un ambiente pericoloso, generando infortuni al personale o decesso, danni alle proprietà o perdite economiche.



**ATTENZIONE:** Identifica informazioni sulle pratiche o le circostanze che possono causare lesioni al personale o decesso, danni alle proprietà o perdite economiche. I simboli Attenzione consentono di identificare o evitare un pericolo e di riconoscerne le conseguenze.



**PERICOLO DI FOLGORAZIONE:** È possibile che sopra o all'interno dell'apparecchiatura, ad esempio un azionamento o un motore, siano presenti etichette che avvertono gli utenti della presenza di tensioni pericolose.



**PERICOLO DI USTIONI:** È possibile che sopra o all'interno dell'apparecchiatura, ad esempio un azionamento o un motore, siano presenti etichette che avvertono gli utenti che le superfici potrebbero raggiungere temperature pericolose.

---

**IMPORTANTE** Identifica informazioni importanti per la buona applicazione e comprensione del prodotto.

---

Rockwell Automation, Allen-Bradley, TechConnect, Architettura Integrata, ControlLogix, ControlLogix-XT, GuardLogix, Logix-XT, Guard I/O, CompactBlock Guard I/O, POINT Guard I/O, PowerFlex, PanelView, PLC-5, DriveLogix, FlexLogix, PhaseManager, ControlFLASH, Logix5000, RSLogix 5000, FactoryTalk, RSNetWorx for EtherNet/IP, RSNetWorx for DeviceNet, RSNetWorx for ControlNet e RSLinx sono marchi commerciali di Rockwell Automation, Inc.

I marchi commerciali che non appartengono a Rockwell Automation sono di proprietà delle rispettive società.

Le informazioni riportate di seguito sono un riepilogo delle modifiche apportate al manuale dall'ultima pubblicazione.

<b>Argomento</b>	<b>Pagine</b>
Informazioni sui controllori 1756-L71S	11, 18, 21, 27, 47
Istruzioni per l'installazione del modulo ESM (Modulo di accumulo energia)	46

**Note:**

**Prefazione**

Informazioni sui controllori GuardLogix 1756 ..... 11  
 Terminologia ..... 12  
 Ulteriori riferimenti ..... 13

**Capitolo 1**

**Cenni generali sul sistema**

Requisiti delle applicazioni di sicurezza ..... 15  
     Numero di rete di sicurezza ..... 15  
     Firma del task di sicurezza ..... 16  
 Distinzione tra componenti standard e di sicurezza ..... 16  
     Dispositivi di interfaccia operatore ..... 16  
 Capacità del flusso di dati del controllore ..... 17  
 Scelta dell'hardware del sistema ..... 18  
     Controllore primario ..... 18  
     Coprocesore di sicurezza ..... 19  
     Chassis ..... 19  
     Alimentatore ..... 19  
 Scelta dei moduli I/O di sicurezza ..... 20  
 Scelta delle reti di comunicazione ..... 20  
 Requisiti di programmazione ..... 21

**Capitolo 2**

**Installazione del controllore**

Precauzioni ..... 23  
     Informazioni su ambiente e custodia ..... 23  
     Sistemi elettronici programmabili (PES) ..... 24  
     Rimozione ed inserimento sotto tensione (RIUP) ..... 24  
     Approvazione nordamericana per l'uso in aree pericolose ..... 25  
     Approvazione europea per l'uso in aree pericolose ..... 26  
     Prevenzione delle scariche elettrostatiche ..... 26  
 Verificare di avere tutti i componenti ..... 27  
     Controllori 1756-L6xS ..... 27  
     Controllori 1756-L7xS ..... 27  
 Installazione di un alimentatore e di uno chassis ..... 28  
 Collegamento della batteria (solo controllori 1756-L6xS) ..... 28  
 Installazione del controllore nello chassis ..... 29  
 Inserimento o rimozione di una scheda di memoria ..... 30  
     Scheda Secure Digital (controllori 1756-L7xS) ..... 31  
     Scheda CompactFlash (controllori 1756-L6xS) ..... 33  
 Connessioni di comunicazione ..... 35  
     Collegamento alla porta USB del controllore 1756-L7xS ..... 35  
     Collegamento alla porta seriale del controllore 1756-L6xS ..... 37  
 Aggiornamento del controllore ..... 40  
     Utilizzo del software ControlFLASH per l'aggiornamento del  
     firmware ..... 40  
     Utilizzo di AutoFlash per l'aggiornamento del firmware ..... 41

Scelta della modalità operativa del controllore.....	42
Utilizzo del selettore a chiave per cambiare la modalità operativa.....	42
Utilizzo del software RSLogix 5000 per cambiare modalità operativa.....	43
Disinstallazione del modulo di alimentazione (ESM).....	44
Installazione di un modulo di alimentazione (ESM).....	46

### Capitolo 3

#### Configurazione del controllore

Creazione di un progetto del controllore.....	47
Impostazione delle password per il blocco/sblocco di sicurezza.....	49
Protezione della firma del task di sicurezza in modalità Esecuzione....	50
Gestione della sostituzione dei moduli I/O.....	51
Abilitazione della sincronizzazione temporale.....	51
Configurazione di un controllore di sicurezza peer.....	52

### Capitolo 4

#### Comunicazione sulle reti

Rete di sicurezza.....	53
Gestione del numero di rete di sicurezza (SNN).....	53
Assegnazione del Numero di rete di sicurezza (SNN).....	55
Modifica del numero di rete di sicurezza (SNN).....	55
Comunicazione EtherNet/IP.....	59
Produzione e consumo dei dati attraverso una rete EtherNet/IP.....	60
Connessioni sulla rete EtherNet/IP.....	60
Esempio di comunicazione EtherNet/IP.....	61
Connessioni EtherNet/IP per moduli I/O CIP Safety.....	62
Connessioni EtherNet/IP standard.....	62
Comunicazione ControlNet.....	63
Produzione e consumo dei dati attraverso una rete ControlNet... ..	63
Connessioni sulla rete ControlNet.....	63
Esempio di comunicazione ControlNet.....	64
Connessioni ControlNet per moduli I/O distribuiti.....	65
Comunicazione DeviceNet.....	65
Connessioni DeviceNet per moduli I/O CIP Safety.....	66
Connessioni DeviceNet standard.....	67
Comunicazione seriale.....	67
Ulteriori riferimenti.....	68

### Capitolo 5

#### Aggiunta, configurazione, monitoraggio e sostituzione di I/O CIP Safety

Aggiunta di moduli I/O CIP Safety.....	69
Configurazione di moduli I/O CIP Safety mediante il software RSLogix 5000.....	70
Impostazione del Numero di rete di sicurezza (SNN).....	71
Utilizzo delle connessioni unicast su reti EtherNet/IP.....	71
Impostazione del limite del tempo di risposta della connessione.....	71
Configurazione dell'intervallo di pacchetto richiesto (RPI).....	72
Visualizzazione del ritardo rete massimo osservato.....	73

Impostazione dei parametri avanzati relativi ai limiti del tempo di risposta della connessione .....	73
Comprensione dell'autenticazione di configurazione .....	75
Configurazione tramite il software RSLogix 5000 .....	75
Proprietario della configurazione diverso (connessione di solo ascolto) .....	76
Ripristino della proprietà dei moduli I/O di sicurezza .....	76
Indirizzamento dei dati I/O di sicurezza .....	76
Monitoraggio dello stato dei moduli I/O di sicurezza .....	77
Reset di un modulo alle condizioni predefinite in fabbrica .....	79
Sostituzione di un modulo tramite il software RSLogix 5000 .....	79
Sostituzione con l'opzione "Configure Only When No Safety Signature Exists" abilitata .....	80
Sostituzione con opzione "Configure Always" abilitata .....	84
Sostituzione di un modulo POINT Guard I/O mediante il software RSNNetWorx for DeviceNet .....	86

## Capitolo 6

### Sviluppo di applicazioni di sicurezza

Task di sicurezza .....	90
Definizione del periodo del task di sicurezza .....	90
Esecuzione del task di sicurezza .....	91
Programmi di sicurezza .....	92
Routine di sicurezza .....	92
Tag di sicurezza .....	92
Tag type .....	93
Data Type .....	94
Scope .....	95
Class .....	96
Constant Value .....	96
External Access .....	96
Tag di sicurezza prodotti/consumati .....	97
Configurazione dei numeri di rete di sicurezza dei controllori di sicurezza peer .....	97
Produzione di un tag di sicurezza .....	99
Consumo di dati di tag di sicurezza .....	100
Mappatura dei tag di sicurezza .....	102
Restrizioni .....	103
Creazione di coppie di mappatura di tag .....	103
Controllo dello stato della mappatura dei tag .....	104
Protezione dell'applicazione di sicurezza .....	105
Blocco di sicurezza del controllore .....	105
Generazione di una firma del task di sicurezza .....	106
Restrizioni software .....	108

<b>Collegamento online con il controllore</b>	<p><b>Capitolo 7</b></p> <p>Connessione del controllore alla rete ..... 109</p> <p>    Connessione del dispositivo EtherNet/IP e del computer ..... 110</p> <p>    Connessione del modulo di comunicazione ControlNet o dello scanner DeviceNet e del computer..... 110</p> <p>    Configurazione di un driver EtherNet/IP, ControlNet o DeviceNet..... 110</p> <p>Analisi dei fattori che influiscono sul collegamento online..... 111</p> <p>    Corrispondenza tra progetto e controllore ..... 111</p> <p>    Corrispondenza della versione del firmware..... 111</p> <p>    Stato di sicurezza/errori ..... 111</p> <p>    Firma del task di sicurezza e stato di blocco/sblocco di sicurezza..... 112</p> <p>Download ..... 113</p> <p>Upload ..... 115</p> <p>Collegamento online ..... 116</p>
<b>Memorizzazione e caricamento di progetti con la memoria non volatile</b>	<p><b>Capitolo 8</b></p> <p>Utilizzo delle schede di memoria per la memoria non volatile..... 119</p> <p>Memorizzazione di un progetto di sicurezza ..... 120</p> <p>Caricamento di un progetto di sicurezza..... 121</p> <p>Utilizzo dei moduli ESM (solo controllori 1756-L7xS) ..... 122</p> <p>    Salvataggio del programma sulla memoria NVS integrata..... 123</p> <p>    Cancellazione del programma dalla memoria NVS integrata..... 123</p> <p>Valutazione del mantenimento dell'orologio interno (WallClockTime) da parte del modulo ESM..... 124</p> <p>Gestione del firmware con Firmware Supervisor..... 124</p>
<b>Monitoraggio dello stato e gestione degli errori</b>	<p><b>Capitolo 9</b></p> <p>Visualizzazione dello stato attraverso la barra di stato ..... 125</p> <p>Monitoraggio delle connessioni..... 126</p> <p>    Tutte le connessioni ..... 126</p> <p>    Connessioni di sicurezza ..... 127</p> <p>Monitoraggio degli indicatori di stato ..... 127</p> <p>Monitoraggio dello stato di sicurezza..... 128</p> <p>Errori del controllore ..... 128</p> <p>    Errori irreversibili del controllore ..... 129</p> <p>    Errori di sicurezza irreversibili nell'applicazione di sicurezza ..... 129</p> <p>    Errori reversibili nell'applicazione di sicurezza..... 129</p> <p>    Visualizzazione degli errori ..... 130</p> <p>    Codici di errore..... 130</p> <p>Sviluppo di una routine di errore..... 131</p> <p>    Routine di errore del programma..... 131</p> <p>    Gestore degli errori del controllore ..... 131</p> <p>    Utilizzo delle istruzioni GSV/SSV ..... 132</p>



	<b>Appendice A</b>	
<b>Indicatori di stato</b>	Indicatori di stato del controllore 1756-L6xS .....	135
	Indicatori di stato del controllore 1756-L7xS .....	136
	Display di stato del controllore 1756-L7xS .....	137
	Messaggi di stato di sicurezza .....	137
	Messaggi di stato generali .....	138
	Messaggi di errore .....	139
	Messaggi relativi agli errori gravi reversibili .....	139
	Codici di errore I/O .....	140
	<b>Appendice B</b>	
<b>Manutenzione della batteria</b>	Stima della durata della batteria .....	143
	Prima che si accenda la spia BAT .....	143
	Dopo l'accensione della spia BAT .....	144
	Quando sostituire la batteria .....	145
	Sostituire la batteria .....	145
	Immagazzinaggio delle batterie di ricambio .....	147
	Ulteriori riferimenti .....	147
	<b>Appendice C</b>	
<b>Modifica del tipo di controllore nei progetti RSLogix 5000</b>	Cambio da controllore standard a controllore di sicurezza .....	149
	Cambio da controllore di sicurezza a controllore standard .....	150
	Passaggio da un controllore GuardLogix 1756 ad un controllore Compact GuardLogix 1768 o viceversa .....	151
	Passaggio da un controllore 1756-L7xS ad un controllore 1756-L6xS o 1768-L4xS .....	151
	Ulteriori riferimenti .....	151
	<b>Appendice D</b>	
<b>Storico delle modifiche</b>	1756-UM020H-EN-P, Aprile 2012 .....	153
	1756-UM020G-EN-P, Febbraio 2012 .....	153
	1756-UM020F-EN-P, Agosto 2010 .....	154
	1756-UM020E-EN-P, Gennaio 2010 .....	154
	1756-UM020D-EN-P, Luglio 2008 .....	154
	1756-UM020C-EN-P, Dicembre 2006 .....	155
	1756-UM020B-EN-P, Ottobre 2005 .....	155
	1756-UM020A-EN-P, Gennaio 2005 .....	155
<b>Indice analitico</b>		



<b>Argomento</b>	<b>Pagina</b>
Informazioni sui controllori GuardLogix 1756	11
Terminologia	12
Ulteriori riferimenti	13

Il presente manuale è una guida all'uso dei controllori GuardLogix™. Vi vengono descritte le procedure specifiche per GuardLogix utilizzate per la configurazione, l'uso e la ricerca guasti sul controllore.

Utilizzare questo manuale se si è responsabili della progettazione, l'installazione, la programmazione o la ricerca dei guasti relativi ai sistemi di controllo che impiegano i controllori GuardLogix.

È necessario avere una conoscenza di base dei circuiti elettrici ed esperienza con la logica a relè. È inoltre necessario avere la formazione e l'esperienza necessarie per la creazione, l'utilizzo e la manutenzione dei sistemi di sicurezza.

Per informazioni dettagliate su argomenti correlati, come la programmazione del controllore GuardLogix ed i requisiti SIL 3/PLC, o informazioni sui componenti Logix standard, consultare l'elenco [Ulteriori riferimenti](#) a pagina [13](#).

## **Informazioni sui controllori GuardLogix 1756**

Sono disponibili due linee di controllori GuardLogix™ 1756. Questi controllori condividono molte funzioni ma hanno anche qualche differenza. La [Tabella 1](#) spiega brevemente tali differenze.

**Tabella 1 – Differenze tra i controllori 1756-L7xS e 1756-L6xS**

<b>Funzione</b>	<b>1756-L7xS</b> (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	<b>1756-L6xS</b> (1756-L61S, 1756-L62S, 1756-L63S, 1756-L6SP)
Supporto dell'orologio e backup per il mantenimento della memoria allo spegnimento	Modulo di alimentazione (ESM)	Batteria
Porte di comunicazione (integrate)	USB	Seriale
Connessioni, controllore	500	250
Memoria, non volatile	Scheda Secure Digital (SD)	Scheda CompactFlash
indicatori di stato	Display a scorrimento ed indicatori di stato a LED	Indicatori di stato a LED

I controllori GuardLogix per ambienti estremi, numeri di catalogo 1756-L73SXT e 1756-L7SPXT, presentano le stesse funzionalità del controllore 1756-L73S, ma sono progettati per resistere a temperature comprese tra -25 e 70 °C.

**IMPORTANTE** I componenti del sistema Logix-XT sono classificati per condizioni ambientali estreme solo se utilizzati correttamente con altri componenti del sistema Logix-XT. L'utilizzo di componenti Logix-XT con componenti del sistema Logix tradizionale annulla la classificazione per ambienti estremi.

## Terminologia

Nella seguente tabella sono riportate le definizioni dei termini utilizzati nel presente manuale.

**Tabella 2 – Termini e definizioni**

Abbreviazione	Termine completo	Definizione
1oo2	Uno di due	Si riferisce alla progettazione comportamentale di un sistema di sicurezza a più processori.
CIP	Common Industrial Protocol	Protocollo di comunicazione progettato per le applicazioni di automazione industriale.
CIP Safety	Common Industrial Protocol – Safety Certified	Versione in classe SIL 3/PLe del CIP.
DC	Copertura diagnostica	Il rapporto tra tasso di guasto rilevato e tasso di guasto totale.
EN	Norme europee.	Norme ufficiali europee.
ESM	Modulo di alimentazione	Utilizzato per supporto dell'orologio e backup per il mantenimento della memoria allo spegnimento dei controllori 1756-L7xS e 1756-L73SXT.
GSV	Get System Value	Istruzione che recupera le informazioni specificate relative allo stato del controllore e le posiziona in un tag di destinazione.
–	Multicast	Trasmissione delle informazioni da un trasmettitore a più ricevitori.
PFD	Probabilità di guasto su domanda	La probabilità media di un sistema di non adempiere alla sua funzione di progetto su domanda.
PFH	Probabilità di guasto all'ora	La probabilità per un sistema di subire un guasto pericoloso all'ora.
PL	Livelli prestazionali	Classe di sicurezza ISO 13849-1.
RPI	Intervallo di pacchetto richiesto	Durante la comunicazione su una rete, l'intervallo previsto di produzione dati.
SNN	Numero di rete di sicurezza	Un numero univoco che identifica una sezione della rete di sicurezza.
SSV	Set System Value	Istruzione che imposta i dati del sistema di controllo.
–	Standard	Un oggetto, task, tag, programma o componente del progetto non relativo alla sicurezza.
–	Unicast	Trasmissione delle informazioni da un trasmettitore ad un ricevitore.

## Ulteriori riferimenti

Questi documenti contengono informazioni aggiuntive sui prodotti Rockwell Automation.

**Tabella 3 – Pubblicazioni correlate ai sistemi ed ai controllori GuardLogix**

Per ulteriori informazioni su	Consultare	Descrizione
Requisiti delle applicazioni (sicurezza)	Manuale di riferimento per la sicurezza Sistemi del controllore GuardLogix, pubblicazione <a href="#">1756-RM093F-IT-P</a>	Contiene requisiti dettagliati per ottenere e mantenere il livello SIL 3/PLC con il sistema del controllore GuardLogix.
Batterie	Direttive per il trattamento delle batterie al litio, pubblicazione <a href="#">AG-5.4</a>	Contiene informazioni sulla conservazione, il trattamento, il trasporto e lo smaltimento delle batterie al litio.
	Sito di riferimento sulle batterie dei controllori programmabili, <a href="http://www.ab.com/programmablecontrol/batteries.html">http://www.ab.com/programmablecontrol/batteries.html</a>	Fornisce le schede di sicurezza (Material Safety Data Sheets – MSDS) delle singole batterie di ricambio.
CIP Sync (sincronizzazione temporale)	Integrated Architecture and CIP Sync Configuration Application Technique, pubblicazione <a href="#">IA-AT003</a>	Fornisce informazioni dettagliate e complete sulle modalità di applicazione della tecnologia CIP Sync per sincronizzare gli orologi in un sistema di controllo Logix.
Progettazione e selezione	Manuale di riferimento – Logix5000 Controllers Design Considerations, pubblicazione <a href="#">1756-RM094</a>	Comprende linee guida per l'ottimizzazione dei sistemi ed informazioni di sistema per le scelte relative alla progettazione dei sistemi, pensate per utenti esperti.
	Controllori ControlLogix Guida alla selezione, pubblicazione <a href="#">1756-SG001K-IT-P</a>	Comprende descrizioni di livello avanzato relative al processo di selezione dei componenti del sistema ControlLogix®, informazioni sulle specifiche principali necessarie per le decisioni iniziali e riferimenti a informazioni specifiche complete.
Guard I/O	Manuale dell'utente Guard I/O DeviceNet Safety Modules, pubblicazione <a href="#">1791DS-UM001</a>	Fornisce informazioni sull'utilizzo dei moduli DeviceNet Safety Guard I/O.
	Manuale dell'utente Moduli di sicurezza Guard I/O EtherNet/IP, pubblicazione <a href="#">1791ES-UM001C-IT-P</a>	Fornisce informazioni sull'uso dei moduli Safety EtherNet/IP Guard I/O.
	Manuale dell'utente Moduli di sicurezza POINT Guard I/O, pubblicazione <a href="#">1734-UM013B-IT-P</a>	Fornisce informazioni sulle procedure di installazione, configurazione ed uso dei moduli POINT Guard I/O™.
Installazione hardware	Istruzioni per l'installazione ControlLogix Chassis and Power Supplies, pubblicazione <a href="#">1756-IN005</a>	Illustra le procedure di installazione e messa a terra degli alimentatori e dello chassis ControlLogix.
	Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione <a href="#">1770-4.1</a>	Fornisce informazioni dettagliate sulla messa a terra ed i collegamenti dei controllori programmabili
Istruzioni (programmazione)	Manuale di riferimento Set di istruzioni per l'applicazione di sicurezza GuardLogix, pubblicazione <a href="#">1756-RM095B-IT-P</a>	Fornisce informazioni sul set di istruzioni dell'applicazione di sicurezza GuardLogix.
	Manuale di riferimento Istruzioni generali per controllori Logix5000, pubblicazione <a href="#">1756-RM097A-IT-P</a>	Fornisce ai programmatori informazioni dettagliate su tutte le istruzioni disponibili per un controllore Logix5000.
	Manuale di riferimento Logix5000 Controllers Motion Instructions, pubblicazione <a href="#">MOTION-RM002</a>	Fornisce ai programmatori tutti i dettagli sulle istruzioni di controllo assi disponibili per un controllore Logix5000.
Controllo assi	Manuale dell'utente SERCOS Motion Configuration and Startup, pubblicazione <a href="#">MOTION-UM001</a>	Spiega come configurare un sistema applicativo di controllo assi SERCOS.
	Manuale dell'utente Motion Coordinated Systems, pubblicazione <a href="#">MOTION-UM002</a>	Spiega come creare e configurare un sistema applicativo di controllo assi coordinato.
	Manuale dell'utente CIP Motion Configuration and Startup, pubblicazione <a href="#">MOTION-UM003</a>	Spiega come configurare un sistema applicativo Integrated Motion su EtherNet/IP.
	Manuale di riferimento CIP Motion, pubblicazione <a href="#">MOTION-RM003</a>	Informazioni dettagliate sulle modalità di controllo assi e sugli attributi per Integrated Motion su EtherNet/IP.
Reti (ControlNet, DeviceNet EtherNet/IP)	Manuale dell'utente EtherNet/IP Modules in Logix5000 Control Systems, pubblicazione <a href="#">ENET-UM001</a>	Spiega come configurare ed utilizzare i moduli EtherNet/IP in un sistema di controllo Logix5000™.
	Manuale dell'utente ControlNet Modules in Logix5000 Control Systems, pubblicazione <a href="#">CNET-UM001</a>	Spiega come configurare ed utilizzare i moduli ControlNet in un sistema di controllo Logix5000.
	Manuale dell'utente DeviceNet Modules in Logix5000 Control Systems, pubblicazione <a href="#">DNET-UM004</a>	Spiega come configurare ed utilizzare i moduli DeviceNet in un sistema di controllo Logix5000.
PhaseManager™	Manuale dell'utente PhaseManager, pubblicazione <a href="#">LOGIX-UM001</a>	Fornisce procedure, guida ed esempi per la configurazione e la programmazione di un controllore Logix5000 per l'uso delle fasi di apparecchiatura.

**Tabella 3 – Pubblicazioni correlate ai sistemi ed ai controllori GuardLogix**

Per ulteriori informazioni su	Consultare	Descrizione
Procedure e task di programmazione	Manuale di programmazione Logix5000 Controllers Common Procedures, pubblicazione <a href="#">1756-PM001</a>	Consente di accedere ai contenuti dei manuali di programmazione della serie di controllori Logix5000, contenenti informazioni sulla gestione dei file di progetto, l'organizzazione dei tag, la programmazione in logica ladder, l'esecuzione di test relativi alle routine, la creazione di istruzioni add-on, i dati relativi allo stato del controllore, la gestione degli errori, l'importazione e l'esportazione dei componenti dei progetti e molto altro ancora.
	Manuale di riferimento Logix5000 Controllers Execution Time and Memory Use, pubblicazione <a href="#">1756-RM087</a>	Suggerisce come stimare l'uso della memoria ed il tempo d'esecuzione della logica programmata e come scegliere tra le varie opzioni di programmazione.
Ridondanza	Manuale dell'utente ControlLogix Redundancy System, pubblicazione <a href="#">1756-UM523</a>	Fornisce istruzioni per la progettazione, lo sviluppo e l'implementazione di un sistema in ridondanza ControlLogix standard.
	Manuale dell'utente ControlLogix Enhanced Redundancy System, pubblicazione <a href="#">1756-UM535</a>	Fornisce istruzioni per la progettazione, lo sviluppo e l'implementazione di un sistema in ridondanza ControlLogix di livello avanzato.

Per consultare o scaricare le pubblicazioni, visitare il sito <http://www.rockwellautomation.com/literature>. Per ordinare copie cartacee della documentazione tecnica, rivolgersi al distributore Allen-Bradley® o all'agente Rockwell Automation di zona.

## Cenni generali sul sistema

Argomento	Pagina
Requisiti delle applicazioni di sicurezza	15
Distinzione tra componenti standard e di sicurezza	16
Capacità del flusso di dati del controllore	17
Scelta dell'hardware del sistema	18
Scelta dei moduli I/O di sicurezza	20
Scelta delle reti di comunicazione	20
Requisiti di programmazione	21

### Requisiti delle applicazioni di sicurezza

Il sistema del controllore GuardLogix è certificato per l'uso in applicazioni di sicurezza fino al livello di integrità di sicurezza (SIL) 3 e Livello prestazionale (e), nei quali lo stato di diseccitazione rappresenta lo stato di sicurezza. I requisiti delle applicazioni di sicurezza comprendono la valutazione delle probabilità di guasto (PFD e PFH), le impostazioni del tempo di risposta del sistema ed i test di verifica funzionale che soddisfano i criteri del livello SIL 3/PLe.

Per informazioni sui requisiti dei sistemi di sicurezza SIL 3 e PLe, comprese le frequenze dei test di validazione funzionale, il tempo di risposta del sistema ed i calcoli della probabilità di guasto PFD/PFH, consultare la pubblicazione Manuale di riferimento per la sicurezza – Sistemi di controllori GuardLogix [1756-RM093](#). Prima di iniziare ad utilizzare un sistema di sicurezza SIL 3, PLe GuardLogix è necessario leggere, comprendere ed osservare questi requisiti.

Le applicazioni di sicurezza SIL 3/PLe basate su GuardLogix richiedono l'uso di almeno un Numero di Rete di Sicurezza (SNN, Safety Network Number) e di una firma del task di sicurezza. Entrambi influiscono sulla configurazione di controllore e I/O e sulla comunicazione di rete.

Per ulteriori informazioni, consultare la pubblicazione Manuale di riferimento per la sicurezza – Sistemi di controllori GuardLogix, [1756-RM093](#).

### Numero di rete di sicurezza

Il Numero di Rete di Sicurezza (SNN, Safety Network Number) deve essere un numero univoco che identifica le sottoreti di sicurezza. Ogni sottorete di sicurezza utilizzata dal controllore per le comunicazioni di sicurezza deve avere un numero SNN univoco. Ogni dispositivo CIP Safety deve essere configurato anche con il numero SNN della sottorete di sicurezza. Il valore SNN può essere assegnato automaticamente o manualmente.

Per informazioni sull'assegnazione del numero SNN, vedere [Gestione del numero di rete di sicurezza \(SNN\) a pagina 53](#).

## Firma del task di sicurezza

La firma del task di sicurezza è costituita da un numero ID, dalla data e dall'ora, che identificano in modo univoco la parte di sicurezza di un progetto, compresi logica di sicurezza, dati e configurazione. Il sistema GuardLogix utilizza la firma del task di sicurezza per determinare l'integrità del progetto e per consentire di verificare che nel controllore di destinazione venga scaricato il progetto corretto. La creazione, la registrazione e la verifica della firma del task di sicurezza sono passaggi obbligati del processo di sviluppo dell'applicazione di sicurezza.

Per ulteriori informazioni, vedere [Generazione di una firma del task di sicurezza a pagina 106](#).

## Distinzione tra componenti standard e di sicurezza

Gli slot di uno chassis del sistema GuardLogix non utilizzati dalla funzione di sicurezza possono essere riempiti con altri moduli ControlLogix certificati in base alle Direttive per la Bassa Tensione ed EMC. Per informazioni sul certificato CE per la famiglia di prodotti Controllori programmabili – ControlLogix, e per determinare quali moduli siano certificati, consultare il sito Web <http://ab.com/certification/ce>.

È necessario creare e documentare una distinzione chiara, logica e visibile tra i componenti standard e quelli di sicurezza dell'applicazione. Per facilitare questa distinzione, il software di programmazione RSLogix 5000 dispone di icone di identificazione della sicurezza per identificare task di sicurezza, programmi di sicurezza, routine di sicurezza e componenti di sicurezza. Inoltre, il software RSLogix 5000 utilizza un attributo di classe di sicurezza visibile ogni volta che si visualizzano task di sicurezza, programmi di sicurezza, routine di sicurezza, tag di sicurezza o proprietà delle istruzioni add-on.

Il controllore non consente di scrivere nei dati dei tag di sicurezza da dispositivi di interfaccia operatore esterni o tramite le istruzioni dei messaggi da controllori peer. Il software RSLogix 5000 è in grado di scrivere i tag di sicurezza quando il controllore GuardLogix è in sblocco di sicurezza, non dispone di una firma del task di sicurezza ed è in funzione senza errori di sicurezza.

In Sistema ControlLogix – Manuale dell'utente, pubblicazione [1756-UM001](#), sono disponibili ulteriori informazioni sull'utilizzo dei dispositivi ControlLogix in applicazioni standard (non di sicurezza).

## Dispositivi di interfaccia operatore

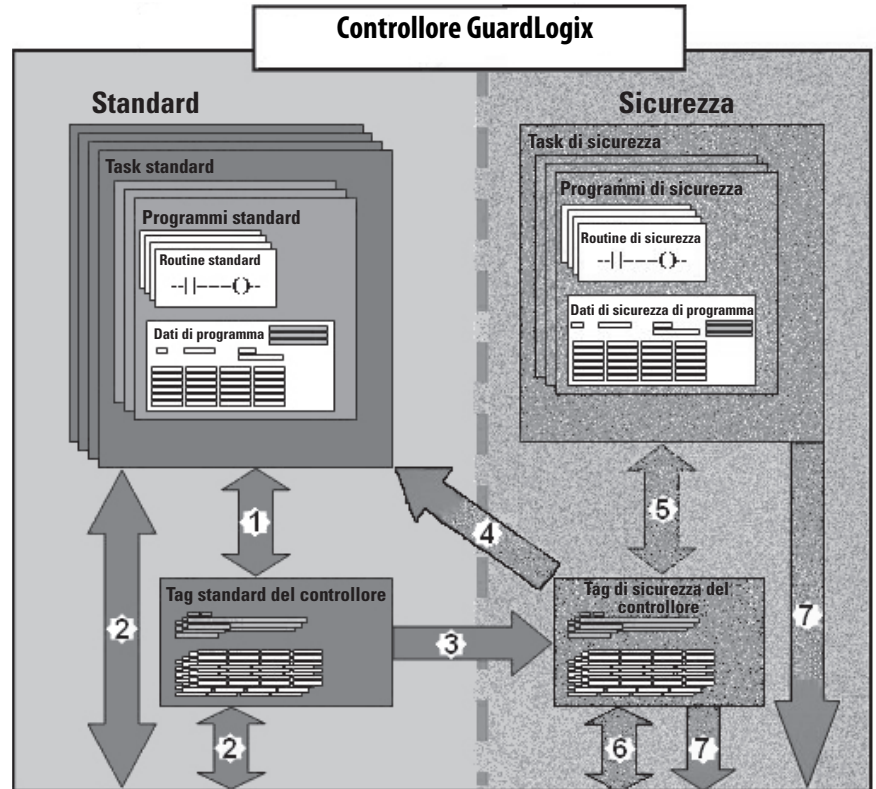
I dispositivi di interfaccia operatore possono essere utilizzati con i controllori GuardLogix. I dispositivi di interfaccia operatore sono in grado di accedere ai tag standard proprio come con qualsiasi altro controllore standard. Tuttavia, i dispositivi di interfaccia operatore non sono in grado di scrivere nei tag di sicurezza che, per tali dispositivi, sono di sola lettura.



## Capacità del flusso di dati del controllore

La figura riportata di seguito illustra il flusso di dati standard e di sicurezza del controllore GuardLogix.

**Figura 1 – Capacità del flusso di dati**



N.	Descrizione
1	I tag e la logica standard si comportano in modo identico a quanto avviene nella piattaforma Logix standard.
2	I dati di tag standard, dell'ambito del programma o del controllore, possono essere scambiati con dispositivi di interfaccia operatore, personal computer ed altri controllori esterni.
3	I controllori GuardLogix sono controllori integrati dotati della possibilità di spostare (mappare) dati da tag standard in tag di sicurezza per utilizzarli all'interno del task di sicurezza.
	 <b>ATTENZIONE:</b> Tali dati non devono essere utilizzati per controllare direttamente un'uscita SIL 3/PL.
4	I tag di sicurezza dell'ambito del controllore possono essere letti direttamente dalla logica standard.
5	I tag di sicurezza possono essere letti o scritti dalla logica di sicurezza.
6	I tag di sicurezza possono essere scambiati dai controllori di sicurezza su reti Ethernet o ControlNet, ivi compresi i controllori GuardLogix 1756 e 1768.
7	I dati di tag di sicurezza, dell'ambito del programma o del controllore, possono essere letti da dispositivi esterni, quali dispositivi di interfaccia operatore, personal computer ed altri controllori standard.
	<b>IMPORTANTE</b> Dopo essere stati letti, tali dati sono considerati di tipo standard e non SIL 3/PL.

## Scelta dell'hardware del sistema

Il sistema GuardLogix supporta le applicazioni di sicurezza SIL 3 e PLe. Il controllore GuardLogix è costituito da un controllore primario e da un coprocessore di sicurezza che funzionano insieme in un'architettura 1oo2. La [Tabella 4](#) elenca i numeri di catalogo dei controllori primari e dei coprocessori di sicurezza.

Il coprocessore di sicurezza deve essere installato nello slot immediatamente a destra del controllore primario. Le versioni principale e secondaria del firmware del controllore primario e del coprocessore di sicurezza devono corrispondere esattamente affinché venga stabilita la partnership di controllo necessaria per le applicazioni di sicurezza.

**Tabella 4 – Numeri di catalogo dei controllori primari e dei corrispondenti coprocessori di sicurezza**

Controllore primario	Coprocessore di sicurezza
1756-L61S, 1756-L62S, 1756-L63S	1756-LSP
1756-L71S, 1756-L72S, 1756-L73S	1756-L7SP
1756-L73SXT	1756-L7SPXT

### Controllore primario

Il controllore primario è il processore che esegue sia le funzioni standard sia quelle di sicurezza e che comunica con il coprocessore di sicurezza per le funzioni di sicurezza del sistema di controllo GuardLogix. Di seguito è riportato un elenco di funzioni standard.

- Controllo I/O
- Logica
- Temporizzazione
- Conteggio
- Generazione rapporti
- Comunicazione
- Calcoli aritmetici
- Manipolazione file dati

Il controllore primario è costituito da un processore centrale, dall'interfaccia I/O e dalla memoria.

**Tabella 5 – Capacità memoria**

Num. di Cat.	Memoria utente (capacità RAM)	
	Task e componenti standard	Task e componenti di sicurezza
1756-L61S	2 MB	1 MB
1756-L62S	4 MB	1 MB
1756-L63S	8 MB	3,75 MB
1756-L71S	2 MB	1 MB
1756-L72S	4 MB	2 MB
1756-L73S,1756-L73SXT	8 MB	4 MB

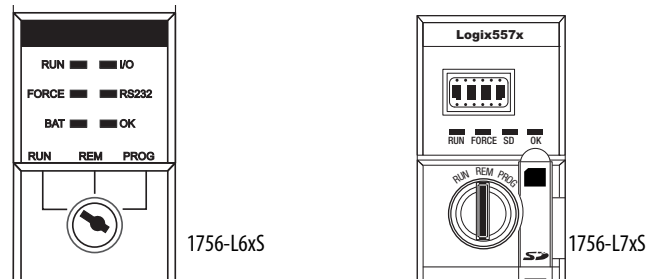
Nel software RSLogix 5000 versione 18 o successive, il controllore GuardLogix supporta gli aggiornamenti del sistema operativo e permette di archiviare e recuperare i programmi utente tramite una scheda di memoria. Tuttavia, nella versione 16 e 17 del software RSLogix 5000, l'utente poteva visualizzare il contenuto di una scheda di memoria solo se era installata nel controllore primario. Prima della versione 16, le schede di memoria non erano supportate.

Per ulteriori informazioni vedere [Capitolo 8, Memorizzazione e caricamento di progetti con la memoria non volatile](#).

Un selettore a chiave a tre posizioni sulla parte anteriore del controllore primario controlla le modalità di funzionamento del controllore. Sono disponibili le seguenti modalità:

- RUN (Esecuzione)
- PROG (Programmazione)
- REM (Remota): questa modalità abilitata dal software può essere Programmazione, Esecuzione o Test

**Figura 2 – Posizione del selettore a chiave**



## Coprocessore di sicurezza

Il coprocessore di sicurezza è quello che fornisce un secondo canale isolato (ridondanza) per le funzioni di sicurezza del sistema.

Il coprocessore di sicurezza non dispone di un selettore a chiave o di una porta di comunicazione. La configurazione ed il funzionamento sono controllati dal controllore primario.

## Chassis

Lo chassis ControlLogix fornisce connessioni fisiche tra i moduli ed il controllore GuardLogix.

## Alimentatore

Gli alimentatori ControlLogix elencati a [pagina 28](#) possono essere utilizzati in applicazioni SIL 3. Per il funzionamento SIL 3 degli alimentatori non sono necessarie configurazioni o collegamenti aggiuntivi.

## Scelta dei moduli I/O di sicurezza

I dispositivi di ingresso ed uscita di sicurezza possono essere collegati all'I/O CIP Safety su reti DeviceNet o EtherNet/IP, permettendo il controllo dei dispositivi di uscita tramite il sistema del controllore GuardLogix attraverso comunicazioni DeviceNet o EtherNet/IP.

Per informazioni aggiornate sui numeri di catalogo, le serie certificate e le versioni firmware disponibili degli I/O CIP Safety, visitare il sito Web <http://www.ab.com/certification/safety>.

## Scelta delle reti di comunicazione

Il controllore GuardLogix supporta funzioni di comunicazione che consentono di:

- distribuire e controllare l'I/O di sicurezza su reti DeviceNet o EtherNet/IP
- distribuire e controllare l'I/O di sicurezza remoto su reti DeviceNet, EtherNet/IP o ControlNet
- produrre e consumare i dati dei tag di sicurezza tra i controllori GuardLogix 1756 e 1768 attraverso una rete Ethernet/IP o ControlNet, oppure all'interno dello stesso chassis ControlLogix
- distribuire e controllare l'I/O standard su reti EtherNet, ControlNet o DeviceNet.

Come interfaccia tra i controllori GuardLogix ed i dispositivi di rete si utilizzano i seguenti moduli di comunicazione.

**Tabella 6 – Moduli di comunicazione**

Come interfaccia tra	Utilizzare il modulo	Fare riferimento alle istruzioni per l'installazione
Il controllore GuardLogix ed i dispositivi DeviceNet	1756-DNB	<a href="#">DNET-IN001</a>
Il controllore GuardLogix ed i dispositivi EtherNet/IP	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR, 1756-EN3TR 1756-EN2TXT	<a href="#">ENET-IN002</a>
Controllori sulla rete ControlNet	1756-CN2, 1756-CN2R 1756-CN2RXT	<a href="#">CNET-IN005</a>

Il controllore GuardLogix può essere collegato al software di programmazione RSLogix 5000 tramite una connessione seriale o USB, un modulo EtherNet, oppure un modulo ControlNet.

I controllori 1756-L6xS sono dotati di una porta seriale. I controllori 1756-L7xS sono dotati di una porta USB.

Per ulteriori informazioni sull'uso dei moduli di comunicazione di rete, vedere [Ulteriori riferimenti a pagina 13](#).

**Requisiti di programmazione**

Il software RSLogix 5000 è lo strumento di programmazione per le applicazioni dei controllori GuardLogix.

Fare riferimento alla [Tabella 7](#) per individuare le versioni software minime da utilizzare con i controllori GuardLogix in uso. Il software RSLogix 5000 versione 15 non supporta SIL (Safety Integrity Level) 3.

**Tabella 7 – Versioni software**

Num. di Cat.	Versione software RSLogix 5000 <sup>(1)</sup>	Versione software RSLinx Classic <sup>(1)</sup>
1756-L61S, 1756-L62S	14	Qualsiasi versione
1756-L63S	16	
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	20	2.59

(1) La presente o successiva.

Le routine di sicurezza includono le istruzioni di sicurezza, che sono un sottoinsieme del set di istruzioni della logica ladder standard, e le istruzioni per le applicazioni di sicurezza. I programmi schedulati nell'ambito del task di sicurezza supportano solo la logica ladder.

**Tabella 8 – Funzioni supportate nelle varie versioni del software RSLogix 5000**

Funzione	Versione 14		Versione 16		Versione 17		Versione 18		Versione 19		Versione 20	
	Task di sicurezza	Task standard	Task di sicurezza	Task standard	Task di sicurezza	Task standard	Task di sicurezza	Task standard	Task di sicurezza	Task standard	Task di sicurezza	Task standard
Istruzioni add-on				X		X	X	X	X	X	X	X
Allarmi ed eventi				X		X		X		X		X
Registro controllore					X	X	X	X	X	X	X	X
Controllo degli accessi ai dati							X	X	X	X	X	X
Routine fasi apparecchiatura				X		X		X		X		X
Task evento				X		X		X		X		X
Firmware Supervisor				X		X	X	X	X	X	X	X
Diagrammi a blocchi funzione (FBD)				X		X		X		X		X
Integrated Motion				X		X		X		X		X
Logica ladder	X	X	X	X	X	X	X	X	X	X	X	X
Cambio di lingua					X	X	X	X	X	X	X	X
Scheda di memoria							X	X	X	X	X	X
Importazione ed esportazione online di componenti dei programmi						X		X		X		X
Routine in diagramma funzionale sequenziale (SFC)				X		X		X		X		X
Testo strutturato				X		X		X		X		X
Connessioni unicast per tag di sicurezza prodotti e consumati									X	X	X	X
Connessioni unicast per moduli I/O di sicurezza su EtherNet/IP											X	X

Per informazioni sull'utilizzo di queste funzioni, consultare la pubblicazione Logix5000 Controllers Common Procedures Programming Manual, [1756-PM001](#), le pubblicazioni elencate in [Ulteriori riferimenti a pagina 13](#) e la guida in linea del software RSLogix 5000.

**Note:**

## Installazione del controllore

Argomento	Pagina
Precauzioni	23
Verificare di avere tutti i componenti	27
Installazione di un alimentatore e di uno chassis	28
Collegamento della batteria (solo controllori 1756-L6xS)	28
Installazione del controllore nello chassis	29
Inserimento o rimozione di una scheda di memoria	30
Connessioni di comunicazione	35
Aggiornamento del controllore	40
Scelta della modalità operativa del controllore	42
Disinstallazione del modulo di alimentazione (ESM)	44
Installazione di un modulo di alimentazione (ESM)	46

### Precauzioni

Leggere e rispettare le seguenti precauzioni d'uso.

### Informazioni su ambiente e custodia



**ATTENZIONE:** Questa apparecchiatura è destinata all'uso in ambienti industriali con Grado di Inquinamento 2, in applicazioni con sovratensione di categoria II, (come definito nello standard IEC 60664-1) ad altitudine fino a 2000 metri senza declassamento.

Questa apparecchiatura è considerata un'apparecchiatura industriale di Gruppo 1, Classe A secondo la pubblicazione 11 dell'IEC/CISPR. Senza le dovute precauzioni, vi potrebbero essere difficoltà nell'assicurare la compatibilità elettromagnetica in ambienti residenziali ed altri ambienti a causa dei disturbi condotti ed irradiati.

L'apparecchiatura viene fornita come apparecchiatura di tipo aperto. Essa deve essere montata all'interno di una custodia adatta alle specifiche condizioni ambientali di utilizzo e progettata specificatamente per evitare lesioni al personale derivanti dall'accesso a parti in tensione. La custodia deve avere opportune caratteristiche ignifughe, al fine di prevenire o di ridurre al minimo la propagazione delle fiamme, deve essere conforme ad un grado di protezione 5 VA o essere approvata per l'applicazione se non metallica. La parte interna della custodia deve essere accessibile solo utilizzando un attrezzo. Le successive sezioni di questa pubblicazione possono contenere ulteriori informazioni circa specifici tipi di custodie richieste per la conformità alle certificazioni di sicurezza di alcuni prodotti.

Oltre alla presente pubblicazione, consultare i seguenti documenti:

- Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione [1770-4.1](#), per ulteriori requisiti di installazione
- Per ulteriori informazioni sui gradi di protezione forniti dai diversi tipi di custodia, vedere gli standard NEMA 250 ed IEC 60529

### Sistemi elettronici programmabili (PES)

---



**ATTENZIONE:** Il personale responsabile dell'applicazione dei sistemi elettronici programmabili (PES) di sicurezza deve conoscere i requisiti di sicurezza nell'applicazione del sistema e deve sapere come utilizzare il sistema.

---

### Rimozione ed inserimento sotto tensione (RIUP)

---





**AVVISO:** Quando si inserisce o si rimuove il modulo con il backplane in tensione, può verificarsi un arco elettrico, che può causare esplosioni in installazioni che si trovano in aree pericolose.

Prima di procedere, assicurarsi di aver tolto alimentazione o che l'area non sia pericolosa. Il ripetuto verificarsi di archi elettrici provoca l'eccessiva usura dei contatti, sia del modulo sia del connettore corrispondente. I contatti usurati possono generare una resistenza elettrica che può incidere negativamente sul funzionamento del modulo.

---




## Approvazione nordamericana per l'uso in aree pericolose

The following information applies when operating this equipment in hazardous locations:	Informations sur l'utilisation de cet équipement en environnements dangereux:
<p>Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.</p>	<p>Les produits marqués « CL I, DIV 2, GP A, B, C, D » ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.</p>
<div style="display: flex; align-items: center;">  <div> <p><b>WARNING: EXPLOSION HAZARD</b></p> <ul style="list-style-type: none"> <li>• Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous.</li> <li>• Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.</li> <li>• Substitution of components may impair suitability for Class I, Division 2.</li> <li>• If this product contains batteries, they must only be changed in an area known to be nonhazardous.</li> </ul> </div> </div>	<div style="display: flex; align-items: center;">  <div> <p><b>AVERTISSEMENT: RISQUE D'EXPLOSION</b></p> <ul style="list-style-type: none"> <li>• Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement.</li> <li>• Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit.</li> <li>• La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2.</li> <li>• S'assurer que l'environnement est classé non dangereux avant de changer les piles.</li> </ul> </div> </div>

### Informazioni per l'impiego dell'apparecchiatura in aree pericolose:

I prodotti contrassegnati con "CL I, DIV 2, GP A, B, C, D" sono adatti all'utilizzo solo in aree pericolose di Classe I Divisione 2 Gruppi A, B, C, D, o in aree non pericolose. Ogni prodotto è fornito di una targhetta dati indicante il codice temperatura dell'area pericolosa. Quando si utilizzano prodotti diversi all'interno di un sistema, per determinare il codice temperatura generale del sistema, è necessario usare il codice temperatura più conservativo (il numero T più basso). L'utilizzo di apparecchiature diverse all'interno del sistema è soggetto ad ispezione da parte delle autorità locali competenti al momento dell'installazione.

	<p><b>AVVISO: RISCHIO DI ESPLOSIONE</b></p> <ul style="list-style-type: none"> <li>• Non scollegare le apparecchiature senza aver prima interrotto l'alimentazione oppure senza essere certi di operare in un ambiente non pericoloso.</li> <li>• Non scollegare le connessioni di questa apparecchiatura senza aver prima interrotto l'alimentazione oppure senza prima essere certi di operare in un ambiente non pericoloso. Fissare le connessioni esterne su questa apparecchiatura mediante viti, fermi scorrevoli, connettori filettati o qualsiasi altro mezzo fornito con questo prodotto.</li> <li>• La sostituzione dei componenti può compromettere l'idoneità per gli ambienti della classe I, Divisione 2.</li> <li>• Se il prodotto contiene batterie, queste vanno sostituite esclusivamente in aree non pericolose.</li> </ul>
---	---

## Approvazione europea per l'uso in aree pericolose

---

### L'apposizione della marcatura Ex sul prodotto certifica quanto segue.

Questa apparecchiatura è destinata all'uso in atmosfere potenzialmente esplosive, come definite dalla Direttiva 94/9/CE dell'Unione Europea, ed è risultata conforme ai requisiti essenziali di sicurezza e salute riguardanti la progettazione e la costruzione di apparecchiature di Categoria 3 destinate all'uso in atmosfere potenzialmente esplosive di Zona 2, riportate nell'Allegato II di questa direttiva.

La conformità ai requisiti essenziali di sicurezza e salute è assicurata dalla conformità alle norme EN 60079-15 ed EN 60079-0.

---



**ATTENZIONE:** Questa apparecchiatura non è resistente alla luce del sole o ad altre fonti di radiazione UV.

---



### AVVISO:

- Questa apparecchiatura deve essere installata in una custodia che garantisca una protezione di livello minimo IP54 quando utilizzata in ambienti di Zona 2.
  - Questa apparecchiatura deve essere utilizzata entro i valori nominali specificati da Rockwell Automation.
  - Questa apparecchiatura deve essere utilizzata solo con backplane certificati ATEX di Rockwell Automation.
  - Fissare le connessioni esterne su questa apparecchiatura mediante viti, fermi scorrevoli, connettori filettati o qualsiasi altro mezzo fornito con questo prodotto.
  - Non scollegare le apparecchiature senza aver prima interrotto l'alimentazione oppure senza essere certi di operare in un ambiente non pericoloso.
- 

## Prevenzione delle scariche elettrostatiche

---



**ATTENZIONE:** Questa apparecchiatura è sensibile alle scariche elettrostatiche che possono causare danni interni e pregiudicare il regolare funzionamento. Quando si maneggia l'apparecchiatura, osservare le seguenti regole generali:

- Toccare un oggetto collegato a terra per scaricare l'elettricità statica.
  - Indossare un braccialetto di messa a terra omologato.
  - Non toccare i connettori o i pin delle schede dei componenti.
  - Non toccare i componenti dei circuiti all'interno dell'apparecchiatura.
  - Usare una postazione di lavoro antistatica, se disponibile.
  - Quando non viene utilizzata, conservare l'apparecchiatura in un imballaggio antistatico.
-

## Verificare di avere tutti i componenti

Prima di iniziare, controllare di avere tutti i componenti necessari.

**IMPORTANTE** Per ottenere il livello SIL 3/PLe, è necessario usare un controllore primario e un coprocessore di sicurezza.

### Controllori 1756-L6xS

Insieme al controllore 1756-L6xS vengono forniti una chiave 1747-KY e la batteria 1756-BA2, mentre con il coprocessore di sicurezza 1756-LSP viene fornita la batteria 1756-BA2.

Per collegare un dispositivo alla porta seriale del controllore (ad esempio per collegare un computer al controllore), utilizzare un cavo seriale 1756-CP3.

Per la memoria non volatile è possibile utilizzare una scheda CompactFlash 1784-CF128 con i controllori GuardLogix 1756-L6xS, versione del firmware 18 e successive.

### Controllori 1756-L7xS

Nel controllore primario e nel coprocessore di sicurezza, sono inclusi i seguenti componenti.

Num. di Cat.	Descrizione	Fornito con
1756-L71S 1756-L72S 1756-L73S	Controllore primario	<ul style="list-style-type: none"> <li>1756-ESMCAP – Modulo di alimentazione (ESM) con condensatore</li> <li>1784-SD1 – Scheda di memoria Secure Digital (SD), 1 GB</li> <li>1747-KY – Chiave</li> </ul>
1756-L7SP	Coprocessore di sicurezza	<ul style="list-style-type: none"> <li>1756-SPESMNSE – Modulo di alimentazione (ESM)</li> </ul>
1756-L73SXT	Controllore primario per temperature estreme	<ul style="list-style-type: none"> <li>1756-ESMCAPXT – Modulo di alimentazione (ESM) con condensatore</li> <li>1747-KY – Chiave</li> </ul>
1756-L7SPXT	Coprocessore di sicurezza per temperature estreme	<ul style="list-style-type: none"> <li>1756-SPESMNSEXT – Modulo di alimentazione (ESM) con condensatore</li> </ul>

È possibile utilizzare le seguenti apparecchiature opzionali.

Se l'applicazione richiede	Usare quanto segue
Memoria non volatile	1784-SD1 (1 GB) o 1784-SD2 (2 GB)
Alcune applicazioni richiedono che il modulo ESM installato scarichi l'energia residua a 200 µJ o meno, prima di rimuoverlo o inserirlo nell'applicazione. <sup>(1)</sup>	1756-ESMNSE per il controllore primario 1756-SPESMNSE per il coprocessore di sicurezza <sup>(2)</sup> Questo modulo ESM non prevede l'alimentazione di backup dell'orologio interno (WallClockTime). Questo modulo ESM, inoltre, può essere utilizzato soltanto con un 1756-L73S (8 MB) o con un controllore di memoria inferiore.
Modulo ESM che protegge il controllore impedendo la connessione USB e l'uso della scheda SD <sup>(1)</sup>	1756-ESMNRM per il controllore primario 1756-SPESMNRM per il coprocessore di sicurezza <sup>(3)</sup> Questo modulo ESM garantisce all'applicazione un grado di sicurezza superiore.

(1) Per informazioni sul tempo di autonomia dei moduli ESM, vedere la sezione [Valutazione del mantenimento dell'orologio interno \(WallClockTime\) da parte del modulo ESM](#) a [pagina 124](#).

(2) Con i controllori primari ed i coprocessori di sicurezza per temperature estreme, usare 1756-ESMNSEXT e 1756-SPESMNSEXT rispettivamente.

(3) Con i controllori primari ed i coprocessori di sicurezza per temperature estreme, usare 1756-ESMNRMXT e 1756-SPESMNRMXT rispettivamente.

## Installazione di un alimentatore e di uno chassis

Prima di installare un controllore, è necessario installare uno chassis ed un alimentatore.

1. Installare uno chassis ControlLogix attenendosi alle corrispondenti istruzioni per l'installazione.

Num. di Cat.	Slot disponibili	Serie	Fare riferimento alle istruzioni per l'installazione
1756-A4	4	B	<a href="#">1756-IN005</a>
1756-A7	7		
1756-A10	10		
1756-A13	13		
1756-A17	17		
1756-A4LXT	4	B	
1756-A5XT	5	B	
1756-A7XT	7	B	
1756-A7LXT	7	B	

I controllori per temperature estreme (XT) richiedono uno chassis XT.

2. Installare un alimentatore ControlLogix attenendosi alle corrispondenti istruzioni per l'installazione.

Num. di Cat.	Descrizione	Serie	Fare riferimento alle istruzioni per l'installazione
1756-PA72	Alimentatore, CA	C	<a href="#">1756-IN005</a>
1756-PB72	Alimentatore, CC		
1756-PA75	Alimentatore, CA	B	
1756-PB75	Alimentatore, CC		
1756-PAXT	Alimentatore XT, CA	B	
1756-PBXT	Alimentatore XT, CC		

I controllori per temperature estreme (XT) richiedono un alimentatore XT.

## Collegamento della batteria (solo controllori 1756-L6xS)

I controllori 1756-L6xS ed il coprocessore di sicurezza 1756-LSP contengono una batteria al litio, che dovrà essere sostituita durante la vita utile del prodotto.



**AVVISO:** Quando si connette o si disconnette la batteria, può verificarsi un arco elettrico, che può causare esplosioni in installazioni che si trovano in aree pericolose. Prima di procedere, assicurarsi di aver tolto alimentazione o che l'area non sia pericolosa.

Per informazioni di sicurezza sul trattamento e lo smaltimento delle batterie al litio anche con perdite, consultare Direttive per il trattamento delle batterie al litio, pubblicazione [AG-5.4](#).

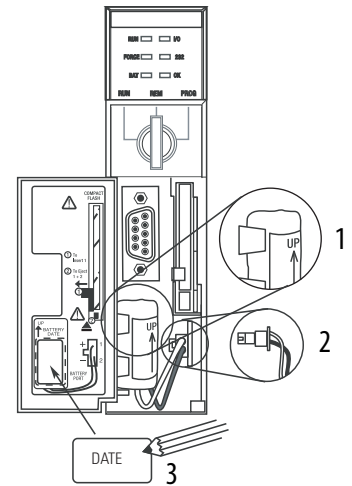
Per far sì che i dati della memoria del controllore vengano mantenuti anche in assenza di alimentazione, è necessario collegare una batteria. Attenersi alla procedura sia per il controllore 1756-L6xS che per il coprocessore di sicurezza 1756-LSP.

### IMPORTANTE

È possibile collegare solo una batteria 1756-BA2 al controllore. Collegando una batteria di tipo diverso, si rischia di danneggiare il controllore.

Per installare una nuova batteria 1756-BA2, procedere come segue.

1. Inserire la batteria come mostrato nella figura.
2. Collegare la batteria:  
+ Rosso  
- Nero
3. Annotare la data di installazione della batteria sull'apposita etichetta e fissare l'etichetta all'interno dello sportellino del controllore.



Per ulteriori informazioni sulla manutenzione della batteria, consultare l'[Appendice B](#).

## Installazione del controllore nello chassis

I controllori possono essere installati o rimossi mentre lo chassis è in tensione ed il sistema funzionante.



**AVVISO:** Se si inserisce o si rimuove il modulo con l'alimentazione backplane inserita, potrebbe verificarsi un arco elettrico, che può causare esplosioni in installazioni che si trovano in aree pericolose.

Prima di procedere, assicurarsi di aver tolto alimentazione o che l'area non sia pericolosa. Il ripetuto verificarsi di archi elettrici provoca l'eccessiva usura dei contatti, sia del modulo sia del connettore corrispondente. I contatti usurati possono generare una resistenza elettrica che può incidere negativamente sul funzionamento del modulo.

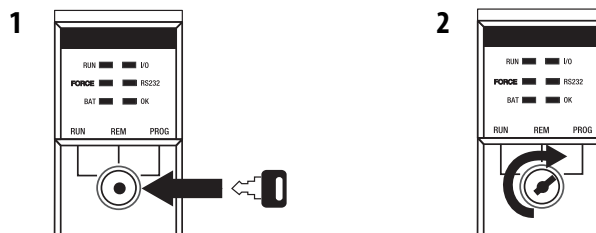
### IMPORTANTE

Nel caso dei controllori 1756-L7xS e dei coprocessori di sicurezza 1756-L7SP, l'ESM inizia a caricare quando viene eseguita una delle seguenti azioni:

- Installazione di controllore e modulo ESM in uno chassis in tensione.
- Messa in tensione di uno chassis in cui è installato un controllore con modulo ESM.
- Installazione di un modulo ESM in un controllore in tensione.

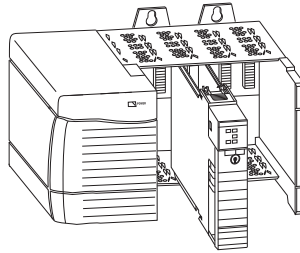
Dopo la messa in tensione, il modulo ESM si carica per un periodo massimo di due minuti, come indicato da CHRG o ESM Charging sul display di stato.

1. Inserire la chiave nel controllore primario.
2. Girare la chiave in posizione PROG.



Il coprocessore di sicurezza non è dotato di selettore a chiave.

3. Allineare le schede circuitali superiore ed inferiore con le guide nello chassis.



4. Far scorrere il controllore nello chassis.

Il controllore è correttamente installato quando allineato con l'alimentatore o gli altri moduli presenti e quando i fermi superiore ed inferiore sono agganciati.

---

**IMPORTANTE** Il coprocessore di sicurezza deve essere installato nello slot immediatamente a destra del controllore primario. Per installare il coprocessore di sicurezza, seguire le stesse procedure di cui ai punti [3](#) e [4](#) sopra.

---

Dopo aver inserito il controllore nello chassis, vedere [Capitolo 9](#) per informazioni sulla lettura degli indicatori di stato del controllore primario e del coprocessore di sicurezza.

## Inserimento o rimozione di una scheda di memoria



---

**AVVISO:** Se si inserisce o si estrae la scheda di memoria con l'alimentazione inserita, potrebbe verificarsi un arco elettrico, che può causare esplosioni in installazioni che si trovano in aree pericolose. Prima di procedere, assicurarsi di aver tolto alimentazione o che l'area non sia pericolosa.

---



---

**ATTENZIONE:** Se **non** si è sicuri del contenuto della scheda di memoria, **prima** di installarla, portare il selettore a chiave del controllore in posizione PROG. A seconda del contenuto della scheda, un ciclo di spegnimento/riaccensione o un errore potrebbero causare il caricamento di un progetto o di un sistema operativo differente nel controllore.

---

I controllori 1756-L7xS funzionano con schede Secure Digital (SD).  
Vedere [pagina 31](#).

Il controllore 1756-L6xS funziona con schede CompactFlash (CF).  
Vedere [pagina 33](#).

## Scheda Secure Digital (controllori 1756-L7xS)

Il controllore 1756-L7xS viene fornito con una scheda SD installata, che è consigliabile lasciare installata.

### *Rimozione della scheda SD*

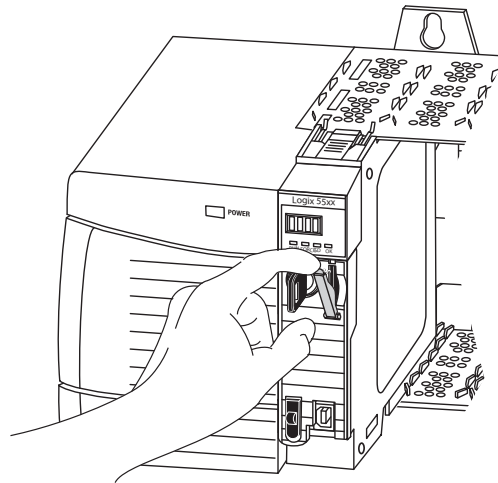
Se si desidera rimuovere la scheda SD dal controllore 1756-L7xS, procedere come segue.

---

**IMPORTANTE** Verificare che l'indicatore di stato della scheda SD sia spento e che la scheda non sia in uso, prima di rimuoverla.

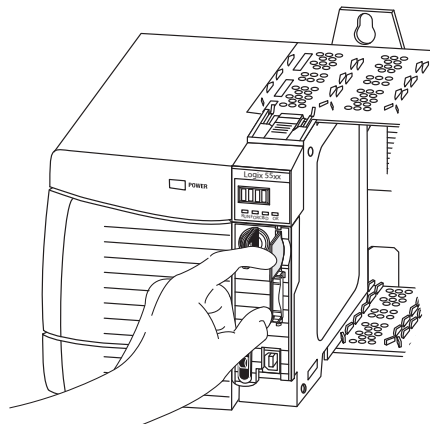
---

1. Portare il selettore a chiave in posizione PROG.
2. Aprire il portellino per accedere alla scheda SD.



32015-M

3. Premere e rilasciare la scheda SD per estrarla.



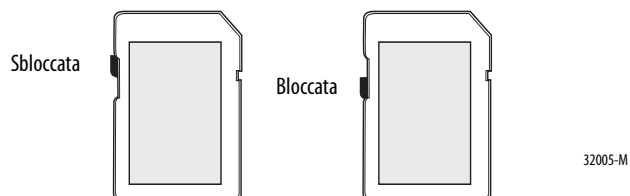
32004-M

4. Rimuovere la scheda SD e chiudere il portellino.

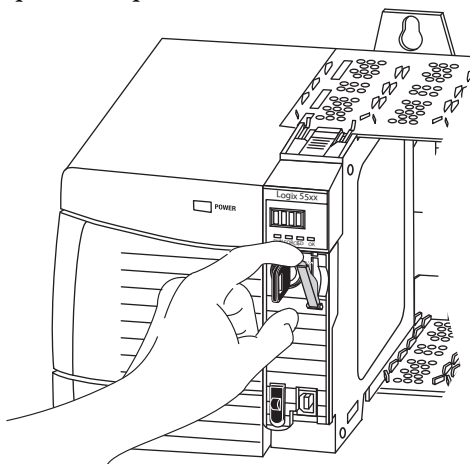
### Installazione della scheda SD

Per installare la scheda SD sui controllori 1756-L7xS, procedere come segue.

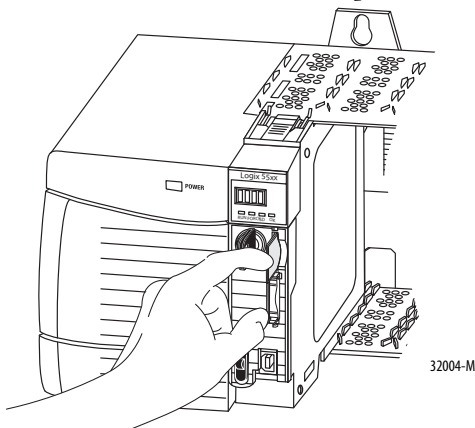
1. Verificare che la scheda SD sia bloccata o sbloccata, a seconda delle preferenze.



2. Aprire il portellino per la scheda SD.

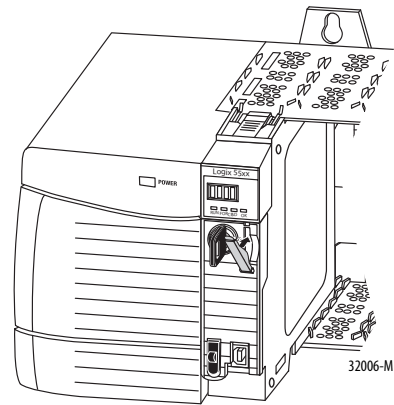


3. Inserire la scheda SD nell'apposito slot.
4. Premere la scheda delicatamente fino a quando scatta in posizione.





5. Chiudere il portellino della scheda SD.



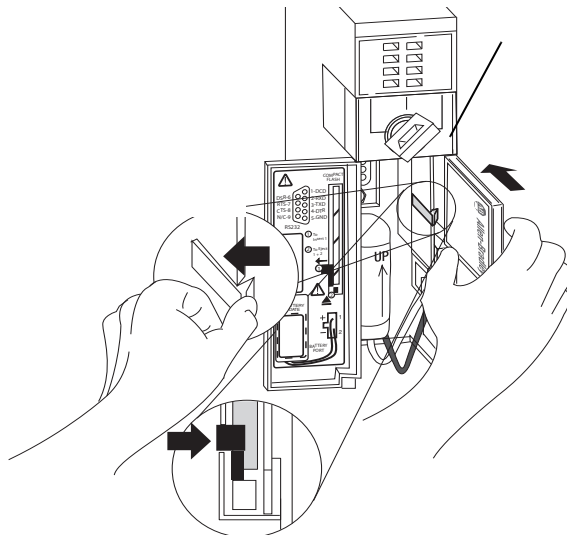
### Scheda CompactFlash (controllori 1756-L6xS)

I controllori 1756-L6xS vengono forniti senza scheda CompactFlash preinstallata.

#### *Inserimento di una scheda CF*

Per inserire la scheda di memoria, procedere come segue.

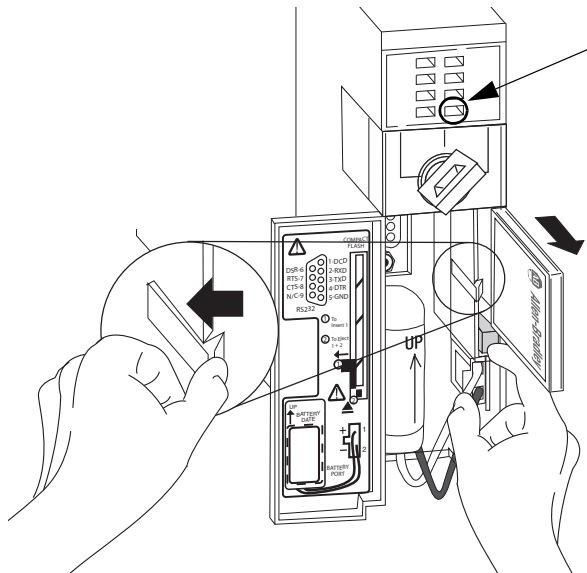
1. Portare il selettore a chiave in posizione PROG.
2. Aprire lo sportellino del controllore.
3. Spingere il dispositivo di chiusura verso sinistra.
4. Inserire la scheda di memoria con il logo A-B rivolto verso sinistra.
5. Sbloccare il dispositivo di chiusura ed assicurarsi che scorra sopra la scheda di memoria.



### Rimozione di una scheda CF

Per rimuovere la scheda di memoria, procedere come segue.

1. Se l'indicatore di stato OK lampeggia in verde, attendere che la luce diventi verde fissa.



2. Aprire lo sportellino del controllore.
3. Spingere e tenere premuto il dispositivo di chiusura verso sinistra.
4. Premere il pulsante di espulsione e rimuovere la scheda.
5. Sbloccare il dispositivo di chiusura.

## Connessioni di comunicazione

I controllori 1756-L7xS sono dotati di una porta USB. Vedere [Collegamento alla porta USB del controllore 1756-L7xS](#).

I controllori 1756-L6xS sono dotati di una porta seriale. Vedere [Collegamento alla porta seriale del controllore 1756-L6xS a pagina 37](#).

### Collegamento alla porta USB del controllore 1756-L7xS

Il controllore ha una porta USB con una presa di Tipo B. La porta è compatibile USB 2.0 e funziona a 12 Mbps.

Per usare la porta USB del controllore, è necessario avere installato sul computer il software RSLinx, versione 2.59 o successiva. Per collegare il computer alla porta USB, usare un cavo USB. Con questo collegamento, è possibile aggiornare il firmware e scaricare i programmi nel controllore direttamente dal computer.

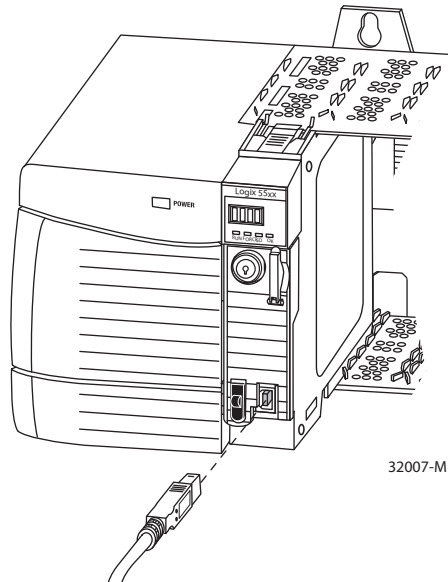


**ATTENZIONE:** La porta USB è adatta solo per la programmazione locale temporanea e non è previsto che sia collegata in modo permanente. Il cavo USB non deve superare i 3,0 m e non deve contenere hub.



**AVVISO:** Non utilizzare la porta USB in aree pericolose.

**Figura 3 – Connessione USB**



Per configurare il software RSLinx in modo da usare una porta USB, è necessario configurare prima un driver USB. Per configurare un driver USB, procedere come segue.

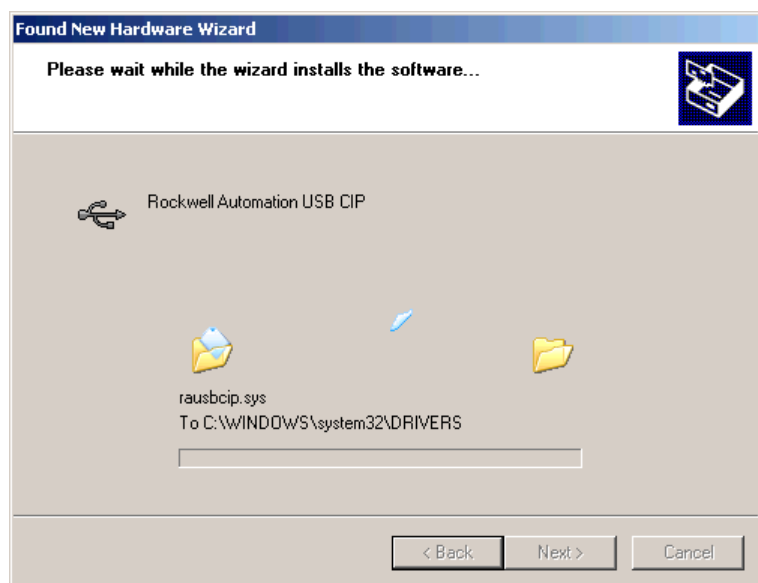
1. Collegare controllore e computer con un cavo USB.
2. Nella finestra di dialogo Found New Hardware Wizard, fare clic su una delle opzioni di connessione a Windows Update e fare clic su Next.



**SUGGERIMENTO** Se il software per il driver USB non si trova e l'installazione viene annullata, verificare di aver installato il software RSLinx Classic, versione 2.59 o successiva.

3. Fare clic su Install the software automatically (raccomandato) e fare clic su Next.

Il software è installato.

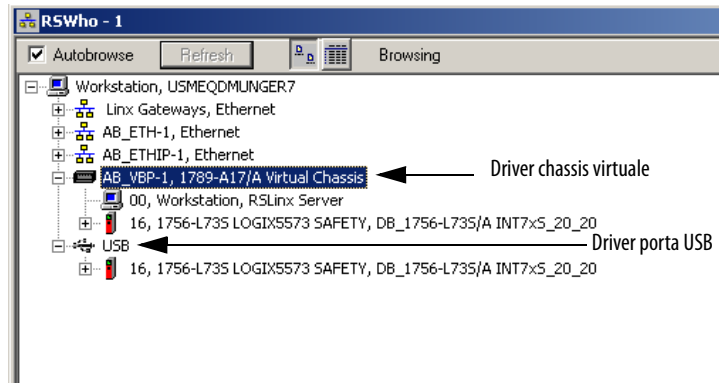


4. Fare clic su Finish per configurare il driver USB.

5. Per selezionare il controllore nel software RSLinx, fare clic su RSWho



Nell'organizer di RSLinx Workstation, il controllore viene visualizzato sotto due driver differenti, uno chassis virtuale e la porta USB. Per selezionare il controllore, è possibile usarli entrambi.



### Collegamento alla porta seriale del controllore 1756-L6xS

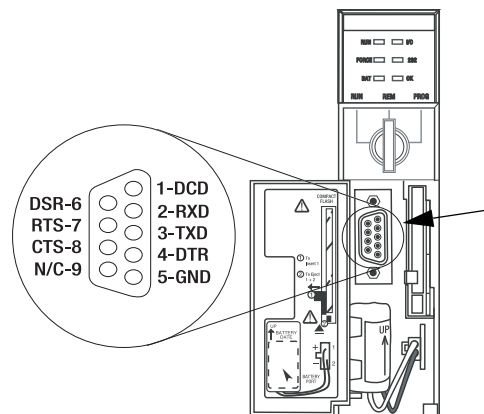


**AVVISO:** Se si collega o scollega il cavo seriale con l'alimentazione del presente modulo o del dispositivo seriale all'altra estremità del cavo attiva, si può generare un arco elettrico, che può causare esplosioni in installazioni che si trovano in aree pericolose.

Assicurarsi di togliere l'alimentazione o accertarsi che l'area sia non pericolosa prima di procedere.

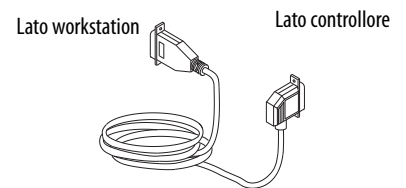
Per la comunicazione RS-232 utilizzare la porta seriale sul controllore 1756-L6xS.

**Figura 4 – Porta seriale**



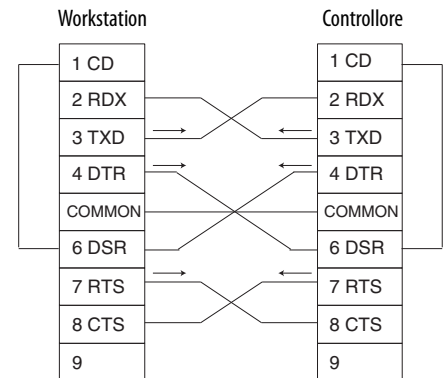
Per collegare una workstation alla porta seriale, utilizzare uno dei seguenti cavi:

- Cavo seriale 1756-CP3
- Cavo 1747-CP3 della famiglia di prodotti SLC (se si usa questo cavo, lo sportellino del controllore potrebbe non chiudersi.)



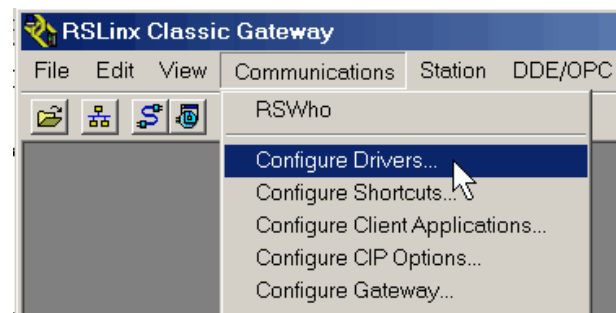
Se ci si costruisce un cavo seriale, adottare i seguenti criteri:

- Limitare la lunghezza a 15,2 m.
- Collegare i connettori come mostrato.
- Collegare lo schermo ad entrambi i connettori.

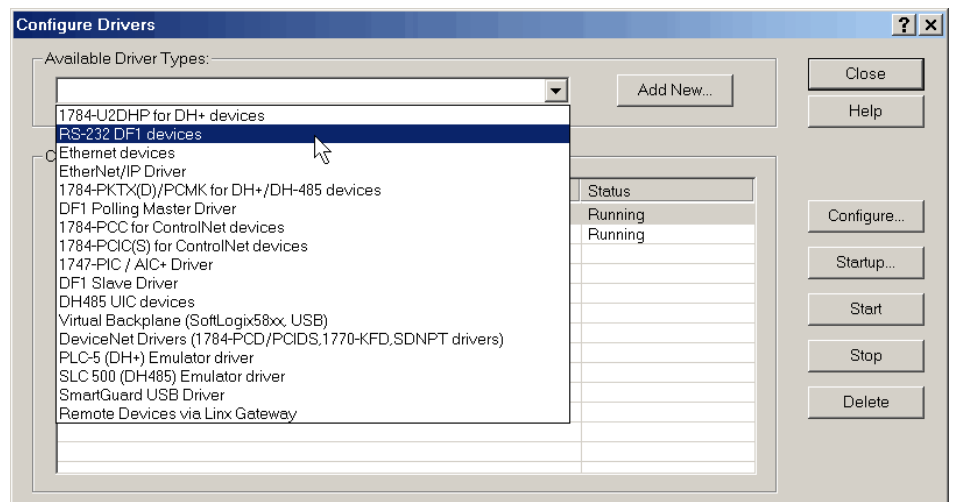


Attenersi alla seguente procedura se per la configurazione del driver del dispositivo RS-232 DF1 per la comunicazione seriale si utilizza il software RSLinx.

1. Nel software RSLinx, dal menu Communications scegliere Configure Drivers.

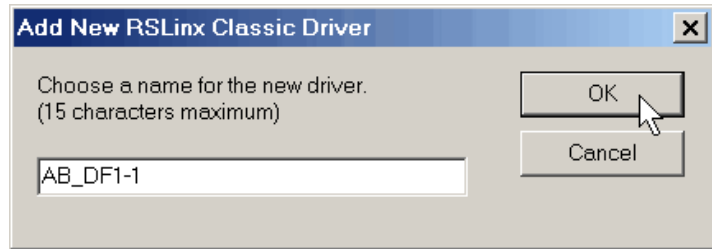


Viene visualizzata la finestra di dialogo Configure Drivers.

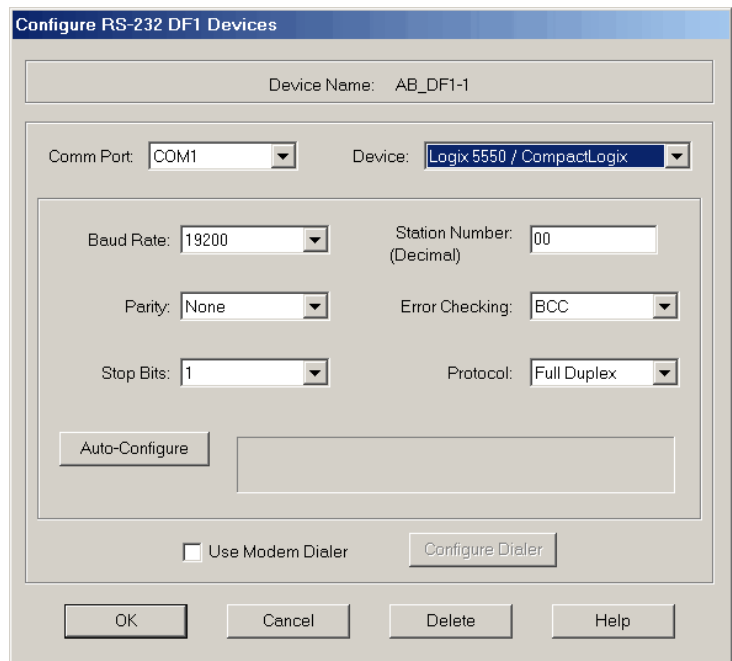


2. Dal menu a discesa Available Driver Types, scegliere il driver del dispositivo RS-232 DF1.
3. Fare clic su Add New.

Viene visualizzata la finestra di dialogo Add New RSLinx Driver.



4. Digitare il nome del driver e fare clic su OK.
5. Specificare le impostazioni della porta seriale.
  - a. Dal menu a discesa Comm Port scegliere la porta seriale della workstation alla quale è connesso il cavo.
  - b. Dal menu a discesa Device, scegliere Logix 5550/CompactLogix.
  - c. Fare clic su Auto-Configure.



6. Se la configurazione automatica viene eseguita correttamente, fare clic su OK.

Se la configurazione automatica non viene eseguita correttamente, verificare che sia stata selezionata la porta di comunicazione corretta.

7. Fare clic su Close.

## Aggiornamento del controllore

I controllori vengono forniti senza firmware. Il firmware del controllore viene fornito insieme al software di programmazione RSLogix 5000. Inoltre, il firmware del controllore può essere scaricato dal sito web dedicato all'assistenza tecnica di Rockwell Automation, all'indirizzo:

<http://www.rockwellautomation.com/support/>.

Per l'aggiornamento del firmware è possibile utilizzare il software ControlFLASH™, fornito insieme al software RSLogix 5000, oppure la funzione AutoFlash del software RSLogix 5000.

### Utilizzo del software ControlFLASH per l'aggiornamento del firmware

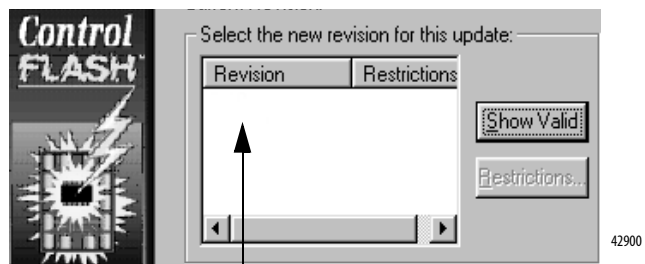
Con il software ControlFLASH, versione 8 o successive (software RSLogix 5000, versione 18 o successive), il coprocessore di sicurezza viene aggiornato automaticamente quando si aggiorna il controllore primario.

---

**IMPORTANTE** Sui controllori 1756-L7xS, se la scheda SD è bloccata e l'opzione Load Image del progetto memorizzato è impostata su On Power Up, il firmware del controllore non viene aggiornato con questa procedura. Vengono invece caricati i progetti ed il firmware memorizzati precedentemente.

---

1. Verificare che la connessione di rete sia effettiva e corretta e che, nel software RSLinx, sia configurato il driver di rete.
2. Aprire il software ControlFLASH.
3. Selezionare Next.
4. Selezionare il numero di catalogo del controllore e fare clic su Next.
5. Espandere la rete fino a visualizzare il controllore.
6. Selezionare il controllore e fare clic su Next.



7. Scegliere la versione a cui si vuole aggiornare il controllore e fare clic su Next.
8. Per avviare l'aggiornamento del controllore, fare clic su Finish e poi su Yes. Dopo l'aggiornamento del controllore, la finestra di dialogo di stato visualizza il messaggio "Update complete".

---

**IMPORTANTE** Lasciare terminare completamente l'aggiornamento del firmware prima di spegnere e riaccendere o interrompere in altro modo l'aggiornamento.

---

**SUGGERIMENTO** Se l'aggiornamento con ControlFLASH del controllore viene interrotto, il controllore 1756-L7xS torna al firmware di avvio, ovvero alla versione firmware 1.xxx.



9. Fare clic su OK.
10. Chiudere il software ControlFLASH.

### Utilizzo di AutoFlash per l'aggiornamento del firmware

Per aggiornare il firmware del controllore con la funzione AutoFlash del software RSLogix 5000, procedere come segue.

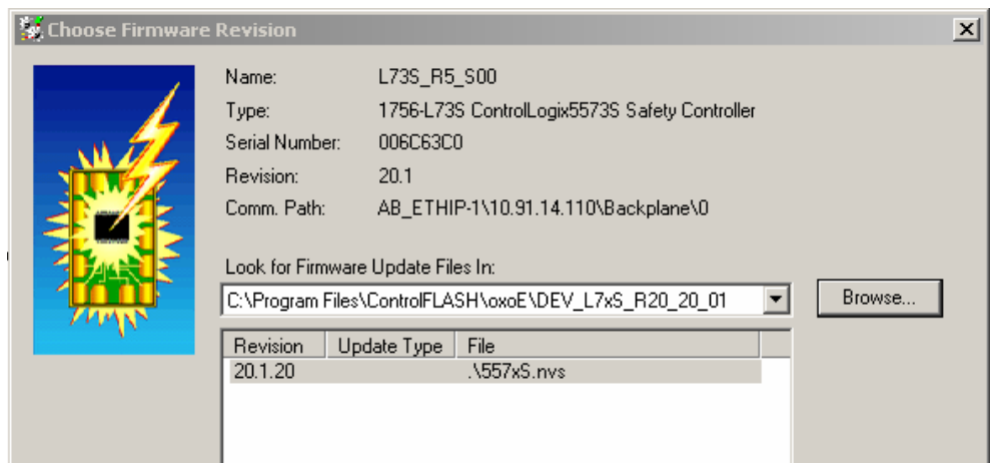
1. Verificare che la connessione di rete sia effettiva e corretta e che, nel software RSLinx, sia configurato il driver di rete.
2. Utilizzare il software di programmazione RSLogix 5000 per creare un progetto del controllore nella versione richiesta.



3. Fare clic su RSWho per specificare il percorso del controllore.



4. Selezionare il controllore e fare clic su Update Firmware.
5. Selezionare la versione del firmware a cui aggiornare.



6. Fare clic su Update.
7. Fare clic su Yes.

Lasciar completare l'aggiornamento firmware senza interruzioni. Quando l'aggiornamento del firmware è terminato, si apre la finestra di dialogo Who Active. È possibile eseguire altre operazioni con il software RSLogix 5000.

## Scelta della modalità operativa del controllore

Fare riferimento a questa tabella per determinare la modalità operativa del controllore.

**Tabella 9 – Modalità operative del controllore**

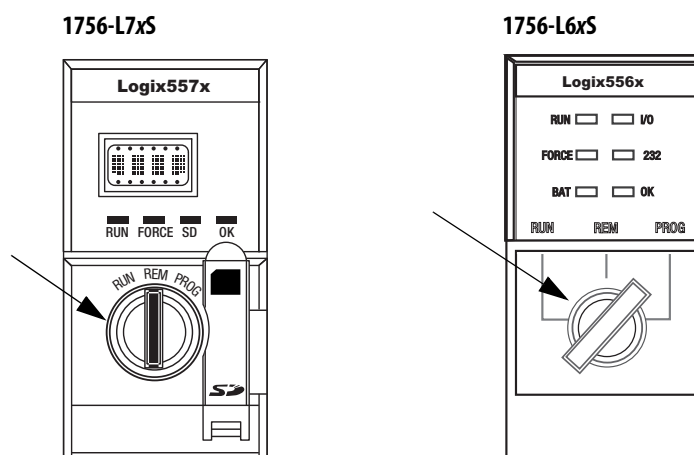
Se si desidera	Selezionare una di queste modalità				
	Esecuzione	Mod. remota			Programmazione
		Esecuzione	Test	Programmazione	
Commutare le uscite sullo stato comandato dalla logica del progetto	X	X			
Commutare le uscite sullo stato configurato per la modalità Programmazione			X	X	X
Eseguire (scandire) task	X	X	X		
Cambiare la modalità del controllore attraverso il software		X	X	X	
Scaricare un progetto		X	X	X	X
Schedulare una rete ControlNet				X	X
Modificare il progetto online		X	X	X	X
Inviare messaggi	X	X	X		
Inviare e ricevere dati in risposta ad un messaggio da un altro controllore	X	X	X	X	X
Produrre e consumare tag	X	X	X	X	X

## Utilizzo del selettore a chiave per cambiare la modalità operativa

Il selettore a chiave sulla parte frontale del controllore può essere utilizzato per portare il controllore in una delle seguenti modalità:

- Programmazione (PROG)
- Controllo remoto (REM)
- Esecuzione (RUN)

**Figura 5 – Selettore a chiave del controllore**



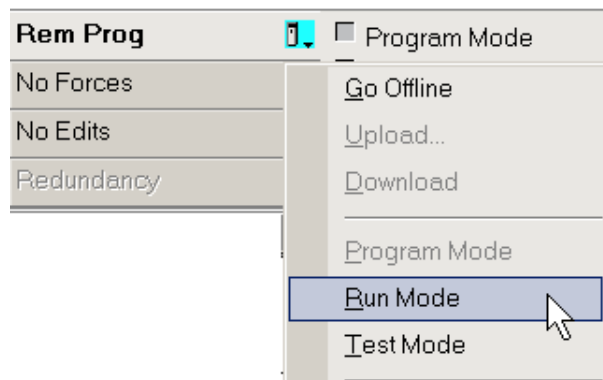
## Utilizzo del software RSLogix 5000 per cambiare modalità operativa

In base alla modalità specificata per il controllore con il selettore a chiave, è possibile cambiare la modalità operativa del controllore utilizzando il software RSLogix 5000.

Con il controllore online ed il selettore a chiave impostato su controllo remoto (REM o posizione centrale), è possibile utilizzare il menu Controller Status nell'angolo superiore sinistro della finestra del software RSLogix 5000 per specificare le seguenti modalità operative:

- Programmazione remota
- Esecuzione remota
- Test remoto

**Figura 6 – Modalità operativa tramite il software RSLogix 5000**



**SUGGERIMENTO** In questo esempio, il selettore a chiave del controllore è impostato su REM (controllo remoto). Se il selettore a chiave del controllore fosse impostato su RUN o PROG, le opzioni del menu sarebbero diverse.

## Disinstallazione del modulo di alimentazione (ESM)

I controllori 1756-L7xS vengono forniti con un modulo ESM preinstallato.

Controllore	Num. di Cat. ESM installato
1756-L7xS – controllore	1756-ESMCAP
1756-L7xSXT – controllore per temperature estreme	1756-ESMCAPXT
1756-L7SP – coprocessore di sicurezza	1756-SPESMNSE
1756-L7SPXT – coprocessore di sicurezza per temperature estreme	1756-SPESMNSEXT

Prima di rimuovere il modulo ESM, considerare quanto segue:

- Anche quando i controllori 1756-L7xS non sono più in tensione, per interruzione dell'alimentazione allo chassis o perché rimossi da uno chassis alimentato, non rimuovere immediatamente il modulo ESM.

Prima di rimuovere il modulo ESM, attendere che l'indicatore di stato OK del controllore passi da verde a rosso fisso e poi si spenga.

- Usare il modulo 1756-ESMNSE se l'applicazione richiede che il modulo ESM installato riduca l'energia residua a 40 µJoule o meno prima di installarlo o rimuoverlo dall'applicazione.
- Una volta installato, il modulo 1756-ESMNRM non può essere rimosso dal controllore 1756-L7xS.

---

**IMPORTANTE** Prima di rimuovere un modulo ESM, apportare al programma le regolazioni necessarie in considerazione delle potenziali modifiche all'attributo WallClockTime.

---

Per rimuovere un modulo 1756-ESMCAP(XT), 1756-ESMNSE(XT) o 1756-SPESMNSE(XT), procedere come segue.



**AVVISO:** Se l'applicazione richiede che il modulo ESM riduca la sua energia residua a 40 µJoule o meno prima di inserirlo o rimuoverlo dal sistema, usare solo il modulo 1756-ESMNSE(XT) per il controllore primario ed il modulo 1756-SPESMNSE(XT) per il coprocessore di sicurezza. In tal caso, prima di rimuovere il modulo ESM, procedere come segue.

- Interrompere l'alimentazione dello chassis.  
Dopo l'interruzione dell'alimentazione, l'indicatore di stato OK del controllore passa da verde a rosso fisso e poi si spegne.
  - Attendere **almeno 20 minuti** perché l'energia residua scenda a 40 µJoule o meno prima di rimuovere il modulo ESM.  
Non è prevista una segnalazione visiva allo scadere dei 20 minuti. **È necessario tenerne conto personalmente.**
- 



**AVVISO:** Se si inserisce o si rimuove il modulo ESM con l'alimentazione backplane inserita, potrebbe verificarsi un arco elettrico, che può causare esplosioni in installazioni che si trovano in aree pericolose.

Prima di procedere, assicurarsi di aver tolto alimentazione o che l'area non sia pericolosa. Il ripetuto verificarsi di archi elettrici provoca l'eccessiva usura dei contatti, sia del modulo sia del connettore corrispondente.

---

**1.** Estrarre la chiave dal selettore a chiave.

---

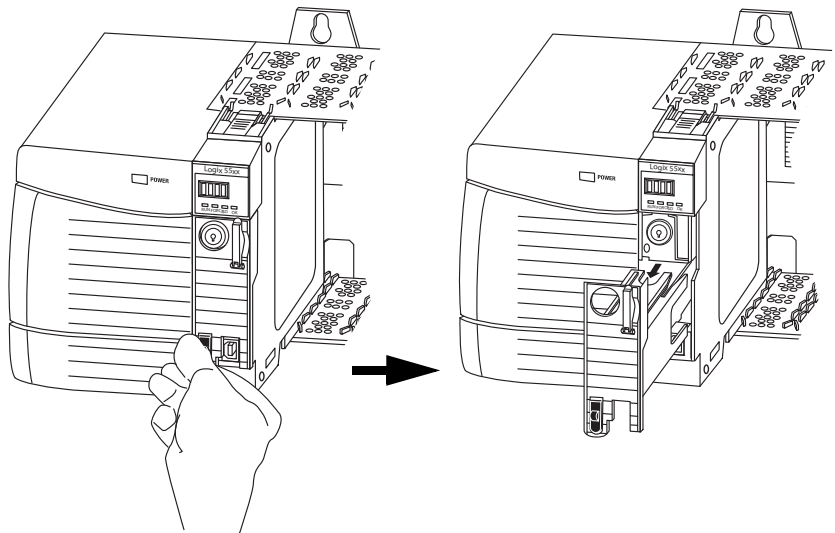
**IMPORTANTE** Il passo successivo dipende da quale delle seguenti condizioni si applica:

- Se il modulo ESM viene rimosso da un controllore 1756-L7xS(XT) in tensione, andare al [passo 2](#).
- Se il modulo ESM viene rimosso da un controllore 1756-L7xS(XT) non in tensione, per interruzione dell'alimentazione dello chassis o per rimozione del controllore da uno chassis alimentato, **non rimuovere** immediatamente il modulo ESM.

Prima di rimuovere il modulo ESM, attendere che l'indicatore di stato OK del controllore passi da verde a rosso fisso e poi si spenga.

Quando l'indicatore di stato OK si spegne, andare al [passo 2](#).

---

**2.** Premere il pulsante di sblocco con il pollice ed estrarre il modulo ESM dal controllore.

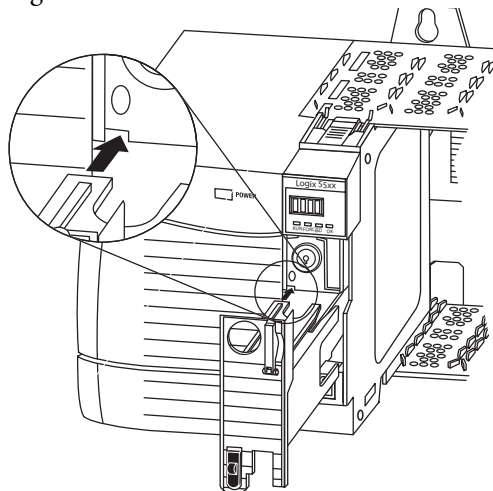
## Installazione di un modulo di alimentazione (ESM)

Tabella 10 – Moduli di alimentazione compatibili

Num. di Cat.	ESM compatibili
1756-L7xS	1756-ESMCAP, 1756-ESMNSE, 1756-ESMNRM
1756-L7xSXT	1756-ESMCAPXT, 1756-ESMNSEXT, 1756-ESMNRMXT
1756-L7SP	1756-SPESMNSE, 1756-SPESMNRM
1756-L7SPXT	1756-SPESMNSEXT, 1756-SPESMNRMXT

Per installare un modulo ESM, procedere come segue. Attenersi alla stessa procedura per il coprocessore di sicurezza.

1. Allineare gli slot ad incastro del modulo ESM e del controllore.



2. Far scorrere il modulo ESM nello chassis fino a quando scatta in posizione.



**ATTENZIONE:** Per evitare di danneggiare il prodotto quando si inserisce il modulo ESM, allinearne nella guida e spingerlo delicatamente fino a quando scatta in posizione.

Dopo l'installazione, il modulo ESM inizia a caricarsi. Lo stato di carica è indicato da uno dei seguenti messaggi di stato:

- ESM Charging
- CHRГ

Dopo aver installato il modulo ESM, possono trascorrere fino a 15 secondi prima di visualizzare i messaggi sullo stato di carica.

**IMPORTANTE** Prima di interrompere l'alimentazione del controllore, lasciar completare l'operazione di carica del modulo ESM. Per verificare che il modulo ESM sia completamente carico, controllare che sul display di stato non compaiano più i messaggi CHRГ o ESM Charging.

**SUGGERIMENTO** Dopo aver installato un modulo ESM, controllare gli attributi dell'oggetto WallClockTime per verificare che l'ora del controllore sia corretta.

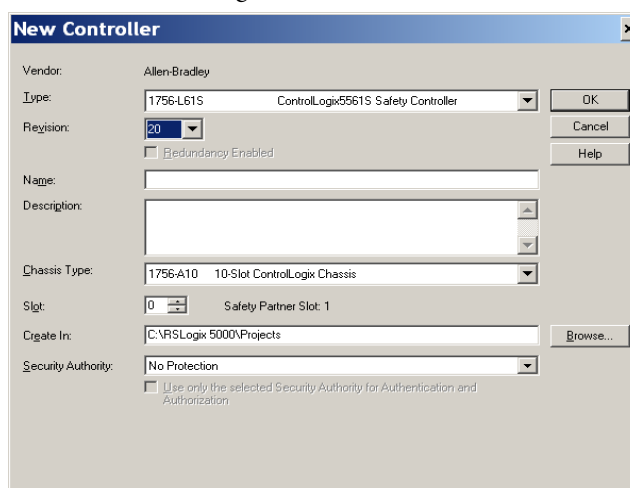
## Configurazione del controllore

Argomento	Pagina
Creazione di un progetto del controllore	47
Impostazione delle password per il blocco/sblocco di sicurezza	49
Gestione della sostituzione dei moduli I/O	51
Abilitazione della sincronizzazione temporale	51
Configurazione di un controllore di sicurezza peer	52

### Creazione di un progetto del controllore

Per configurare e programmare un controllore si utilizza il software RSLogix 5000 per creare e gestire un progetto per il controllore.

1. Creare un progetto nel software RSLogix 5000 facendo clic sul pulsante New nella barra degli strumenti principale.
2. Dal menu a tendina Type, selezionare un controllore GuardLogix:
  - 1756-L61S ControlLogix5561S Controller
  - 1756-L62S ControlLogix5562S Controller
  - 1756-L63S ControlLogix5563S Controller
  - 1756-L71S ControlLogix5571S Controller
  - 1756-L72S ControlLogix5572S Controller
  - 1756-L73S ControlLogix5573S Controller



3. Specificare la versione principale del firmware per il controllore.
4. Digitare un nome per il controllore.

Quando si crea un progetto, il nome del progetto corrisponde al nome del controllore. Tuttavia, è possibile rinominare il progetto o il controllore.

5. Selezionare la dimensione dello chassis.
6. Immettere il numero di slot del controllore.

Nella finestra di dialogo New Controller viene visualizzata la posizione dello slot del coprocessore di sicurezza in base al numero di slot immesso per il controllore primario.

Se il numero di slot selezionato per il controllore primario non permette il posizionamento del coprocessore di sicurezza immediatamente a destra del controllore primario, verrà richiesto di immettere nuovamente un numero di slot valido.

7. Specificare la cartella in cui memorizzare il progetto del controllore di sicurezza.
8. Nel caso di RSLogix 5000, versione 20 o successive, scegliere un'opzione di Security Authority.

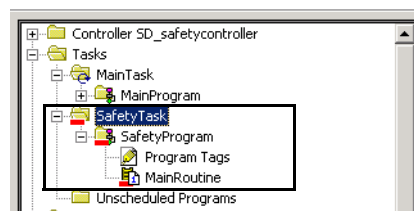
Per informazioni dettagliate sulla sicurezza, consultare il manuale di programmazione Protezione dei controllori Logix5000, pubblicazione [1756-PM016](#).

9. Fare clic su OK.

Il software RSLogix 5000 crea automaticamente un task ed un programma di sicurezza.

All'interno del programma di sicurezza viene inoltre creata una routine di sicurezza principale della logica ladder denominata MainRoutine.

**Figura 7 – Task di sicurezza nell'organizer del controllore**



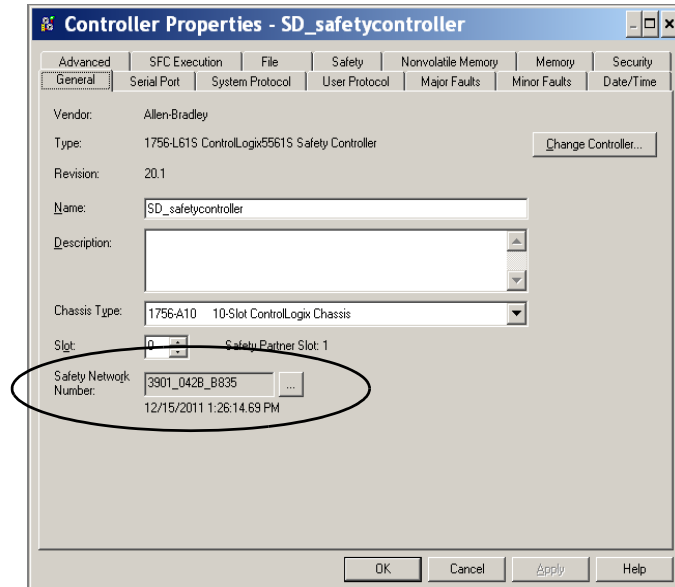
Una barra rossa sotto l'icona consente di distinguere i programmi e le routine di sicurezza dai componenti del progetto standard dell'organizer del controllore RSLogix 5000.

Quando viene creato un nuovo progetto di sicurezza, il software RSLogix 5000 genera automaticamente anche un numero rete di sicurezza (SNN, Safety Network Number) basato sul tempo.

Tale valore SNN definisce il backplane dello chassis locale come sottorete di sicurezza. Esso può essere visualizzato e modificato mediante la scheda General nella finestra di dialogo Controller Properties.

Per la maggior parte delle applicazioni, questo numero di rete di sicurezza (SNN) automatico basato sul tempo è sufficiente. Tuttavia, in alcuni casi può risultare utile l'inserimento di un SNN specifico.



**Figura 8 – Safety Network Number**

**SUGGERIMENTO** Per cambiare da controllore standard a controllore di sicurezza e viceversa, è possibile utilizzare la finestra di dialogo Controller Properties facendo clic su Change Controller. Questa azione ha implicazioni sia per i progetti standard che per quelli di sicurezza.

Per ulteriori informazioni sulle conseguenze del cambiamento dei controllori, vedere [Appendice C, Modifica del tipo di controllore nei progetti RSLogix 5000](#).

**Tabella 11 – Ulteriori riferimenti**

Riferimento	Descrizione
<a href="#">Capitolo 6, Sviluppo di applicazioni di sicurezza.</a>	Contiene ulteriori informazioni su task, programmi e routine di sicurezza
<a href="#">Capitolo 4, Comunicazione sulle reti</a>	Fornisce ulteriori informazioni sulla gestione del numero SNN

## Impostazione delle password per il blocco/sblocco di sicurezza

Il blocco di sicurezza del controllore contribuisce a proteggere i componenti di controllo di sicurezza dalle modifiche. La funzione di blocco può essere utilizzata solo per i componenti di sicurezza, ad esempio, task, programmi, routine e tag, ma non può essere utilizzata per i componenti standard. Il blocco di sicurezza per il progetto del controllore può essere attivato o disattivato in linea o offline.

La funzione di blocco e sblocco di sicurezza utilizza due password separate. Le password sono opzionali.

Per impostare le password, procedere come indicato di seguito.

1. Scegliere Tools > Safety > Change Password.
2. Dal menu a tendina What Password, selezionare Safety Lock oppure Safety Unlock.



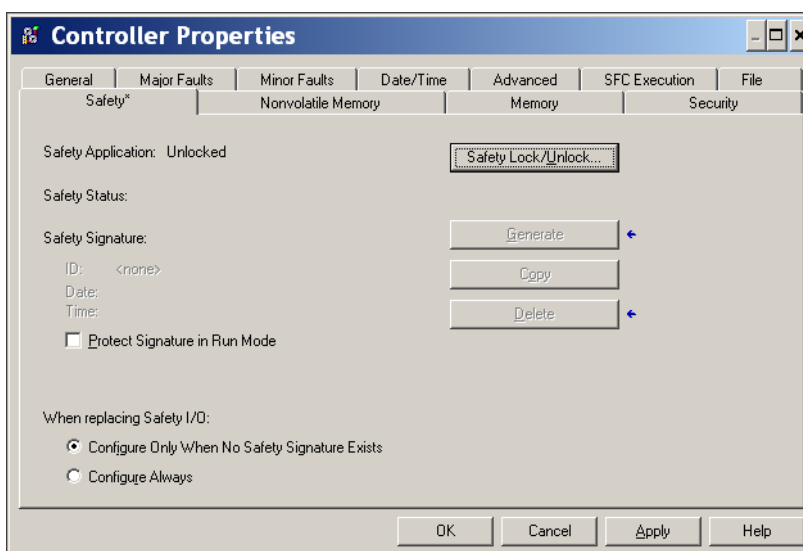
3. Inserire la vecchia password, se esistente.
4. Inserire e confermare la nuova password.
5. Fare clic su OK.

Le password possono avere una lunghezza compresa tra 1 e 40 caratteri e non vi è distinzione tra maiuscole e minuscole. È possibile utilizzare lettere, valori numerici ed i seguenti simboli:

‘ ~ ! @ # \$ % ^ & \* ( ) \_ + , - = { } | [ ] \ ; : ; ? / .

## Protezione della firma del task di sicurezza in modalità Esecuzione

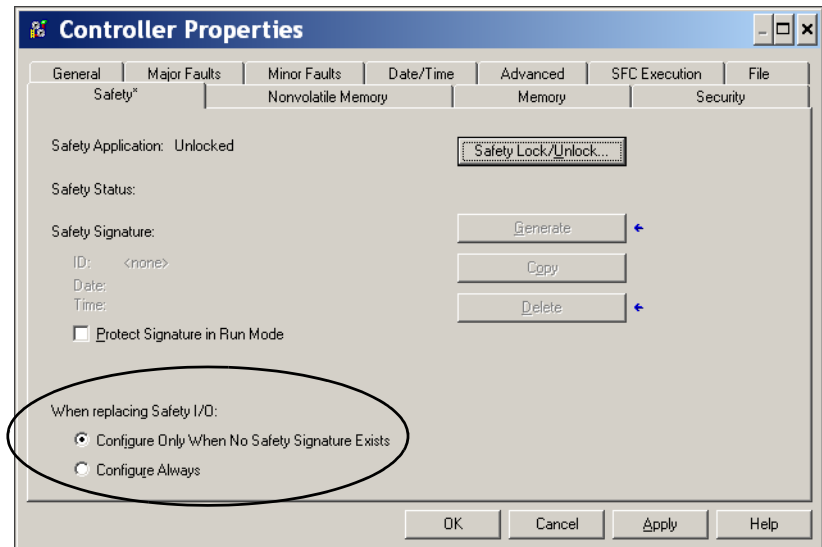
È possibile prevenire la creazione o la cancellazione della firma del task di sicurezza mentre il controllore è in modalità Esecuzione o Esecuzione remota, a prescindere dal fatto che l'applicazione di sicurezza sia bloccata o sbloccata, selezionando Protect Signature in Run Mode sulla scheda Safety della finestra di dialogo Controller Properties.



## Gestione della sostituzione dei moduli I/O

La scheda Safety della finestra di dialogo Controller Properties consente di definire la modalità di gestione della sostituzione di un modulo I/O nel sistema da parte del controllore. Questa opzione consente di determinare se il controllore imposta il numero di rete di sicurezza (SNN, Safety Network Number) di un modulo I/O con il quale ha una connessione e per il quale dispone di dati di configurazione quando<sup>(1)</sup> è presente una firma del task di sicurezza.

**Figura 9 – Opzioni per la sostituzione dei moduli I/O**



**ATTENZIONE:** Abilitare l'opzione Configure Always solo se l'intero sistema di controllo CIP Safety inostradabile non è utilizzato per mantenere il livello SIL 3 durante la sostituzione ed il collaudo funzionale di un modulo.

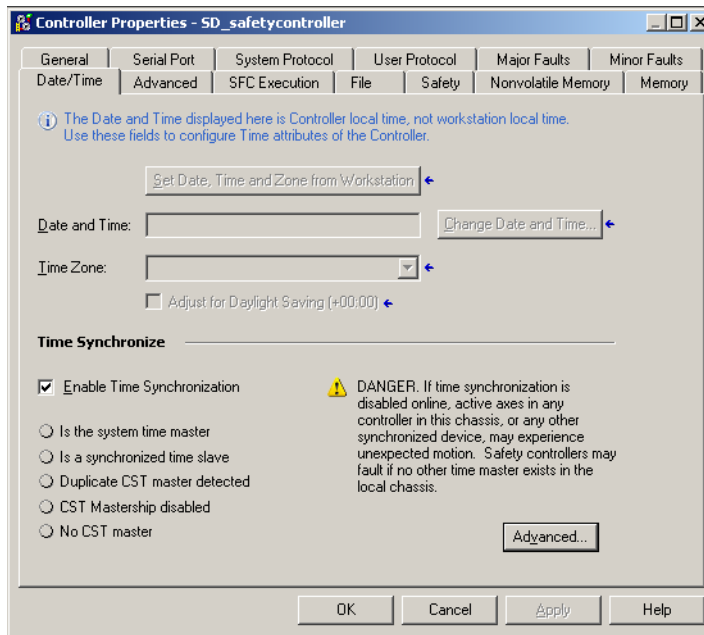
Per ulteriori informazioni, vedere il [Capitolo 5, Aggiunta, configurazione, monitoraggio e sostituzione di I/O CIP Safety](#).

## Abilitazione della sincronizzazione temporale

In un sistema del controllore GuardLogix, occorre designare un dispositivo dello chassis locale come master CST (tempo di sistema coordinato). Affinché il controllore possa diventare il master CST, è necessario abilitare Time Synchronization nella scheda Date/Time della finestra di dialogo Controller Properties. La sincronizzazione temporale è un meccanismo standard per la sincronizzazione degli orologi in una rete di dispositivi distribuiti.

(1) La firma del task di sicurezza è un numero utilizzato per identificare in modo univoco la logica, i dati e la configurazione di ciascun progetto, proteggendo pertanto il livello di integrità di sicurezza del sistema (SIL). Per ulteriori informazioni vedere [Firma del task di sicurezza a pagina 16](#) e [Generazione di una firma del task di sicurezza a pagina 106](#).

Figura 10 – Scheda Date/Time



Per ulteriori informazioni sulla sincronizzazione temporale, consultare la pubblicazione Integrated Architecture™ and CIP Sync Configuration Application Solution [IA-AT003](#).

### Configurazione di un controllore di sicurezza peer

Per consentire il consumo di tag standard o di sicurezza, è possibile aggiungere un controllore di sicurezza peer alla cartella di configurazione I/O del progetto di sicurezza. Per condividere i dati di sicurezza tra i controllori peer, è possibile produrre e consumare tag di sicurezza dell'ambito del controllore.

Per i dettagli sulla configurazione dei controllori di sicurezza peer e su produzione/consumo dei tag di sicurezza, vedere [Tag di sicurezza prodotti/consumati a pagina 97](#).

## Comunicazione sulle reti

Argomento	Pagina
Rete di sicurezza	53
Comunicazione EtherNet/IP	59
Comunicazione ControlNet	63
Comunicazione DeviceNet	65
Comunicazione seriale	67
Ulteriori riferimenti	68

### Rete di sicurezza

Il protocollo CIP Safety è un protocollo di sicurezza da nodo finale a nodo finale che consente l'instradamento di messaggi CIP Safety da e verso dispositivi CIP Safety tramite ponte, switch e router.

Per mantenere un elevato livello di integrità quando si esegue l'instradamento attraverso bridge, switch o router standard, ciascun nodo finale all'interno di un sistema di controllo CIP Safety instradabile deve avere un riferimento univoco. Tale riferimento univoco è una combinazione del numero di sicurezza della rete (SNN) e dell'indirizzo di nodo del dispositivo di rete.

### Gestione del numero di rete di sicurezza (SNN)

Il valore SNN assegnato ai dispositivi di sicurezza su un segmento di rete deve essere univoco. Accertarsi che ai seguenti elementi sia assegnato un valore SNN univoco:

- Ogni rete CIP Safety che contiene dispositivi di sicurezza
- Ogni chassis che contiene uno o più controllori GuardLogix

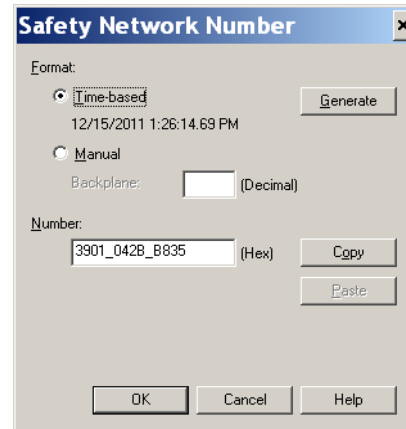
**SUGGERIMENTO** Alle sottoreti CIP Safety o agli chassis ControlBus che contengono più di un dispositivo di sicurezza è possibile assegnare più numeri rete di sicurezza. **Tuttavia, per semplicità, si consiglia di utilizzare un unico valore SNN univoco per ciascuna sottorete CIP Safety.**

Il valore SNN può essere assegnato dal software (basato sul tempo) oppure dall'utente (manuale). I due formati del valore SNN sono descritti nelle seguenti sezioni.

### Numero rete di sicurezza basato sul tempo

Se viene selezionato il formato basato sul tempo, il valore SNN generato rappresenta la data e l'ora in cui il numero è stato generato, in base al personal computer in cui è eseguito il software di configurazione.

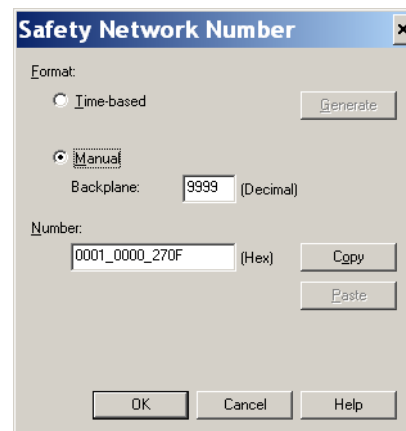
**Figura 11 – Formato basato sul tempo**



### Numero rete di sicurezza manuale

Se viene selezionato il formato manuale, il numero SNN rappresenta i valori decimali immessi compresi tra 1 e 9999.

**Figura 12 – Immissione manuale**



## Assegnazione del Numero di rete di sicurezza (SNN)

È possibile consentire a RSLogix 5000 di assegnare automaticamente un valore SNN, oppure assegnarlo manualmente.

### *Assegnazione automatica*

Quando viene creato un controllore o un modulo nuovo, un valore SNN basato sul tempo viene assegnato automaticamente tramite il software di configurazione. Ai nuovi moduli di sicurezza aggiunti successivamente alla stessa rete CIP Safety viene assegnato lo stesso valore SNN definito all'interno dell'indirizzo di livello più basso sulla rete CIP Safety.

### *Assegnazione manuale*

L'opzione manuale è destinata ai sistemi CIP Safety instradabili in cui il numero di sottoreti della rete e di reti di interconnessione è minimo ed in cui gli utenti desiderano gestire ed assegnare i valori SNN in modo logico in base all'applicazione specifica.

Vedere [Modifica del numero di rete di sicurezza \(SNN\) a pagina 55](#).

---

<b>IMPORTANTE</b>	Se si assegna un SNN manualmente, assicurarsi che l'ampliamento del sistema non determini una duplicazione delle combinazioni SNN ed indirizzo di nodo.
-------------------	---

---

### *Automatico e manuale*

Per gli utenti tipici, l'assegnazione automatica di un SNN è sufficiente. Tuttavia, la modifica manuale del valore SNN è necessaria nei seguenti casi:

- Se si utilizzano tag consumati.
- Se il progetto consuma i dati di sicurezza in ingresso da un modulo la cui configurazione appartiene ad un altro dispositivo.
- Se il progetto di sicurezza viene copiato in un'altra installazione hardware all'interno dello stesso sistema CIP Safety instradabile.

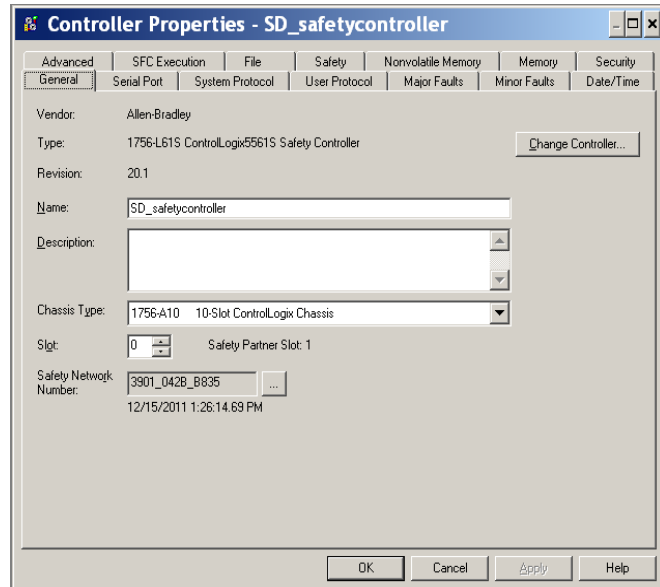
## Modifica del numero di rete di sicurezza (SNN)

Prima di modificare il valore SNN, è necessario eseguire le seguenti operazioni:

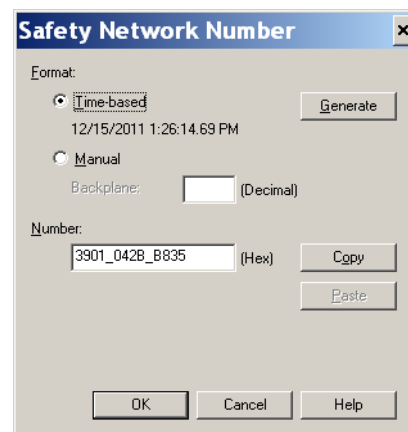
- Sbloccare il progetto, se è in blocco di sicurezza.  
Vedere [Blocco di sicurezza del controllore a pagina 105](#).
- Eliminare la firma del task di sicurezza, se è presente.  
Vedere [Eliminazione della firma del task di sicurezza a pagina 108](#).

*Modifica del numero di rete di sicurezza (SNN) del controllore*

1. Nell'organizer del controllore, fare clic con il pulsante destro del mouse sul controllore e selezionare Properties.
2. Nella scheda General della finestra di dialogo Controller Properties, fare clic su [...] a destra del numero rete di sicurezza per aprire la finestra di dialogo Safety Network Number.



3. Fare clic su Time-based, quindi su Generate.



4. Fare clic su OK.

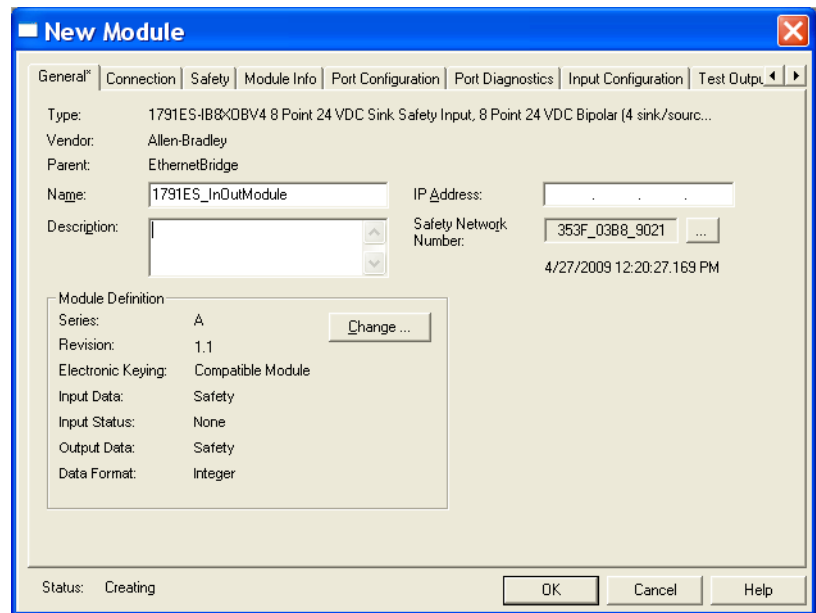
*Modifica del numero di rete di sicurezza (SNN) dei moduli I/O di sicurezza sulla rete CIP Safety*



Questo esempio si riferisce ad una rete EtherNet/IP.

1. Ricercare il primo modulo di comunicazione EtherNet/IP nella struttura di configurazione I/O.
2. Espandere i moduli I/O di sicurezza disponibili attraverso il modulo di comunicazione EtherNet/IP.



- Per visualizzare la scheda General, fare doppio clic sul primo modulo I/O di sicurezza.

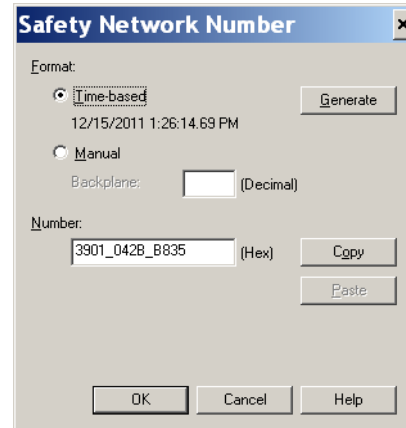



- Per aprire la finestra di dialogo Safety Network Number, fare clic su  a destra del numero rete di sicurezza.
- Per generare un nuovo valore SNN per la rete EtherNet/IP, selezionare Time-based e fare clic su Generate.
- Fare clic su OK.
- Per copiare il nuovo valore SNN negli Appunti di Windows, fare clic su Copy.
- Aprire la scheda General della finestra di dialogo Module Properties del modulo I/O di sicurezza successivo del modulo EtherNet/IP specifico.
- Per aprire la finestra di dialogo Safety Network Number, fare clic su  a destra del numero rete di sicurezza.
- Per incollare il valore SNN della rete EtherNet/IP all'interno del dispositivo, selezionare Time-based e fare clic su Paste.
- Fare clic su OK.
- Ripetere i passi [8...10](#) per i moduli I/O di sicurezza rimanenti nella struttura di tale modulo di comunicazione EtherNet/IP.
- Ripetere i passi [2...10](#) per i moduli di comunicazione di rete rimanenti nella struttura di configurazione I/O.

*Operazione di copia ed incolla di un numero di rete di sicurezza (SNN)*

Se la configurazione del modulo appartiene ad un altro controllore, può essere necessario copiare ed incollare il valore SNN dal proprietario della configurazione nel modulo della struttura di configurazione I/O.

1. Nello strumento di configurazione software del proprietario della configurazione del modulo, aprire la finestra di dialogo Safety Network Number relativa al modulo.



2. Fare clic su Copy.
3. Fare clic sulla scheda General nella finestra di dialogo Module Properties del modulo I/O nella struttura di configurazione I/O del progetto del controllore consumatore.  
Il controllore consumatore non è il proprietario della configurazione.
4. Per aprire la finestra di dialogo Safety Network Number, fare clic su  a destra del numero rete di sicurezza.
5. Fare clic su Paste.
6. Fare clic su OK.

## Comunicazione EtherNet/IP

Per la comunicazione di rete EtherNet/IP in un sistema GuardLogix, è possibile scegliere tra diversi moduli. Per la comunicazione CIP Safety, che comprende il controllo dei moduli I/O di sicurezza, scegliere uno dei moduli elencati nella [Tabella 12](#), eccetto il modulo 1756-EWEB, che non supporta la comunicazione CIP Safety.

La [Tabella 12](#) elenca i moduli e le loro funzioni primarie.

**Tabella 12 – Moduli di comunicazione EtherNet/IP e capacità**

Modulo	Funzioni
1756-ENBT	<ul style="list-style-type: none"> <li>• Collegamento dei controllori ai moduli I/O (necessità di una scheda per gli I/O distribuiti).</li> <li>• Comunicazione con altri dispositivi EtherNet/IP (messaggi).</li> <li>• Percorso per la condivisione dei dati tra controllori Logix5000 (produzione/consumo).</li> <li>• Collegamento in ponte dei nodi EtherNet/IP per instradare i messaggi ai dispositivi su altre reti.</li> </ul>
1756-EN2T	<ul style="list-style-type: none"> <li>• Stesse funzioni del modulo 1756-ENBT ma con capacità doppia per applicazioni più esigenti.</li> <li>• Connessione temporanea per la configurazione tramite porta USB.</li> <li>• Configurazione rapida degli indirizzi IP tramite selettori rotativi.</li> </ul>
1756-EN2F	<ul style="list-style-type: none"> <li>• Stesse funzioni di un modulo 1756-EN2T.</li> <li>• Collegamento dei cavi in fibra tramite un connettore LC.</li> </ul>
1756-EN2TXT	<ul style="list-style-type: none"> <li>• Stesse funzioni di un modulo 1756-EN2T.</li> <li>• Funzionamento in ambienti estremi con temperature comprese nel campo -25...70 °C.</li> </ul>
1756-EN2TR	<ul style="list-style-type: none"> <li>• Stesse funzioni di un modulo 1756-EN2T.</li> <li>• Supporto delle comunicazioni su topologia ad anello per una rete ad anello DLR (Device Level Ring) a prova di singolo guasto.</li> </ul>
1756-EN3TR	<ul style="list-style-type: none"> <li>• Stesse funzioni di un modulo 1756-EN2TR.</li> <li>• Tre porte per connessione DLR.</li> </ul>
1756-EWEB	<ul style="list-style-type: none"> <li>• Pagine web personalizzabili per l'accesso esterno alle informazioni del controllore.</li> <li>• Accesso remoto, tramite browser Internet, ai tag di un controllore ControlLogix locale.</li> <li>• Comunicazione con altri dispositivi EtherNet/IP (messaggi).</li> <li>• Collegamento in ponte dei nodi EtherNet/IP per instradare i messaggi ai dispositivi su altre reti.</li> <li>• Supporto di dispositivi Ethernet non basati su EtherNet/IP con interfaccia socket.</li> </ul> <p>Questo modulo non supporta tag I/O o tag prodotti/consumati né la comunicazione CIP Safety.</p>

I moduli di comunicazione EtherNet/IP dispongono delle seguenti funzioni:

- Supporto messaggistica, tag prodotti/consumati, interfaccia operatore e I/O distribuiti
- Messaggi incapsulati all'interno del protocollo TCP/UDP/IP standard
- Un livello di applicazione comune con le reti ControlNet e DeviceNet
- Interfaccia mediante cavo a doppino intrecciato, non schermato, RJ45, categoria 5
- Supporto del funzionamento half/full-duplex a 10 M o 100 M
- Funzionamento con switch standard
- Schedulazione di rete non richiesta
- Tabelle di instradamento non richieste

Questi prodotti software sono disponibili per le reti EtherNet/IP.

**Tabella 13 – Software per moduli EtherNet/IP**

Software	Scopo	Necessario
Software di programmazione RSLogix 5000	Questo software è necessario per la configurazione del progetto del controllore e la definizione della comunicazione EtherNet/IP.	Si
Utilità BOOTP/DHCP	Questa utilità è fornita con il software RSLogix 5000. È possibile utilizzarla per l'assegnazione di indirizzi IP ai dispositivi su una rete EtherNet/IP.	No
Software RSNetWorx for EtherNet/IP	Questo software può essere utilizzato per configurare dispositivi EtherNet/IP mediante indirizzi IP e/o nomi host.	No
Software RSLinx	Questo software può essere utilizzato per configurare i dispositivi, stabilire comunicazioni tra i dispositivi e svolgere attività di diagnostica.	Si

## Produzione e consumo dei dati attraverso una rete EtherNet/IP

Il controllore supporta la produzione (invio) ed il consumo (ricezione) dei tag su una rete Ethernet/IP. Tutti i tag prodotti e consumati richiedono connessioni. Il numero totale di tag producibili e consumabili è limitato dal numero di connessioni disponibili.

## Connessioni sulla rete EtherNet/IP

Configurando il controllore di sicurezza per la comunicazione con altri dispositivi nel sistema, si determina indirettamente il numero di connessioni utilizzate dal controllore. Le connessioni sono allocazioni di risorse che garantiscono una comunicazione tra i dispositivi più affidabile se paragonata ai messaggi non connessi (istruzioni di messaggio).

Le connessioni EtherNet/IP non sono schedate. Una connessione non schedata viene attivata dall'intervallo di pacchetto richiesto (RPI, Requested Packet Interval) per il controllo I/O o dal programma (ad esempio un'istruzione MSG). La messaggistica non schedata consente di inviare e ricevere i dati quando necessario.

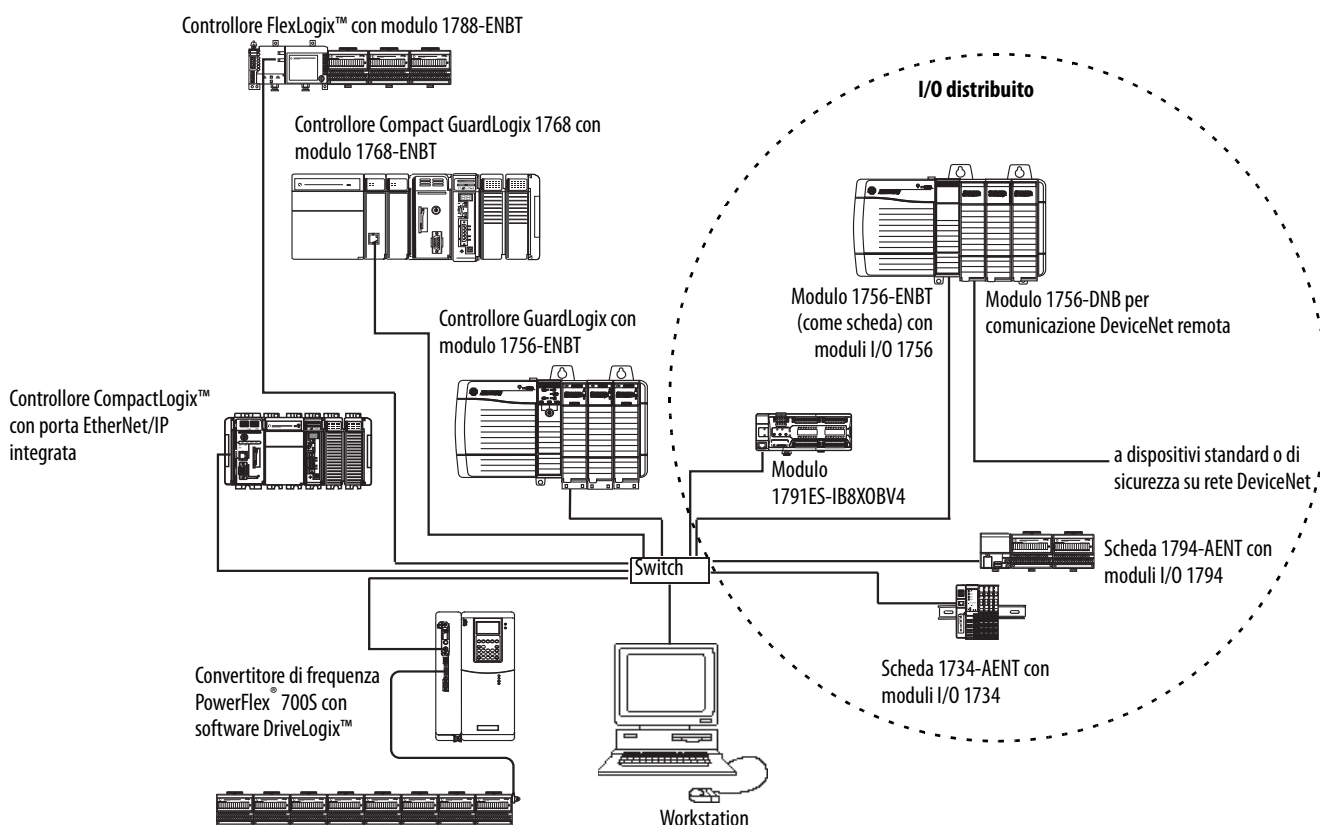
I moduli di comunicazione EtherNet/IP supportano 128 connessioni CIP (Common Industrial Protocol) su una rete EtherNet/IP.

## Esempio di comunicazione EtherNet/IP

Questo esempio illustra quanto segue:

- I controllori possono produrre e consumare tra loro tag standard o di sicurezza.
- I controllori possono generare istruzioni MSG che inviano/ricevono dati standard o configurano dispositivi.<sup>(1)</sup>
- Il modulo di comunicazione EtherNet/IP può essere utilizzato come bridge, consentendo al controllore di sicurezza di produrre e consumare dati standard e di sicurezza.
- Il personal computer può eseguire upload/download di progetti sui controllori.
- Il personal computer può configurare dispositivi sulla rete EtherNet/IP.

**Figura 13 – Esempio di comunicazione EtherNet/IP**

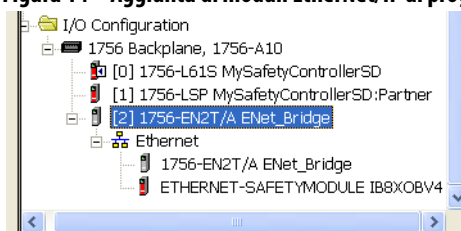


(1) I controllori GuardLogix non supportano le istruzioni MSG per i dati di sicurezza.

## Connessioni EtherNet/IP per moduli I/O CIP Safety

I moduli I/O CIP Safety su reti EtherNet/IP vengono aggiunti al progetto nel modulo di comunicazione EtherNet/IP, come descritto al [Capitolo 5, Aggiunta, configurazione, monitoraggio e sostituzione di I/O CIP Safety](#). Quando si aggiunge un modulo I/O CIP Safety, il software RSLogix 5000 crea automaticamente per tale modulo tag di dati di sicurezza definiti nell'ambito del controllore.

Figura 14 – Aggiunta di moduli EtherNet/IP al progetto



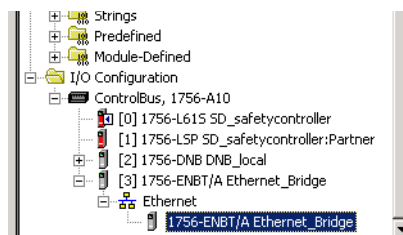
## Connessioni EtherNet/IP standard

Per utilizzare un modulo EtherNet/IP standard con il controllore di sicurezza, è necessario aggiungere il modulo al progetto del controllore di sicurezza e scaricare il progetto sul controllore GuardLogix.

1. Per configurare il modulo, definire indirizzo IP, maschera di sottorete e gateway.

Parametro EtherNet/IP	Descrizione
IP address	L'indirizzo IP identifica il modulo in modo univoco. L'indirizzo IP si presenta nella forma xxx.xxx.xxx.xxx, dove ogni xxx corrisponde ad un numero compreso tra 0 e 255. Tuttavia, vi sono alcuni valori che non possono essere utilizzati come primo ottetto dell'indirizzo: <ul style="list-style-type: none"> <li>• 000.xxx.xxx.xxx</li> <li>• 127.xxx.xxx.xxx</li> <li>• 223...255.xxx.xxx.xxx</li> </ul>
Subnet Mask	L'indirizzamento della sottorete è un'estensione dello schema dell'indirizzo IP che consente ad un sito di utilizzare un solo ID di rete per più reti fisiche. L'instradamento fuori dal sito continua dividendo l'indirizzo IP in un ID di rete ed in un ID host tramite la classe. All'interno di un sito, la maschera di sottorete è utilizzata per suddividere l'indirizzo IP in un ID di rete personalizzato ed in un ID host. Per default, questo campo è impostato a 0.0.0.0. Se si modifica la maschera di sottorete di un modulo già configurato, è necessario spegnere e riaccendere perché la modifica diventi attiva.
Gateway	Il gateway connette singole reti fisiche in un sistema di reti. Quando un nodo deve comunicare con un nodo su un'altra rete, il gateway trasferisce i dati tra le due reti. Per default, questo campo è impostato a 0.0.0.0.

2. Dopo avere installato fisicamente un modulo EtherNet/IP ed impostato il relativo indirizzo IP, è necessario aggiungere il modulo all'organizer del controllore nel progetto del controllore GuardLogix.



3. Per scaricare il progetto, utilizzare il software RSLogix 5000.

## Comunicazione ControlNet

Per le comunicazioni ControlNet, scegliere un modulo 1756-CNB o 1756-CNBR per comunicazioni standard, oppure un modulo 1756-CN2, 1756-CN2R o 1756-CN2RXT per comunicazioni di sicurezza.

**Tabella 14 – Moduli ControlNet**

Se l'applicazione	Selezionare
<ul style="list-style-type: none"> <li>Controlla i moduli I/O standard</li> <li>Richiede una scheda per I/O distribuiti sui collegamenti ControlNet</li> <li>Comunica con altri dispositivi ControlNet (messaggi)</li> <li>Condivide dati standard con altri controllori Logix5000 (produzione/consumo)</li> <li>Funge da bridge con i link ControlNet per instradare i messaggi a dispositivi su altre reti</li> </ul>	1756-CNB
<ul style="list-style-type: none"> <li>Svolge le stesse funzioni di un modulo 1756-CNB</li> <li>È compatibile anche con i supporti ControlNet ridondanti</li> </ul>	1756-CNBR
<ul style="list-style-type: none"> <li>Svolge le stesse funzioni supportate dal modulo 1756-CNB con prestazioni superiori</li> <li>Supporta la comunicazione CIP Safety</li> </ul>	1756-CN2
<ul style="list-style-type: none"> <li>Svolge le stesse funzioni di un modulo 1756-CN2</li> <li>È compatibile anche con i supporti ControlNet ridondanti</li> </ul>	1756-CN2R
<ul style="list-style-type: none"> <li>Esegue le stesse funzioni di un modulo 1756-CN2R</li> <li>Funziona in ambienti estremi con temperature di -25...70 °C</li> </ul>	1756-CN2RXT

Questi prodotti software sono disponibili per le reti ControlNet.

**Tabella 15 – Software per moduli ControlNet**

Software	Scopo	Necessario
Software di programmazione RSLogix 5000	Questo software è necessario per la configurazione del progetto GuardLogix e la definizione della comunicazione ControlNet.	Sì
Software RSNetWorx per ControlNet	Questo software è necessario per configurare la rete ControlNet, definire il tempo di aggiornamento della rete (NUT, Network Update Time) e schedulare la rete ControlNet.	Sì
Software RSLinx	Questo software può essere utilizzato per configurare i dispositivi, stabilire comunicazioni tra i dispositivi e svolgere attività di diagnostica.	Sì

I moduli di comunicazione ControlNet forniscono quanto segue:

- Supportano messaggistica, tag standard e di sicurezza prodotti/consumati ed I/O distribuiti
- Supportano l'utilizzo di ripetitori con cavi coassiali o fibre ottiche per consentire l'isolamento e l'aumento della distanza.

### Produzione e consumo dei dati attraverso una rete ControlNet

Il controllore GuardLogix supporta la produzione (invio) ed il consumo (ricezione) dei tag su reti ControlNet. Il numero totale di tag producibili o consumabili è limitato dal numero di connessioni disponibili nel controllore GuardLogix.

### Connessioni sulla rete ControlNet

Configurando il controllore per la comunicazione con altri dispositivi nel sistema, si determina il numero di connessioni utilizzate dal controllore. Le connessioni sono allocazioni di risorse che garantiscono una comunicazione tra i dispositivi più affidabile se paragonata ai messaggi non connessi.

Le connessioni ControlNet possono essere schedate o non schedate.

**Tabella 16 – Connessioni ControlNet**

Tipo di collegamento	Descrizione
Schedata (univoca per la rete ControlNet)	<p>Una connessione schedata è univoca per la comunicazione ControlNet. Una connessione schedata consente di inviare e ricevere dati ripetutamente in base ad un intervallo prestabilito, che è l'intervallo di pacchetto richiesto (RPI, Requested Packet Interval). Ad esempio, una connessione ad un modulo I/O è una connessione schedata, poiché vengono ricevuti ripetutamente dati dal modulo in un intervallo specificato. Altri tipi di connessioni schedate includono le connessioni a:</p> <ul style="list-style-type: none"> <li>• Dispositivi di comunicazione</li> <li>• Tag prodotti/consumati</li> </ul> <p>Su una rete ControlNet, per abilitare le connessioni schedate e stabilire un tempo di aggiornamento della rete (NUT, Network Update Time), occorre utilizzare il software RSNetWorx per ControlNet. La schedulazione di una connessione riserva una larghezza di banda della rete per la gestione specifica della connessione.</p>
Non schedata	<p>Una connessione non schedata è un trasferimento di messaggi tra controllori che viene attivato dall'intervallo di pacchetto richiesto (RPI, Requested Packet Interval) o dal programma (ad esempio un'istruzione MSG). La messaggistica non schedata consente di inviare e ricevere i dati quando necessario.</p> <p>Le connessioni non schedate utilizzano la larghezza di banda della rete rimanente dopo l'allocazione delle connessioni schedate.</p> <p>Le connessioni di sicurezza prodotte/consumate non sono schedate.</p>

I moduli di comunicazione 1756-CNB e 1756-CNBR supportano 64 connessioni CIP su una rete ControlNet. Tuttavia, è consigliabile configurare non più di 48 connessioni per mantenere le prestazioni ottimali.

Il modulo 1756-CN2 supporta 128 connessioni CIP sulla rete ControlNet.

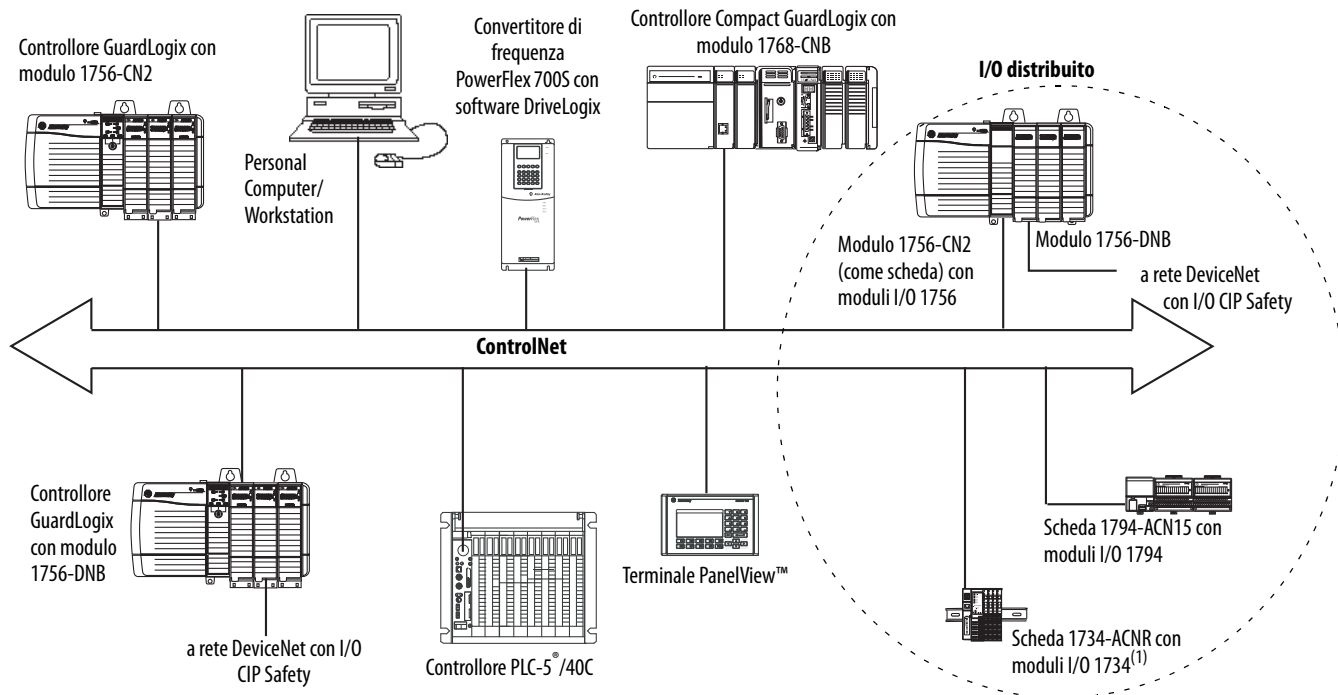
### Esempio di comunicazione ControlNet

Questo esempio illustra quanto segue:

- I controllori GuardLogix possono produrre e consumare tra loro tag standard o di sicurezza.
- I controllori GuardLogix possono generare istruzioni MSG che inviano/ricevono dati standard o configurano dispositivi.<sup>(1)</sup>
- Il modulo 1756-CN2 può essere utilizzato come ponte, consentendo al controllore GuardLogix di produrre e consumare dati standard e di sicurezza da e verso dispositivi I/O
- Il personal computer può eseguire upload/download di progetti sui controllori.
- Il personal computer può configurare dispositivi sulla rete ControlNet, nonché la rete stessa.

(1) I controllori GuardLogix non supportano le istruzioni MSG per i dati di sicurezza.



**Figura 15 – Esempio di comunicazione ControlNet**

(1) La scheda 1734-ACN non supporta i moduli I/O di sicurezza POINT Guard.

## Connessioni ControlNet per moduli I/O distribuiti

Per comunicare con i moduli I/O distribuiti in una rete ControlNet, è necessario aggiungere un ponte ControlNet, una scheda ControlNet e moduli I/O nella cartella di configurazione I/O del controllore.

## Comunicazione DeviceNet

Per comunicare e scambiare dati con i moduli I/O CIP Safety su reti DeviceNet, è necessario un modulo 1756-DNB nello chassis locale.

Per informazioni sulla modalità di installazione del modulo 1756-DNB, fare riferimento alle istruzioni per l'installazione ControlLogix DeviceNet Scanner Module, pubblicazione [1756-IN566](#).

Il modulo 1756-DNB supporta la comunicazione con i dispositivi DeviceNet Safety e DeviceNet standard. Pertanto, è possibile utilizzare entrambe le tipologie.

Questi prodotti software vengono utilizzati con le reti DeviceNet ed il modulo 1756-DNB.

**Tabella 17 – Software da utilizzare con le reti DeviceNet**

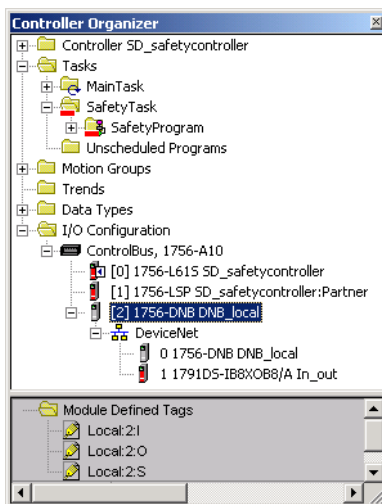
Software	Utilizzato per	Necessario/opzionale
RSLogix 5000	<ul style="list-style-type: none"> <li>• Configurare progetti ControlLogix.</li> <li>• Definire la comunicazione DeviceNet.</li> </ul>	Necessario
RSNetWorx™ for DeviceNet	<ul style="list-style-type: none"> <li>• Configurare i dispositivi DeviceNet.</li> <li>• Definire l'elenco di scansione per tali dispositivi.</li> </ul>	
RSLinx Classic o RSLinx Enterprise	<ul style="list-style-type: none"> <li>• Configurare i dispositivi di comunicazione.</li> <li>• Eseguire attività di diagnostica.</li> <li>• Attivare le comunicazioni tra i dispositivi.</li> </ul>	

### Connessioni DeviceNet per moduli I/O CIP Safety

Per accedere ai dispositivi CIP Safety sulle reti DeviceNet, aggiungere un modulo 1756-DNB alla struttura di configurazione I/O del progetto del controllore GuardLogix.

I moduli I/O CIP Safety sulle reti DeviceNet vengono aggiunti al progetto nel modulo 1756-DNB, come descritto al [Capitolo 5, Aggiunta, configurazione, monitoraggio e sostituzione di I/O CIP Safety](#). Quando si aggiunge un modulo I/O CIP Safety, il software RSLogix 5000 crea automaticamente per tale modulo tag di dati di sicurezza definiti nell'ambito del controllore.

**Figura 16 – Modulo DeviceNet nel controllore nella struttura di configurazione I/O**



## Connessioni DeviceNet standard

Se si utilizzano I/O DeviceNet standard con il controllore GuardLogix, è necessario allocare due connessioni per ciascun modulo 1756-DNB: una connessione è per lo stato del modulo e la configurazione, mentre l'altra è una connessione ottimizzata per rack per i dati I/O DeviceNet.

Per utilizzare il modulo 1756-DNB per l'accesso ai dati standard tramite la rete DeviceNet, è necessario utilizzare il software RSNetWorx per DeviceNet per eseguire le seguenti operazioni:

- Creare un file di configurazione per la rete.
- Configurare ciascun dispositivo standard sulla rete.
- Configurare il modulo 1756-DNB.
- Aggiungere dispositivi I/O standard all'elenco di scansione 1756-DNB.

Quando si aggiunge il modulo 1756-DNB alla configurazione I/O del controllore, il software RSLogix 5000 crea automaticamente un gruppo di tag standard per i dati di ingresso, uscita e di stato della rete.

## Comunicazione seriale

Per utilizzare il controllore GuardLogix su una rete seriale, è necessario disporre di:

- Una workstation con una porta seriale
- Il software RSLinx per configurare il driver di comunicazione seriale
- il software RSLogix 5000 per configurare la porta seriale del controllore

Perché il controllore comunichi con una workstation o un altro dispositivo sulla rete seriale, è necessario:

1. Configurare il driver di comunicazione seriale per la workstation.
2. Configurare la porta seriale del controllore.

**Tabella 18 – Modalità di comunicazione seriale**

Utilizzare la modalità	Per le seguenti informazioni
Punto-punto DF1	Comunicazione tra il controllore ed un altro dispositivo compatibile con il protocollo DF1. Questa è la modalità di sistema predefinita. Questa modalità viene generalmente utilizzata per programmare il controllore attraverso la relativa porta seriale.
Master DF1	Controllo dell'interrogazione e della trasmissione dei messaggi tra i nodi master e slave. La rete master/slave comprende un controllore configurato come nodo master ed un massimo di 254 nodi slave. I nodi slave devono essere collegati per mezzo di modem o line driver. Una rete master/slave può avere numeri di nodo compresi tra 0 e 254. Ciascun nodo deve avere un indirizzo di nodo univoco. Inoltre, devono esistere almeno 2 nodi per definire il collegamento come rete (1 stazione master e 1 stazione slave costituiscono due nodi).
Slave DF1	Controllore utilizzato come stazione slave in una rete di comunicazione seriale master/slave. Se coesistono più stazioni slave sulla rete, collegare le stazioni slave al master attraverso i modem o i line driver. Quando sulla rete è presente un'unica stazione slave, non è necessario un modem per connettere la stazione slave al master. È possibile configurare i parametri di controllo per nessun handshaking. È possibile connettere da 2 a 255 nodi ad un link. In modalità DF1 slave, un controllore utilizza il protocollo DF1 half-duplex. Un nodo è assegnato come master e controlla gli accessi al link. Tutti gli altri nodi sono stazioni slave e devono attendere l'autorizzazione dal master prima di eseguire la trasmissione.
DH-485	Comunicazione con altri dispositivi DH-485 multi-master, rete a passaggio di token che permette la programmazione e la messaggistica peer-to-peer.

## Ulteriori riferimenti

Riferimento	Descrizione
Manuale dell'utente EtherNet/IP Modules in Logix5000 Control Systems, pubblicazione <a href="#">ENET-UM001</a>	Contiene informazioni dettagliate sulla configurazione e l'utilizzo dei moduli di comunicazione EtherNet/IP in un sistema di controllo Logix5000
Manuale dell'utente ControlNet Modules in Logix5000 Control Systems, pubblicazione <a href="#">CNET-UM001</a>	Contiene informazioni dettagliate sulla configurazione e l'utilizzo dei moduli di comunicazione ControlNet in un sistema di controllo Logix5000
Manuale dell'utente DeviceNet Modules in Logix5000 Control Systems, pubblicazione <a href="#">DNET-UM004</a>	Contiene informazioni dettagliate sulla configurazione e l'utilizzo del modulo 1756-DNB in un sistema di controllo Logix5000

## Aggiunta, configurazione, monitoraggio e sostituzione di I/O CIP Safety

Argomento	Pagina
Aggiunta di moduli I/O CIP Safety	69
Configurazione di moduli I/O CIP Safety mediante il software RSLogix 5000	70
Impostazione del Numero di rete di sicurezza (SNN)	71
Utilizzo delle connessioni unicast su reti EtherNet/IP	71
Impostazione del limite del tempo di risposta della connessione	71
Comprensione dell'autenticazione di configurazione	75
Ripristino della proprietà dei moduli I/O di sicurezza	76
Indirizzamento dei dati I/O di sicurezza	76
Monitoraggio dello stato dei moduli I/O di sicurezza	77
Reset di un modulo alle condizioni predefinite in fabbrica	79
Sostituzione di un modulo tramite il software RSLogix 5000	79
Sostituzione di un modulo POINT Guard I/O mediante il software RSNetWorx for DeviceNet	86

Per ulteriori informazioni sull'installazione, la configurazione e l'utilizzo di moduli I/O CIP Safety, consultare le seguenti risorse:

- Manuale dell'utente Guard I/O DeviceNet Safety Modules, pubblicazione [1791DS-UM001](#)
- Manuale dell'utente Moduli di sicurezza Guard I/O EtherNet/IP, pubblicazione [1791ES-UM001](#)
- Manuale di installazione ed uso Moduli di sicurezza POINT Guard I/O, pubblicazione [1734-UM013](#)
- Guida in linea del software RSLogix 5000

### Aggiunta di moduli I/O CIP Safety

Quando si aggiunge un modulo al sistema, è necessario definire una configurazione per il modulo, comprendente i seguenti elementi:

- Indirizzo del nodo per reti DeviceNet

L'indirizzo di nodo di un modulo I/O CIP Safety sulle reti DeviceNet non è configurabile mediante il software RSLogix 5000. Tali indirizzi, infatti, vengono impostati mediante selettori rotativi sui moduli.

- Indirizzo IP per reti EtherNet/IP

Per impostare l'indirizzo IP, è possibile regolare i selettori rotativi sul modulo, utilizzare il software DHCP fornito da Rockwell Automation oppure recuperare l'indirizzo predefinito dalla memoria non volatile.

- Numero della rete di sicurezza (SNN)  
Per informazioni sull'impostazione del valore SNN, vedere a pagina 71.
- Autenticazione di configurazione  
Per informazioni su quando l'autenticazione di configurazione è impostata automaticamente o è necessario impostarla manualmente, vedere a pagina 75.
- Limite del tempo di risposta  
Per informazioni sull'impostazione del limite del tempo di risposta, vedere a pagina 71.
- Parametri di test, uscita ed ingresso di sicurezza

Per configurare i moduli I/O CIP Safety tramite il controllore GuardLogix è possibile utilizzare il software RSLogix 5000.

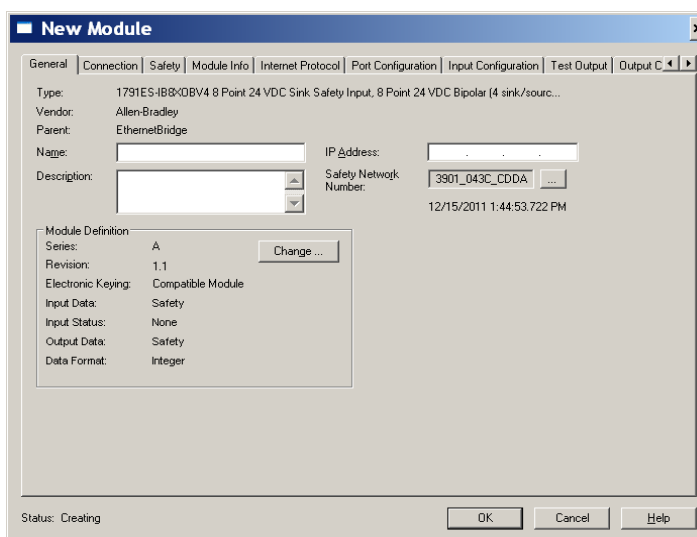
**SUGGERIMENTO** I moduli I/O di sicurezza supportano dati standard e di sicurezza. La configurazione dei moduli determina i dati disponibili.

## Configurazione di moduli I/O CIP Safety mediante il software RSLogix 5000


Il modulo I/O CIP Safety deve essere aggiunto al modulo di comunicazione nella cartella di configurazione I/O del progetto RSLogix 5000.

**SUGGERIMENTO** Quando si è online, non è possibile aggiungere o eliminare un modulo I/O CIP Safety.

1. Fare clic con il pulsante destro del mouse sulla rete appropriata quindi selezionare New Module.
2. Espandere la categoria Safety e selezionare un modulo I/O CIP Safety.
3. Specificare le proprietà del modulo.



- a. Modificare le impostazioni nel campo Module Definition, se necessario, facendo clic su Change.
- b. Immettere un nome per il nuovo modulo.
- c. Inserire l'indirizzo di nodo o indirizzo IP del modulo utilizzato nella rete di collegamento.  
Nel menu a discesa sono inclusi solo i numeri di nodo non utilizzati.

- d. Modificare il numero rete di sicurezza (SNN, Safety Network Number), se necessario, facendo clic sul pulsante .

Per ulteriori informazioni, vedere a pagina [71](#).

- e. Impostare i parametri di configurazione del modulo utilizzando le schede Input Configuration, Test Output e Output Configuration.

Per ulteriori informazioni sulla configurazione del modulo I/O CIP Safety, fare riferimento alla guida in linea di RSLogix 5000.

- f. Impostare il limite del tempo di risposta della connessione utilizzando la scheda Safety.

Per ulteriori informazioni, vedere a pagina [71](#).

## Impostazione del Numero di rete di sicurezza (SNN)

Quando si aggiungono nuovi moduli I/O di sicurezza, l'assegnazione di un valore SNN basato sul tempo è automatica. Ai moduli di sicurezza aggiunti successivamente alla stessa rete viene assegnato lo stesso valore SNN definito all'interno dell'indirizzo di livello più basso sulla rete CIP Safety.

Per la maggior parte delle applicazioni, questo valore SNN basato sul tempo ed automatico è sufficiente. Tuttavia, in alcuni casi è necessario modificare un valore SNN.

Vedere [Assegnazione del Numero di rete di sicurezza \(SNN\) a pagina 55](#).

## Utilizzo delle connessioni unicast su reti EtherNet/IP

Con il software RSLogix 5000 versione 20 o successive, è possibile configurare i moduli I/O EtherNet/IP per l'utilizzo di connessioni unicast. Le connessioni unicast sono connessioni punto a punto tra un nodo sorgente ed un nodo di destinazione. Per questo tipo di connessione, non bisogna inserire un campo RPI minimo o massimo o un valore predefinito.

Per configurare le connessioni unicast, accedere alla scheda Connection e selezionare Use Unicast Connection over Ethernet/IP.

## Impostazione del limite del tempo di risposta della connessione

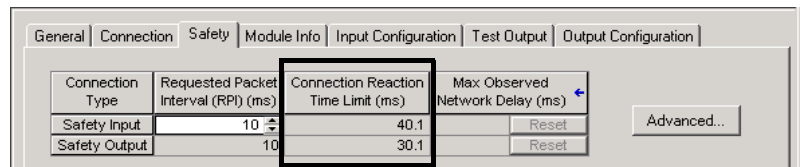
Connection Reaction Time Limit (tempo limite di risposta della connessione) è la durata massima dei pacchetti di sicurezza sulla connessione associata. Se la durata dei dati utilizzati dal dispositivo consumatore è superiore al limite del tempo di risposta della connessione, si verifica un errore di connessione. Il tempo limite di risposta della connessione è determinato tramite le seguenti equazioni:

$$\text{Tempo limite di risposta della connessione in ingresso} = \text{RPI ingresso} \times [\text{Moltiplicatore timeout} + \text{Moltiplicatore ritardo rete}]$$

$$\text{Limite del tempo di risposta della connessione in uscita} = \text{Periodo del task di sicurezza} \times [\text{Moltiplicatore timeout} + \text{Moltiplicatore ritardo rete} - 1]$$

Connection Reaction Time Limit è visualizzato nella scheda Safety della finestra di dialogo Module Properties.

**Figura 17 – Limite del tempo di risposta della connessione**



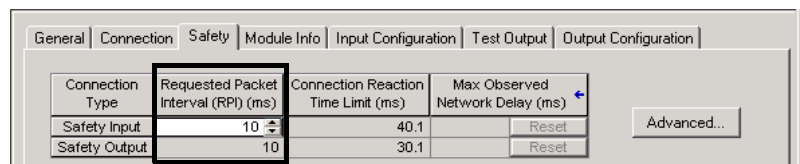
### Configurazione dell'intervallo di pacchetto richiesto (RPI)

L'RPI specifica l'intervallo di aggiornamento dei dati durante la connessione. Ad esempio, un modulo di ingresso produce dati secondo l'intervallo RPI assegnato.

Per le connessioni di ingresso di sicurezza, è possibile impostare l'intervallo RPI nella scheda Safety della finestra di dialogo Module Properties. L'intervallo RPI viene inserito per incrementi di 1 ms, in un intervallo compreso tra 1 e 100 ms. Il valore predefinito è 10 ms.

Quando l'intervallo RPI viene modificato tramite il software RSLogix 5000, il parametro del limite del tempo di risposta della connessione viene immediatamente regolato.

**Figura 18 – Intervallo di pacchetto richiesto**



Per le connessioni di uscita di sicurezza, l'intervallo RPI è fissato al periodo del task di sicurezza. Se il limite di tempo di risposta della connessione corrispondente non è soddisfacente, è possibile regolare il periodo del task di sicurezza dalla finestra di dialogo Safety Task Properties.

Per ulteriori informazioni sul periodo del task di sicurezza, vedere [Definizione del periodo del task di sicurezza a pagina 90](#).

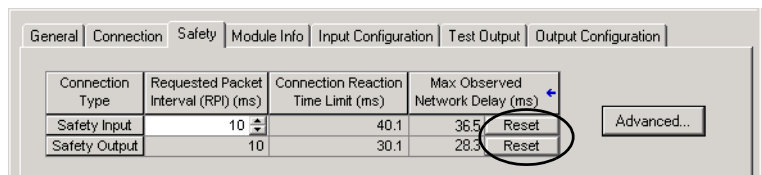
Per applicazioni standard, l'intervallo RPI è generalmente sufficiente. Per requisiti più complessi, utilizzare il pulsante Advanced per modificare i parametri di Connection Reaction Time Limit, come descritto a pagina [73](#).



## Visualizzazione del ritardo rete massimo osservato

Quando il controllore GuardLogix riceve un pacchetto di sicurezza, il software registra il ritardo di rete massimo osservato. Nel caso degli ingressi di sicurezza, in corrispondenza di Maximum Observed Network Delay viene visualizzato il ritardo del percorso dal modulo di ingresso al controllore e del ritorno della conferma al modulo di ingresso. Nel caso delle uscite di sicurezza, viene visualizzato il ritardo del percorso dal controllore al modulo di uscita e del ritorno della conferma al controllore. Il parametro Maximum Observed Network Delay è mostrato nella scheda Safety della finestra di dialogo Module Properties. Se si è online, è possibile azzerare questo parametro facendo clic su Reset.

**Figura 19 – Reset di Max Observed Network Delay**

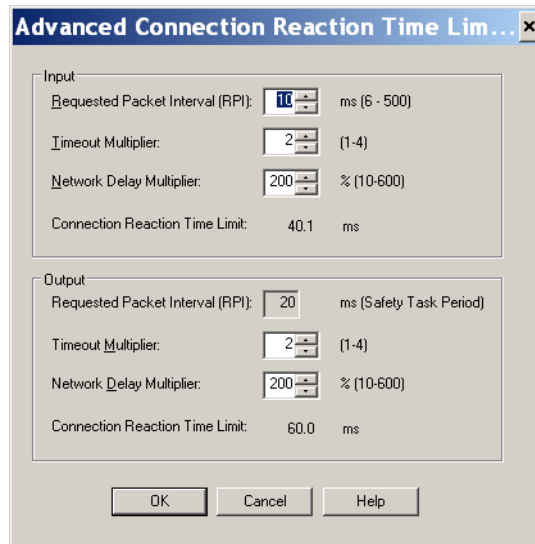


### IMPORTANTE

Il ritardo di rete massimo effettivo dal produttore al consumatore è inferiore al valore visualizzato nel campo Maximum Network Delay della scheda Safety. In generale, il ritardo massimo effettivo dei messaggi è pari a circa la metà del valore Maximum Network Delay visualizzato.

## Impostazione dei parametri avanzati relativi ai limiti del tempo di risposta della connessione

**Figura 20 – Configurazione avanzata**



### Timeout Multiplier

Il parametro Timeout Multiplier determina il numero di RPI di attesa di un pacchetto prima di dichiarare il timeout della connessione. Ciò si traduce nel numero di messaggi che possono andare persi prima che venga dichiarato un errore di connessione.

Ad esempio, un valore pari a 1 in questo parametro indica che i messaggi devono essere ricevuti entro ciascun intervallo RPI. Un valore 2 indica che 1 messaggio può andare perso se almeno 1 messaggio viene ricevuto in 2 volte l'RPI (2 x RPI).

### *Network Delay Multiplier*

Il parametro Network Delay Multiplier definisce il tempo di trasferimento del messaggio applicato dal protocollo CIP Safety. Il valore di Network Delay Multiplier specifica il ritardo del percorso produttore-consumatore e del ritorno della conferma al produttore. È possibile utilizzare questo parametro per ridurre o aumentare il limite del tempo di risposta della connessione nei casi in cui il tempo di trasferimento del messaggio applicato è notevolmente inferiore o superiore all'intervallo RPI. Ad esempio, la regolazione di questo parametro può essere utile quando l'RPI di una connessione di uscita corrisponde alla lunghezza del periodo del task di sicurezza.

Nei casi in cui l'intervallo RPI degli ingressi o delle uscite è relativamente lento o veloce rispetto al ritardo del messaggio applicato, il valore di Network Delay Multiplier può essere approssimato utilizzando uno dei due metodi riportati di seguito.

**Metodo 1:** utilizzare il rapporto tra l'intervallo RPI degli ingressi ed il periodo del task di sicurezza. Utilizzare questo metodo solo a patto che si verifichino tutte le seguenti condizioni:

- Il percorso o il ritardo è quasi uguale al percorso di uscita o al ritardo.
- L'intervallo RPI degli ingressi è stato configurato in modo che il tempo di trasferimento effettivo del messaggio di ingresso sia inferiore a quello dell'intervallo RPI degli ingressi.
- Il periodo del task di sicurezza è lento rispetto all'intervallo RPI degli ingressi.

In queste condizioni, il valore di Output Network Delay Multiplier può essere approssimato come segue:

Moltiplicatore ritardo rete in ingresso x [RPI degli ingressi ÷ Periodo del task di sicurezza]

---

#### **ESEMPIO**

#### **Calcolo approssimativo del moltiplicatore ritardo rete in uscita**

Se:

RPI degli ingressi = 10 ms

Moltiplicatore ritardo rete in ingresso = 200%

Periodo del task di sicurezza = 20 ms

Pertanto, il moltiplicatore ritardo rete in uscita equivale a:

$200\% \times [10 \div 20] = 100\%$

---

**Metodo 2:** utilizzare il Ritardo di rete massimo osservato. Se il sistema funziona per un periodo prolungato nelle peggiori condizioni di carico, il Moltiplicatore ritardo rete può essere impostato da Maximum Observed Network Delay. Questo metodo può essere utilizzato su una connessione di ingresso o uscita. Dopo che il sistema ha funzionato per un periodo di tempo prolungato nelle condizioni di carico peggiori, annotare il Ritardo rete massimo osservato.

Il Moltiplicatore ritardo rete può essere approssimato tramite la seguente equazione:

$$[\text{Ritardo rete massimo osservato} + \text{Fattore correttivo}] \div \text{RPI}$$

<b>ESEMPIO</b>	<b>Calcolo del moltiplicatore ritardo rete da ritardo rete massimo osservato</b>
	Se:
	RPI = 50 ms
	Ritardo rete massimo osservato = 20 ms
	Fattore correttivo= 10
	Pertanto, il Moltiplicatore ritardo rete equivale a:
	$[20 + 10] \div 50 = 60\%$

**Tabella 19 – Ulteriori riferimenti**

<b>Riferimento</b>	<b>Descrizione</b>
Manuale di riferimento per la sicurezza – Sistemi di controllori GuardLogix, pubblicazione <a href="#">1756-RM093</a>	Fornisce informazioni sul calcolo dei tempi di risposta.
Manuale dell'utente Guard I/O DeviceNet Safety Modules, pubblicazione <a href="#">1791DS-UM001</a>	
Manuale dell'utente Moduli di sicurezza Guard I/O EtherNet/IP, pubblicazione <a href="#">1791ES-UM001</a>	

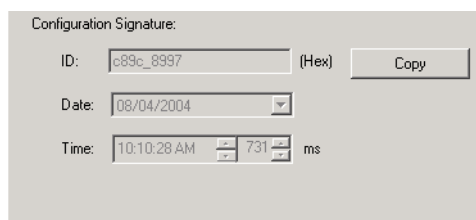
## Comprensione dell'autenticazione di configurazione

Ogni dispositivo di sicurezza ha un'autenticazione di configurazione univoca, che definisce la configurazione del modulo. L'autenticazione di configurazione è composta da un numero ID, data ed ora ed è utilizzata per verificare la configurazione di un modulo.

### Configurazione tramite il software RSLogix 5000

Quando il modulo I/O viene configurato utilizzando il software RSLogix 5000, l'autenticazione di configurazione viene generata automaticamente. È possibile visualizzare e copiare l'autenticazione di configurazione tramite la scheda Safety nella finestra di dialogo Module Properties.

**Figura 21 – Visualizzazione e copia dell'autenticazione di configurazione**



## Proprietario della configurazione diverso (connessione di solo ascolto)

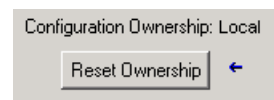
Se la configurazione del modulo I/O appartiene ad un altro controllore, occorre copiare l'autenticazione di configurazione del modulo dal progetto del proprietario ed incollarla nella scheda Safety della finestra di dialogo Module Properties.

**SUGGERIMENTO** Se il modulo è configurato solo per gli ingressi, è possibile copiare ed incollare l'autenticazione di configurazione. Se il modulo è dotato di uscite di sicurezza, queste appartengono al controllore proprietario della configurazione, pertanto la casella di testo dell'autenticazione di configurazione non è disponibile.

## Ripristino della proprietà dei moduli I/O di sicurezza

Quando il software RSLogix 5000 è online, nella scheda Safety della finestra di dialogo Module Properties viene visualizzata la proprietà di configurazione corrente. Quando la configurazione appartiene al progetto aperto, viene visualizzato "Local". Quando la configurazione appartiene ad un secondo dispositivo, viene visualizzato Remote insieme al numero rete di sicurezza (SNN) ed all'indirizzo di nodo o al numero di slot del proprietario della configurazione. Se la lettura del modulo non riesce, viene visualizzato un errore di comunicazione.

In modalità online, è possibile ripristinare la configurazione predefinita del modulo facendo clic su Reset Ownership.



**SUGGERIMENTO** Qualora esistano modifiche in sospeso delle proprietà del modulo, una firma del task di sicurezza oppure un blocco di sicurezza, non è possibile ripristinare la proprietà.

## Indirizzamento dei dati I/O di sicurezza

Quando si aggiunge un modulo alla cartella di configurazione I/O, il software RSLogix 5000 crea automaticamente per tale modulo dei tag definiti nell'ambito del controllore.

Le informazioni I/O vengono presentate come set di tag. Ciascun tag utilizza una struttura di dati, a seconda del tipo e delle funzioni del modulo I/O. Il nome di un tag è basato sul nome del modulo utilizzato nel sistema.

L'indirizzo di un dispositivo I/O CIP Safety si basa sul seguente formato:

Modulename:Type.Member

**Tabella 20 – Formato dell'indirizzo dei moduli I/O CIP Safety**

Dove	È
Modulename	Il nome del modulo I/O CIP Safety
Type	Tipo di dati
	Ingresso: I
	Uscita: O
Member	Dati specifici dal modulo I/O
	Modulo solo ingresso: Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members
	Modulo solo uscita: Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:O.Output Members
	I/O misti: Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members Modulename:O.Output Members

**Tabella 21 – Ulteriori riferimenti**

Riferimento	Descrizione
<a href="#">Capitolo 9, Monitoraggio dello stato e gestione degli errori</a>	Contiene informazioni sul monitoraggio dei dati dei tag di sicurezza
Manuale di programmazione Dati I/O e tag dei controllori Logix5000, pubblicazione <a href="#">1756-PM004</a>	Fornisce informazioni sull'indirizzamento dei moduli I/O standard

## Monitoraggio dello stato dei moduli I/O di sicurezza

Lo stato dei moduli I/O di sicurezza può essere monitorato per mezzo di messaggi espliciti o tramite gli indicatori di stato dei moduli I/O.

Le seguenti pubblicazioni forniscono informazioni relative alla ricerca guasti sui moduli I/O:

- Manuale dell'utente Guard I/O DeviceNet Safety Modules, pubblicazione [1791DS-UM001](#)
- Manuale dell'utente Guard I/O EtherNet/IP Modules, pubblicazione [1791ES-UM001](#)
- Manuale di installazione ed uso Moduli di sicurezza POINT Guard I/O, pubblicazione [1734-UM013](#)

Tabella 22 – Funzionamento degli indicatori di stato

Indicatore	Stato	Descrizione		
		Moduli Guard I/O DeviceNet	Moduli Guard I/O EtherNet/IP	Moduli POINT Guard I/O
Stato del modulo (MS)	Spento	Alimentazione assente.		
	Verde, acceso	Funzionamento normale.		
	Verde, lampeggiante	Dispositivo in stato di riposo.		
	Rosso, lampeggiante	Errore reversibile.	Si è verificato un errore reversibile oppure è in corso un aggiornamento del firmware.	
	Rosso, acceso	Errore irreversibile.		
	Rosso/verde, lampeggiante	Autodiagnosi in corso.	È in corso la procedura di autodiagnosi oppure il modulo non è configurato correttamente. Per ulteriori informazioni, fare riferimento all'indicatore di stato della rete.	
Stato della rete (NS)	Spento	Dispositivo non in linea o non alimentato.		
	Verde, acceso	Dispositivo in linea, connessioni stabilite.		
	Verde, lampeggiante	Dispositivo in linea, nessuna connessione stabilita.		
	Rosso, lampeggiante	Timeout della comunicazione.	Si è verificato un timeout della comunicazione oppure è in corso un aggiornamento del firmware.	
	Rosso, acceso	Errore di comunicazione. Il dispositivo ha rilevato un errore che ha impedito la comunicazione di rete.		
	Rosso/verde, lampeggiante	Dispositivo nello stato di errore di comunicazione o impostazione del numero rete di sicurezza (SNN) in corso.	Autodiagnosi in corso.	Non applicabile.
Punti di ingresso (INx)	Spento	Ingresso di sicurezza OFF.		
	Giallo, acceso	Ingresso di sicurezza ON.		
	Rosso, acceso	Errore nel circuito di ingresso.		
	Rosso, lampeggiante	Se è stato selezionato il funzionamento a doppio canale, si è verificato un errore nel circuito di ingresso partner.		
Punti di uscita (Ox)	Spento	Uscita di sicurezza OFF.		
	Giallo, acceso	Uscita di sicurezza ON.		
	Rosso, acceso	Errore nel circuito di uscita.		
	Rosso, lampeggiante	Se è stato selezionato il funzionamento a doppio canale, si è verificato un errore nel circuito di uscita partner.		
Test punti di uscita (Tx)	Spento	Non applicabile.	Uscita OFF.	Non applicabile.
	Giallo, acceso		Uscita ON.	
	Rosso, acceso		Errore nel circuito di uscita.	
LOCK (blocco)	Giallo, acceso	Configurazione del dispositivo bloccata.		
	Giallo, lampeggiante	Configurazione del dispositivo valida, ma il dispositivo non è bloccato.		
	Giallo, spento	Dati di configurazione non validi o assenti, oppure il dispositivo è già stato configurato tramite il software RSLogix 5000.		
IN PWR (alimentazione ingresso)	Verde, spento	Alimentazione ingresso assente.		
	Verde, acceso	La tensione di alimentazione di ingresso è conforme alle specifiche.		
	Giallo, acceso	La tensione di alimentazione di ingresso non è conforme alle specifiche.		
OUT PWR (alimentazione uscita)	Verde, spento	Alimentazione di uscita assente.		
	Verde, acceso	La tensione di alimentazione di uscita è conforme alle specifiche.		
	Giallo, acceso	La tensione di alimentazione di uscita non è conforme alle specifiche.		
PWR	Verde, spento	Alimentazione assente.		
	Verde, acceso	Non applicabile.		
	Giallo, acceso	La tensione di alimentazione non è conforme alle specifiche.		

## Reset di un modulo alle condizioni predefinite in fabbrica

Se il modulo Guard I/O era già stato utilizzato in precedenza, cancellare la configurazione preesistente prima di installarlo su una rete di sicurezza resettandolo alle condizioni predefinite in fabbrica.

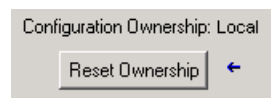
Quando il software RSLogix 5000 è online, nella scheda Safety della finestra di dialogo Module Properties viene visualizzata la proprietà della configurazione corrente. Quando la configurazione appartiene al progetto aperto, viene visualizzato "Local". Quando la configurazione appartiene ad un secondo dispositivo, viene visualizzato Remote insieme al numero rete di sicurezza (SNN) ed all'indirizzo di nodo o al numero di slot del proprietario della configurazione. Se la lettura del modulo non riesce, viene visualizzato un errore di comunicazione.

Se la connessione è Local, è necessario inibire la connessione del modulo prima di resettare la proprietà. Per inibire il modulo, procedere come segue.

1. Fare clic con il pulsante destro del mouse sul modulo e selezionare Properties.
2. Fare clic sulla scheda Connection.
3. Selezionare Inhibit Connection.
4. Fare clic su Apply e quindi su OK.

Per resettare il modulo alla configurazione predefinita in fabbrica in modalità online, procedere come segue.

1. Fare clic con il pulsante destro del mouse sul modulo e selezionare Properties.
2. Fare clic sulla scheda Safety.
3. Fare clic su Reset Ownership.



**SUGGERIMENTO** Qualora esistano modifiche in sospenso delle proprietà del modulo, una firma del task di sicurezza oppure un blocco di sicurezza, non è possibile ripristinare la proprietà.

## Sostituzione di un modulo tramite il software RSLogix 5000

Per sostituire un modulo Guard I/O su una rete Ethernet, è possibile utilizzare il software RSLogix 5000. Per la sostituzione di un modulo Guard I/O su una rete DeviceNet, la scelta del software dipende dal tipo di modulo.

**Tabella 23 – Software**

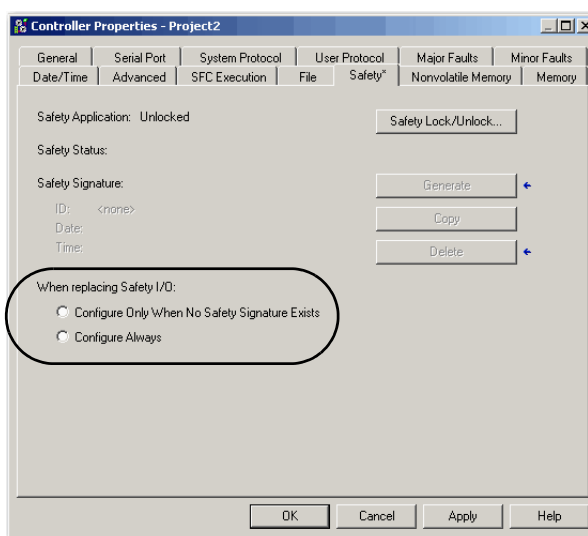
Se si utilizza	Usare	Vedere
Modulo Guard I/O 1791DS con scheda 1756-DNB	Software RSLogix 5000	sotto
Modulo POINT Guard I/O 1734 con scheda 1734-PDN	Software RSNetWorx for DeviceNet	<a href="#">Sostituzione di un modulo POINT Guard I/O mediante il software RSNetWorx for DeviceNet a pagina 86</a>

Se si sta utilizzando una parte del sistema CIP Safety per garantire la conformità al livello SIL 3 durante la sostituzione ed il collaudo funzionale del modulo, non è possibile utilizzare la funzione Configure Always. Andare a [Sostituzione con l'opzione "Configure Only When No Safety Signature Exists" abilitata a pagina 80](#).

Se l'intero sistema di controllo CIP Safety instradabile non viene utilizzato per garantire la conformità con il livello SIL 3/PLe durante la sostituzione ed il test funzionale di un modulo, è possibile utilizzare la funzione Configure Always. Andare a [Sostituzione con opzione "Configure Always" abilitata a pagina 84](#).

La sostituzione del modulo si configura sulla scheda Safety del controllore GuardLogix.

**Figura 22 – Sostituzione dei moduli I/O di sicurezza**



### Sostituzione con l'opzione "Configure Only When No Safety Signature Exists" abilitata

Quando viene sostituito un modulo, la configurazione viene scaricata dal controllore di sicurezza se il DeviceID del nuovo modulo corrisponde all'originale. Il DeviceID è una combinazione dell'indirizzo di nodo/IP e del numero di rete di sicurezza (SNN) e viene aggiornato ogni volta che viene impostato il numero SNN.


Se il progetto è configurato come "Configure Only When No Safety Signature Exists", fare riferimento ai punti corrispondenti nella [Tabella 24](#) per sostituire un modulo POINT Guard I/O in base allo scenario effettivo. Una volta completata correttamente la procedura, il DeviceID corrisponde all'originale e consente al controllore di sicurezza di scaricare la corretta configurazione del modulo e di ristabilire la connessione di sicurezza.

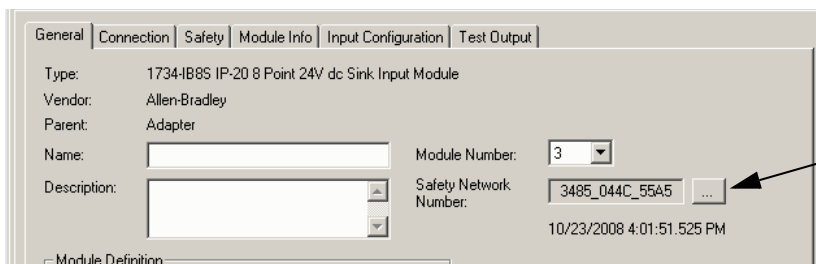


**Tabella 24 – Sostituzione di un modulo**

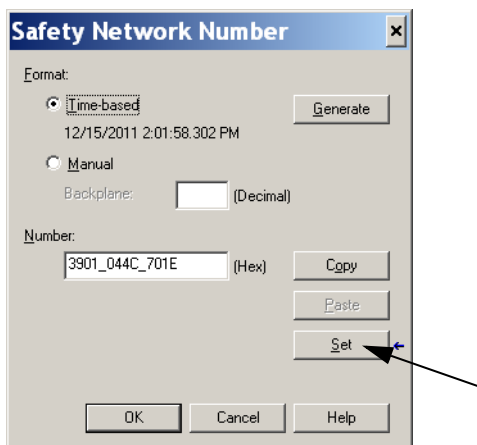
Con firma di sicurezza GuardLogix	Condizione modulo sostitutivo	Intervento necessario
No	Senza SNN (originale)	Nessuna. Il modulo è pronto all'uso.
Si o No	Stesso SNN della configurazione task di sicurezza originale	Nessuna. Il modulo è pronto all'uso.
Si	Senza SNN (originale)	<a href="#">Vedere Scenario 1 – Modulo sostitutivo nelle condizioni predefinite in fabbrica e presenza della firma di sicurezza a pagina 81.</a>
Si	SNN differente dalla configurazione task di sicurezza originale	<a href="#">Vedere Scenario 2 – Numero SNN del modulo sostitutivo diverso dall'originale e presenza della firma di sicurezza a pagina 82.</a>
No	SNN differente dalla configurazione task di sicurezza originale	<a href="#">Vedere Scenario 3 – Numero SNN del modulo sostitutivo diverso dall'originale ed assenza della firma di sicurezza a pagina 84.</a>

*Scenario 1 – Modulo sostitutivo nelle condizioni predefinite in fabbrica e presenza della firma di sicurezza*

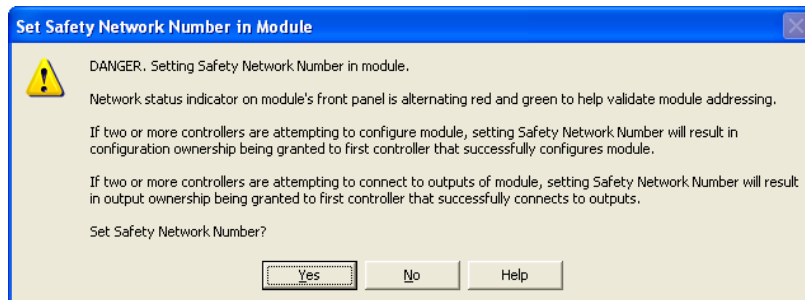
1. Rimuovere il modulo I/O in uso ed installare quello nuovo.
2. Fare clic con il pulsante destro del mouse sul modulo POINT Guard I/O sostitutivo e selezionare Properties.
3. Per aprire la finestra di dialogo Safety Network Number, fare clic su  a destra del numero rete di sicurezza.



4. Fare clic su Set.



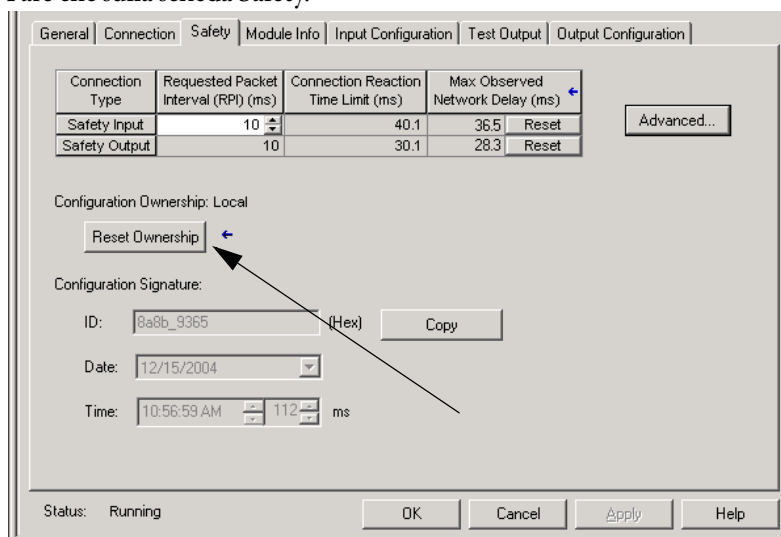
5. Verificare che l'indicatore di stato della rete (NS) lampeggi con luce alternata rossa/verde sul modulo corretto prima di fare clic su Yes nella finestra di dialogo di conferma per impostare l'SNN ed accettare il modulo sostitutivo.




6. Seguire le procedure aziendali per il test funzionale del modulo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.

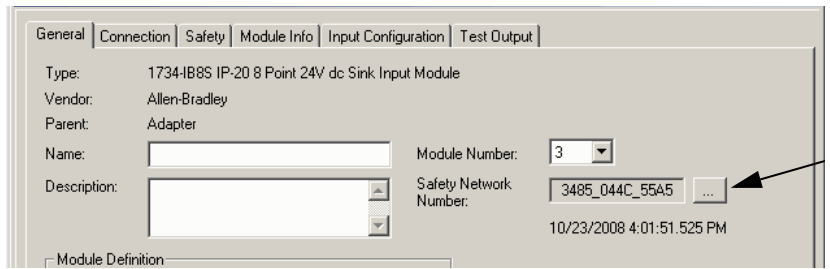
*Scenario 2 – Numero SNN del modulo sostitutivo diverso dall'originale e presenza della firma di sicurezza*

1. Rimuovere il modulo I/O in uso ed installare quello nuovo.
2. Fare clic con il pulsante destro del mouse sul proprio modulo POINT Guard I/O e selezionare Properties.
3. Fare clic sulla scheda Safety.

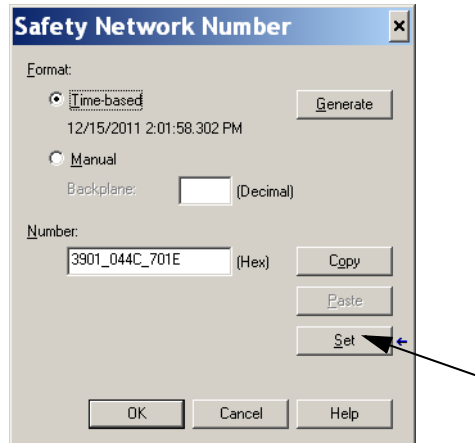


4. Fare clic su Reset Ownership.
5. Fare clic su OK.
6. Fare clic con il pulsante destro del mouse sul controllore e selezionare Properties.

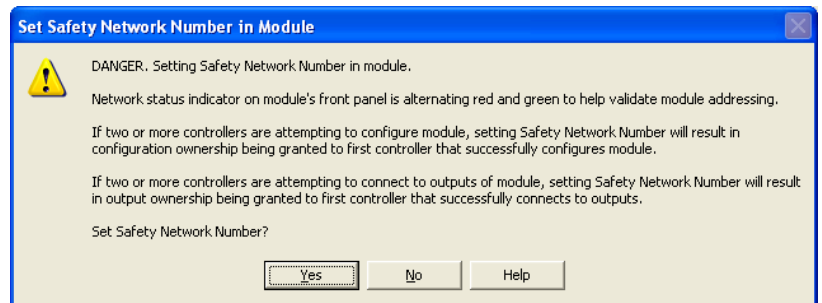
- Per aprire la finestra di dialogo Safety Network Number, fare clic su  a destra del numero rete di sicurezza.



- Fare clic su Set.



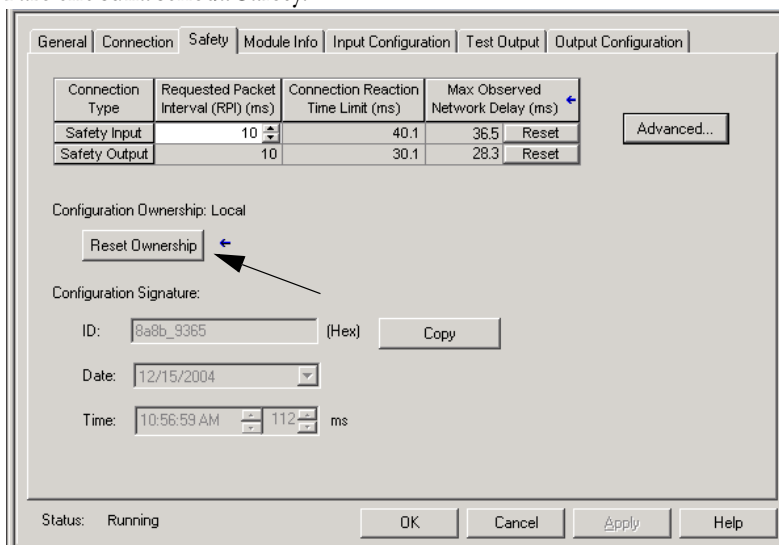
- Verificare che l'indicatore di stato della rete (NS) lampeggi con luce alternata rossa/verde sul modulo corretto prima di fare clic su Yes nella finestra di dialogo di conferma per impostare l'SNN ed accettare il modulo sostitutivo.



- Seguire le procedure aziendali per il test funzionale del modulo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.

*Scenario 3 – Numero SNN del modulo sostitutivo diverso dall'originale ed assenza della firma di sicurezza*

1. Rimuovere il modulo I/O in uso ed installare quello nuovo.
2. Fare clic con il pulsante destro del mouse sul proprio modulo POINT Guard I/O e selezionare Properties.
3. Fare clic sulla scheda Safety.



4. Fare clic su Reset Ownership.
5. Fare clic su OK.
6. Seguire le procedure aziendali per il test funzionale del modulo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.

**Sostituzione con opzione “Configure Always” abilitata**



**ATTENZIONE:** Abilitare la funzione “Configure Always” solo se l'intero sistema di controllo CIP Safety **non** è utilizzato per mantenere il livello SIL 3 durante la sostituzione ed il test funzionale di un modulo.

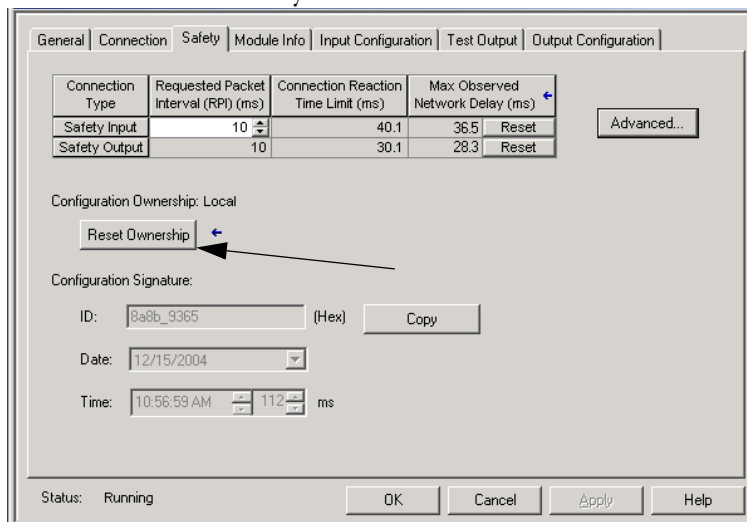
Non posizionare i moduli impostati su valori predefiniti (out of the box) su una rete CIP Safety con la funzione Configure Always abilitata, a meno che non si stia seguendo la presente procedura di sostituzione.

Se nel software RSLogix 5000 la funzione “Configure Always” è abilitata, il controllore verifica e si collega automaticamente a un modulo sostitutivo che soddisfi tutti i seguenti requisiti:

- Il controllore dispone di dati di configurazione per un modulo compatibile nell'indirizzo di rete specificato.
- Il modulo è nelle condizioni predefinite in fabbrica o ha un numero SNN che corrisponde alla configurazione.

Se il progetto è configurato per “Configure Always”, seguire la procedura adeguata per sostituire un modulo POINT Guard I/O.

1. Rimuovere il modulo I/O in uso ed installare quello nuovo.
  - a. Se il modulo è nelle condizioni predefinite in fabbrica, andare al punto 6.  
Non è necessaria alcuna azione da parte del controllore GuardLogix per assumere la proprietà del modulo.
  - b. In caso di errore di mancata corrispondenza del numero SNN, andare al punto successivo per resettare il modulo alle condizioni predefinite in fabbrica.
2. Fare clic con il pulsante destro del mouse sul proprio modulo POINT Guard I/O e selezionare Properties.
3. Fare clic sulla scheda Safety.



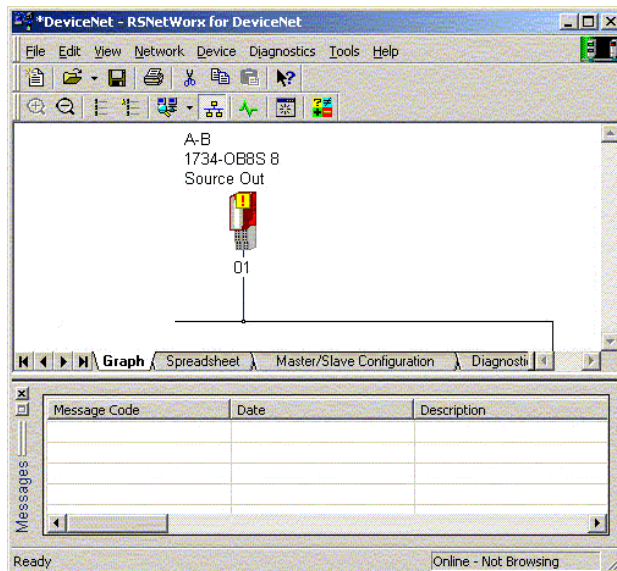
4. Fare clic su Reset Ownership.
5. Fare clic su OK.
6. Seguire le procedure aziendali per il test funzionale del modulo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.

## Sostituzione di un modulo POINT Guard I/O mediante il software RSNetWorx for DeviceNet

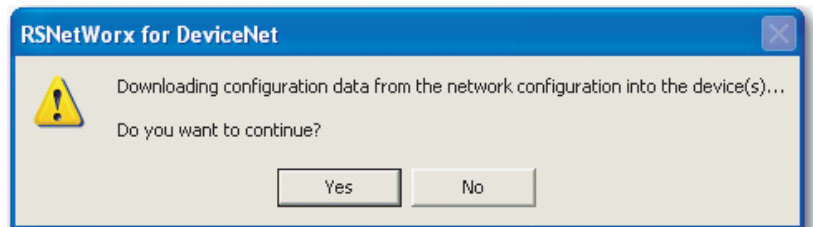
Per sostituire un modulo POINT Guard I/O quando modulo e controllore si trovano una rete DeviceNet, procedere come segue.

1. Sostituire il modulo e far corrispondere il numero di nodo del modulo originale.
2. Nel software RSNetWorx for DeviceNet, aprire il progetto.

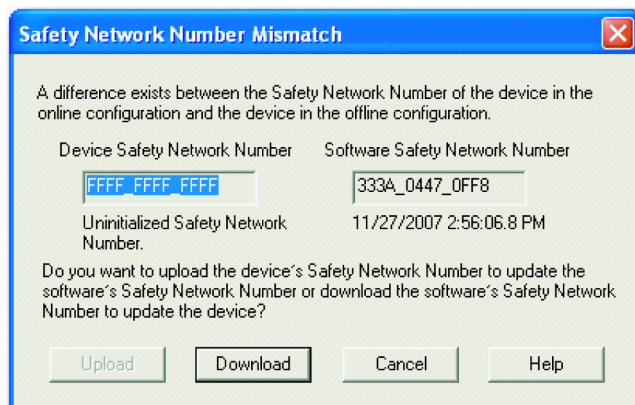
Se è nuovo o ha un numero SNN che non corrisponde a quello del modulo originale, il modulo sostitutivo viene visualizzato con un punto esclamativo.



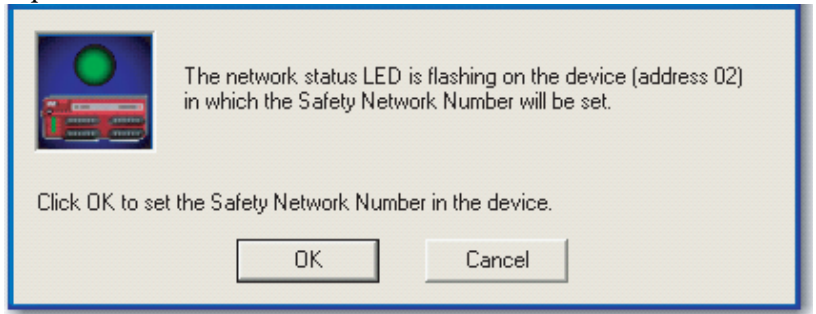
3. Fare clic con il pulsante destro del mouse sul modulo e selezionare Download to Device.



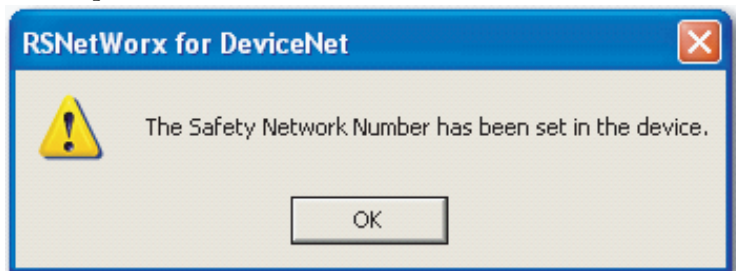
4. Fare clic su Yes per confermare.
5. Fare clic su Download nella finestra di dialogo Safety Network Number Mismatch per impostare il numero SNN sul modulo sostitutivo.



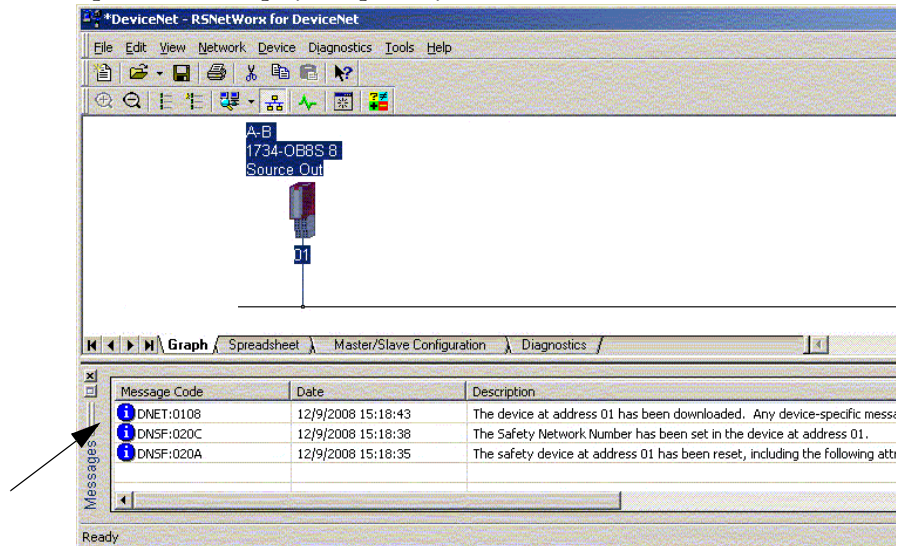
- Verificare che l'indicatore dello stato della rete (NS) lampeggi sul modulo corretto e fare clic su OK per impostare il numero SNN su quel dispositivo.



Il software RSNetWorx for DeviceNet conferma che il numero SNN è stato impostato.



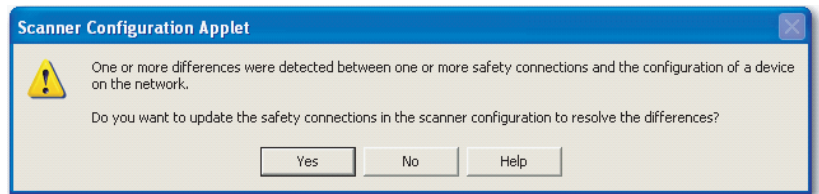
Una volta completato e riuscito il download, la vista del progetto principale visualizza questo messaggio: "The device at address xx has been downloaded. Any device-specific messages related to the download operation are displayed separately."



Presumendo che questa sia la configurazione corretta acquisita dal file DNT originale, il numero SNN e l'autenticazione di configurazione ora corrispondono all'originale. Se il controllore è già collegato, viene stabilita una connessione. Il controllore non ha bisogno di uscire dalla modalità Esecuzione per il download nel modulo sostitutivo.

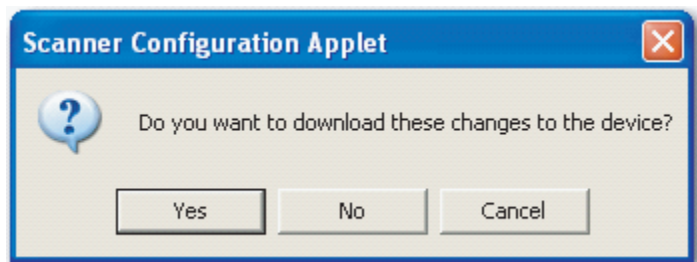
Se si scarica questa configurazione per uso temporaneo, inserire il modulo nella rete ed esso si collega automaticamente al controllore.

Se la configurazione scaricata nel modulo non proviene dal file DNT originale, l'autenticazione di configurazione non corrisponderà all'originale. Anche se si ricreano gli stessi parametri in un nuovo file DNT, le parti relative ad ora e data dell'autenticazione saranno diverse e la connessione al controllore non avviene. In tal caso, fare clic sulla scheda Safety Connection del controllore che ha segnalato la diversa autenticazione di configurazione e che offre la possibilità di far corrispondere la nuova autenticazione di configurazione. Tuttavia, sarebbe prima necessario riconvalidare il sistema di sicurezza perché non sta usando il file DNT originale.



7. Fare clic su Yes.

Questa azione interrompe la modalità Esecuzione del controllore ed invita a scaricare le modifiche.



8. Fare clic su Yes per scaricare la nuova configurazione di connessione nel controllore SmartGuard.

Al termine del download, riportare il controllore in modalità Esecuzione e la connessione al modulo sostitutivo viene stabilita.

9. Seguire le procedure aziendali per il test funzionale del modulo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.



## Sviluppo di applicazioni di sicurezza

Argomento	Pagina
Task di sicurezza	90
Programmi di sicurezza	92
Routine di sicurezza	92
Tag di sicurezza	92
Tag di sicurezza prodotti/consumati	97
Mappatura dei tag di sicurezza	102
Protezione dell'applicazione di sicurezza	105
Restrizioni software	108

In questo capitolo vengono descritti i componenti di un progetto di sicurezza e vengono fornite informazioni relative all'utilizzo delle funzioni che contribuiscono a proteggere l'integrità dell'applicazione di sicurezza, come la firma del task di sicurezza ed il blocco di sicurezza.

Per le regole generali ed i requisiti relativi allo sviluppo ed alla messa in servizio di applicazioni di sicurezza SIL 3 e PLe, consultare la pubblicazione Manuale di riferimento per la sicurezza – Sistemi di controllori GuardLogix, [1756-RM093](#).

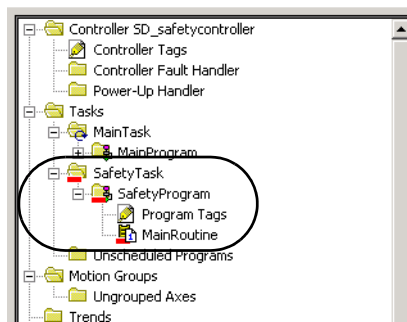
In questo manuale di riferimento per la sicurezza vengono trattati i seguenti argomenti:

- Creazione di una specifica dettagliata del progetto
- Sviluppo, documentazione e collaudo dell'applicazione
- Generazione della firma del task di sicurezza per l'identificazione e la protezione del progetto
- Conferma del progetto mediante la stampa o la visualizzazione del progetto caricato e confronto manuale delle configurazioni, dei dati di sicurezza e della logica del programma di sicurezza
- Verifica del progetto tramite test case, simulazioni, test di verifica funzionale e, se richiesto, una verifica di sicurezza indipendente
- Blocco dell'applicazione di sicurezza
- Calcolo del tempo di risposta del sistema

## Task di sicurezza

Quando viene creato un progetto per il controllore di sicurezza, il software RSLogix 5000 genera automaticamente un task di sicurezza con un programma di sicurezza ed una routine (di sicurezza) principale.

**Figura 23 – Task di sicurezza nell’organizer del controllore**



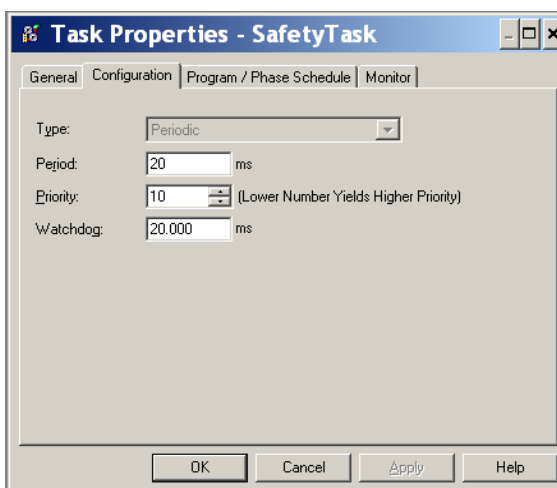
All’interno del task di sicurezza, è possibile utilizzare diversi programmi di sicurezza, costituiti da più routine di sicurezza. Il controllore GuardLogix supporta un task di sicurezza. Il task di sicurezza non può essere eliminato.

Inoltre, non è possibile schedulare programmi standard o eseguire routine standard all’interno del task di sicurezza.

## Definizione del periodo del task di sicurezza

Il task di sicurezza è un task periodico. La priorità del task ed il tempo del watchdog vengono specificati nella finestra di dialogo Task Properties – Safety Task. Per accedere alla finestra di dialogo, fare clic con il pulsante destro del mouse sul task di sicurezza e selezionare Properties.

**Figura 24 – Configurazione del periodo del task di sicurezza**



Il task di sicurezza deve avere una priorità alta. L'utente deve specificare il periodo ed il watchdog del task di sicurezza (entrambi in ms). Il periodo del task di sicurezza è il periodo in cui viene eseguito il task di sicurezza. Il watchdog del task di sicurezza è il tempo massimo consentito per l'esecuzione del task, dall'avvio fino al completamento.

Il periodo del task di sicurezza è limitato ad un massimo di 500 ms e non può essere modificato in modalità online. Accertarsi che il task di sicurezza possa completare l'esecuzione logica prima dell'attivazione successiva. Se si verifica un timeout del watchdog del task di sicurezza, viene generato un errore di sicurezza irreversibile nel controllore di sicurezza.

Il periodo del task di sicurezza influisce direttamente sul tempo di risposta del sistema.

La pubblicazione Manuale di riferimento per la sicurezza – Sistemi di controllori GuardLogix, [1756-RM093](#), contiene informazioni dettagliate sul calcolo del tempo di risposta del sistema.

## **Esecuzione del task di sicurezza**

Il task di sicurezza viene eseguito allo stesso modo di un task periodico standard, con le seguenti eccezioni:

- L'esecuzione del task di sicurezza non inizia finché il controllore primario ed il coprocessore di sicurezza non stabiliscono la relazione di controllo. (I task standard, tuttavia, vengono eseguiti non appena il controllore passa in modalità Esecuzione).
- Tutti i tag di ingresso di sicurezza (immessi, consumati e mappati) vengono aggiornati e bloccati all'inizio dell'esecuzione del task di sicurezza.

Per informazioni sulla mappatura dei tag di sicurezza, vedere a pagina [102](#).

- I valori dei tag di uscita di sicurezza (emessi e prodotti) vengono aggiornati alla conclusione dell'esecuzione del task di sicurezza.

## Programmi di sicurezza

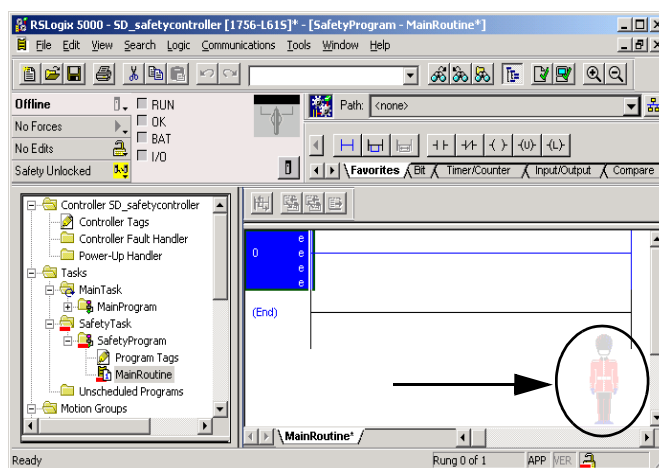
I programmi di sicurezza possiedono tutti gli attributi dei programmi standard, con l'eccezione che è possibile schedarli solo nel task di sicurezza e possono contenere solo componenti di sicurezza. I programmi di sicurezza possono includere solo routine di sicurezza, una delle quali deve essere designata come routine principale ed una come routine di errore.

I programmi di sicurezza non possono contenere routine o tag standard.

## Routine di sicurezza

Le routine di sicurezza possiedono tutti gli attributi delle routine standard, ma possono esistere esclusivamente all'interno di un programma di sicurezza. Attualmente, per le routine di sicurezza è possibile utilizzare solo il linguaggio ladder.

**SUGGERIMENTO** Il software RSLogix 5000 utilizza una filigrana per distinguere visivamente le routine di sicurezza da quelle standard.



## Tag di sicurezza

Un tag è l'area della memoria di un controllore in cui vengono memorizzati i dati. I tag rappresentano il meccanismo di base per l'allocazione della memoria, per la creazione di riferimenti dei dati per la logica e per il monitoraggio dei dati. I tag di sicurezza possiedono tutti gli attributi dei tag standard con l'aggiunta di meccanismi certificati per garantire l'integrità dei dati SIL 3.

Al momento della creazione, al tag vengono assegnate le seguenti proprietà:

- Name
- Description (facoltativa)
- Tag type
- Data Type
- Scope
- Class
- Style
- External Access

È inoltre possibile specificare se il valore del tag deve essere una costante.

Per creare un tag di sicurezza, aprire la finestra di dialogo New Tag facendo clic con il pulsante destro del mouse su Controller Tags o Program Tags e selezionare New Tag.

**Figura 25 – Creazione di un nuovo tag**

## Tag type

La [Tabella 25](#) definisce i quattro possibili tipi di tag: base, alias, produced e consumed.

**Tabella 25 – Quattro tipi di tag**

Tipo di tag	Descrizione
Base	I tag di base memorizzano i valori che la logica deve utilizzare all'interno del progetto.
Alias	Un tag che fa riferimento ad un altro tag. Un tag alias può fare riferimento ad un altro tag alias o ad un tag base. Un tag alias può fare riferimento anche al componente di un altro tag, tramite il riferimento al membro di una struttura, all'elemento di una matrice o ad un bit incluso in un tag o in un membro. <b>IMPORTANTE:</b> nelle applicazioni di sicurezza non è consentita la creazione di alias tra tag standard e tag di sicurezza. Al contrario, i tag standard possono essere mappati ai tag di sicurezza mediante la mappatura dei tag di sicurezza. Vedere <a href="#">Mappatura dei tag di sicurezza a pagina 102</a> .
Prodotto	Il tag prodotto è un tag del controllore che può essere utilizzato anche da altri controllori. I dati possono essere consumati (ricevuti) contemporaneamente da un massimo di 15 controllori. Un tag prodotto invia i propri dati ad uno o più tag consumatori senza usare la logica. I dati del tag prodotto vengono inviati in base all'intervallo RPI (Requested Packet Interval, intervallo di pacchetti richiesto) del tag consumatore.
Consumato	Un tag consumato è un tag che riceve i dati da un tag prodotto. Il tipo di dati del tag consumato deve corrispondere al tipo di dati del tag prodotto. L'intervallo di pacchetto richiesto (RPI) del tag consumato determina il periodo di aggiornamento dei dati.

## Data Type

Il tipo di dati permette di definire il tipo di dati memorizzati nel tag, ad esempio bit o numeri interi.

I tipi di dati possono essere combinati per formare delle strutture. Una struttura è caratterizzata da un tipo di dati univoco corrispondente ad un'esigenza specifica. All'interno di una struttura, ciascun tipo di dati viene definito membro. Analogamente ai tag, ai membri vengono associati un nome ed un tipo di dati. È possibile creare strutture personalizzate come tipi di dati definiti dall'utente.

I controllori Logix contengono tipi di dati predefiniti da utilizzare con istruzioni specifiche.

Per i tag di sicurezza sono ammessi solo i seguenti tipi di dati.

**Tabella 26 – Tipi di dati validi per i tag di sicurezza**

AUX_VALVE_CONTROL	DCI_STOP_TEST_MUTE	MANUAL_VALVE_CONTROL
BOOL	DINT	MUTING_FOUR_SENSOR_BIDIR
CAM_PROFILE	DIVERSE_INPUT	MUTING_TWO_SENSOR_ASYM
CAMSHAFT_MONITOR	EIGHT_POS_MODE_SELECTOR	MUTING_TWO_SENSOR_SYM
CB_CONTINUOUS_MODE	EMERGENCY_STOP	MOTION_INSTRUCTION
CB_CRANKSHAFT_POS_MONITOR	ENABLE_PENDANT	PHASE
CB_INCH_MODE	EXT_ROUTINE_CONTROL	PHASE_INSTRUCTION
CB_SINGLE_STROKE_MODE	EXT_ROUTINE_PARAMETERS	REDUNDANT_INPUT
CONFIGURABLE_ROUT	FBD_BIT_FIELD_DISTRIBUTE	REDUNDANT_OUTPUT
CONNECTION_STATUS	FBD_CONVERT	SAFETY_MAT
CONTROL	FBD_COUNTER	SERIAL_PORT_CONTROL
COUNTER	FBD_LOGICAL	SFC_ACTION
DCA_INPUT	FBD_MASK_EQUAL	SFC_STEP
DCAF_INPUT	FBD_MASKED_MOVE	SFC_STOP
DCI_MONITOR	FBD_TIMER	SINT
DCI_START	FIVE_POS_MODE_SELECTOR	STRING
DCI_STOP	INT	THRS_ENHANCED
DCI_STOP_TEST	LIGHT_CURTAIN	TIMER
DCI_STOP_TEST_LOCK	MAIN_VALVE_CONTROL	TWO_HAND_RUN_STATION

I tipi di dati REAL sono validi nei progetti dei controllori 1756-L7xS, ma non sono validi nei progetti dei controllori 1756-L6xS o 1768-L4xS.

### IMPORTANTE

La restrizione include i tipi di dati definiti dall'utente che contengono tipi di dati predefiniti.

## Scope

L'ambito di un tag determina il punto in cui è possibile accedere ai dati del tag. Al momento della creazione, un tag viene definito come tag del controllore (dati globali) o tag del programma per un programma di sicurezza o standard specifico (dati locali). I tag di sicurezza possono essere definiti nell'ambito del controllore o del programma di sicurezza.

### *Tag del controllore*

Se i tag di sicurezza vengono inclusi nell'ambito del controllore, tutti i programmi possono accedere ai dati di sicurezza. I tag devono essere definiti nell'ambito del controllore se utilizzati nei seguenti casi:

- Per più programmi del progetto
- Per produrre o consumare dati
- Per la comunicazione con l'interfaccia operatore di un terminale PanelView
- Per la mappatura dei tag di sicurezza  
Per ulteriori informazioni, vedere [Mappatura dei tag di sicurezza a pagina 102](#).

I tag di sicurezza dell'ambito del controllore possono essere letti dalle routine standard, ma non consentono la scrittura.

---

**IMPORTANTE** I tag di sicurezza dell'ambito del controllore possono essere letti da qualsiasi routine standard. La frequenza di aggiornamento dei tag di sicurezza si basa sul periodo del task di sicurezza.

---

I tag associati ai dati di sicurezza prodotti o consumati ed agli I/O di sicurezza devono essere necessariamente tag di sicurezza dell'ambito del controllore. Per i tag di sicurezza prodotti/consumati, è necessario creare un tipo di dati definito dall'utente ed il primo membro della struttura di tag deve essere riservato allo stato della connessione. Tale membro è un tipo di dato predefinito denominato CONNECTION\_STATUS.

**Tabella 27 – Ulteriori riferimenti**

Riferimento	Descrizione
<a href="#">Connessioni di sicurezza</a> a pagina 127	Fornisce ulteriori informazioni sul membro CONNECTION_STATUS
Manuale di programmazione Dati I/O e tag dei controllori Logix5000, pubblicazione <a href="#">1756-PM004</a>	Fornisce istruzioni per la creazione di tipi di dati definiti dall'utente

### *Tag definiti nell'ambito del programma*

Se i tag vengono definiti nell'ambito del programma, i dati non sono accessibili da altri programmi. Il riutilizzo di nomi di tag definiti nell'ambito di un programma è consentito in programmi diversi.

I tag di sicurezza definiti nell'ambito di un programma di sicurezza possono essere letti o scritti solo da una routine di sicurezza definita nell'ambito dello stesso programma di sicurezza.

## Class

I tag possono essere classificati come tag standard o di sicurezza. I tag classificati come tag di sicurezza devono avere un tipo di dati valido per i tag di sicurezza.

Quando vengono creati tag definiti nell'ambito di un programma, la classe viene specificata automaticamente a seconda che il tag sia stato creato in un programma standard o di sicurezza.

La classe dei tag dell'ambito del controllore, invece, deve essere selezionata manualmente.

## Constant Value

Quando un tag viene designato come valore costante, non può essere modificato dalla logica del controllore o da un'applicazione esterna come un pannello operatore. I tag con valori costanti non possono essere forzati.

Il software RSLogix 5000 può modificare i tag standard e di sicurezza con valori costanti, a patto che non sia presente una firma del task di sicurezza. I tag di sicurezza non possono essere modificati se è presente una firma del task di sicurezza.

## External Access

La proprietà External Access definisce il livello di accesso consentito per i dispositivi esterni, ad esempio un pannello operatore, per la visualizzazione o la modifica dei valori dei tag. Questa impostazione non influisce sull'accesso tramite il software RSLogix 5000. Il valore predefinito è lettura/scrittura.

**Tabella 28 – Livelli di External Access**

Impostazione di External Access	Descrizione
None	I tag non sono accessibili dall'esterno del controllore.
Read Only	È possibile selezionare o leggere i tag ma non scriverli dall'esterno del controllore.
Read/Write	È possibile selezionare o leggere i tag standard e scriverli dall'esterno del controllore.

Nel caso dei tag alias, il tipo di accesso esterno corrisponde al tipo configurato per il tag di destinazione base.



## Tag di sicurezza prodotti/ consumati

Per trasferire i dati di sicurezza tra controllori GuardLogix, si utilizzano tag di sicurezza prodotti e consumati. I tag prodotti e consumati richiedono connessioni. Il tipo di connessione di default per i tag prodotti e consumati è unicast nel software RSLogix 5000 versione 19 e successive.

**Tabella 29 – Connessioni prodotte e consumate**

Tag	Descrizione della connessione
Prodotto	Un controllore GuardLogix può produrre (inviare) tag di sicurezza verso altri controllori GuardLogix 1756 o 1768. Il controllore produttore utilizza un'unica connessione per ciascun consumatore.
Consumato	I controllori GuardLogix possono consumare (ricevere) tag di sicurezza da altri controllori GuardLogix 1756 o 1768. Ciascun tag consumato consuma una connessione.

I tag di sicurezza prodotti e consumati sono soggetti alle seguenti restrizioni:

- Solo i tag di sicurezza definiti nell'ambito controllore possono essere condivisi.
- La dimensione dei tag di sicurezza prodotti e consumati è limitata a 128 byte.
- Le coppie di tag prodotti/consumati devono essere dello stesso tipo di dati definito dall'utente.
- Il primo membro del tipo di dati definito dall'utente deve essere il tipo di dati predefinito CONNECTION\_STATUS.
- L'intervallo di pacchetto richiesto (RPI, Requested Packet Interval) del tag di sicurezza consumato deve corrispondere al periodo del task di sicurezza del controllore GuardLogix produttore.

Per configurare correttamente i tag di sicurezza prodotti e consumati per la condivisione dei dati tra controllori di sicurezza peer, è necessario configurare correttamente i controllori di sicurezza peer, produrre un tag di sicurezza e consumare un tag di sicurezza, come descritto di seguito.

## Configurazione dei numeri di rete di sicurezza dei controllori di sicurezza peer

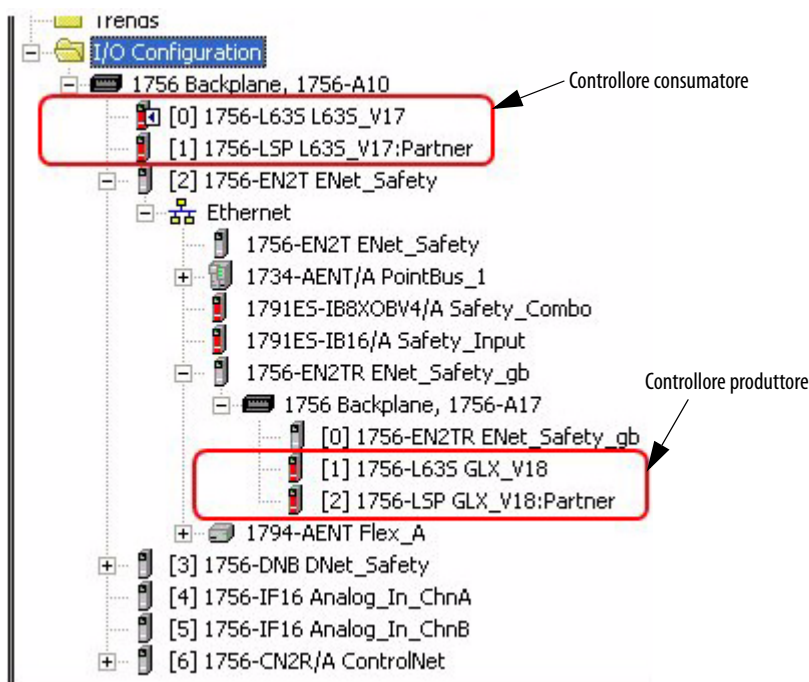
Il controllore di sicurezza peer è soggetto agli stessi requisiti di configurazione del controllore di sicurezza locale. Il controllore di sicurezza peer deve inoltre essere dotato di un numero di rete di sicurezza (SNN). Il valore SNN del controllore di sicurezza peer varia in base al relativo posizionamento nel sistema.

**Tabella 30 – SNN e posizione del controllore**


Posizione del controllore di sicurezza peer	SNN
Collocato nello chassis locale	I controllori GuardLogix collocati in uno chassis comune devono avere lo stesso valore SNN.
Collocato in un altro chassis	Il controllore deve avere un valore SNN univoco.

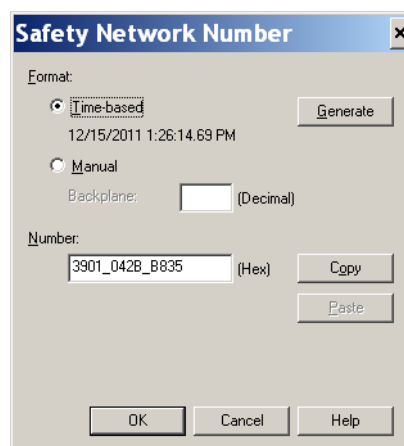
Per copiare ed incollare il numero SNN, procedere come segue.

1. Aggiungere il controllore produttore all'albero I/O del controllore consumatore.



2. Nel progetto del controllore produttore, fare clic con il pulsante destro del mouse sul controllore produttore e selezionare Controller Properties.
3. Copiare il numero SNN del controllore produttore.

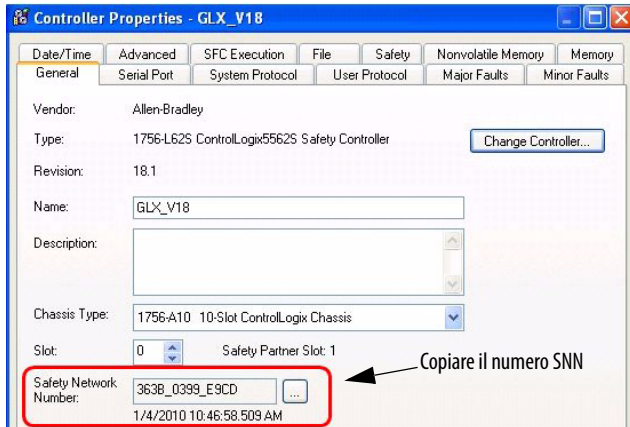
**SUGGERIMENTO** Un valore SNN può essere copiato ed incollato mediante i pulsanti della finestra di dialogo Safety Network Number. Aprire le rispettive finestre di dialogo Safety Network Number facendo clic su  a destra dei campi SNN nelle finestre di dialogo delle proprietà.



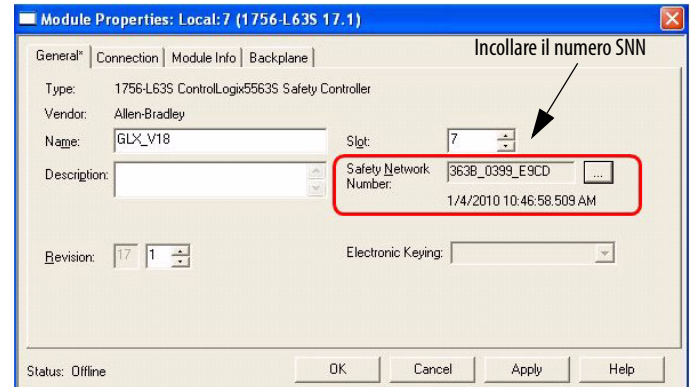
4. Nel progetto del controllore consumatore, fare clic con il pulsante destro del mouse sul controllore produttore e selezionare Module Properties.

## 5. Incollare il numero SNN del controllore produttore nel campo SNN.

### Finestra di dialogo Controller Properties del produttore nel progetto del produttore



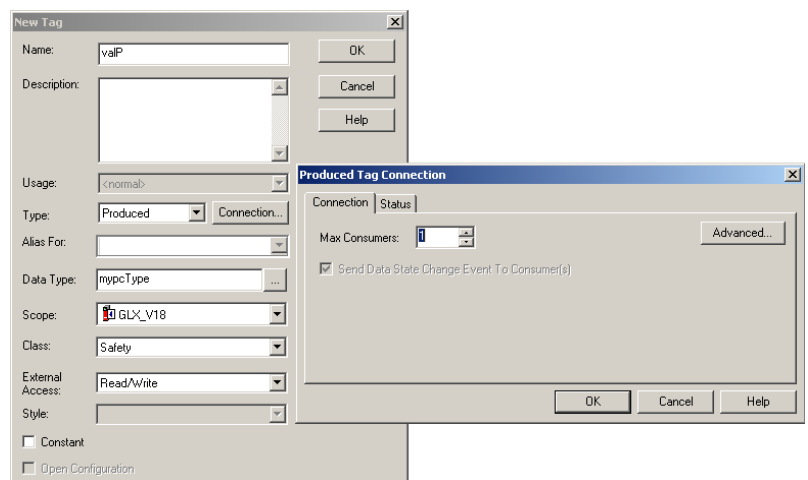
### Finestra di dialogo Module Properties nel progetto del consumatore



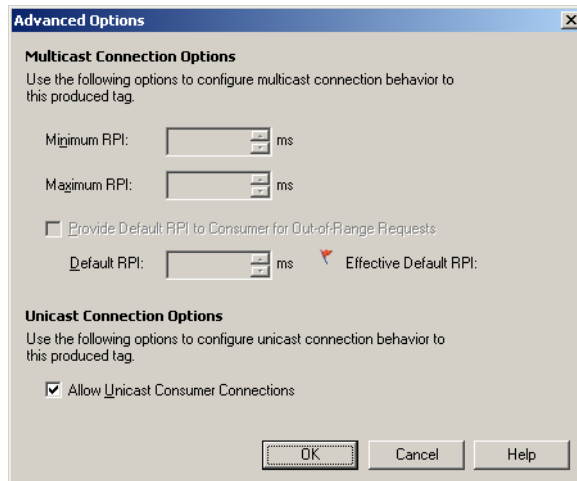
## Produzione di un tag di sicurezza

Per produrre un tag di sicurezza, attenersi alla seguente procedura.

1. Nel progetto del controllore produttore, creare un tipo di dati definito dall'utente per definire la struttura dei dati da produrre.  
Assicurarsi che il primo membro dei dati abbia CONNECTION\_STATUS come tipo di dati.
2. Fare clic con il pulsante destro del mouse su Controller Tags e selezionare New Tag.
3. Impostare il tipo su Produced, la classe su Safety ed il tipo di dati sul tipo definito dall'utente e creato al passo 1.
4. Fare clic su Connection ed inserire il numero di consumatori.



5. Fare clic su Advanced se si desidera cambiare il tipo di connessione deselectando “Allow Unicast Consumer Connections”.



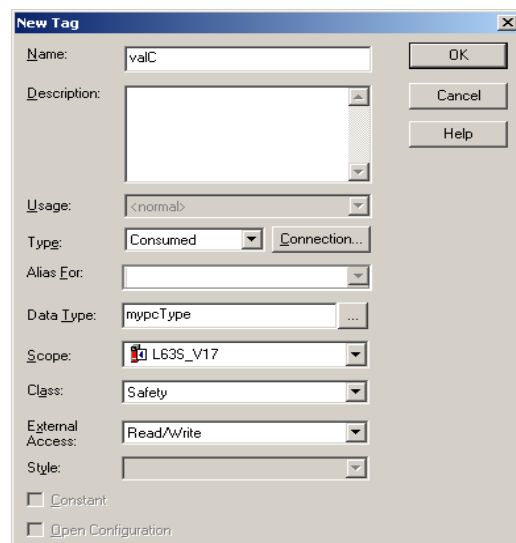
6. Fare clic su OK.

## Consumo di dati di tag di sicurezza

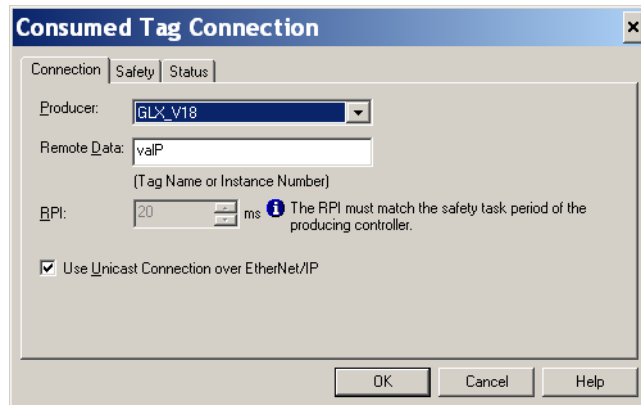
Per consumare i dati prodotti da un altro controllore, attenersi ai seguenti punti.

1. Nel progetto del controllore consumatore, creare un tipo di dati definito dall'utente identico a quello creato nel progetto del produttore.
 

**SUGGERIMENTO** Il tipo di dati definito dall'utente può essere copiato dal progetto del produttore ed incollato nel progetto del consumatore.
2. Fare clic con il pulsante destro del mouse su Controller Tags e selezionare New Tag.
3. Impostare il tipo su Consumed, la classe su Safety ed il tipo di dati sul tipo definito dall'utente e creato al passo 1.



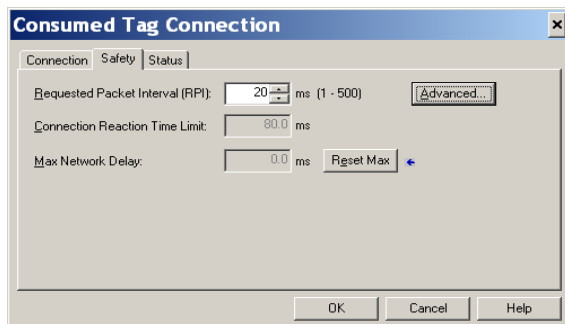
- Fare clic su Connection per aprire la finestra di dialogo Consumed Tag Connection.



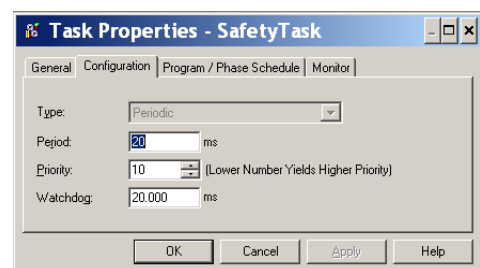
- Selezionare il controllore che produce i dati.
- Immettere il nome del tag prodotto.
- Fare clic sulla scheda Safety.
- Inserire l'intervallo di pacchetto richiesto (RPI) per la connessione mediante incrementi di 1 ms.

Il valore predefinito è 20 ms.

**Progetto del consumatore**



**Progetto del produttore**

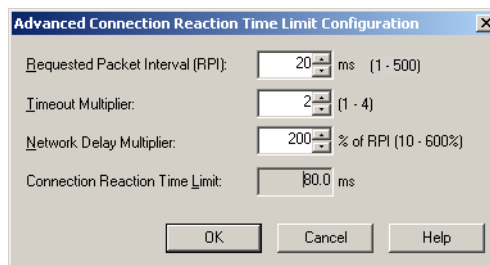


L'RPI specifica l'intervallo di aggiornamento dei dati durante la connessione. L'intervallo RPI del tag di sicurezza consumato deve essere identico al periodo del task di sicurezza del progetto di sicurezza produttore.

Il Connection Reaction Time Limit (tempo limite di risposta della connessione) è la durata massima dei pacchetti di sicurezza sulla connessione associata. Per semplici requisiti di temporizzazione, è possibile regolare l'intervallo RPI per ottenere un tempo limite di risposta della connessione accettabile.

Il parametro Max Network Delay corrisponde al massimo ritardo di trasferimento osservato dal momento in cui i dati sono stati prodotti fino al momento in cui sono stati ricevuti. Se si è online, è possibile azzerare il parametro Max Network Delay facendo clic su Reset Max.

9. Se il tempo Connection Reaction Time Limit è accettabile, fare clic su OK; per requisiti più complessi, fare clic su Advanced per impostare i parametri di Advanced Connection Reaction Time Limit.



Il parametro Timeout Multiplier determina il numero di RPI di attesa di un pacchetto prima di dichiarare il timeout della connessione.

Il parametro Network Delay Multiplier definisce il tempo di trasferimento del messaggio applicato dal protocollo CIP Safety. Esso specifica il ritardo del percorso produttore-consumatore-produttore. È possibile utilizzare Network Delay Multiplier per aumentare o ridurre il Connection Reaction Time Limit.

**Tabella 31 – Ulteriori riferimenti**

Riferimento	Descrizione
Pagine <a href="#">71...75</a>	Fornisce ulteriori informazioni sull'impostazione dell'RPI e sulla comprensione della modalità con cui i parametri Max. Network Delay, Timeout Multiplier e Network Delay Multipliers influiscono sul tempo di risposta della connessione
<a href="#">Capitolo 9</a>	Contiene ulteriori informazioni sul tipo di dati predefinito CONNECTION_STATUS
Manuale di programmazione Tag prodotti e consumati dei controllori Logix5000, pubblicazione <a href="#">1756-PM011</a>	Fornisce informazioni dettagliate sull'utilizzo di tag prodotti e consumati

## Mappatura dei tag di sicurezza

L'accesso ai tag standard dell'ambito del controllore non può essere effettuato direttamente con una routine di sicurezza. Per poter utilizzare i dati di tag standard all'interno di routine di task di sicurezza, i controllori GuardLogix dispongono di una funzione di mappatura dei tag di sicurezza che consente di copiare i valori dei tag standard nella memoria dei tag di sicurezza.

## Restrizioni

La mappatura dei tag di sicurezza è soggetta alle seguenti restrizioni:

- La coppia tag di sicurezza-tag standard deve essere definita nell'ambito del controllore.
- I tipi di dati della coppia tag di sicurezza-tag standard devono corrispondere.
- Non è consentito l'uso di tag alias.
- La mappatura deve essere definita per l'intero tag. Ad esempio, non è consentito l'uso di myTimer.pre se myTimer è un tag TIMER.
- Una coppia di mappatura è costituita da un tag standard mappato ad un tag di sicurezza.
- Non è possibile mappare un tag standard ad un tag di sicurezza definito come costante.
- La mappatura di tag non può essere modificata in presenza delle seguenti condizioni:
  - se il progetto è in blocco di sicurezza
  - se esiste una firma del task di sicurezza
  - se il selettore a chiave è in posizione RUN
  - se si è verificato un errore di sicurezza irreversibile
  - se la relazione tra il controllore principale ed il coprocessore di sicurezza non è valida.

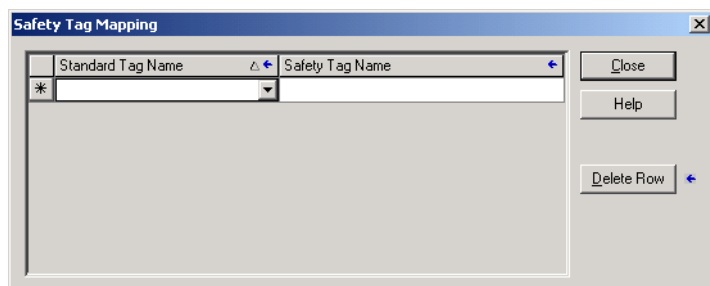


**ATTENZIONE:** durante l'utilizzo di dati standard in una routine di sicurezza, l'utente deve predisporre una soluzione affidabile per garantire che i dati siano utilizzati in modo adeguato. L'utilizzo di dati standard in un tag di sicurezza non li rende dati di sicurezza. Non si può controllare direttamente un'uscita di sicurezza SIL 3/PLe con i dati di tag standard.

Per ulteriori informazioni, consultare la pubblicazione Manuale di riferimento per la sicurezza – Sistemi di controllori GuardLogix, [1756-RM093](#).

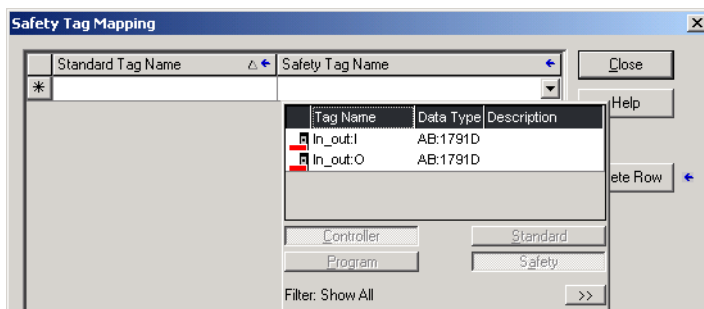
## Creazione di coppie di mappatura di tag

1. Per accedere alla finestra di dialogo Safety Tag Mapping, selezionare Map Safety Tags dal menu Logic.



2. Aggiungere un tag esistente nella colonna Standard Tag Name or Safety Tag Name digitando il nome del tag nella cella o selezionando un tag dal menu a tendina.

Fare clic sulla freccia per visualizzare una finestra di dialogo di esplorazione dei tag filtrati. Nella colonna Standard Tag Name sono visualizzati solo tag standard dell'ambito del controllore. Nella colonna Safety Tag Name sono visualizzati solo tag di sicurezza dell'ambito del controllore.



3. Aggiungere un nuovo tag nella colonna Standard Tag Name o Safety Tag Name facendo clic con il pulsante destro del mouse nella cella vuota, selezionando New Tag e digitando il nome del tag nella cella.
4. Fare clic con il pulsante destro del mouse nella cella e selezionare New tagname, dove tagname corrisponde al testo digitato nella cella.

### Controllo dello stato della mappatura dei tag

Nell'ultima colonna a sinistra della finestra di dialogo Safety Tag Mapping è indicato lo stato della coppia mappata.

Tabella 32 – Icone dello stato di mappatura dei tag

Contenuto della cella	Descrizione
Vuota	La mappatura dei tag è valida.
	Durante il funzionamento offline, l'icona raffigurante una X indica che la mappatura dei tag non è valida. È possibile spostarsi su una nuova riga o chiudere la finestra di dialogo Safety Tag Mapping. <sup>(1)</sup> Durante il funzionamento online, una mappa di tag non valida causa un messaggio d'errore in cui viene indicato il motivo per il quale l'associazione non è valida. Non è possibile spostarsi su un'altra riga o chiudere la finestra di dialogo Safety Tag Mapping nel caso in cui sia presente un errore di mappatura dei tag.
	Indica la riga attiva.
	Indica la riga Create New Mapped Tag.
	Indica una modifica in sospeso.

(1) La mappatura dei tag viene controllata anche durante la verifica del progetto. La presenza di una mappatura di tag non valida causa un errore di verifica del progetto.

Per ulteriori informazioni, vedere le restrizioni relative alla mappatura dei tag a pagina [103](#).



## Protezione dell'applicazione di sicurezza

Per proteggere il programma applicativo da modifiche non autorizzate è possibile attivare il blocco di sicurezza del controllore e generare e registrare la firma del task di sicurezza.

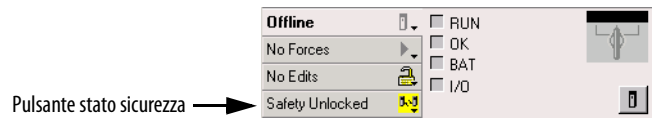
### Blocco di sicurezza del controllore

Il controllore GuardLogix può essere impostato in blocco di sicurezza allo scopo di impedire modifiche ai componenti di controllo correlati alla sicurezza. La funzione di blocco di sicurezza può essere utilizzata solo con i componenti di sicurezza, come il task di sicurezza, i programmi di sicurezza, le routine di sicurezza, le istruzioni add-on di sicurezza, i tag di sicurezza, l'I/O di sicurezza e la firma del task di sicurezza.



Quando il controllore è in blocco di sicurezza, non è possibile eseguire le operazioni indicate di seguito nella sezione dell'applicazione riservata alla sicurezza:

- Programmazione o modifica online/offline (incluse le istruzioni add-on di sicurezza)
- Forzatura degli I/O di sicurezza
- Modifica dello stato di inibizione degli I/O di sicurezza o delle connessioni prodotte
- Manipolazione dei dati di sicurezza (ad eccezione della logica delle routine di sicurezza)
- Generazione o eliminazione della firma del task di sicurezza

**SUGGERIMENTO** Il testo relativo al pulsante dello stato di sicurezza sulla barra di stato indica lo stato del blocco di sicurezza.



Nella barra delle applicazioni vengono inoltre visualizzate le icone riportate di seguito ad indicare lo stato di blocco di sicurezza del controllore di sicurezza.

-  = controllore in blocco di sicurezza
-  = controllore non in blocco di sicurezza

È possibile impostare il blocco di sicurezza del progetto del controllore indipendentemente dalla modalità di funzionamento (online o offline) e a prescindere dalla disponibilità del sorgente del programma, purché non siano presenti forzature di sicurezza o modifiche di sicurezza online in sospeso.

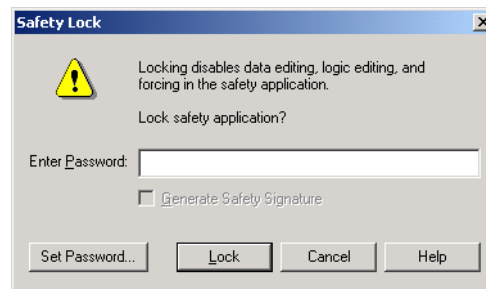
Lo stato in blocco di sicurezza o sblocco di sicurezza non può essere modificato se il selettore a chiave è in posizione RUN.

**SUGGERIMENTO** Le azioni di attivazione e disattivazione del blocco di sicurezza vengono incluse nel registro del controllore.

Per ulteriori informazioni sulla consultazione del registro del controllore, consultare il manuale di programmazione Controllori Logix5000 – Informazioni e stato, pubblicazione [1756-PM015](#).

È possibile attivare e disattivare il blocco di sicurezza del controllore mediante la scheda Safety della finestra di dialogo Controller Properties oppure selezionando Tools>Safety>Safety Lock/Unlock.

**Figura 26 – Blocco di sicurezza del controllore**



Se la funzione di blocco di sicurezza viene utilizzata tramite l’inserimento di una password, occorre inserirla nel campo Enter Password. In caso contrario, fare clic su Lock.

Nella finestra di dialogo Safety Lock è inoltre possibile impostare o modificare la password. Vedere a pagina [49](#).

La funzione di blocco di sicurezza descritta in questa sezione e le funzioni di sicurezza standard di RSLogix possono essere utilizzate per applicazioni relative al controllore GuardLogix.

Per informazioni sulle funzioni di sicurezza di RSLogix 5000, consultare la pubblicazione Logix5000 Controllers Security Programming Manual, [1756-PM016](#).

## Generazione di una firma del task di sicurezza

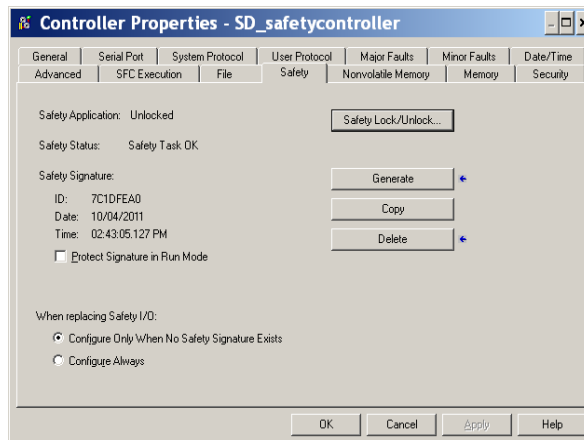
Prima di eseguire il test di verifica, è necessario generare la firma del task di sicurezza. La firma del task di sicurezza può essere generata solo se si è online, con il controllore GuardLogix non in blocco di sicurezza in modalità Programmazione e se non sono presenti forzature di sicurezza, modifiche online di sicurezza in sospenso o errori di sicurezza. Lo stato di sicurezza deve essere Safety Task OK.

Inoltre, è impossibile generare una firma del task di sicurezza se il controllore è in modalità Esecuzione con la protezione della modalità Esecuzione abilitata.

**SUGGERIMENTO** Per visualizzare lo stato di sicurezza corrente, utilizzare il pulsante di stato di sicurezza sulla barra online (vedere a pagina [126](#)) oppure accedere alla scheda Safety nella finestra di dialogo Controller Properties come mostrato a pagina [107](#).

La firma del task di sicurezza può essere generata mediante la scheda Safety della finestra di dialogo Controller Properties facendo clic su Generate. È anche possibile selezionare Tools>Safety>Generate Signature.

**Figura 27 – Scheda Safety**



Se esiste una firma precedente, viene richiesto di sovrascriverla.

**SUGGERIMENTO** La creazione e l'eliminazione di una firma del task di sicurezza vengono registrate nel registro del controllore.

Per ulteriori informazioni sulla consultazione del registro del controllore, consultare il manuale di programmazione Controllori Logix5000 – Informazioni e stato, pubblicazione [1756-PM015](#).

Se è presente una firma del task di sicurezza, non è possibile eseguire le seguenti azioni nella sezione relativa alla sicurezza dell'applicazione:

- Programmazione o modifica online/offline (incluse istruzioni add-on di sicurezza).
- Forzatura degli I/O di sicurezza
- Modifica dello stato di inibizione degli I/O di sicurezza o dei controllori produttori
- Manipolazione dei dati di sicurezza (ad eccezione della logica delle routine di sicurezza)

#### *Copia della firma del task di sicurezza*

È possibile utilizzare il pulsante Copy per creare un record della firma del task di sicurezza da utilizzare per la documentazione, il confronto e la convalida di un progetto di sicurezza. Fare clic su Copy per copiare i componenti ID, Date e Time negli Appunti di Windows.

### Eliminazione della firma del task di sicurezza

Fare clic su Delete per eliminare la firma del task di sicurezza. La firma del task di sicurezza non può essere eliminata nei seguenti casi:

- Il controllore è in blocco di sicurezza.
- Il controllore è in modalità Esecuzione con il selettore a chiave su RUN.
- Il controllore è in modalità Esecuzione o Esecuzione remota con la protezione della modalità di esecuzione abilitata.



**ATTENZIONE:** Se si elimina la firma del task di sicurezza, occorre testare e convalidare nuovamente il sistema per verificarne la conformità a SIL 3/PLe. Per ulteriori informazioni sui requisiti SIL 3/PLe, consultare la pubblicazione Manuale di riferimento per la sicurezza – Sistemi di controllori GuardLogix, [1756-RM093](#).

## Restrizioni software

Le restrizioni che limitano la disponibilità di alcune voci di menu e funzioni (ossia le funzioni Taglia, Incolla, Elimina, Trova e sostituisci) sono imposte dal software di programmazione allo scopo di proteggere da modifiche i componenti preposti alla sicurezza nei seguenti casi:

- Il controllore è in blocco di sicurezza.
- Esiste una firma del task di sicurezza.
- Sono presenti errori di sicurezza.
- Lo stato di sicurezza è uno dei seguenti:
  - Coprocessore mancante
  - Coprocessore non disponibile
  - Hardware incompatibile
  - Firmware incompatibile

Se si verifica anche solo una di queste condizioni, non è possibile:

- Creare o modificare gli oggetti di sicurezza, ivi compresi programmi di sicurezza, routine di sicurezza, tag di sicurezza, istruzioni Add-on di sicurezza e moduli I/O di sicurezza.

---

**IMPORTANTE** I tempi di scansione del task e dei programmi di sicurezza possono essere reimpostati in modalità online.

---

- Applicare forzature ai tag di sicurezza.
- Creare nuove mappature dei tag di sicurezza.
- Modificare o eliminare mappature di tag.
- Modificare o eliminare tipi di dati definiti dall'utente utilizzati dai tag di sicurezza.
- Modificare il nome, la descrizione, il tipo di chassis e lo slot del controllore ed il Numero Rete di Sicurezza (SNN).
- Modificare o eliminare la firma del task di sicurezza mentre è attivo il blocco di sicurezza.

## Collegamento online con il controllore

Argomento	Pagina
Connessione del controllore alla rete	109
Analisi dei fattori che influiscono sul collegamento online	111
Download	113
Upload	115
Collegamento online	116

### Connessione del controllore alla rete

Connettere il controllore alla rete, se non è stato fatto.

**Tabella 33 – Connessioni di comunicazione**

Per questo tipo di connessione	Usare	Vedere
Seriale	Cavo 1756-CP3 o 1747-CP3	<a href="#">Collegamento alla porta seriale del controllore 1756-L6xS a pagina 37</a>
USB	Cavo USB 2.0	<a href="#">Collegamento alla porta USB del controllore 1756-L7xS a pagina 35</a>
EtherNet/IP	Modulo EtherNet/IP in uno slot libero nello stesso chassis del controllore	<a href="#">Connessione del dispositivo EtherNet/IP e del computer a pagina 110</a>
DeviceNet	Modulo 1756-DNB in uno slot libero nello stesso chassis del controllore	<a href="#">Connessione del modulo di comunicazione ControlNet o dello scanner DeviceNet e del computer a pagina 110</a>
ControlNet	Modulo 1756-CN2 in uno slot libero nello stesso chassis del controllore	<a href="#">Connessione del modulo di comunicazione ControlNet o dello scanner DeviceNet e del computer a pagina 110</a>

## Connessione del dispositivo EtherNet/IP e del computer

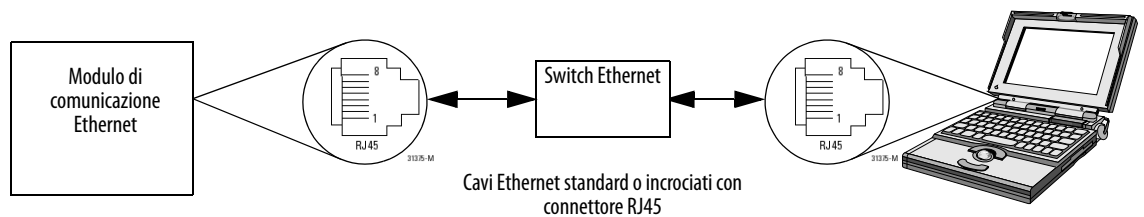


**AVVISO:** Se si connette o disconnette il cavo di comunicazione con il modulo o qualsiasi dispositivo sulla rete alimentato, può verificarsi un arco elettrico, che può causare esplosioni in installazioni che si trovano in aree pericolose.

Prima di procedere, assicurarsi di aver tolto alimentazione o che l'area non sia pericolosa.

Connettere il dispositivo EtherNet/IP ed il computer utilizzando un cavo Ethernet.

Figura 28 – Connessioni Ethernet



## Connessione del modulo di comunicazione ControlNet o dello scanner DeviceNet e del computer

Per accedere alla rete ControlNet o DeviceNet, è possibile scegliere tra le due opzioni seguenti:

- Eseguire la connessione direttamente alla rete.
- Eseguire la connessione ad una rete seriale o EtherNet/IP e passare (ponte) alla rete richiesta. Per eseguire questa operazione, non è necessaria programmazione aggiuntiva.

## Configurazione di un driver EtherNet/IP, ControlNet o DeviceNet

Per informazioni sulla configurazione di un driver, consultare la pubblicazione appropriata:

- EtherNet/IP Modules in Logix5000 Control Systems, pubblicazione [ENET-UM001](#)
- Manuale dell'utente ControlNet Modules in Logix5000 Control Systems, pubblicazione [CNET-UM001](#)
- DeviceNet Modules in Logix5000 Control Systems, pubblicazione [DNET-UM004](#)

## Analisi dei fattori che influiscono sul collegamento online

Il software RSLogix 5000 determina se è possibile collegarsi online con un controllore di destinazione a seconda che il progetto offline sia nuovo o siano state apportate modifiche. Se il progetto è nuovo, è necessario prima scaricarlo nel controllore. Se sono state apportate modifiche al progetto, verrà richiesto di effettuare l'upload o il download. Se non sono state apportate modifiche, è possibile collegarsi online per controllare l'esecuzione del progetto.

Diversi fattori influiscono su questi processi, compresa la funzione di corrispondenza tra progetto e controllore, lo stato di sicurezza e gli errori, l'esistenza di una firma del task di sicurezza e lo stato di blocco/sblocco di sicurezza del progetto e del controllore.

### Corrispondenza tra progetto e controllore

La funzione di corrispondenza tra progetto e controllore influisce sui processi di download, upload e collegamento online di progetti standard e di sicurezza.

Se la funzione Project to Controller Match è abilitata nel progetto offline, il software RSLogix 5000 confronta il numero seriale del controllore nel progetto offline con quello del controllore connesso. Se non corrispondono, è necessario annullare il download/l'upload, eseguire la connessione al controllore corretto, oppure confermare di essere collegati al controllore corretto per aggiornare il numero seriale nel progetto, in modo che corrisponda al controllore di destinazione.

### Corrispondenza della versione del firmware

La corrispondenza della versione del firmware influisce sul processo di download. Se la versione del controllore non corrisponde a quella del progetto, verrà richiesto di aggiornare il firmware del controllore. Il software RSLogix 5000 consente di aggiornare il firmware come parte della sequenza di download.

---

**IMPORTANTE** Per aggiornare il firmware del controllore, è necessario prima installare un kit di aggiornamento del firmware. Un kit di aggiornamento viene spedito in un CD supplementare insieme al software RSLogix 5000.

---

**SUGGERIMENTO** Per aggiornare il firmware è anche possibile selezionare ControlFLASH™ dal menu Tools del software RSLogix 5000.

### Stato di sicurezza/errori

L'upload della logica di programma ed il collegamento online sono consentiti indipendentemente dallo stato di sicurezza. Lo stato di sicurezza e gli errori influiscono solo sul processo di download.

È possibile visualizzare lo stato di sicurezza dalla scheda Safety nella finestra di dialogo Controller Properties.

## Firma del task di sicurezza e stato di blocco/sblocco di sicurezza

L'esistenza di una firma del task di sicurezza e lo stato di blocco/sblocco di sicurezza del controllore influiscono sia sui processi di upload che di download.

### *Durante l'upload*

Se il controllore ha una firma del task di sicurezza, quest'ultima e lo stato di blocco del task di sicurezza vengono caricati con il progetto. Ad esempio, se il progetto nel controllore non era in blocco di sicurezza, il progetto offline rimane tale dopo l'upload, anche se era bloccato prima dell'upload.

In seguito ad un upload, la firma del task di sicurezza nel progetto offline corrisponde alla firma del task di sicurezza nel controllore.

### *Durante il download*

L'esistenza di una firma del task di sicurezza e lo stato di blocco di sicurezza del controllore determinano la possibilità di eseguire o meno un download.

**Tabella 34 – Effetto del blocco di sicurezza e della firma del task di sicurezza sull'operazione di download**

Stato del blocco di sicurezza	Stato della firma del task di sicurezza	Funzionalità di download
Controllore non in blocco di sicurezza	La firma del task di sicurezza nel progetto offline corrisponde alla firma del task di sicurezza nel controllore.	Vengono scaricati tutti i componenti standard del progetto. I tag di sicurezza vengono reinizializzati ai valori presenti al momento della creazione della firma del task di sicurezza. Il task di sicurezza non viene scaricato. Lo stato del blocco di sicurezza corrisponde allo stato nel progetto offline.
	Le firme del task di sicurezza non corrispondono.	Se il controllore aveva una firma del task di sicurezza, quest'ultima viene cancellata automaticamente e viene scaricato l'intero progetto. Lo stato del blocco di sicurezza corrisponde allo stato nel progetto offline.
Controllore in blocco di sicurezza	Le firme del task di sicurezza corrispondono.	Se il progetto offline ed il controllore sono in blocco di sicurezza, vengono scaricati tutti i componenti standard del progetto ed il task di sicurezza viene reinizializzato con i valori presenti al momento della creazione della firma del task di sicurezza. Se il progetto offline non è in blocco di sicurezza ma il controllore sì, il download viene bloccato e per proseguire con il download occorre prima sbloccare il controllore.
	Le firme del task di sicurezza non corrispondono.	È necessario innanzitutto lo sblocco di sicurezza del controllore per consentire il download. Se il controllore aveva una firma del task di sicurezza, quest'ultima viene cancellata automaticamente e viene scaricato l'intero progetto. Lo stato del blocco di sicurezza corrisponde allo stato nel progetto offline.

### **IMPORTANTE**

Durante il download su un controllore non in blocco di sicurezza, se il firmware del controllore differisce da quello del progetto offline, adottare una delle seguenti soluzioni:

- Aggiornare il controllore in modo che corrisponda al progetto offline. Una volta completato l'aggiornamento, l'intero progetto viene scaricato.
- Aggiornare il progetto alla versione del controllore.


Se si aggiorna il progetto, la firma del task di sicurezza viene cancellata ed è necessario ripetere la convalida del sistema.



## Download

Per trasferire il progetto dal computer al controllore, attenersi alla seguente procedura.



1. Portare il selettore a chiave del controllore su REM.
2. Aprire il progetto RSLogix 5000 da scaricare.
3. Definire il percorso al controllore.
  - a. Fare clic su Who Active .
  - b. Selezionare il controllore.  
Per aprire un livello, fare clic sul segno +. Se è già stato selezionato un controllore, assicurarsi che si tratti del controllore corretto.
4. Fare clic su Download.

Il software confronta le seguenti informazioni nel progetto offline e nel controllore:

- numero seriale del controllore (se è selezionata la corrispondenza tra progetto e controllore)
- versioni principale e secondaria del firmware
- stato di sicurezza
- firma del task di sicurezza (se presente)
- stato del blocco di sicurezza

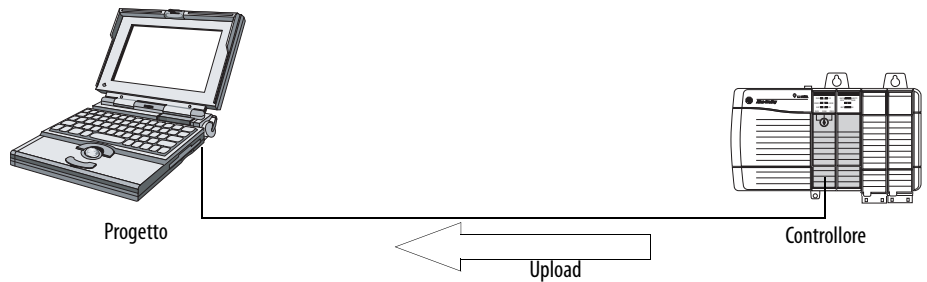
5. Per completare il download in base alle risposte del software, attenersi alle istruzioni riportate nella seguente tabella.


Se nel software è presente la seguente indicazione	Procedere come segue
Download nel controllore.	Scegliere Download. Il progetto viene scaricato nel controllore ed il software RSLogix 5000 viene collegato in linea.
Impossibile eseguire il download nel controllore. Mancata corrispondenza tra il numero seriale del progetto offline e quello del controllore. Il controllore selezionato può non essere corretto.	Eeguire la connessione al controllore corretto oppure verificare che il controllore utilizzato sia quello appropriato. Se si tratta del controllore corretto, selezionare la casella di controllo Update project serial number per consentire l'esecuzione del download. Il numero seriale del progetto viene modificato in modo da corrispondere al numero seriale del controllore.
Impossibile eseguire il download nel controllore. La versione principale del progetto offline ed il firmware del controllore non sono compatibili.	Selezionare Update Firmware. Selezionare la versione richiesta e fare clic su Update. Confermare la selezione facendo clic su Yes.
Impossibile eseguire il download nel controllore. Coprocessore di sicurezza mancante o non disponibile.	Annullare il processo di download. Installare un coprocessore di sicurezza compatibile prima di eseguire il download.
Impossibile eseguire il download nel controllore. La versione del firmware del coprocessore di sicurezza non è compatibile con il controllore primario.	Aggiornare la versione del firmware del coprocessore di sicurezza. Selezionare Update Firmware. Selezionare la versione richiesta e fare clic su Update. Confermare la selezione facendo clic su Yes.
Impossibile eseguire il download nel controllore. La partnership di sicurezza non è stata stabilita.	Annullare il processo di download e provare ad eseguire un nuovo download.
Impossibile eseguire il download nel controllore. La firma del task di sicurezza non compatibile non può essere eliminata quando il progetto è in blocco di sicurezza.	Annullare il processo di download. Per eseguire il download del progetto, è necessario disattivare il blocco di sicurezza del progetto offline, eliminare la firma del task di sicurezza e quindi scaricare il progetto. <b>IMPORTANTE:</b> il sistema di sicurezza richiede una nuova convalida.
Impossibile eseguire il download conservando la firma del task di sicurezza. La revisione secondaria del firmware del controllore non è compatibile con la firma del task di sicurezza del progetto offline.	<ul style="list-style-type: none"> <li>Se la versione secondaria del firmware non è compatibile, per conservare la firma del task di sicurezza aggiornare la versione del firmware nel controllore in modo che corrisponda esattamente al progetto offline. Scaricare quindi il progetto offline.</li> <li>Per procedere con il download indipendentemente dall'incompatibilità della firma del task di sicurezza, fare clic su Download. La firma del task di sicurezza viene cancellata.</li> </ul> <b>IMPORTANTE:</b> il sistema di sicurezza richiede una nuova convalida.
Impossibile eseguire il download nel controllore. Il controllore è bloccato. Le firme del task di sicurezza del controllore e del progetto offline non corrispondono.	Selezionare Unlock. Viene visualizzata la finestra di dialogo Safety Unlock for Download. Se è selezionata la casella di controllo Delete Signature e si sceglie Unlock, è necessario confermare l'eliminazione selezionando Yes.
Si verificherà un errore di sicurezza irreversibile sul controllore di sicurezza. Non è stato designato un master CST (tempo di sistema coordinato).	Selezionare Enable Time Synchronization e fare clic su Download per procedere.

Se il download viene eseguito correttamente, lo stato di blocco di sicurezza e la firma del task di sicurezza del controllore corrispondono al progetto scaricato. I dati di sicurezza vengono inizializzati ai valori esistenti al momento della creazione della firma del task di sicurezza.

## Upload

Per trasferire un progetto dal controllore al computer, attenersi alla seguente procedura.



1. Definire il percorso al controllore.
  - a. Fare clic su Who Active .
  - b. Selezionare il controllore.  
Per espandere un livello, fare clic sul segno +. Se è già stato selezionato un controllore, assicurarsi che si tratti del controllore corretto.
2. Fare clic su Upload.
3. Se il file di progetto non esiste, selezionare File>Select>Yes.
4. Se il file di progetto è già stato creato, selezionarlo.

Se è attivata la corrispondenza tra il progetto ed il controllore, il software RSLogix 5000 controlla se il numero seriale del progetto aperto ed il numero seriale del controllore corrispondono.

Se i numeri seriali del controllore non corrispondono, è possibile procedere in uno dei seguenti modi:

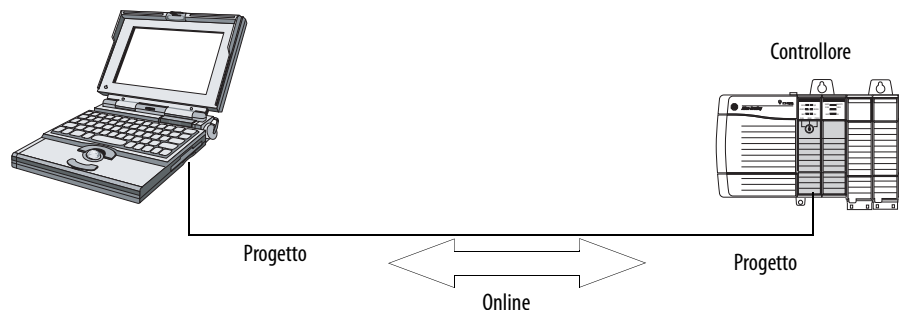
- Annullare l'upload ed eseguire la connessione ad un controllore corrispondente. Dopodiché, avviare nuovamente la procedura di upload.
  - Selezionare un nuovo progetto da caricare oppure selezionare un altro progetto scegliendo Select File.
  - Aggiornare il numero seriale del progetto in modo che corrisponda al controllore selezionando la casella di controllo Update Project Serial Number, quindi l'opzione Upload.
5. Il software controlla se il progetto aperto corrisponde al progetto del controllore.
    - a. Se i progetti non corrispondono, è necessario selezionare un file corrispondente oppure annullare il processo di upload.
    - b. Se i progetti corrispondono, il software controlla se sono state apportate modifiche al progetto offline (aperto).
  6. Il software verifica la presenza di modifiche nel progetto offline.
    - a. Se non sono state apportate modifiche al progetto offline, è possibile collegarsi online senza eseguire l'upload. Fare clic su Go Online.
    - b. Se sono state apportate modifiche al progetto aperto non presenti nel controllore, è possibile scegliere di caricare il progetto, annullare l'upload oppure selezionare un altro file.

Se si seleziona Upload, vengono caricate le applicazioni standard e di sicurezza. Se è stata configurata una firma del task di sicurezza, anch'essa viene caricata. Lo stato di blocco di sicurezza del progetto riflette lo stato originale del progetto in linea (controllore).


**SUGGERIMENTO** Prima di eseguire l'upload, se è presente una firma del task di sicurezza offline oppure il progetto offline è in blocco di sicurezza ma il controllore non lo è o non dispone di una firma del task di sicurezza, la firma del task di sicurezza offline e lo stato di blocco di sicurezza saranno sostituiti dai valori in linea (sblocco di sicurezza senza firma del task di sicurezza). Se non si desidera apportare tali modifiche in modo permanente, non salvare il progetto offline al termine dell'upload.

## Collegamento online

Per passare online e monitorare un progetto in esecuzione sul controllore, attenersi alla seguente procedura.



### 1. Definire il percorso al controllore.

a. Fare clic su Who Active .

b. Selezionare il controllore.

Per espandere un livello, fare clic sul segno +. Se è già stato selezionato un controllore, assicurarsi che si tratti del controllore corretto.

### 2. Fare clic su Go Online.

Il software esegue le seguenti verifiche:

- I numeri seriali del progetto offline e del controllore corrispondono (se è selezionata la funzione di corrispondenza tra il progetto ed il controllore)?
- Il progetto offline contiene modifiche non presenti nel progetto del controllore?
- Le versioni del progetto offline e del firmware del controllore corrispondono?
- Il progetto offline o il controllore sono in blocco di sicurezza?
- Il progetto offline ed il controllore hanno firme del task di sicurezza compatibili?

3. Per connettersi al controllore, seguire le indicazioni riportate nella tabella che segue.

**Tabella 35 – Connessione al controllore**

Se nel software è presente la seguente indicazione	Procedere come segue
Impossibile eseguire la connessione al controllore. Mancata corrispondenza tra il numero seriale del progetto offline e quello del controllore. Il controllore selezionato può non essere corretto.	Eseguire la connessione al controllore corretto, selezionare un altro file di progetto oppure selezionare la casella di controllo Update project serial number e scegliere Go Online. . . per eseguire la connessione al controllore ed aggiornare il numero seriale del progetto offline in modo che corrisponda al controllore.
Impossibile eseguire la connessione al controllore. La versione del progetto offline ed il firmware del controllore non sono compatibili.	Scegliere una delle seguenti opzioni: <ul style="list-style-type: none"> <li>Selezionare Update Firmware. Selezionare la versione richiesta e fare clic su Update. Confermare la selezione facendo clic su Yes.</li> <li><b>IMPORTANTE:</b> il progetto online viene eliminato.</li> <li>Per mantenere il progetto in linea, annullare il processo in linea ed installare una versione del software RSLogix 5000 compatibile con la versione del firmware del controllore.</li> </ul>
È necessario eseguire l'upload o il download per collegarsi online utilizzando il progetto aperto.	Scegliere una delle seguenti opzioni: <ul style="list-style-type: none"> <li>Upload per aggiornare il progetto offline.</li> <li>Download per aggiornare il progetto del controllore.</li> <li>Selezionare File per selezionare un altro progetto offline.</li> </ul>
Impossibile eseguire la connessione conservando la firma del task di sicurezza. La revisione secondaria del firmware del controllore non è compatibile con la firma del task di sicurezza del progetto offline.	<ul style="list-style-type: none"> <li>Per conservare la firma del task di sicurezza quando la versione secondaria del firmware non è compatibile, aggiornare la versione del firmware nel controllore in modo che corrisponda esattamente al progetto offline. Collegarsi quindi online al controllore.</li> <li>Per procedere con il download indipendentemente dall'incompatibilità della firma del task di sicurezza, fare clic su Download. La firma del task di sicurezza viene cancellata.</li> <li><b>IMPORTANTE:</b> il sistema di sicurezza richiede una nuova convalida.</li> </ul>
Impossibile eseguire la connessione al controllore. La firma del task di sicurezza non compatibile non può essere eliminata mentre il progetto è in blocco di sicurezza.	Annullare il processo online. È necessario disattivare il blocco di sicurezza del progetto offline prima del collegamento online.

Quando il controllore ed il software RSLogix 5000 sono in linea, lo stato di blocco di sicurezza e la firma del task di sicurezza del controllore corrispondono al progetto del controllore. Lo stato di blocco di sicurezza e la firma del task di sicurezza del progetto offline vengono sovrascritti dal controllore. Se non si desidera apportare tali modifiche al progetto offline in modo permanente, non salvare il file di progetto al termine del collegamento online.

**Note:**

## Memorizzazione e caricamento di progetti con la memoria non volatile

Argomento	Pagina
Utilizzo delle schede di memoria per la memoria non volatile	119
Memorizzazione di un progetto di sicurezza	120
Caricamento di un progetto di sicurezza	121
Utilizzo dei moduli ESM (solo controllori 1756-L7xS)	122
Valutazione del mantenimento dell'orologio interno (WallClockTime) da parte del modulo ESM	124
Gestione del firmware con Firmware Supervisor	124

### Utilizzo delle schede di memoria per la memoria non volatile

I controllori GuardLogix, versione 18 o successive, supportano una scheda di memoria per la memoria non volatile. La memoria non volatile consente di mantenere una copia del progetto sul controllore. Il controllore non richiede alimentazione o una batteria per il mantenimento di questa copia.

Il progetto memorizzato può essere caricato dalla memoria non volatile alla memoria utente del controllore:

- Ad ogni accensione
- Quando non è presente alcun progetto nel controllore e quest'ultimo viene acceso
- In qualsiasi momento tramite il software RSLogix 5000

---

**IMPORTANTE** Nella memoria non volatile vengono memorizzati i contenuti della memoria utente quando si salva il progetto:

- Le modifiche apportate in seguito alla memorizzazione del progetto non vengono salvate nella memoria non volatile.
- Se si apportano delle modifiche al progetto ma non vengono memorizzate, queste ultime vengono sovrascritte quando si carica il progetto dalla memoria non volatile. In tal caso, è necessario eseguire l'upload o il download del progetto per collegarsi online.
- Per salvare modifiche quali modifiche online, valori dei tag, o una schedulazione della rete ControlNet, è necessario memorizzare nuovamente il progetto in seguito all'esecuzione delle modifiche.

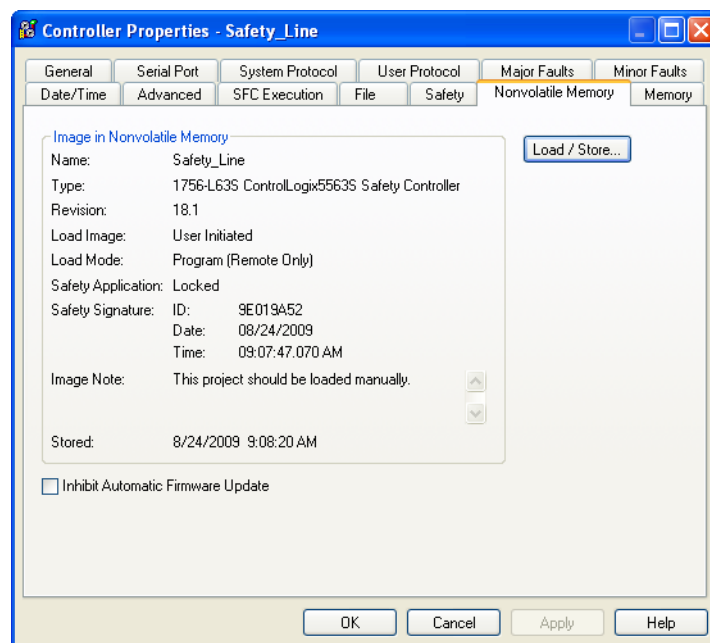
---

Se è installata una scheda di memoria, è possibile visualizzarne i contenuti tramite la scheda Nonvolatile Memory della finestra di dialogo Controller Properties. Se sulla scheda è memorizzata un'applicazione di sicurezza, vengono visualizzati lo stato del blocco di sicurezza e la firma del task di sicurezza.



**ATTENZIONE:** Non rimuovere la scheda di memoria mentre il controllore sta leggendo o scrivendo su di essa, processo indicato dall'indicatore di stato OK che lampeggia in verde. Questa operazione potrebbe provocare il danneggiamento dei dati presenti sulla scheda o nel controllore, o l'alterazione dell'ultimo firmware caricato nel controllore. Lasciare la scheda nel controllore finché la luce dell'indicatore di stato OK non diventa verde fissa.

Figura 29 – Scheda Nonvolatile Memory



Per informazioni dettagliate sull'utilizzo della memoria non volatile, consultare il manuale di programmazione Logix5000 Controllers Nonvolatile Memory, pubblicazione [1756-PM017](#).

## Memorizzazione di un progetto di sicurezza

Non è possibile memorizzare un progetto di sicurezza se lo stato del task di sicurezza è Task di sicurezza non funzionante. Quando si memorizza un progetto di sicurezza, i firmware del controllore primario e del coprocessore di sicurezza vengono salvati sulla scheda di memoria.

Se non è presente alcuna applicazione nel controllore, è possibile salvare solo il firmware del controllore di sicurezza se è stata stabilita una partnership valida. Il caricamento del solo firmware non determina l'annullamento della condizione Task di sicurezza non funzionante.

Se è presente una firma del task di sicurezza quando si memorizza un progetto, avviene quanto segue:

- I tag di sicurezza vengono memorizzati insieme ai valori che assumevano al momento della creazione della firma.
- I tag standard vengono aggiornati.
- La firma del task di sicurezza corrente viene salvata.



Quando si memorizza un progetto applicativo di sicurezza su una scheda di memoria, si consiglia di selezionare Program (Remote Only) come modalità di caricamento, ossia la modalità a cui deve passare il controllore in seguito al caricamento.

## Caricamento di un progetto di sicurezza

Il caricamento può essere avviato solo dalla memoria non volatile in presenza delle seguenti condizioni:

- Il tipo di controllore specificato dal progetto memorizzato nella memoria non volatile corrisponde al tipo di controllore.
- Le versioni principale e secondaria apportate al progetto nella memoria non volatile corrispondono alle versioni principali e secondarie del controllore.
- Il controllore non è in modalità Esecuzione.

Esistono varie opzioni relative alle condizioni in cui è possibile caricare il progetto nella memoria utente del controllore.

**Tabella 36 – Opzioni di caricamento di un progetto**

Se si desidera caricare il progetto	Selezionare questa opzione di Load Image	Note
Ad ogni accensione o in caso di spegnimento e riaccensione	All'accensione	<ul style="list-style-type: none"> <li>• Durante un ciclo di spegnimento e riaccensione si perdono le eventuali modifiche online, i valori dei tag e la schedulazione della rete non memorizzati nella memoria non volatile.</li> <li>• Il controllore carica il progetto memorizzato ed il firmware ad ogni accensione, indipendentemente dal firmware o dall'applicazione presenti sul controllore. Il caricamento si verifica indipendentemente dal fatto che il controllore sia in blocco di sicurezza o disponga di una firma del task di sicurezza.</li> <li>• Per caricare il progetto è sempre possibile utilizzare il software RSLogix 5000.</li> </ul>
Se non è presente alcun progetto nel controllore e si esegue l'accensione o si disattiva e riattiva l'alimentazione dello chassis	Se la memoria è danneggiata	<ul style="list-style-type: none"> <li>• Ad esempio, se la batteria si scarica ed il controllore non viene alimentato, il progetto viene cancellato dalla memoria. Quando viene ripristinata l'alimentazione, questa opzione di caricamento fa sì che il progetto venga ricaricato nel controllore.</li> <li>• Se è necessario, il controllore aggiorna il firmware sul controllore primario o il coprocessore di sicurezza. Viene anche caricata l'applicazione memorizzata nella memoria non volatile, ed il controllore passa alla modalità selezionata, Programmazione o Esecuzione.</li> <li>• Per caricare il progetto è sempre possibile utilizzare il software RSLogix 5000.</li> </ul>
Solo tramite il software RSLogix 5000	Avviato dall'utente	<ul style="list-style-type: none"> <li>• Se il tipo di controllore e le versioni principali e secondarie del progetto nella memoria non volatile corrispondono al tipo di controllore ed alle versioni principali e secondarie del controllore, è possibile avviare un caricamento, indipendentemente dallo stato del task di sicurezza.</li> <li>• Il caricamento di un progetto in un controllore in blocco di sicurezza può essere eseguito solo se la firma del task di sicurezza del progetto memorizzato nella memoria non volatile corrisponde al progetto presente nel controllore.</li> <li>• Se le firme non corrispondono o se il controllore è in blocco di sicurezza senza una firma del task di sicurezza, viene richiesto di sbloccare preventivamente il controllore. <b>IMPORTANTE:</b> quando si sblocca il controllore e si avvia un caricamento dalla memoria non volatile, lo stato del blocco di sicurezza, le password e la firma del task di sicurezza vengono impostati sui valori contenuti nella memoria non volatile al termine del caricamento.</li> <li>• Se il firmware presente sul controllore primario è nella stessa versione di quello presente nella memoria non volatile, se necessario, il firmware del coprocessore di sicurezza viene aggiornato, l'applicazione memorizzata nella memoria non volatile viene caricata, così il task di sicurezza assume lo stato Task di sicurezza funzionante ed il controllore passa alla modalità selezionata, Programmazione o Esecuzione.</li> </ul>

**IMPORTANTE** Prima di usare il software ControlFLASH, verificare che la scheda SD sia sbloccata, se è impostato il caricamento all'accensione. In caso contrario, i dati aggiornati rischiano di essere sovrascritti dal firmware sulla scheda di memoria.

## Utilizzo dei moduli ESM (solo controllori 1756-L7xS)

I moduli ESM GuardLogix possono essere utilizzati per quanto segue:

- Alimentare i controllori 1756-L7xS per salvare il programma sulla memoria non volatile (NVS) integrata nei controllori dopo l'interruzione dell'alimentazione allo chassis o la rimozione del controllore da una chassis alimentato.

---

**IMPORTANTE** Quando si usa un modulo ESM per salvare il programma sulla memoria NVS integrata, il programma **non** viene salvato sulla scheda SD installata nel controllore.

---

- Cancellare il programma dalla memoria non volatile integrata del controllore 1756-L7xS. Per ulteriori informazioni, consultare [Cancellazione del programma dalla memoria NVS integrata](#)

La tabella che segue descrive i moduli ESM.

**Tabella 37 – Moduli di alimentazione**

Num. di Cat.	Descrizione
1756-ESMCAP(XT)	ESM con condensatore I controllori 1756-L7xS vengono forniti con questo modulo ESM installato.
1756-ESMNSE(XT)	ESM con condensatore senza alimentazione di backup dell'orologio interno (WallClockTime) Da utilizzare se l'applicazione richiede che il modulo ESM installato riduca l'energia residua a 200 µJ o meno prima di installarlo o rimuoverlo dall'applicazione. Questo modulo ESM, inoltre, può essere utilizzato soltanto con un 1756-L73S (8 MB) o con un controllore di memoria inferiore.
1756-ESMNRM(XT)	ESM con condensatore di sicurezza (non rimovibile) Questo modulo aumenta il grado di sicurezza dell'applicazione prevenendo l'accesso fisico al connettore USB ed alla scheda SD.
1756-SPEMNSE(XT)	ESM con condensatore e senza alimentazione di backup WallClockTime per il coprocessore di sicurezza Da utilizzare se l'applicazione richiede che il modulo ESM installato riduca l'energia residua a 200 µJ o meno prima di installarlo o rimuoverlo dall'applicazione. Il coprocessore di sicurezza 1756-L7SPXT per temperature estreme viene fornito con il modulo 1756-SPEMNSEXT installato.
1756-SPEMNRM(XT)	ESM con condensatore di sicurezza (non rimovibile) per il coprocessore di sicurezza

## Salvataggio del programma sulla memoria NVS integrata

Per salvare il programma sulla memoria NVS quando si interrompe l'alimentazione del controllore, procedere come segue.

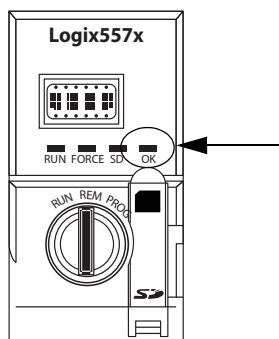
1. Interrompere l'alimentazione del controllore.

L'alimentazione può essere interrotta in due modi:

- Interrompendo l'alimentazione allo chassis con il controllore installato.
- Rimuovendo il controllore dallo chassis alimentato.

Subito dopo l'interruzione dell'alimentazione del controllore, l'indicatore di stato OK diventa rosso fisso e rimane così per tutto il tempo di salvataggio del programma.

**Figura 30 – Indicatore di stato OK.**



2. Non rimuovere il modulo ESM dal controllore fino allo spegnimento dell'indicatore di stato OK.
3. Se necessario, rimuovere il modulo ESM dal controllore solo quando l'indicatore di stato OK passa da rosso fisso a spento.

## Cancellazione del programma dalla memoria NVS integrata

Se l'applicazione lo consente, procedere come segue per cancellare il programma dalla memoria non volatile integrata nel controllore 1756-L7xS.

1. Rimuovere il modulo ESM dal controllore.
2. Interrompere l'alimentazione del controllore scollegando quella dello chassis in cui il controllore è installato o rimuovendo il controllore da uno chassis alimentato.
3. Reinstallare il modulo ESM nel controllore.
4. Ripristinare l'alimentazione del controllore.
  - a. Se il controllore è già installato nello chassis, rialimentare lo chassis.
  - b. Se il controllore non è installato nello chassis, reinstallare il controllore nello chassis e rialimentare lo chassis.

## Valutazione del mantenimento dell'orologio interno (WallClockTime) da parte del modulo ESM

Il modulo ESM permette il mantenimento dell'attributo WallClockTime del controllore in mancanza di alimentazione. Fare riferimento alla tabella che segue per stimare il tempo di mantenimento del modulo ESM in base alla temperatura del controllore ed al modulo ESM installato.

**Tabella 38 – Temperatura e tempo di mantenimento**

Temperatura	Tempo di mantenimento (in giorni)		
	1756-ESMCAP(XT)	1756-ESMNRM(XT) 1756-SPESMNRM(XT)	1756-ESMNSE(XT) 1756-SPESMNSE(XT)
20 °C	12	12	0
40 °C	10	10	0
60 °C	7	7	0

## Gestione del firmware con Firmware Supervisor

A partire dal software RSLogix 5000, versione 18, è possibile utilizzare la funzione Firmware Supervisor per gestire il firmware sui controllori. Firmware Supervisor consente ai controllori di aggiornare automaticamente i dispositivi:

- I moduli locale e remoto possono essere aggiornati mentre si trovano in modalità Programmazione o Esecuzione.
- La codifica elettronica deve essere configurata per la corrispondenza esatta.
- Il kit del firmware per il dispositivo di destinazione deve risiedere nella scheda di memoria del controllore.
- Il dispositivo deve supportare l'aggiornamento del firmware tramite ControlFLASH.

Firmware Supervisor supporta prodotti I/O distribuiti non modulari installati direttamente sulla rete senza adattatori, ivi compresi i moduli I/O CIP Safety installati su reti EtherNet/IP. I moduli I/O CIP Safety su reti DeviceNet ed i moduli POINT Guard I/O non sono ancora supportati.

Per abilitare Firmware Supervisor, attenersi alla seguente procedura.

1. Dalla finestra di dialogo Controller Properties, fare clic sulla scheda Nonvolatile Memory.
2. Fare clic su Load/Store.
3. Dal menu a discesa Automatic Firmware Updates, selezionare Enable e Store Files to Image.

Il software RSLogix 5000 trasferisce i kit del firmware dal computer alla scheda di memoria del controllore affinché possano essere utilizzati da Firmware Supervisor.

**SUGGERIMENTO** Disabilitando Firmware Supervisor, si disabilitano soltanto gli aggiornamenti del firmware tramite Supervisor. Ciò non riguarda gli aggiornamenti del firmware del controllore che vengono eseguiti quando l'immagine del controllore viene ricaricata dalla scheda di memoria.

## Monitoraggio dello stato e gestione degli errori

Argomento	Pagina
Visualizzazione dello stato attraverso la barra di stato	125
Monitoraggio delle connessioni	126
Monitoraggio dello stato di sicurezza	128
Errori del controllore	128
Sviluppo di una routine di errore	131

Per informazioni sull'interpretazione degli indicatori di stato e dei messaggi del controllore, vedere l'[Appendice A, Indicatori di stato](#).

### Visualizzazione dello stato attraverso la barra di stato

Nella barra di stato sono visualizzate le informazioni sul progetto e sul controllore, compresi lo stato del controllore, lo stato delle forzature, lo stato di modifica online e lo stato di sicurezza.

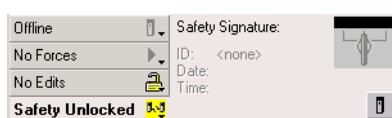
**Figura 31 – Pulsanti di stato**



Quando è selezionato il pulsante di stato del controllore come mostrato sopra, nella barra di stato vengono visualizzati la modalità (RUN) e lo stato (OK) del controllore. La spia BAT indica sia lo stato del controllore primario che del coprocessore di sicurezza. Se entrambi o uno dei due dispositivi presentano un errore della batteria, l'indicatore di stato si illumina. L'indicatore I/O mostra lo stato sia dell'I/O standard che quello di sicurezza e funziona esattamente come l'indicatore di stato sul controllore. L'I/O con lo stato d'errore più significativo viene visualizzato accanto all'indicatore di stato.





Quando è selezionato il pulsante Stato di sicurezza come mostrato di seguito, nella barra di stato viene visualizzata la firma del task di sicurezza.


**Figura 32 – Visualizzazione online della firma di sicurezza**



Il pulsante Stato di sicurezza indica se il controllore è in blocco o sblocco di sicurezza oppure se presenta un errore. Viene inoltre visualizzata un'icona indicante lo stato di sicurezza.

**Tabella 39 – Icona dello stato di sicurezza**

Se lo stato di sicurezza è	Viene visualizzata l'icona
Task di sicurezza OK	
Task di sicurezza non funzionante	
Partner mancante Partner non disponibile Hardware non compatibile Firmware non compatibile	
Offline	


Le icone sono verdi quando il controllore è in blocco di sicurezza, gialle quando il controllore non è in blocco di sicurezza e rosse quando il controllore presenta un errore di sicurezza. Se è presente una firma del task di sicurezza, l'icona include un piccolo segno di spunta. 

## Monitoraggio delle connessioni

È possibile monitorare lo stato delle connessioni standard e di sicurezza.

### Tutte le connessioni

Se la comunicazione con un dispositivo nella configurazione I/O del controllore non avviene entro 100 ms, si verifica un timeout della comunicazione ed il controllore genera i seguenti avvisi:

- L'indicatore I/O sulla parte anteriore del controllore lampeggia in verde.
- Viene mostrato un simbolo di avviso  sulla cartella di configurazione I/O e sul dispositivo in cui si è verificato il timeout.
- Viene generato un errore del modulo a cui si può accedere attraverso la scheda Connections della finestra di dialogo Module Properties del modulo o attraverso l'istruzione GSV.



**ATTENZIONE:** Gli I/O di sicurezza e le connessioni prodotte e consumate non possono essere configurate per generare automaticamente un errore del controllore quando la connessione viene interrotta. Pertanto, occorre monitorare gli errori di connessione per accertarsi che il sistema di sicurezza mantenga l'integrità SIL 3/PLe.

Vedere [Connessioni di sicurezza](#).

## Connessioni di sicurezza

Per i tag associati ai dati di sicurezza prodotti o consumati, è possibile monitorare lo stato delle connessioni di sicurezza utilizzando il membro CONNECTION\_STATUS. Per monitorare le connessioni di ingresso ed uscita, i tag I/O di sicurezza dispongono di un membro per lo stato di connessione denominato SafetyStatus. Entrambi i tipi di dati contengono due bit: RunMode e ConnectionFaulted.

Il valore RunMode indica se i dati consumati vengono aggiornati attivamente da un dispositivo che si trova in modalità Run (1) o in stato Idle (0). Lo stato di riposo è indicato se la connessione è chiusa, si è verificato un errore del task di sicurezza o il controllore remoto oppure il dispositivo è in modalità programmazione o test.

Il valore ConnectionFaulted indica se la connessione di sicurezza tra il produttore di sicurezza ed il consumatore di sicurezza è Valid (0) o Faulted (1). Se ConnectionFaulted viene impostato su Faulted (1) a seguito della perdita della connessione fisica, i dati di sicurezza vengono azzerati.

Nella seguente tabella sono descritte le combinazioni degli stati RunMode e ConnectionFaulted.

**Tabella 40 – Stato delle connessioni di sicurezza**

Stato RunMode	Stato ConnectionFaulted	Funzionamento della connessione di sicurezza
1 = Esecuzione	0 = Valido	I dati vengono controllati attivamente dal dispositivo produttore, che si trova in modalità Esecuzione.
0 = Riposo	0 = Valido	La connessione è attiva ed il dispositivo produttore si trova nello stato di riposo. I dati di sicurezza vengono azzerati.
0 = Riposo	1 = In errore	La connessione di sicurezza è in errore. Lo stato del dispositivo produttore è sconosciuto. I dati di sicurezza vengono azzerati.
1 = Esecuzione	1 = In errore	Stato non valido.

Se il modulo è inibito, il bit ConnectionFaulted viene impostato su Faulted (1) ed il bit RunMode viene impostato su Idle (0) per ciascuna connessione associata al modulo. Di conseguenza, i dati di sicurezza consumati vengono azzerati.

## Monitoraggio degli indicatori di stato

Tutti i controllori Logix, inclusi i GuardLogix, supportano le keyword di stato utilizzabili nella logica per monitorare determinati eventi specifici.

Per ulteriori informazioni sull'utilizzo delle keyword, consultare il manuale di programmazione Controllori Logix5000 – Informazioni e stato, pubblicazione [1756-PM015](#).

## Monitoraggio dello stato di sicurezza

Per visualizzare informazioni relative allo stato di sicurezza del controllore, utilizzare il pulsante di stato di sicurezza sulla barra di stato e nella scheda Safety nella finestra di dialogo Controller Properties.

Figura 33 – Stato del task di sicurezza



I valori possibili per lo stato di sicurezza sono:

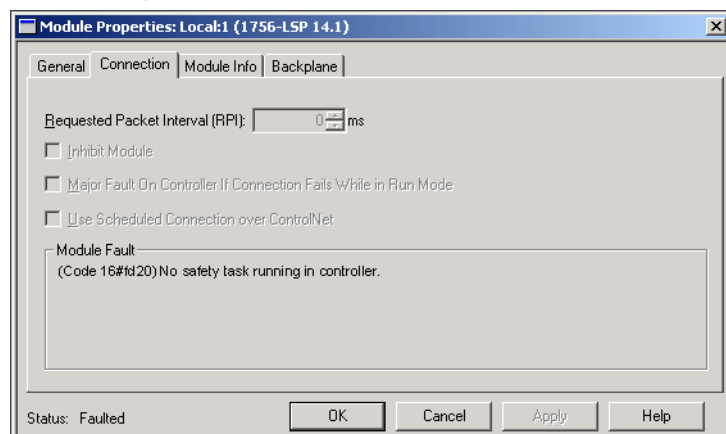
- Coprocessore di sicurezza mancante o non disponibile.
- Hardware del coprocessore di sicurezza non compatibile con il controllore primario.
- Firmware del coprocessore di sicurezza non compatibile con il controllore primario.
- Task di sicurezza non funzionante.
- Task di sicurezza funzionante.

Ad eccezione dell'ultima, le descrizioni riportate sopra indicano che sono presenti errori di sicurezza irreversibili.

Per informazioni sui codici di errore e le misure correttive, vedere [Errori di sicurezza gravi \(Tipo 14\) a pagina 130](#).

Lo stato del coprocessore di sicurezza può essere visualizzato nella scheda Connections della finestra di dialogo Module Properties.

Figura 34 – Stato del coprocessore di sicurezza



## Errori del controllore

Gli errori all'interno del sistema GuardLogix possono essere errori del controllore irreversibili, errori di sicurezza irreversibili nell'applicazione di sicurezza oppure errori di sicurezza reversibili nell'applicazione di sicurezza.



## Errori irreversibili del controllore

Questi errori si verificano quando la diagnostica interna del controllore non funziona. Se si verifica un errore irreversibile del controllore, l'esecuzione del task di sicurezza si interrompe ed i moduli I/O CIP Safety passano allo stato di sicurezza. Per il ripristino è necessario scaricare nuovamente il programma applicativo.

## Errori di sicurezza irreversibili nell'applicazione di sicurezza

Se si verifica un errore di sicurezza irreversibile in un'applicazione di sicurezza, la logica di sicurezza ed il protocollo di sicurezza vengono interrotti. Gli errori del watchdog del task di sicurezza e della partnership di controllo rientrano in questa categoria.

Se si verifica un errore di sicurezza irreversibile del task di sicurezza che viene azzerato nel gestore degli errori del controllore, l'esecuzione dell'applicazione standard non viene interrotta.



**ATTENZIONE:** L'esclusione dell'errore di sicurezza non ne consente l'azzeramento. Se si esclude l'errore di sicurezza, è responsabilità dell'utente provare che tale operazione consente un funzionamento sicuro.

È necessario fornire prova all'agenzia di certificazione che continuando a far funzionare una parte del sistema, il funzionamento è sicuro.

Se è presente una firma del task di sicurezza, è sufficiente azzerare l'errore per consentire l'esecuzione del task di sicurezza. Se la firma del task di sicurezza non è stata configurata, il task di sicurezza non può continuare ad essere eseguito finché non viene nuovamente scaricata l'intera applicazione.

## Errori reversibili nell'applicazione di sicurezza

Se nell'applicazione di sicurezza si verificano errori reversibili, il sistema può interrompere o meno l'esecuzione del task di sicurezza, a seconda che l'errore venga gestito o meno dal gestore degli errori del programma nell'applicazione di sicurezza.

Se un errore reversibile viene azzerato da programma, il task di sicurezza può continuare senza interruzioni.

Se un errore reversibile nell'applicazione di sicurezza non viene azzerato da programma, si verifica un errore di sicurezza reversibile di tipo 14, codice 2. L'esecuzione del programma di sicurezza viene interrotta e le connessioni del protocollo di sicurezza vengono chiuse e riaperte per la reinizializzazione. Le uscite di sicurezza vengono impostate nello stato di sicurezza ed il produttore dei tag di sicurezza consumati comanda ai consumatori di impostarle in uno stato di sicurezza.

Gli errori reversibili consentono di modificare l'applicazione standard e di sicurezza nel modo necessario per correggere la causa dell'errore. Tuttavia, se è stata configurata una firma del task di sicurezza o il controllore è in blocco di sicurezza, è necessario sbloccarlo ed eliminare la firma del task di sicurezza prima di poter modificare l'applicazione di sicurezza.

## Visualizzazione degli errori

La finestra di dialogo Recent Faults sulla scheda Major Faults della finestra di dialogo Controller Properties contiene altre due schede, una per gli errori standard e l'altra per gli errori di sicurezza.

Anche il display di stato dei controllori 1756-L7xS visualizza i codici di errore accompagnati da un breve messaggio di stato, come spiegato all'inizio di pagina [137](#).

## Codici di errore

La [Tabella 41](#) mostra i codici di errore specifici dei controllori GuardLogix. Il tipo ed il codice corrispondono al tipo ed al codice visualizzati nella scheda Major Faults della finestra di dialogo Controller Properties e nell'oggetto PROGRAM, attributo MAJORFAULTRECORD (o MINORFAULTRECORD).

**Tabella 41 – Errori di sicurezza gravi (Tipo 14)**

Codice	Causa	Stato	Azione correttiva
01	Watchdog del task scaduto. Il task utente non è stato completato in un periodo di tempo specificato. Un errore di programma ha causato un loop infinito, il programma è troppo complesso per essere eseguito alla velocità specificata, un task con priorità più alta impedisce il completamento di questo task, oppure il coprocessore di sicurezza è stato rimosso.	Irreversibile	Rimuovere l'errore. Se è presente una firma del task di sicurezza, la memoria di sicurezza viene reinizializzata e viene avviata l'esecuzione del task di sicurezza. Se non è presente una firma del task di sicurezza, è necessario scaricare nuovamente il programma per consentire l'esecuzione del task di sicurezza. Installare il coprocessore di sicurezza, se è stato rimosso.
02	È presente un errore in una routine del task di sicurezza.	Reversibile	Correggere l'errore nella logica del programma utente.
03	Il coprocessore di sicurezza è mancante.	Irreversibile	Installare un coprocessore di sicurezza compatibile.
04	Il coprocessore di sicurezza non è disponibile.	Irreversibile	Installare un coprocessore di sicurezza compatibile.
05	L'hardware del coprocessore di sicurezza non è compatibile.	Irreversibile	Installare un coprocessore di sicurezza compatibile.
06	Il firmware del coprocessore di sicurezza non è compatibile.	Irreversibile	Aggiornare il coprocessore di sicurezza, in modo che le versioni principale e secondaria del firmware corrispondano con il controllore primario.
07	Task di sicurezza non funzionante. Questo errore si verifica quando la logica di sicurezza non è valida, ad esempio in caso di non corrispondenza nella logica tra il controllore primario ed il coprocessore di sicurezza, se si verifica un timeout del watchdog, oppure se la memoria è danneggiata.	Irreversibile	Rimuovere l'errore. Se è presente una firma del task di sicurezza, la memoria di sicurezza viene reinizializzata tramite la firma del task di sicurezza e viene avviata l'esecuzione del task di sicurezza. Se non è presente una firma del task di sicurezza, è necessario scaricare nuovamente il programma per consentire l'esecuzione del task di sicurezza.
08	Tempo di sistema coordinato (CST) non trovato.	Irreversibile	Rimuovere l'errore. Configurare un dispositivo come master CST.
09	Errore irreversibile del controllore del coprocessore di sicurezza.	Irreversibile	Rimuovere l'errore e scaricare il programma. Se il problema persiste, sostituire il coprocessore di sicurezza.

Se la batteria del coprocessore di sicurezza 1756-LSP risulta mancante o deve essere sostituita, si verifica un errore minore di tipo reversibile (10), codice 11.

Per informazioni sulla sostituzione della batteria, vedere [Appendice B](#).

Il manuale di programmazione Controllori Logix5000 – Errori gravi, minori e I/O, pubblicazione [1756-PM014E-IT-P](#) contiene informazioni dettagliate relative ai codici di errore comuni ai controllori Logix.

## Sviluppo di una routine di errore

Se si verifica una condizione d'errore sufficientemente grave da determinare lo spegnimento del controllore, quest'ultimo genera un errore grave ed arresta l'esecuzione della logica.

A seconda del tipo di applicazione, può non essere necessario che tutti gli errori di sicurezza causino lo spegnimento dell'intero sistema. In queste situazioni, è possibile utilizzare una routine di errore per rimuovere un errore specifico e far continuare a funzionare la parte di controllo standard del sistema oppure configurare alcune uscite perché rimangano attive.



**ATTENZIONE:** È necessario fornire prova all'agenzia di certificazione che continuando a far funzionare una parte del sistema, il funzionamento è sicuro.

Il controllore supporta due livelli per la gestione degli errori gravi:

- routine di errore del programma
- gestore degli errori del controllore

Entrambe le routine possono utilizzare le istruzioni GSV e SSV, come descritto a pagina [132](#).

### Routine di errore del programma

Ciascun programma può avere una propria routine di errore. Il controllore esegue la routine di errore del programma quando si verifica un errore dell'istruzione. Se la routine di errore del programma non consente di rimuovere l'errore oppure la routine di errore del programma non esiste, il controllore procede all'esecuzione del gestore degli errori del controllore, se presente.

### Gestore degli errori del controllore

Il gestore degli errori del controllore è un componente opzionale che viene eseguito quando la routine di errore del programma non è in grado di rimuovere l'errore o non esiste.

È possibile creare solo un programma per il gestore degli errori del controllore. Dopo avere creato il programma, è necessario configurare una routine come routine principale.

Per informazioni dettagliate sulla creazione e i test relativi alle routine di errore, consultare il manuale di programmazione Controllori Logix5000 – Errori gravi, minori e I/O, pubblicazione [1756-PM014E-IT-P](#).

## Utilizzo delle istruzioni GSV/SSV

I controllori Logix memorizzano i dati di sistema in oggetti anziché in file di stato. È possibile utilizzare le istruzioni Get System Value (GSV) e Set System Value (SSV) per estrarre ed impostare i dati del controllore.

L'istruzione GSV recupera le informazioni specificate e le posiziona in una destinazione specifica. L'istruzione SSV cambia l'attributo specifico con i dati dall'origine dell'istruzione. Quando si immette un'istruzione GSV o SSV, nel software di programmazione vengono visualizzate le classi degli oggetti, i nomi degli oggetti ed i nomi degli attributi per ciascuna istruzione.

Per i task standard, è possibile utilizzare l'istruzione GSV per ottenere i valori degli attributi disponibili. Quando si utilizza l'istruzione SSV, nel software vengono visualizzati solo gli attributi impostabili dall'utente.

Per il task di sicurezza, le istruzioni GSV e SSV sono più limitate. Si noti che le istruzioni SSV nei task di sicurezza ed in quelli standard non possono impostare il bit 0 (errore grave in caso di errore) nell'attributo della modalità di un modulo I/O di sicurezza.

Per gli oggetti di sicurezza, la [Tabella 42](#) riporta gli attributi per i quali è possibile ottenere valori utilizzando l'istruzione GSV e quelli di cui è consentita l'impostazione utilizzando l'istruzione SSV, nei task sia standard che di sicurezza.



**ATTENZIONE:** Utilizzare le istruzioni GSV/SSV con molta attenzione. La modifica degli oggetti può causare operazioni del controllore non previste o infortuni al personale.

Tabella 42 – Accessibilità di GSV/SSV

Oggetto di sicurezza	Nome attributo	Tipo di dati	Descrizione attributo	Accessibile dal task di sicurezza		Accessibile dai task standard	
				GSV	SSV	GSV <sup>(4)</sup>	SSV
Task di sicurezza	Instance	DINT	Fornisce il numero di istanza di questo oggetto del task. I valori validi sono compresi tra 0 e 31.	✓		✓	
	MaximumInterval	DINT[2]	L'intervallo di tempo massimo tra le esecuzioni successive del task.			✓	✓
	MaximumScanTime	DINT	Il tempo di esecuzione massimo registrato (ms) per il task.			✓	✓
	MinimumInterval	DINT[2]	L'intervallo di tempo minimo tra le esecuzioni successive del task.			✓	✓
	Priority	INT	Priorità relativa di questo task rispetto ad altri task. I valori validi sono compresi tra 0 e 15.	✓		✓	
	Rate	DINT	Periodo del task (in ms) o valore di timeout per il task (in ms).	✓		✓	
	Watchdog	DINT	Limite di tempo (in ms) per l'esecuzione di tutti i programmi associati al task.	✓		✓	
Programma di sicurezza	Instance	DINT	Fornisce il numero di istanza dell'oggetto del programma.	✓		✓	
	MajorFaultRecord <sup>(1)</sup>	DINT[11]	Registra gli errori gravi per il programma.	✓	✓	✓	
	MaximumScanTime	DINT	Il tempo di esecuzione massimo registrato (ms) per il programma.			✓	✓
Routine di sicurezza	Instance	DINT	Fornisce il numero di istanza di questo oggetto di routine. I valori validi sono compresi tra 0 e 65.535.	✓			

**Tabella 42 – Accessibilità di GSV/SSV**

Oggetto di sicurezza	Nome attributo	Tipo di dati	Descrizione attributo	Accessibile dal task di sicurezza		Accessibile dai task standard	
				GSV	SSV	GSV <sup>(4)</sup>	SSV
Controllore di sicurezza	SafetyLocked	SINT	Indica se il controllore è in blocco o sblocco di sicurezza.	✓		✓	
	SafetyStatus <sup>(2)</sup>	INT	Specifica lo stato di sicurezza come: <ul style="list-style-type: none"> <li>• Task di sicurezza funzionante. (1000000000000000)</li> <li>• Task di sicurezza non funzionante. (1000000000000001)</li> <li>• Coprocessore mancante. (0000000000000000)</li> <li>• Coprocessore non disponibile. (0000000000000001)</li> <li>• Hardware non compatibile. (0000000000000010)</li> <li>• Firmware non compatibile. (0000000000000011)</li> </ul>			✓	
	SafetySignatureExists	SINT	Indica se la firma del task di sicurezza è presente.	✓		✓	
	SafetySignatureID	DINT	Numero di identificazione a 32 bit.			✓	
	SafetySignature	Stringa <sup>(3)</sup>	Numero di identificazione a 32 bit.			✓	
	SafetyTaskFaultRecord <sup>(1)(2)</sup>	DINT[11]	Registra gli errori del task di sicurezza.			✓	
AOI (sicurezza)	LastEditDate	LINT	Marca temporale e di data dell'ultima modifica apportata alla definizione di un'istruzione add-on.			✓	
	SignatureID	DINT	Numero ID.			✓	
	SafetySignatureID	DINT	Numero di identificazione a 32 bit.			✓	

(1) Per ulteriori informazioni su come accedere a questo attributo, vedere [Accesso agli attributi FaultRecord a pagina 133](#).

(2) Per ulteriori informazioni su come accedere a questo attributo, vedere [Acquisizione di informazioni sugli errori a pagina 134](#).

(3) Lunghezza = 37.

(4) Dal task standard, l'accessibilità GSV degli attributi dell'oggetto di sicurezza è la stessa degli attributi dell'oggetto standard.

### Accesso agli attributi FaultRecord

Per semplificare l'accesso agli attributi MajorFaultRecord e SafetyTaskFaultRecord occorre creare una struttura definita dall'utente.

**Tabella 43 – Parametri di accesso agli attributi FaultRecord**

Nome	Tipo di dati	Stile	Descrizione
TimeLow	DINT	Decimale	32 bit inferiori del valore di registrazione ora e data dell'errore
TimeHigh	DINT	Decimale	32 bit superiori del valore di registrazione ora e data dell'errore
Type	INT	Decimale	Tipo di errore (programma, I/O o altro)
Code	INT	Decimale	Codice univoco per questo errore (dipendente dal tipo di errore)
Info	DINT[8]	Esadecimale	Informazioni specifiche sull'errore (dipendenti dal tipo di errore e dal codice)

Per ulteriori informazioni sull'utilizzo delle istruzioni GSV e SSV, consultare il capitolo dedicato alle istruzioni di ingresso/uscita del manuale di riferimento Istruzioni generali per controllori Logix5000, pubblicazione [1756-RM003K-IT-P](#).

### *Acquisizione di informazioni sugli errori*

Gli attributi `SafetyStatus` e `SafetyTaskFaultRecord` consentono di acquisire informazioni relative agli errori irreversibili. Per acquisire e memorizzare le informative relative agli errori si utilizza un'istruzione `GSV` nel gestore degli errori del controllore. L'istruzione `GSV` può essere utilizzata in un task standard insieme ad una routine del gestore degli errori del controllore che azzerà l'errore e permette il proseguimento dell'esecuzione dei task standard.

## Indicatori di stato

Argomento	Pagina
Indicatori di stato del controllore 1756-L6xS	135
Indicatori di stato del controllore 1756-L7xS	136
Display di stato del controllore 1756-L7xS	137

### Indicatori di stato del controllore 1756-L6xS

Lo stato del controllore primario e del coprocessore di sicurezza sono visualizzati da indicatori di stato a LED.

**Tabella 44 – Descrizione degli indicatori di stato del controllore 1756-L6xS**

Indicatore	Stato	Descrizione del controllore primario	Descrizione del coprocessore di sicurezza
RUN	Spento	Non sono in esecuzione task dell'utente. Il controllore è in modalità Programmazione (PROG).	N/D
	Verde	Il controllore è in modalità Esecuzione (RUN).	N/D
SAFE RUN	Spento	N/D	Il task di sicurezza dell'utente o le uscite di sicurezza sono disabilitati. Il controllore è in modalità Programmazione, in modalità test oppure il task di sicurezza presenta un errore.
	Verde	N/D	Il task di sicurezza dell'utente e le uscite di sicurezza sono abilitati. L'applicazione di sicurezza è in esecuzione. La firma del task di sicurezza è presente.
	Verde, lampeggiante	N/D	Il task di sicurezza dell'utente e le uscite di sicurezza sono abilitati. L'applicazione di sicurezza è in esecuzione. La firma del task di sicurezza non è presente.
FORCE	Spento	Nessuna forzatura, standard o di sicurezza, è abilitata sul controllore.	N/D
	Giallo	Le forzature standard e/o di sicurezza sono state abilitate.	N/D
	Giallo, lampeggiante	Uno o più indirizzi I/O, standard e/o di sicurezza, sono stati forzati sullo stato on o off, ma le forzature non sono abilitate.	N/D
BAT	Spento	La batteria è in grado di supportare la memoria.	La batteria è in grado di supportare la memoria.
	Rosso	La batteria non è in grado di supportare la memoria.	La batteria non è in grado di supportare la memoria.
OK	Spento	Nessuna alimentazione applicata.	Nessuna alimentazione applicata.
	Verde	Il controllore funziona senza errori.	Il coprocessore di sicurezza funziona senza errori.
	Rosso, lampeggiante	Errore irreversibile o reversibile non gestito nel gestore degli errori. Tutti i task dell'utente, sia standard che di sicurezza, vengono interrotti.	N/D
	Rosso	Errore del controllore all'accensione o errore irreversibile.	Errore del controllore all'accensione o errore irreversibile.
I/O <sup>(1)</sup>	Spento	Nessuna attività. Non è configurato alcun I/O.	N/D
	Verde	Il controllore comunica con tutti i dispositivi I/O configurati, sia standard, sia di sicurezza.	N/D
	Verde, lampeggiante	Uno o più dispositivi I/O non rispondono.	N/D
	Rosso, lampeggiante	Il controllore non comunica con l'I/O configurato.	N/D

**Tabella 44 – Descrizione degli indicatori di stato del controllore 1756-L6xS**

Indicatore	Stato	Descrizione del controllore primario	Descrizione del coprocessore di sicurezza
RS232	Spento	Non vi è alcuna attività.	N/D
	Verde	I dati vengono ricevuti o trasmessi.	N/D
SAFETY TASK	Spento	N/D	Nessuna partnership stabilita. Il controllore primario è mancante, non funziona correttamente o la sua versione del firmware non è compatibile con quella del coprocessore di sicurezza.
	Verde	N/D	Lo stato del controllore di sicurezza è OK. Il tempo di sistema coordinato (CST) è sincronizzato e le connessioni I/O di sicurezza sono state stabilite.
	Verde, lampeggiante	N/D	Lo stato del controllore di sicurezza è OK. Il tempo di sistema coordinato (CST) non è sincronizzato sul controllore primario o sul coprocessore di sicurezza.
	Rosso	N/D	La partnership è stata persa e non è stata stabilita una nuova partnership. Il controllore primario è mancante, non funziona correttamente o la sua versione del firmware non è compatibile con quella del coprocessore di sicurezza.
	Rosso, lampeggiante	N/D	Task di sicurezza non funzionante.

(1) L'I/O include i tag prodotti/consumati da altri controllori.

## Indicatori di stato del controllore 1756-L7xS

Lo stato del controllore primario viene visualizzato attraverso quattro indicatori.

**Tabella 45 – Descrizione degli indicatori di stato del controllore primario 1756-L7xS**

Indicatore	Stato	Descrizione
RUN	Spento	Non sono in esecuzione task dell'utente. Il controllore è in modalità Programmazione (PROG).
	Verde	Il controllore è in modalità Esecuzione (RUN).
FORCE	Spento	Nessuna forzatura, standard o di sicurezza, è abilitata sul controllore.
	Giallo	Le forzature standard e/o di sicurezza sono state abilitate. <b>Se si installa (aggiunge) una forzatura, agire con cautela perché diventa immediatamente attiva.</b>
	Giallo, lampeggiante	Uno o più indirizzi I/O, standard e/o di sicurezza, sono stati forzati sullo stato on o off, ma le forzature non sono abilitate. <b>Se si abilitano forzature I/O, agire con cautela perché l'azione coinvolge anche tutte le forzature I/O esistenti.</b>
SD	Spento	Nessuna attività in corso nella scheda di memoria.
	Verde, lampeggiante	Il controllore sta leggendo o scrivendo sulla scheda di memoria. Non rimuovere la scheda di memoria mentre il controllore è in fase di lettura o scrittura.
	Verde	
	Rosso, lampeggiante	La scheda di memoria non ha un file system valido.
Rosso	La scheda di memoria non è riconosciuta dal controllore.	



**Tabella 45 – Descrizione degli indicatori di stato del controllore primario 1756-L7xS**

Indicatore	Stato	Descrizione
OK	Spento	Nessuna alimentazione applicata.
	Verde	Il controllore funziona senza errori.
	Rosso, lampeggiante	<ul style="list-style-type: none"> <li>Errore irreversibile o reversibile non gestito nel gestore degli errori. Tutti i task dell'utente, sia standard che di sicurezza, vengono interrotti.</li> <li>Se il controllore è nuovo, appena disimballato, è necessario un aggiornamento firmware. Il display di stato indica Firmware Installation Required.</li> </ul>
	Rosso	<ul style="list-style-type: none"> <li>Il controllore sta eseguendo la procedura di diagnostica prevista all'accensione</li> <li>Si è verificato un errore grave irreversibile ed il programma è stato cancellato dalla memoria.</li> <li>Allo spegnimento, la carica del condensatore nel modulo ESM (Energy Storage Module) viene scaricata.</li> <li>Il controllore è alimentato ma non funzionante.</li> <li>Il controllore sta caricando un progetto nella memoria non volatile.</li> </ul>

Il coprocessore di sicurezza 1756-L7SP ha un indicatore di stato OK.

**Tabella 46 – Indicatore di stato 1756-L7SP**

Indicatore	Stato	Descrizione
OK	Spento	Nessuna alimentazione applicata.
	Verde	Il coprocessore di sicurezza funziona senza errori.
	Rosso	Errore del controllore all'accensione o errore irreversibile.

## Display di stato del controllore 1756-L7xS

Nel display di stato del controllore 1756-L7xS vengono visualizzati a scorrimento messaggi relativi alla versione del firmware del controllore, allo stato del modulo ESM, allo stato del progetto e ad errori gravi.

## Messaggi di stato di sicurezza

Il display del controllore primario può visualizzare i seguenti messaggi. Il coprocessore di sicurezza visualizza "L7SP".

**Tabella 47 – Display di stato di sicurezza**

Messaggio	Interpretazione
No Safety Signature	Il task di sicurezza è in modalità Esecuzione senza una firma del task di sicurezza.
Safety Partner Missing	Coprocessore di sicurezza mancante o non disponibile.
Hardware Incompatible	Hardware del coprocessore di sicurezza non compatibile con quello del controllore primario.
Firmware Incompatible	Versione firmware del coprocessore di sicurezza non compatibile con quella del controllore primario.
No CST Master	Impossibile trovare un master CST (tempo di sistema coordinato)
Safety Task Inoperable	Logica di sicurezza non valida. Ad esempio, mancata corrispondenza tra il controllore primario ed il coprocessore di sicurezza, timeout del watchdog o danneggiamento della memoria.
Safety Unlocked	Il controllore è in modalità Esecuzione con una firma di sicurezza ma non in blocco di sicurezza.

## Messaggi di stato generali

I messaggi descritti nella [Tabella 48](#) vengono generalmente visualizzati all'accensione, allo spegnimento e mentre il controllore è in funzione. Questi messaggi indicano lo stato del controllore e del modulo ESM.

**Tabella 48 – Display di stato generale**

Messaggio	Interpretazione
Nessun messaggio	Il controllore è spento o si è verificato un errore grave irreversibile (MNRF). Controllare l'indicatore di stato OK per stabilire se il controllore è abilitato e determinarne lo stato.
TEST	Il controllore sta eseguendo le prove previste all'accensione.
PASS	Le prove previste all'accensione hanno avuto risultato positivo.
SAVE	Allo spegnimento, un progetto viene salvato sulla scheda SD. Per ulteriori informazioni di stato, è possibile controllare anche l'indicatore SD (vedere <a href="#">pagina 136</a> ). Attendere il completamento dell'operazione di salvataggio prima di rimuovere la scheda SD o interrompere l'alimentazione.
LOAD	All'accensione del controllore, dalla scheda SD viene caricato un progetto. Per ulteriori informazioni di stato, è possibile controllare anche l'indicatore SD (vedere <a href="#">pagina 136</a> ). Attendere il completamento dell'operazione di caricamento prima di rimuovere il modulo ESM o interrompere l'alimentazione.
UPDT	All'accensione, viene eseguito un aggiornamento firmware dalla scheda SD. Per ulteriori informazioni di stato, è possibile controllare anche l'indicatore SD (vedere <a href="#">pagina 136</a> ). Se non si desidera l'aggiornamento del firmware all'accensione, modificare l'opzione Load Image del controllore.
CHRG	Il modulo ESM con condensatore è in fase di carica.
1756-L7x/X	Numero di catalogo e serie del controllore.
Rev XX.xxx	Versioni principale e secondaria del firmware per il controllore.
No Project	Sul controllore non è caricato alcun progetto. Per caricare un progetto, utilizzare il software RSLogix 5000 per scaricare il progetto nel controllore oppure utilizzare una scheda SD per caricare il progetto nel controllore.
<i>Project Name</i>	Nome del progetto attualmente caricato nel controllore. Il nome indicato è basato sul nome del progetto specificato nel software RSLogix 5000.
BUSY	I moduli I/O associati al controllore non sono ancora pienamente alimentati. Attendere che i moduli I/O completino le fasi di accensione ed autodiagnostica.
Corrupt Certificate Received	Il certificato di sicurezza associato al firmware è danneggiato. Accedere all'indirizzo <a href="http://www.rockwellautomation.com/support/">http://www.rockwellautomation.com/support/</a> e scaricare la versione firmware che si desidera installare. Sostituire la versione firmware precedentemente installata con quella scaricata dal sito web di assistenza tecnica.
Corrupt Image Received	Il file del firmware è danneggiato. Accedere all'indirizzo <a href="http://www.rockwellautomation.com/support/">http://www.rockwellautomation.com/support/</a> e scaricare la versione firmware che si desidera installare. Sostituire la versione firmware precedentemente installata con quella scaricata dal sito web di assistenza tecnica.
ESM Not Present	Manca un modulo ESM e, allo spegnimento, il controllore non può salvare l'applicazione. Inserire un modulo ESM compatibile e, se si utilizza un modulo ESM con condensatore, non interrompere l'alimentazione fino al completo caricamento del modulo.
ESM Incompatible	Il modulo ESM è incompatibile con le dimensioni della memoria del controllore. Sostituire il modulo ESM incompatibile con uno compatibile.
ESM Hardware Failure	Il modulo ESM è in guasto e, in caso di spegnimento, il controllore non può salvare il programma. Sostituire il modulo ESM prima di interrompere l'alimentazione del controllore, in modo da poter salvare il programma.
ESM Energy Low	Il modulo ESM con condensatore non ha energia sufficiente a permettere al controllore di salvare il programma in caso di spegnimento. Sostituire il modulo ESM.
ESM Charging	Il modulo ESM con condensatore è in fase di carica. Non interrompere l'alimentazione fino al completamento della carica.
Flash in Progress	È in corso un aggiornamento del firmware avviato mediante ControlFLASH o AutoFlash. Lasciar completare l'aggiornamento firmware senza interruzioni.
Firmware Installation Required	Il controllore sta usando il firmware di avvio (versione 1.xxx) e richiede un aggiornamento firmware. Aggiornare il firmware del controllore.
SD Card Locked	La scheda SD installata è bloccata.

## Messaggi di errore

Se il controllore è in stato di errore, sul display di stato viene visualizzato uno dei seguenti messaggi.

**Tabella 49 – Messaggi di errore<sup>(1)</sup>**

Messaggio	Interpretazione
Major Fault TXX:CXX message	Rilevamento di un errore grave di Tipo XX e Codice XX. Ad esempio, se il display di stato visualizza Major Fault T04:C42 Invalid JMP Target, significa che un'istruzione JMP è programmata per passare ad un'istruzione LBL non valida.
I/O Fault Local:X #XXXX message	Si è verificato un errore I/O in un modulo dello chassis locale. Vengono indicati il numero di slot ed il codice di errore, accompagnati da una breve descrizione. Ad esempio, il messaggio I/O Fault Local:3 #0107 Connection Not Found indica che una connessione al modulo I/O locale nello slot tre non è aperta. Adottare la misura correttiva specifica per il tipo di errore indicato.
I/O Fault ModuleName #XXXX message	Si è verificato un errore I/O su un modulo nello chassis remoto. Il nome del modulo in errore, come configurato nell'albero di configurazione I/O del software RSLogix 5000, è accompagnato dal codice di errore e da una breve descrizione. Ad esempio, I/O Fault My_Module #0107 Connection Not Found indica che una connessione al modulo designato come "My_Module" non è aperta. Adottare la misura correttiva specifica per il tipo di errore indicato.
I/O Fault ModuleParent:X #XXXX message	Si è verificato un errore I/O su un modulo nello chassis remoto. È indicato il nome "parent" del modulo perché, nell'albero di configurazione I/O del software RSLogix 5000 non è configurato alcun nome. Inoltre, il codice di errore è accompagnato da una breve descrizione. Ad esempio, I/O Fault My_CNet:3 #0107 Connection Not Found indica che una connessione ad un modulo nello slot 3 dello chassis con il modulo di comunicazione denominato "My_CNet" non è aperta. Adottare la misura correttiva specifica per il tipo di errore indicato.
X I/O Faults	Sono presenti errori I/O e X = il numero di errori I/O presenti. In presenza di più errori I/O, il controllore segnala il primo errore registrato. Quando ogni errore I/O è stato risolto, il numero di errori indicato diminuisce ed il messaggio di errore I/O indica l'errore successivo. Adottare la misura correttiva specifica per il tipo di errore indicato.

(1) Per i dettagli sui codici di errore, consultare il manuale di programmazione Controllori Logix5000 – Errori gravi, minori e I/O, pubblicazione [1756-PM014](#).

## Messaggi relativi agli errori gravi reversibili

Gli errori gravi reversibili vengono segnalati da Major Fault TXX:CXX message sul display di stato del controllore. La [Tabella 50 a pagina 140](#) elenca i tipi di guasto, i codici ed i messaggi associati che vengono visualizzati sul display di stato.

Per descrizioni dettagliate e metodi di ripristino consigliati per gli errori gravi reversibili, consultare il manuale di programmazione Controllori Logix5000 – Errori gravi, minori e I/O, pubblicazione [1756-PM014](#).

**Tabella 50 – Messaggi di stato degli errori gravi reversibili**

Tipo	Codice	Messaggio	Tipo	Codice	Messaggio
1	1	Run Mode Powerup	7	41	Bad Restore Type
1	60	Non-recoverable	7	42	Bad Restore Revision
1	61	Non-recoverable – Diagnostics Saved	7	43	Bad Restore Checksum
1	62	Non-recoverable – Program Saved	8	1	Keyswitch Change Ignored
3	16	I/O Connection Failure	11	1	Positive Overtravel Limit Exceeded
3	20	Chassis Failure	11	2	Negative Overtravel Limit Exceeded
3	21		11	3	Position Error Tolerance Exceeded
3	23	Connection Failure	11	4	Encoder Channel Connection Fault
4	16	Unknown Instruction	11	5	Encoder Noise Event Detected
4	20	Invalid Array Subscript	11	6	SERCOS Drive Fault
4	21	Control Structure LEN or POS < 0	11	7	Synchronous Connection Fault
4	31	Invalid JSR Parameter	11	8	Servo Module Fault
4	34	Timer Failure	11	9	Asynchronous Connection Fault
4	42	Invalid JMP Target	11	10	Motor Fault
4	82	SFC Jump Back Failure	11	11	Motor Thermal Fault
4	83	Value Out of Range	11	12	Drive Thermal Fault
4	84	Stack Overflow	11	13	SERCOS Communications Fault
4	89	Invalid Target Step	11	14	Inactive Drive Enable Input Detected
4	90	Invalid Instruction	11	15	Drive Phase Loss Detected
4	91	Invalid Context	11	16	Drive Guard Fault
4	92	Invalid Action	11	32	Motion Task Overlap Fault
4	990	Definiti dall'utente	11	33	CST Reference Loss Detected
4	991		18	1	CIP Motion Initialization Fault
4	992		18	2	CIP Motion Initialization Fault Mfg
4	993		18	3	CIP Motion Axis Fault
4	994		18	4	CIP Motion Axis Fault Mfg
4	995		18	5	CIP Motion Fault
4	996		18	6	CIP Module Fault
4	997		18	7	Motion Group Fault
4	998		18	8	CIP Motion Configuration Fault
4	999		18	9	CIP Motion APR Fault
6	1	Task Watchdog Expired	18	10	CIP Motion APR Fault Mfg
7	40	Save Failure	18	128	CIP Motion Guard Fault

### Codici di errore I/O

Gli errori I/O segnalati dal controllore vengono visualizzati sul display di stato in uno dei seguenti formati:

- I/O Fault Local:*X #XXXX message*
- I/O Fault *ModuleName #XXXX message*
- I/O Fault *ModuleParent:X #XXXX message*

La prima parte del formato indica la posizione del modulo in errore. Il metodo di indicazione della posizione dipende dalla configurazione I/O e dalle proprietà dei moduli specificate nel software RSLogix 5000.

L'ultima parte del formato, #XXXX message, può essere utilizzata per diagnosticare il tipo di errore I/O e le possibili misure correttive. Per i dettagli su ogni codice di errore I/O, consultare il manuale di programmazione Controllori Logix5000 – Errori gravi, minori e I/O, pubblicazione [1756-PM014](#).

**Tabella 51 – Messaggi di errore I/O**

Codice	Messaggio	Codice	Messaggio
#0001	Connection Failure	#0115	Wrong Device Type
#0002	Insufficient Resource	#0116	Wrong Revision
#0003	Invalid Value	#0117	Invalid Connection Point
#0004	IOI Syntax	#0118	Invalid Configuration Format
#0005	Destination Unknown	#0119	Module Not Owned
#0006	Partial Data Transferred	#011A	Out of Connection Resources
#0007	Connection Lost	#0203	Connection Timeout
#0008	Service Unsupported	#0204	Unconnected Message Timeout
#0009	Invalid Attribute Value	#0205	Invalid Parameter
#000A	Attribute List Error	#0206	Message Too Large
#000B	State Already Exists	#0301	No Buffer Memory
#000C	Object Mode Conflict	#0302	Bandwidth Not Available
#000D	Object Already Exists	#0303	No Bridge Available
#000E	Attribute Not Settable	#0304	ControlNet Schedule Error
#000F	Permission Denied	#0305	Signature Mismatch
#0010	Device State Conflict	#0306	CCM Not Available
#0011	Reply Too Large	#0311	Invalid Port
#0012	Fragment Primitive	#0312	Invalid Link Address
#0013	Insufficient Command Data	#0315	Invalid Segment Type
#0014	Attribute Not Supported	#0317	Connection Not Scheduled
#0015	Data Too Large	#0318	Invalid Link Address
#0100	Connection In Use	#0319	No Secondary Resources Available
#0103	Transport Not Supported	#031E	No Available Resources
#0106	Ownership Conflict	#031F	No Available Resources
#0107	Connection Not Found	#0800	Network Link Offline
#0108	Invalid Connection Type	#0801	Incompatible Multicast RPI
#0109	Invalid Connection Size	#0802	Invld Safety Conn Size
#0110	Module Not Configured	#0803	Invld Safety Conn Format
#0111	RPI Out of Range	#0804	Invld Time Correct Conn Format
#0113	Out of Connections	#0805	Invld Ping Intrvl EPI Multiplier
#0114	Wrong Module	#0806	Time Coord Msg Min Multiplier

**Messaggi di errore I/O (continua)**

Codice	Messaggio
#0807	Time Expectation Multiplier
#0808	Timeout Multiplier
#0809	Invl Max Consumer Number
#080A	Invl CPCRC
#080B	Time Correction Conn ID Invl
#080C	Safety Cfg Signature Mismatch
#080D	Safety Netwk Num Not Set OutOfBx
#080E	Safety Netwk Number Mismatch
#080F	Cfg Operation Not Allowed
#0814	Data Type Mismatch
#FD01	Bad Backplane EEPROM
#FD02	No Error Code
#FD03	Missing Required Connection
#FD04	No CST Master
#FD05	Axis or GRP Not Assigned
#FD06	SERCOS Transition Fault
#FD07	SERCOS Init Ring Fault
#FD08	SERCOS Comm Fault
#FD09	SERCOS Init Node Fault
#FD0A	Axis Attribute Reject
#FD1F	Safety Data Fault
#FD20	No Safety Task Running
#FD21	Invl Safety Conn Parameter
#FE01	Invalid Connection Type
#FE02	Invalid Update Rate
#FE03	Invalid Input Connection
#FE04	Invalid Input Data Pointer
#FE05	Invalid Input Data Size
#FE06	Invalid Input Force Pointer
#FE07	Invalid Output Connection

Codice	Messaggio
#FE08	Invalid Output Data Pointer
#FE09	Invalid Output Data Size
#FE0A	Invalid Output Force Pointer
#FE0B	Invalid Symbol String
#FE0C	Invalid Scheduled P/C Instance
#FE0D	Invalid Symbol Instance
#FE0E	Module Firmware Updating
#FE0F	Invalid Firmware File Revision
#FE10	Firmware File Not Found
#FE11	Firmware File Invalid
#FE12	Automatic Firmware Update Failed
#FE13	Update Failed – Active Connection
#FE14	Searching Firmware File
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
–	

## Manutenzione della batteria

Argomento	Pagina
Stima della durata della batteria	143
Quando sostituire la batteria	145
Sostituire la batteria	145
Immagazzinaggio delle batterie di ricambio	147

I controllori primari GuardLogix 1756-L6xS ed i coprocessori di sicurezza 1756-LSP contengono una batteria al litio che può essere necessario sostituire. I controllori GuardLogix 1756-L7xS ed i coprocessori di sicurezza 1756-L7SP sono privi di batteria.

### Stima della durata della batteria

La durata della batteria varia in base alla temperatura dello chassis, alla dimensione del progetto ed alla frequenza con cui il controllore viene acceso e spento. La durata della batteria non dipende dal fatto che il controllore sia o meno alimentato.

### Prima che si accenda la spia BAT

Utilizzare la presente tabella per stimare la durata minima della batteria prima che la spia BAT diventi rossa.

**Tabella 52 – Stima spia batteria (durata minima)**

Temperatura 2,54 cm sotto lo chassis	Cicli di spegnimento ed accensione al giorno	Dimensione del progetto			
		1 MB	2 MB	4 MB	8 MB
Da 0 a 40 °C	3	3 anni	3 anni	26 mesi	20 mesi
	2 o meno	3 anni	3 anni	3 anni	31 mesi
Da 41 a 45 °C	3	2 anni	2 anni	2 anni	20 mesi
	2 o meno	2 anni	2 anni	2 anni	2 anni
Da 46 a 50 °C	3 o meno	16 mesi	16 mesi	16 mesi	16 mesi
Da 51 a 55 °C	3 o meno	11 mesi	11 mesi	11 mesi	11 mesi
Da 56 a 60 °C	3 o meno	8 mesi	8 mesi	8 mesi	8 mesi

#### ESEMPIO

Nelle seguenti condizioni, la batteria durerà almeno 20 mesi prima che la spia BAT diventi rossa.

- La temperatura max. 2,54 cm sotto lo chassis è pari a 45 °C.
- L'unità viene spenta e riaccesa tre volte al giorno.
- Il controllore contiene un progetto di 8 MB.

## Dopo l'accensione della spia BAT

**IMPORTANTE** Se la spia BAT si accende per la prima volta quando si attiva l'alimentazione del controllore, significa che l'autonomia della batteria è inferiore al tempo riportato in [Tabella 53](#). L'autonomia della batteria si riduce progressivamente, scaricandosi lentamente ma in modo costante. La carica della batteria può essersi parzialmente consumata mentre il controllore era spento e non era possibile che la spia BAT si accendesse.

**Tabella 53 – Durata della batteria dopo l'accensione della spia BAT con luce rossa (durata minima)**

Temperatura, Max. 25,4 mm sotto lo chassis	Cicli di spegnimento e riaccensione	Dimensione del progetto			
		1 MB	2 MB	4 MB	8 MB
Da 0 a 20 °C	3 al giorno	26 settimane	18 settimane	12 settimane	9 settimane
	1 al giorno	26 settimane	26 settimane	26 settimane	22 settimane
	1 al mese	26 settimane	26 settimane	26 settimane	26 settimane
Da 21 a 40 °C	3 al giorno	18 settimane	14 settimane	10 settimane	8 settimane
	1 al giorno	24 settimane	21 settimane	18 settimane	16 settimane
	1 al mese	26 settimane	26 settimane	26 settimane	26 settimane
Da 41 a 45 °C	3 al giorno	12 settimane	10 settimane	7 settimane	6 settimane
	1 al giorno	15 settimane	14 settimane	12 settimane	11 settimane
	1 al mese	17 settimane	17 settimane	17 settimane	17 settimane
Da 46 a 50 °C	3 al giorno	10 settimane	8 settimane	6 settimane	6 settimane
	1 al giorno	12 settimane	11 settimane	10 settimane	9 settimane
	1 al mese	12 settimane	12 settimane	12 settimane	12 settimane
Da 51 a 55 °C	3 al giorno	7 settimane	6 settimane	5 settimane	4 settimane
	1 al giorno	8 settimane	8 settimane	7 settimane	7 settimane
	1 al mese	8 settimane	8 settimane	8 settimane	8 settimane
Da 56 a 60 °C	3 al giorno	5 settimane	5 settimane	4 settimane	4 settimane
	1 al giorno	6 settimane	6 settimane	5 settimane	5 settimane
	1 al mese	6 settimane	6 settimane	6 settimane	6 settimane



## Quando sostituire la batteria

Quando la batteria è scarica per circa il 95%, il controllore genera i seguenti avvisi:

- la spia BAT nella parte anteriore del controllore si accende (rosso fisso)
- si verifica un errore minore (tipo 10, codice 10 per il controllore).



**ATTENZIONE:** Per evitare perdite di sostanze chimiche potenzialmente pericolose, sostituire la batteria in base al seguente programma, anche se la spia BAT è spenta:

**Tabella 54 – Programma di sostituzione della batteria**

Se la temperatura 2,54 cm sotto lo chassis è	Sostituire la batteria ogni
Da -25 a 35 °C	Sostituzione non necessaria
Da 36 a 40 °C	3 anni
Da 41 a 45 °C	2 anni
Da 46 a 50 °C	16 mesi
Da 51 a 55 °C	11 mesi
Da 56 a 70 °C	8 mesi

### **IMPORTANTE**

Poiché il controllore GuardLogix è di tipo 1002 (a due processori), si raccomanda di sostituire contemporaneamente entrambe le batterie del controllore.

## Sostituire la batteria

Questo controllore contiene una batteria al litio, che dovrà essere sostituita durante la vita utile del prodotto. Per il trattamento e lo smaltimento delle batterie occorre adottare precauzioni di sicurezza specifiche.



**ATTENZIONE:** Il controllore utilizza una batteria al litio che contiene agenti chimici potenzialmente pericolosi.

Prima di trattare o smaltire una batteria, consultare la pubblicazione Direttive per il trattamento delle batterie al litio, [AG-5.4](#).



**AVVISO:** Quando si collega o scollega la batteria, può verificarsi un arco elettrico, che può causare esplosioni in installazioni che si trovano in aree pericolose. Prima di procedere, assicurarsi di aver tolto alimentazione o che l'area non sia pericolosa.

### **IMPORTANTE**

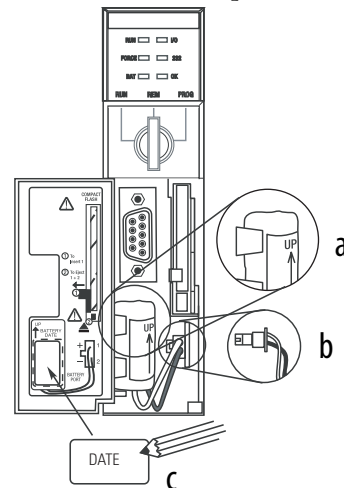
Se si rimuove la batteria ed in seguito si verifica un'interruzione dell'alimentazione, il progetto nel controllore andrà perso.

Per sostituire la batteria, attenersi alla procedura riportata di seguito.

1. Alimentare lo chassis.
2. La batteria mostra segni di perdite o danni?

Se	Procedere come segue
Si	Prima di trattare la batteria, consultare la pubblicazione Direttive per il trattamento delle batterie al litio, pubblicazione <a href="#">AG-5.4</a>
No	Andare al passo successivo.

3. Rimuovere la batteria usata.
4. Installare una batteria 1756-BA2 nuova.
  - a. Inserire la batteria come mostrato nella figura.
  - b. Collegare la batteria:
    - + Rosso
    - Nero
  - c. Annotare la data di installazione della batteria sull'apposita etichetta e fissare l'etichetta all'interno dello sportellino del controllore.



**ATTENZIONE:** Installare solo una batteria 1756-BA2. Se si installa una batteria diversa, il controllore può danneggiarsi.

5. Verificare se la spia BAT nella parte anteriore del controllore è spenta.

Se	Procedere come segue
Si	Andare al passo successivo.
No	<ol style="list-style-type: none"> <li>1. Controllare che la batteria sia connessa correttamente al controllore.</li> <li>2. Se la spia BAT rimane accesa, installare un'altra batteria 1756-BA2.</li> <li>3. Se la spia BAT rimane accesa dopo l'installazione della seconda batteria di cui al punto 2, rivolgersi al rappresentante o al distributore Rockwell Automation di zona.</li> </ol>

---

## 6. Smaltire la batteria usata rispettando le normative locali.



**AVVISO:** Non bruciare né smaltire le batterie al litio con i rifiuti generici. Possono esplodere o rompersi violentemente. Rispettare tutte le normative locali che regolano lo smaltimento di questo genere di materiali. L'utilizzatore è legalmente responsabile dei pericoli creati durante lo smaltimento della batteria.

---



**ATTENZIONE:** Questo prodotto contiene una batteria al litio stagna di cui potrebbe essere necessaria la sostituzione durante la vita utile del prodotto.

Quando la batteria giunge al termine della sua vita utile, deve essere smaltita separatamente dai rifiuti urbani indifferenziati.

La raccolta e il riciclaggio delle batterie contribuiscono alla salvaguardia dell'ambiente ed alla conservazione delle risorse naturali, in quanto si riutilizzano materiali preziosi.

---

## Immagazzinaggio delle batterie di ricambio



**ATTENZIONE:** Se immagazzinate in modo errato, le batterie possono rilasciare sostanze chimiche potenzialmente pericolose. Conservare le batterie in un ambiente fresco e asciutto. Si raccomandano 25 °C con un'umidità relativa dal 40 al 60%. È possibile conservare le batterie fino a 30 giorni a temperature comprese tra -45 °C e 85 °C, ad esempio durante il trasporto. Per evitare possibili perdite, non conservare le batterie a temperature superiori a 60 °C per un periodo superiore a 30 giorni.

---

## Ulteriori riferimenti

Per informazioni sul trattamento, la conservazione e lo smaltimento delle batterie al litio, consultare la pubblicazione Direttive per il trattamento delle batterie al litio, [AG-5.4](#).

**Note:**

## Modifica del tipo di controllore nei progetti RSLogix 5000

Argomento	Pagina
Cambio da controllore standard a controllore di sicurezza	149
Cambio da controllore di sicurezza a controllore standard	150
Passaggio da un controllore GuardLogix 1756 ad un controllore Compact GuardLogix 1768 o viceversa	151
Passaggio da un controllore 1756-L7xS ad un controllore 1756-L6xS o 1768-L4xS	151
Ulteriori riferimenti	151

Dal momento che per i controllori di sicurezza sono previsti requisiti speciali, e che questi ultimi non supportano determinate funzioni standard, è necessario apprendere la procedura di modifica del tipo di controllore (da controllore standard a controllore di sicurezza o viceversa) nel progetto RSLogix 5000. Il cambio del controllore influisce su quanto segue:

- Funzioni supportate
- Configurazione fisica del progetto, ossia coprocessore di sicurezza ed I/O di sicurezza
- Proprietà del controllore
- Componenti del progetto, quali task, programmi, routine e tag
- Istruzioni Add-on di sicurezza.

### Cambio da controllore standard a controllore di sicurezza

Per cambiare correttamente tipo di controllore, passando da un controllore standard ad uno di sicurezza, lo slot dello chassis immediatamente a destra del controllore primario di sicurezza deve essere disponibile per il coprocessore di sicurezza.

Dopo la conferma del cambiamento del progetto da controllore standard a controllore di sicurezza, vengono creati i componenti di sicurezza per soddisfare i requisiti minimi del controllore di sicurezza:

- Il task di sicurezza viene creato solo se il numero massimo di task scaricabili non è stato raggiunto. Il task di sicurezza viene inizializzato con i valori predefiniti.
- Vengono creati i componenti di sicurezza (ossia task di sicurezza, programma di sicurezza e così via).
- Viene generato un numero di rete di sicurezza (SNN), basato su data ed ora, per lo chassis locale.

- Le eventuali funzioni del controllore standard non supportate dal controllore di sicurezza, ad esempio la ridondanza, vengono rimosse dalla finestra di dialogo Controller Properties.

## Cambio da controllore di sicurezza a controllore standard

Dopo la conferma del cambiamento del progetto da controllore di sicurezza a controllore standard, alcuni componenti vengono modificati ed altri eliminati, come descritto di seguito:

- Il coprocessore di sicurezza, 1756-LSP, viene eliminato dallo chassis I/O.
- I moduli I/O di sicurezza ed i relativi tag vengono eliminati.
- Task, programmi e routine di sicurezza vengono cambiati in task, programmi e routine standard.
- Tutti i tag di sicurezza, ad eccezione dei tag consumati, vengono cambiati in tag standard. I tag di sicurezza consumati vengono eliminati.
- Le mappature dei tag di sicurezza vengono eliminate.
- Il numero rete di sicurezza (SNN) viene eliminato.
- Le password di blocco e sblocco di sicurezza vengono eliminate.
- Se il controllore standard supporta funzioni che non erano disponibili con il controllore di sicurezza, tali funzioni risulteranno visibili nella finestra di dialogo Controller Properties.

**SUGGERIMENTO** I controllori di sicurezza peer non vengono eliminati, anche se non è rimasta alcuna connessione.

- Le istruzioni potrebbero ancora fare riferimento a moduli che sono stati cancellati e pertanto determinare errori durante le verifiche.
- I tag consumati vengono cancellati quando si elimina il modulo che li ha prodotti.
- A seguito dei cambiamenti nel sistema descritti sopra, le istruzioni di sicurezza ed i tag I/O di sicurezza non vengono verificati.

Se il progetto del controllore di sicurezza contiene istruzioni add-on di sicurezza, è necessario rimuoverle dal progetto o cambiarne la classe in standard prima di cambiare tipo di controllore.

## **Passaggio da un controllore GuardLogix 1756 ad un controllore Compact GuardLogix 1768 o viceversa**

Quando si cambia tipo di controllore di sicurezza, la classe dei tag, delle routine e dei programmi non viene modificata. Gli eventuali moduli I/O non più compatibili con il controllore di destinazione vengono eliminati.

La rappresentazione del coprocessore di sicurezza viene aggiornata affinché quest'ultimo sia visualizzato correttamente sul controllore di destinazione:

- Quando si passa a un controllore GuardLogix 1756, il coprocessore di sicurezza viene creato nello slot x (slot primario + 1).
- Quando si passa ad un controllore Compact GuardLogix 1768, il coprocessore di sicurezza viene rimosso poiché è interno al controllore Compact GuardLogix.

**SUGGERIMENTO** Il controllore GuardLogix 1756 supporta 100 programmi di sicurezza nel task di sicurezza, mentre il controllore Compact GuardLogix 1768 ne supporta 32.

## **Passaggio da un controllore 1756-L7xS ad un controllore 1756-L6xS o 1768-L4xS**

Le istruzioni a virgola mobile – come FAL, FLL, FSC, SIZE, CMP, SWPB e CPT sono supportate dai controllori 1756-L7xS, ma non dai controllori 1756-L6xS e 1768-L4xS. Se il programma di sicurezza contiene queste istruzioni, verranno generati errori di verifica al passaggio da un controllore 1756-L7xS ad un controllore 1756-L6xS o 1768-L4xS.

## **Ulteriori riferimenti**

Per ulteriori informazioni sulle istruzioni Add-on, consultare il manuale di programmazione Istruzioni add-on per controllori Logix5000, pubblicazione [1756-PM010](#).

**Note:**



## Storico delle modifiche

Questo manuale è stato aggiornato con informazioni relative a nuovi controllori, moduli, applicazioni e funzionalità del software RSLogix 5000. In questa appendice sono riepilogate brevemente le modifiche apportate in ogni versione precedente del manuale.

Per sapere quali modifiche sono state apportate alle versioni precedenti, fare riferimento a questa Appendice. Ciò può risultare particolarmente utile se si decide di aggiornare l'hardware o il software in base alle informazioni aggiunte nelle precedenti versioni di questo manuale.

### **1756-UM020H-EN-P, Aprile 2012**

Correzione dell'elenco di alimentatori supportati.

### **1756-UM020G-EN-P, Febbraio 2012**

- Aggiunta di informazioni sui controllori 1756-L7xS e 1756-L73SXT
- Aggiornamento dell'elenco di Ulteriori riferimenti
- Aggiunta di un capitolo sull'installazione del controllore
- Aggiunta di informazioni sull'uso di connessioni unicast per moduli I/O su reti EtherNet/IP
- Aggiunta di informazioni sull'installazione
- Aggiunta di informazioni sulla protezione della modalità Esecuzione per la firma del task di sicurezza
- Aggiornamento delle procedure di sostituzione I/O con esame di vari casi di sostituzione
- Aggiornamento del valore massimo dell'intervallo di pacchetto richiesto (RPI)
- Aggiunta dei tipi di dati DCA\_INPUT e DCAF\_INPUT nell'elenco di tipi validi per i tag di sicurezza
- Riorganizzazione delle informazioni sui tag di sicurezza prodotti e consumati e la configurazione di controllori di sicurezza peer in modo che tutte le informazioni siano raggruppate nel Capitolo 6
- Aggiunta di informazioni sulle conseguenze del blocco di una scheda SD su un aggiornamento del firmware
- Aggiunta di informazioni sull'uso del modulo ESM (Modulo di accumulo energia) per memoria non volatile
- Spostamento delle tabelle di descrizione degli indicatori di stato in un'appendice ed aggiornamento delle informazioni per la ricerca guasti
- Aggiornamento delle informazioni sulle tempistiche di sostituzione della batteria sui controllori 1756-L6xS

- Aggiunta di informazioni sul passaggio ad un controllore 1756-L7xS
- Aggiunta dell'appendice Storico delle modifiche

### **1756-UM020F-EN-P, Agosto 2010**

- I controllori GuardLogix sono supportati da RSLogix 5000, versione 19
- Il tipo di connessione di default per i tag di sicurezza prodotti e consumati è unicast

### **1756-UM020E-EN-P, Gennaio 2010**

- Aggiunta di istruzioni Add-On ad alta integrità e di sicurezza nell'elenco delle funzioni di RSLogix 5000 supportate
- Abilitazione della sincronizzazione temporale
- Aggiornamento degli esempi di modifica del numero di rete di sicurezza (SNN) dei moduli I/O di sicurezza sulla rete CIP Safety per la visualizzazione dei moduli I/O di sicurezza EtherNet/IP
- Chiarimento delle informazioni relative all'indirizzamento Ethernet
- Connessioni ControlNet per moduli I/O distribuiti
- Definizione di un tag come costante
- Impostazione del livello di accesso esterno per i dati dei tag
- Aggiornamento delle procedure di produzione e consumo dei tag di sicurezza
- Restrizione relativa alla mappatura dei tag con valori costanti
- Aggiornamento della tabella delle risposte del software durante il download
- Accessibilità GSV/SSV dell'oggetto di sicurezza AOI
- Memorizzazione e caricamento di progetti con la memoria non volatile
- Aggiornamento delle informazioni relative allo smaltimento della batteria
- Passaggio da un controllore GuardLogix 1756 ad un controllore Compact GuardLogix 1768 o viceversa

### **1756-UM020D-EN-P, Luglio 2008**

- Aggiornamento della tabella Ulteriori riferimenti con inserimento di nuovi manuali
- Informazioni sul controllore 1756-L63S
- Informazioni generali sulla programmazione con il software RSLogix 5000, versione 17, incluse versioni del software supportate e migliorie
- utilizzo di un modulo 1756-EN2T in un sistema basato su GuardLogix
- Informazioni sui moduli di sicurezza Guard I/O EtherNet/IP
- Aggiornamento dell'elenco di tipi di dati validi per i tag di sicurezza
- Le azioni di blocco e sblocco di sicurezza vengono salvate nel registro
- La creazione e l'eliminazione di una firma di sicurezza vengono salvate nel registro
- Il processo di download ora prevede il controllo del master CST (tempo di sistema coordinato)
- Aggiornamento della descrizione del codice di errore relativo al mancato funzionamento del task di sicurezza

- Il valore della firma di sicurezza è accessibile tramite istruzione GSV
- Informazioni sui tipi di dati per attributi accessibili tramite istruzioni GSV e SSV
- Consultazione delle informazioni sugli errori tramite istruzione GSV
- Aggiornamento delle informazioni sulla certificazione
- Aggiornamento delle informazioni sull'autonomia stimata della batteria
- Aggiornamento delle informazioni relative allo smaltimento corretto della batteria

### **1756-UM020C-EN-P, Dicembre 2006**

- Informazioni sul flusso di dati del controllore GuardLogix
- Il controllore non supporta l'esecuzione di aggiornamenti del sistema operativo tramite CompactFlash
- Il task di sicurezza non supporta le istruzioni Add-On o il software FactoryTalk® Alarms and Events
- Il valore massimo di RPI per le connessioni di sicurezza è stato modificato da 500 ms a 100 ms
- L'elenco di tipi di dati non validi per i programmi di sicurezza è stato sostituito da un elenco di tipi di dati validi
- Revisione della descrizione delle connessioni di sicurezza prodotte e consumate
- Revisione della descrizione dell'effetto della funzione di blocco di sicurezza e della firma di sicurezza sul download
- Aggiunta certificazione UL NRGF
- Aggiunti valori PFD (probabilità di guasto su domanda) e PFH (probabilità di guasto all'ora) nelle specifiche del controllore

### **1756-UM020B-EN-P, Ottobre 2005**

Il software di programmazione RSLogix 5000, versione 14.01 e successive, non esegue più il confronto delle serie hardware tra coprocessore di sicurezza e controllore primario o tra controllore e firma di sicurezza nel progetto.

### **1756-UM020A-EN-P, Gennaio 2005**

Versione iniziale.



## Numerics

**1747-CP3** 38, 109  
**1747-KY** 27  
**1756-Axx** 28  
**1756-BA2** 27, 28, 146  
**1756-CN2** 63  
**1756-CN2R** 63  
**1756-CN2RXT** 63  
**1756-CNB** 63  
**1756-CNBR** 63  
**1756-CP3** 27, 38, 109  
**1756-DNB** 65, 67, 109  
**1756-EN2F** 59  
**1756-EN2T** 59  
**1756-EN2TR** 59  
**1756-EN2TXT** 59  
**1756-EN3TR** 59  
**1756-ENBT** 59  
**1756-ESMCAP** 27, 44, 46, 122, 124  
**1756-ESMCAPXT** 27, 44, 46, 122, 124  
**1756-ESMNRM** 27, 44, 46, 122, 124  
**1756-ESMNRMXT** 27, 46, 122, 124  
**1756-ESMNSE** 27, 44, 46, 122, 124  
**1756-ESMNSEXT** 27, 46, 122, 124  
**1756-EWEB** 59  
**1756-PA72** 28  
**1756-PA75** 28  
**1756-PAXT** 28  
**1756-PB72** 28  
**1756-PB75** 28  
**1756-PBXT** 28  
**1756-SPESMCAP** 27, 44  
**1756-SPESMNRM** 27, 46, 122  
**1756-SPESMNRMXT** 27, 46, 122  
**1756-SPESMNSE** 27, 44, 46, 122  
**1756-SPESMNSEXT** 27, 44, 46, 122  
**1784-CF128** 27  
**1784-SD1** 27  
**1784-SD2** 27

## A

**aggiornamenti** 19  
**aggiornamenti automatici del firmware** 124  
**aggiornamento**  
   firmware 40, 41  
**alimentatore**  
   numeri di catalogo 19, 28  
**ambiente** 23  
**ambiente estremo**  
   alimentatore 28  
   chassis 28  
   componenti del sistema 12  
   controllore 12

## approvazione per l'uso in aree pericolose

  europa 26  
   Nord America 25

## archiviazione dei programmi utente 19

### attributi

  oggetto di sicurezza 132

### autenticazione di configurazione

  componenti 75  
   copia 75  
   definizione 75

### AutoFlash

  aggiornamento firmware 41

## B

### barra di stato 125

### batteria 27

  collegare 145  
   connettere 28, 29, 146  
   durata 143, 144  
   errore 125, 130  
   immagazzinaggio 147  
   installazione 146  
   procedura di sostituzione 145  
   programma di sostituzione 145  
   scollegare 145, 146  
   smaltimento 147

### batteria al litio 145, 147

### bit ConnectionFaulted 127

### bit RunMode 127

### blocco di sicurezza 105

  controllore 106  
   effetto sul download 112  
   effetto sull'upload 112  
   icona 105  
   password 106

## C

### cambio del controllore 149–150

### cancellazione

  errori 129  
   programma 123

### capacità RAM 18

### caricamento di un progetto 121

  all'accensione 121  
   avviato dall'utente 121  
   se la memoria è danneggiata 121

### chassis 19

  numeri di catalogo 28

### CIP Safety 12, 53, 85

### classe 96

### codici di errore

  display di stato 130  
   errori di sicurezza gravi 130  
   messaggi I/O 140

### codifica elettronica 124

### collegamento online 116

  fattori 111

**componenti del sistema Logix-XT**

vedere ambiente estremo.

**comunicazione 20**

- moduli 20
- rete ControlNet 63
- rete DeviceNet 65
- rete EtherNet/IP 59
- rete seriale 67

**condizioni predefinite in fabbrica 81**

reset modulo 79

**configurazione avanzata del tempo di risposta della connessione 73****configure always 84**

casella di controllo 51

**CONNECTION\_STATUS 97, 127****connessione**

- monitoraggio 126
- non schedulata 64
- rete ControlNet 63
- rete EtherNet/IP 60
- schedulata 64
- stato 127
- USB 35

**connessione di solo ascolto 76****connessioni non schedulate 64****connessioni schedulate 64****consumo dati tag 100****controllo remoto 42, 43****controllore**

- ambiente estremo 12
- cambio del tipo 149–151
- configurazione 47
- corrispondenza 111
- funzioni differenti 11
- gestore degli errori 131
- installazione 29
- mancata corrispondenza numero seriale 114, 117
- modalità 42
- modalità operativa 42, 43
- numero seriale 111
- properties 48
- registrazione
  - blocco/sblocco sicurezza 105
  - firma del task di sicurezza 107

**controllore Compact GuardLogix 151****controllore Compact GuardLogix 1768 151****controllore di sicurezza peer**

- condivisione dati 97
- configurazione 52
- posizione 97
- SNN 97, 98

**controllore primario**

- descrizione 18
- memoria utente 18
- modalità 19
- panoramica dell'hardware 18

**controllori GuardLogix**

differenze 11

**ControlNet**

- configurazione del driver 110
- connessioni 63, 110
- esempio 64
- moduli di comunicazione 20
- modulo 63, 109
- non schedulata 64
- panoramica 63
- schedulata 64
- software 63

**copertura diagnostica 12****copia**

- firma del task di sicurezza 107
- numero di rete di sicurezza 58

**coprocessore di sicurezza**

- configurazione 19
- descrizione 19
- indicatori di stato 135
- stato 128

**corrispondenza tra progetto e controllore 111****creazione di un progetto 47****custodia 23****D****dati standard in una routine di sicurezza 103****DeviceNet**

- comunicazione 65
- configurazione del driver 110
- connessioni 67, 110
- modulo 109
- software 66

**DF1 68****DH-485 68****dispositivi di interfaccia operatore 16****download**

- effetto del blocco di sicurezza 112
- effetto della corrispondenza del controllore 111
- effetto della corrispondenza della versione del firmware 111
- effetto della firma del task di sicurezza 112
- effetto dello stato di sicurezza 111
- processo 113–114

**driver**

- ControlNet 110
- DeviceNet 110
- EtherNet/IP 110
- USB 36

**driver del dispositivo RS-232 DF1 38****E****eliminazione**

firma del task di sicurezza 108

**errore**

- cancellazione 129
- irreversibile controllore 129
- messaggi 139
- reversibile 129, 139
- routine 131–133
- sicurezza irreversibile 128, 129

**errore di sicurezza irreversibile** 128, 129

riavvio del task di sicurezza 129

**errore irreversibile controllore** 129**errore reversibile** 129, 139

cancellazione 129

**errori di sicurezza gravi** 130**errori di verifica**

cambio del tipo di controllore 151

**errori gravi reversibili** 139**ESM**

vedere modulo di alimentazione

**EtherNet/IP**

capacità modulo 59

configurazione del driver 110

configurazione esemplificativa 61

connessioni 60, 110

esempio 61

moduli 59

moduli di comunicazione 20

moduli I/O CIP Safety 62

moduli I/O standard 62

modulo 109

panoramica 59

parametri di rete 62

software 60

uso della connessione 60

**external access** 92, 96**F****file DNT** 87, 88**finestra di dialogo New Controller** 47**firma del task di sicurezza** 96

copia 107

descrizione 16

effetto sul download 112

effetto sull'upload 112

eliminazione 108

generazione 106

memorizzazione di un progetto 120

operazioni non consentite 107

restrizioni 108

visualizzazione 125

**Firmware Supervisor** 124**forzatura** 107**funzioni di sicurezza di RSLogix** 106**G****gateway** 62**get system value (GSV)**

accessibilità 132

definizione 12

utilizzo 132

**I****I/O**

codici di errore 140

indicatore 126

sostituzione modulo 51

**I/O CIP Safety**

aggiunta 69

autenticazione di configurazione 75

dati di stato 77

indirizzo di nodo 69

monitoraggio dello stato 77

reset ownership 76

**incolla**

numero di rete di sicurezza 58

**indicatore BAT** 125**indicatori di stato** 127

moduli I/O 78

**indirizzo**

modulo I/O CIP Safety 77

**indirizzo di nodo** 69**Indirizzo IP** 69**intervallo di pacchetto richiesto** 97

dati tag prodotto 93

definizione 12

I/O CIP Safety 72

tag consumati 93

tag consumato 101

**IP address** 62**Istruzioni add-on** 21, 150**K****kit di aggiornamento firmware** 111, 124**L****Livelli prestazionali** 12**Livelli prestazionali (LP)** 15**LOCK (blocco)**

vedere blocco di sicurezza.

**M****Major Recoverable Fault**

messaggi 139

**MajorFaultRecord** 133**massimo ritardo di rete osservato** 73

reset 101

**memoria**

capacità 18

scheda 19

**memoria non volatile** 119–124

scheda 119

**memoria utente** 18

**memorizzazione di un progetto** 120**messaggi**

- errore 139
- stato di sicurezza 137
- stato generale 138

**messaggi di stato generali** 138**messaggio**

- display di stato 138

**modalità**

- operativa 42

**modalità Esecuzione** 42**modalità operativa** 42**modalità programmazione** 42**modifica** 107**modulo**

- ControlNet 20
- DeviceNet 20
- EtherNet/IP 20, 59
- indicatore di stato 78
- properties
  - scheda Connection 76

**modulo di alimentazione** 27

- 1756-ESMCAP 27
- definizione 12
- disinstallazione 44
- in carica 29, 46
- installazione 46
- memoria non volatile 122
- tempo di mantenimento 124

**modulo Guard I/O**

- sostituzione 79–88

**monitoraggio**

- connessioni 126
- stato 77

**multicast** 12**N****network delay multiplier** 74, 102**numero di rete di sicurezza** 53

- assegnazione 53
- assegnazione automatica 55
- assegnazione manuale 55
- basato sul tempo 54
- copia 58
- copia ed incolla 58
- definizione 12
- descrizione 15
- formati 53
- gestione 53
- impostazione 71
- incolla 58
- mancata corrispondenza 86
- manuale 54
- modifica 55
- modifica del valore SNN del controllore 56
- modifica del valore SNN dell'I/O 56
- visualizzazione 48

**numero di slot** 48**numero seriale** 111**O****oggetto di sicurezza**

- attributi 132

**P****password**

- caratteri validi 50
- impostazione 49

**periodo task di sicurezza** 72, 91, 97**PFD (probabilità di guasto su domanda)**

- definizione 12

**PFH (probabilità di guasto all'ora)**

- definizione 12

**produzione di un tag** 99**produzione e consumo di tag** 60, 63, 97**progetti di sicurezza**

- funzioni 21

**programma di sostituzione**

- batteria 145

**programmazione** 107**programmi di sicurezza** 92**proprietà**

- configurazione 76
- ripristino 76

**proprietario della configurazione** 76

- identificazione 76
- ripristino 76, 79

**protezione dell'applicazione****di sicurezza** 105–108

- blocco di sicurezza 105
- firma del task di sicurezza 106
- funzioni di sicurezza di RSLogix 106

**protezione della firma in modalità esecuzione**

50

**protezione modalità esecuzione** 106, 108**protocollo di controllo ed informazioni**

- definizione 12

**pulsante Change Controller** 49**R****radiazione UV** 26**reset**

- modulo 79
- proprietà 76, 79

**restrizioni**

- mappatura dei tag di sicurezza 103
- programmazione 108
- se è stata configurata una firma di sicurezza 107
- se in blocco di sicurezza 105
- software 108

**rimozione ed inserimento sotto tensione****(RIUP)** 24**RIUP**

- vedere rimozione ed inserimento sotto tensione (RIUP)



**routine di errore del programma** 131  
**routine di sicurezza** 92  
 utilizzo di dati standard 103  
**RPI**  
 vedere intervallo di pacchetto richiesto

## S

**SafetyTaskFaultRecord** 133  
**salvataggio del programma**  
 memoria non volatile 123  
**sblocco controllore** 106  
**sblocco di sicurezza**  
 controllore 106  
 icona 105  
**scarica elettrostatica** 26  
**scheda CF**  
 Vedere scheda CompactFlash.  
**Scheda CompactFlash** 27, 30  
 vedere anche scheda di memoria.  
**scheda CompactFlash**  
 inserimento 33  
 rimozione 34  
**scheda di memoria** 119, 120, 121, 124  
 installazione 30  
 rimozione 30  
**scheda Major Faults** 130  
**scheda Minor Faults** 130  
**scheda Safety** 106, 107, 128  
 autenticazione di configurazione 75  
 blocco di sicurezza 106  
 blocco di sicurezza del controllore 106  
 dati connessione 72  
 generazione di una firma del task  
 di sicurezza 107  
 sblocco 106  
 sostituzione modulo 80  
 visualizzazione dello stato  
 di sicurezza 111, 128  
**scheda SD**  
 vedere scheda secure digital.  
**scheda secure digital** 27, 30  
 installazione 32  
 rimozione 31  
 vedere anche scheda di memoria.  
**selettore a chiave** 19, 42  
**seriale**  
 cavo 27  
 comunicazione 67  
 driver 38  
 porta 37  
 configurazione 67  
 connessione 37  
 rete 67  
 software 67  
**set system value (SSV)**  
 accessibilità 132  
 utilizzo 132  
**simbolo di avviso** 126

**sincronizzazione temporale** 51, 114  
**SNN**  
 Vedere numero rete di sicurezza  
**software**  
 restrizioni 108  
 rete ControlNet 63  
 rete EtherNet/IP 60  
 reti DeviceNet 66  
 USB 35  
**software ControlFLASH** 40, 111, 121, 124  
**software RSLinx Classic**  
 versione 21  
**software RSLogix 5000**  
 reset modulo 79  
 restrizioni 108  
 versioni 21  
**software RSNetWorx for DeviceNet**  
 sostituzione modulo 86  
**sostituzione**  
 configure always abilitata 84  
 configure only . . . enabled 80  
 modulo Guard I/O 79–88  
**spia BAT** 144, 146  
**stato**  
 coprocessore di sicurezza 128  
 display 137–142  
 indicatori 135–137  
 messaggi 137  
 messaggi di errore 139  
 messaggi, display 138  
**stato della rete**  
 indicatore 78, 82, 83, 87  
**stato di sicurezza** 15  
 effetto sul download 111  
 firma del task di sicurezza 106  
 programmazione delle restrizioni 108  
 pulsante 106, 126  
 visualizzazione 111, 125, 128  
**subnet mask** 62

## T

**tag**  
 alias 93  
 ambito 95  
 base 93  
 classe 96  
 constant value 96  
 consumato 93, 97  
 dati di sicurezza prodotti/consumati 94, 95  
 dell'ambito del programma 95  
 denominazione 76  
 external access 92, 96  
 I/O di sicurezza 94, 95  
 panoramica 92  
 prodotto 93, 97  
 tag dell'ambito del controllore 95  
 tipo 93  
 tipo di dati 94  
 Vedere anche  
 tag di sicurezza.

**tag alias** 93  
**tag base** 93  
**tag constant value** 96  
**tag consumato** 93, 97  
**tag definiti nell'ambito del programma** 95  
**tag dell'ambito del controllore** 95  
**tag di sicurezza**  
     creazione 93  
     dell'ambito del controllore 95  
     dell'ambito del programma di sicurezza 95  
     descrizione 92  
     mappatura 102–104  
     tipi di dati validi 94  
**tag prodotto** 93, 97  
**task di sicurezza** 90  
     esecuzione 91  
     priority 90  
     tempo di watchdog 90  
**tempi di scansione**  
     reset 108  
**tempo di mantenimento**  
     modulo di alimentazione 124  
**tempo di risposta** 91  
**tempo di sistema coordinato** 114, 137  
**tempo di watchdog** 90  
**tempo limite di risposta**  
     I/O CIP Safety 71  
**tempo limite di risposta della**  
     **connessione** 71, 101  
**terminologia** 12  
**timeout multiplier** 73, 102  
**tipi di dati**  
     CONNECTION\_STATUS 97  
**tipi di dati REAL** 94  
**trasformazione**  
     Vedere cambio del controllore.

## U

**unicast** 12  
     connessioni 71, 97, 100  
**upload**  
     effetto del blocco di sicurezza 112  
     effetto della corrispondenza  
         del controllore 111  
     effetto della firma del task di sicurezza 112  
     processo 115  
**USB**  
     cavo 35, 109  
     connessione 35  
     driver 36  
     porta 35  
     software richiesto 35  
     tipo 35

## V

**versione firmware**  
     aggiornamento 40, 41  
     corrispondenza 111  
     gestione 124  
     mancata corrispondenza 112, 114, 117  
**visualizzazione**  
     stato di sicurezza 111

## W

**WallClockTime** 122, 124  
     modulo di alimentazione 124  
     oggetto 46

## X

**XT**  
     vedere ambiente estremo.



## Assistenza Rockwell Automation

Rockwell Automation fornisce informazioni tecniche sul Web per assistere i clienti nell'utilizzo dei prodotti. All'indirizzo <http://www.rockwellautomation.com/support/>, è possibile consultare manuali tecnici, una knowledge base di domande frequenti, note tecniche ed applicative, scaricare codici di esempio e service pack ed utilizzare la funzione MySupport, personalizzabile per utilizzare al meglio tali strumenti.

Per ottenere ulteriore assistenza telefonica per l'installazione, la configurazione e la ricerca guasti, sono disponibili i programmi di assistenza TechConnect<sup>SM</sup>. Per ulteriori informazioni, contattare il proprio distributore di zona o il rappresentante Rockwell Automation, oppure visitare il sito <http://www.rockwellautomation.com/support/>.

## Assistenza per l'installazione

Se si verifica un problema entro le prime 24 ore dall'installazione, si prega di consultare le informazioni contenute in questo manuale. Per richiedere assistenza durante la messa in servizio iniziale del prodotto, rivolgersi all'Assistenza Clienti.

Stati Uniti o Canada	1.440.646.3434
Al di fuori degli Stati Uniti o del Canada	Utilizzare il <a href="#">Worldwide Locator</a> sul sito <a href="http://www.rockwellautomation.com/support/americas/phone_en.html">http://www.rockwellautomation.com/support/americas/phone_en.html</a> , oppure contattare il rappresentante Rockwell Automation di zona.

## Restituzione di prodotti nuovi non funzionanti

Rockwell Automation testa tutti i prodotti per garantire che siano completamente funzionanti al momento della spedizione dall'impianto di produzione. Tuttavia, se il prodotto non funziona e deve essere restituito, procedere come segue:

Stati Uniti	Rivolgersi al proprio distributore. Per completare la procedura di restituzione è necessario fornire al distributore il numero di pratica dell'Assistenza Clienti (per ottenerne uno chiamare il numero telefonico riportato sopra).
Fuori dagli Stati Uniti	Per la procedura di restituzione, si prega di contattare il rappresentante Rockwell Automation di zona.

## Commenti relativi alla documentazione

I commenti degli utenti sono molto utili per capire le loro esigenze in merito alla documentazione. Per proporre dei suggerimenti su eventuali migliorie da apportare al presente documento, compilare il modulo [RA-DU002](#), disponibile sul sito <http://www.rockwellautomation.com/literature/>.

**[www.rockwellautomation.com](http://www.rockwellautomation.com)**

### Power, Control and Information Solutions Headquarters

Americhe: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496, USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444

Europa/Medio Oriente/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgio, Tel: +32 2 663 0600, Fax: +32 2 663 0640

Asia: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: +852 2887 4788, Fax: +852 2508 1846

Italia: Rockwell Automation S.r.l., Via Gallarate 215, 20151 Milano, Tel: +39 02 334471, Fax: +39 02 33447701, [www.rockwellautomation.it](http://www.rockwellautomation.it)

Svizzera: Rockwell Automation AG, Via Cantonale 27, 6928 Manno, Tel: 091 604 62 62, Fax: 091 604 62 64, Customer Service: Tel: 0848 000 279