Manuale di riferimento per la sicurezza

Allen-Bradley

Sistemi di controllo GuardLogix 5570

Numeri di catalogo 1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT, 1756-L7SP, 1756-L7SPXT, 1756-L72EROMS, applicazioni Logix Designer Studio 5000

Istruzioni originali

Importanti informazioni per l'utente

Prima di installare, configurare, utilizzare o manutenere questo prodotto, leggere questo documento e quelli elencati nella sezione "Altre risorse" riguardanti le operazioni di installazione, configurazione ed utilizzo di questa apparecchiatura. Gli utenti devono conoscere bene le istruzioni di installazione e cablaggio oltre che i requisiti di codici, leggi e norme applicabili nel loro complesso.

Le attività che includono operazioni di installazione, regolazione, messa in servizio, utilizzo, montaggio, smontaggio e manutenzione devono essere realizzate da personale adeguatamente addestrato, nel rispetto delle prassi applicabili.

Se questa apparecchiatura viene utilizzata diversamente da come specificato dal costruttore, la protezione fornita dall'apparecchiatura può essere compromessa.

In nessun caso Rockwell Automation, Inc. sarà obbligata per legge o responsabile di danni indiretti o conseguenti derivanti dall'utilizzo o dall'applicazione di queste apparecchiature.

Gli esempi e gli schemi riportati nel presente manuale sono inclusi soltanto per scopi illustrativi. Viste le numerose variabili ed i numerosi requisiti associati con qualsiasi installazione particolare, Rockwell Automation, Inc. non può assumersi la responsabilità o l'obbligo per legge relativi all'utilizzo effettivo sulla base degli esempi e dei diagrammi.

Rockwell Automation, Inc. non si assume alcuna responsabilità di brevetto per quanto riguarda l'utilizzo di informazioni, circuiti elettrici, apparecchiature o software descritti nel presente manuale.

È vietata la riproduzione integrale o parziale dei contenuti del presente manuale senza permesso scritto di Rockwell Automation, Inc.

In tutto il presente manuale, quando risulta necessario, vengono utilizzate note per mettere in evidenza considerazioni sulla sicurezza.

	**AVVISO:** Identifica informazioni sulle pratiche o circostanze che possono causare un'esplosione in un ambiente pericoloso con possibili conseguenti lesioni personali o morte, danni materiali e perdita economica.
	**ATTENZIONE:** Identifica le informazioni sulle pratiche o circostanze che possono determinare lesioni personali o morte, danni materiali o perdita economica. I simboli Attenzione consentono di identificare o evitare un pericolo e di riconoscerne le conseguenze.
IMPORTANTE	Identifica informazioni che sono cruciali per una corretta applicazione e per la comprensione del prodotto.

Anche sull'apparecchiatura o al suo interno, possono essere apposte etichette che segnalano la necessità di adottare precauzioni specifiche.

	**PERICOLO DI FOLGORAZIONE:** Potranno essere collocate delle etichette sull'apparecchiatura o al suo interno, per esempio su azionamento o motore, per attirare l'attenzione dell'utente sulla tensione potenzialmente pericolosa presente.
	**PERICOLO DI USTIONI:** Potranno essere collocate delle etichette sull'apparecchiatura o al suo interno, per esempio su azionamento o motore, per attirare l'attenzione dell'utente sulle superfici che potrebbero raggiungere temperature potenzialmente pericolose.
	**PERICOLO DI ARCO ELETTRICO:** Sull'apparecchiatura o al suo interno – ad es. in un motor control center – possono essere apposte etichette che avvisano del rischio di arco elettrico. L'arco elettrico può provocare lesioni gravi o letali. Indossare adeguati dispositivi di protezione individuale (DPI). Seguire TUTTI i requisiti regolamentari relativi alle pratiche di lavoro in sicurezza ed ai dispositivi di protezione individuale (DPI).

Questo manuale contiene informazioni nuove ed aggiornate.

Informazioni nuove ed aggiornate

Questa tabella contiene le modifiche apportate a questa versione.

Argomento	Pagina
Modifica dei riferimenti al modulo I/O di sicurezza come al più generico dispositivo I/O di sicurezza, come appropriato	In tutto il manuale
Aggiunta del numero di catalogo di Armor™ GuardLogix®, 1756-L72EROMS, sulla copertina	Copertina
Aggiunta delle informazioni sui servoazionamenti Kinetix® 5500 all'elenco dei componenti certificati SIL-3	16
Aggiunta del modulo 1756-EN2TRXT all'elenco dei moduli interfaccia di comunicazione	23
Aggiunta di una nota relativa al fatto che il progetto non esegue la verifica della presenza di combinazioni duplicate di SNN ed indirizzo di nodo	35
Aggiunta di un riferimento al manuale dell'utente Servoazionamenti Kinetix 5500 per informazioni sull'utilizzo di Motion Direct Commands in applicazioni di sicurezza	72
Aggiunta di dati di sicurezza aggiornati (IEC 61508 Ed 2, 2010) per i moduli Guard I/O™	Appendice E
Aggiunta di dati di sicurezza per i moduli 1734-IB8S, serie B e 1734-OB8S, serie B	Appendice E
Aggiornamento dei dati PFH per i moduli 1734-IE4S	Appendice E

Note:

Capitolo 5

Caratteristiche dei tag di sicurezza, del task di sicurezza e dei programmi di sicurezza

Capitolo 6

Sviluppo dell'applicazione di sicurezza

Capitolo 7

Monitoraggio dello stato e gestione degli errori

Appendice A

Istruzioni di sicurezza

Appendice B

Istruzioni Add-On di sicurezza

Appendice C

Tempi di risposta

Nel presente manuale viene descritto il sistema di controllo GuardLogix 5570, **type-approved** e certificato per l'uso in applicazioni di sicurezza fino al livello SIL CL 3 incluso, in conformità alle normative IEC 61508 e IEC 62061, ed applicazioni di sicurezza fino al livello prestazionale PLe (Categoria 4) incluso, in conformità alla normativa ISO 13849-1.

Utilizzare questo manuale se si è responsabili dello sviluppo, del funzionamento o della manutenzione di un sistema di sicurezza basato su un controllore GuardLogix 5570 che usa l'applicazione Logix Designer Studio 5000®, versione 21.000 o successiva. Leggere e comprendere i concetti ed i requisiti di sicurezza riportati nel presente manuale prima di utilizzare un sistema di sicurezza basato sul controllore GuardLogix 5570.

Per i requisiti di sicurezza relativi ai controllori GuardLogix 5570 nei p rogetti RSLogix™ 5000, consultare il manuale di riferimento per la sicurezza GuardLogix Controllers, pubblicazione 1756-RM093.

Ambiente Studio 5000

Studio 5000 Automation Engineering and Design Environment™ combina elementi di sviluppo e progettazione in un ambiente comune. Il primo elemento dell'ambiente Studio 5000 è l'applicazione Logix Designer. L'applicazione Logix Designer è il rebranding del software RSLogix 5000 e continua ad essere il prodotto destinato alla programmazione dei controllori Logix5000™ per soluzioni di controllo discreto, di processo, batch, controllo assi, sicurezza e basate su azionamenti.

L'ambiente Studio 5000 rappresenta la base delle funzionalità e degli strumenti futuri di progettazione e sviluppo di Rockwell Automation®. Un unico ambiente in cui i progettisti possono sviluppare tutti gli elementi di un sistema di controllo.

Terminologia

La seguente tabella definisce i termini utilizzati nel presente manuale.

Tabella 1 – Termini e definizioni

Abbreviazione	Termine completo	Definizione
1oo2	One Out of Two (uno di due)	Identifica l'architettura del controllore elettronico programmabile.
CIP	Common Industrial Protocol	Un protocollo di comunicazione industriale utilizzato dai sistemi di automazione basati su Logix5000 su reti di comunicazione Ethernet™, ControlNet™ e DeviceNet™.
CIP Safety	Common Industrial Protocol – Safety	Versione SIL 3 del protocollo CIP.
DC	copertura diagnostica	Il rapporto tra il tasso di guasto rilevato ed il tasso di guasto complessivo.
EN	Norma europea.	Lo standard europeo ufficiale.
GSV	Get System Value	Un'istruzione della logica ladder che recupera informazioni specifiche sullo stato del controllore e le colloca in un tag di destinazione.
PC	Personal Computer	Computer utilizzato per interfacciare e controllare un sistema basato su Logix attraverso l'ambiente Studio 5000.
PFD	Probabilità di guasto su domanda	La probabilità media di un sistema di non adempiere alla sua funzione di sicurezza quando ne viene richiesto l'intervento.
PFH	Probabilità di guasto all'ora	La probabilità per un sistema di subire un errore pericoloso in un'ora.
PL	Livello prestazionale	Classe di sicurezza ISO 13849-1.
SNN	Numero della rete di sicurezza	Un numero univoco che identifica una sezione della rete di sicurezza.
SSV	Set System Value	Un'istruzione della logica ladder che imposta i dati del sistema di controllo.
--	Standard	Qualsiasi oggetto, task, tag, programma o componente del progetto non considerato relativo alla sicurezza (ossia, il termine "controllore standard" si riferisce genericamente ad un controllore ControlLogix® o CompactLogix™).

Altre risorse

Questi documenti contengono altre informazioni sui prodotti correlati di Rockwell Automation.

Risorsa	Descrizione
Manuale dell'utente GuardLogix 5570 Controllers, pubblicazione 1756-UM022	Fornisce informazioni sulle modalità di installazione, configurazione, programmazione ed utilizzo dei controllori GuardLogix 5570 nei progetti Logix Designer Studio 5000
Manuale di riferimento Set di istruzioni per l'applicazione di sicurezza GuardLogix, pubblicazione 1756-RM095	Fornisce informazioni sull'insieme di istruzioni GuardLogix per applicazioni di sicurezza
Manuale dell'utente Guard I/O DeviceNet Safety Modules, pubblicazione 1791DS-UM001	Fornisce informazioni sull'utilizzo dei moduli di sicurezza Guard I/O DeviceNet
Manuale dell'utente Moduli di sicurezza Guard I/O EtherNet/IP, pubblicazione 1791ES-UM001	Fornisce informazioni sull'utilizzo dei moduli di sicurezza Guard I/O EtherNet/IP
Manuale dell'utente Moduli di sicurezza POINT Guard I/O, pubblicazione 1734-UM013	Fornisce informazioni sull'installazione e l'utilizzo dei moduli POINT Guard I/O™
Manuale dell'utente Servoazionamenti Kinetix 5500, pubblicazione 2198-UM001	Fornisce informazioni sull'installazione e l'utilizzo dei servoazionamenti Kinetix 5500
Manuale di riferimento per la sicurezza Using ControlLogix in SIL 2 Applications, pubblicazione 1756-RM001	Descrive i requisiti previsti per l'uso dei controllori ControlLogix e del task standard GuardLogix nelle applicazioni di controllo di sicurezza SIL 2
Manuale di riferimento Istruzioni generali per controllori Logix5000, pubblicazione 1756-RM003	Fornisce informazioni sull'insieme di istruzioni Logix5000
Manuale di programmazione Logix Common Procedures, pubblicazione 1756-PM001	Fornisce informazioni sulla programmazione dei controllori Logix5000, oltre che sulla gestione dei file di progetto, sull'organizzazione dei tag, sulla programmazione e la prova delle routine e sul trattamento degli errori
Manuale di programmazione Istruzioni add-on per controllori Logix5000, pubblicazione 1756-PM010	Fornisce informazioni relative alla creazione ed all'uso di istruzioni standard ed Add On di sicurezza in applicazioni Logix
Manuale dell'utente ControlLogix System, pubblicazione 1756-UM001	Fornisce informazioni sull'utilizzo di controllori ControlLogix in applicazioni standard
Manuale dell'utente DeviceNet Modules in Logix5000 Control Systems, pubblicazione DNET-UM004	Fornisce informazioni sull'utilizzo del modulo 1756-DNB in un sistema di controllo Logix5000

Risorsa	Descrizione
Manuale dell'utente EtherNet/IP Modules in Logix5000 Control Systems, pubblicazione ENET-UM001	Fornisce informazioni sull'utilizzo del modulo 1756-ENBT in un sistema di controllo Logix5000
Manuale dell'utente ControlNet Modules in Logix5000 Control Systems, pubblicazione CNET-UM001	Fornisce informazioni sull'utilizzo del modulo 1756-CNB in sistemi di controllo Logix5000
Manuale di riferimento Logix5000 Controllers Execution Time and Memory Use, pubblicazione 1756-RM087	Fornisce informazioni sulla stima del tempo d'esecuzione delle istruzioni e sul relativo utilizzo della memoria
Manuale di riferimento Logix Import Export, pubblicazione 1756-RM084	Fornisce informazioni sull'utilizzo della funzione Import/Export di Logix Designer
Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione 1770-4.1	Fornisce criteri generali per l'installazione di un sistema industriale Rockwell Automation
Certificazioni di prodotto, http://www.ab.com	Fornisce le dichiarazioni di conformità, i certificati ed ulteriori dettagli sulle certificazioni

Le pubblicazioni possono essere visualizzate o scaricate all'indirizzo http://www.rockwellautomation.com/literature/. Per ordinare le copie cartacee della documentazione tecnica, contattare il distributore Allen-Bradley® o il rappresentante Rockwell Automation di zona.

Note:

Significato di livello di integrità della sicurezza (SIL)

Certificazione SIL 3

I sistemi di controllo GuardLogix 5570 sono type-approved e certificati per l'uso in applicazioni di sicurezza fino al livello SIL CL3 incluso, in conformità alle normative IEC 61508 e IEC 62061, ed in applicazioni di sicurezza fino al livello prestazionale PLe (Categoria 4) incluso, in conformità alla normativa ISO 13849-1. I requisiti SIL si basano sulle norme vigenti al momento della certificazione.

IMPORTANTE Quando il controllore GuardLogix è in modalità Run (Esecuzione) o Program (Programmazione) ed il programma applicativo non è stato validato, è l'utente ad essere responsabile del mantenimento delle condizioni di sicurezza.

Inoltre, i task standard nei controllori GuardLogix possono essere usati sia per applicazioni standard che per applicazioni di sicurezza SIL 2, come spiegato nel manuale di riferimento Using ControlLogix in SIL 2 Applications, pubblicazione 1756-RM001. In ogni caso, non usare variabili e task SIL 2 o standard per realizzare loop di sicurezza di livello superiore. Il task di sicurezza è l'unico task certificato per applicazioni SIL 3.

Per creare programmi per i controllori GuardLogix 5570, utilizzare l'applicazione Logix Designer Studio 5000.

TÜV Rheinland ha approvato i sistemi di controllo GuardLogix 5570 per l'utilizzo in applicazioni di sicurezza fino al livello SIL CL 3, in cui lo stato diseccitato è lo stato di sicurezza. Tutti gli esempi relativi agli I/O inclusi nel presente manuale si basano sul raggiungimento dello stato diseccitato come stato di sicurezza per i tipici sistemi di arresto d'emergenza (Emergency Shutdown, ESD) e sicurezza macchine.

IMPORTANTE L'utente del sistema è responsabile di quanto segue:

- impostazione, classificazione SIL e validazione di qualsiasi sensore o attuatore collegato al sistema GuardLogix
- gestione del progetto e collaudo funzionale
- controllo degli accessi al sistema di sicurezza, inclusa gestione della password
- programmazione dell'applicazione e configurazione dei dispositivi nel rispetto delle istruzioni fornite in questo manuale di riferimento per la sicurezza e nel manuale dell'utente GuardLogix 5570 Controllers, pubblicazione 1756-UM022

Durante l'applicazione della sicurezza funzionale, limitare l'accesso solo a personale qualificato e autorizzato in possesso della debita formazione ed esperienza. La funzione di blocco di sicurezza, con password, è fornita nell'applicazione Logix Designer.

Per informazioni sull'uso della funzione di blocco di sicurezza, consultare il manuale dell'utente Controllori GuardLogix 5570, pubblicazione 1756-UM022.

Test di verifica funzionale

La norma IEC 61508 prevede che l'utente esegua diverse prove funzionali delle apparecchiature utilizzate nel sistema. Le prove funzionali vengono eseguite ad intervalli definiti dall'utente. Ad esempio, le prove funzionali possono essere eseguite una volta all'anno, una volta ogni 15 anni o quando si ritengano opportune.

Per i controllori GuardLogix 5570 è previsto un intervallo massimo per le prove funzionali di 20 anni. Altri componenti del sistema, quali i dispositivi I/O di sicurezza, i sensori e gli attuatori possono avere intervalli di tempo più brevi per le prove funzionali. Includere il controllore nel test di verifica funzionale degli altri componenti del sistema di sicurezza.

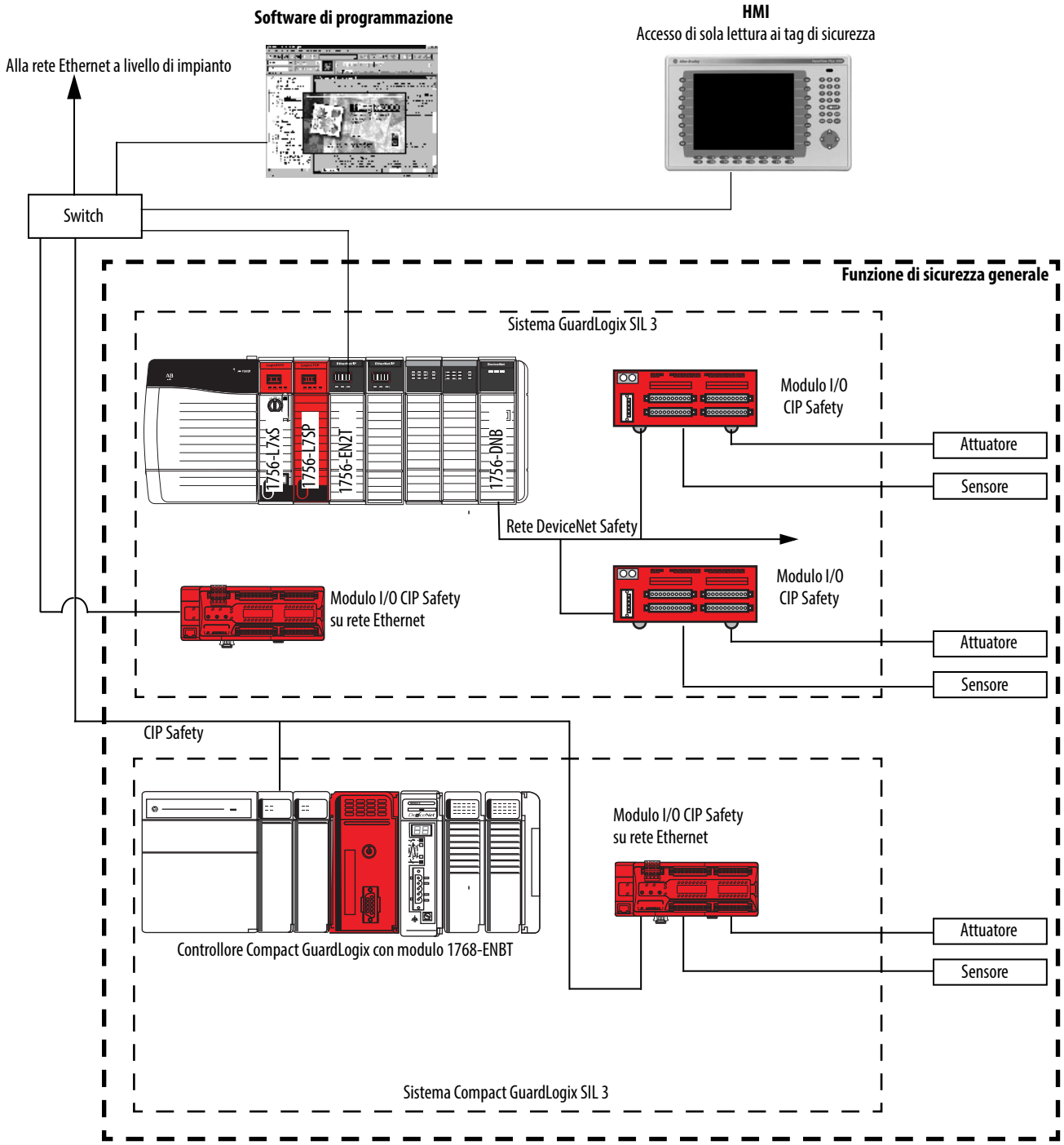
IMPORTANTE Le applicazioni specifiche dell'utente determinano la frequenza delle prove funzionali. Tuttavia ci si riferisce principalmente ai dispositivi I/O di sicurezza ed alla strumentazione di campo.

Architettura GuardLogix per applicazioni SIL 3

La seguente illustrazione mostra una tipica funzione SIL che include:

- la funzione di sicurezza complessiva
- la parte GuardLogix nell'ambito della funzione di sicurezza complessiva
- il modo in cui altri dispositivi (ad es. interfaccia operatore) sono collegati e funzionano senza utilizzare la funzione di sicurezza

Figura 1 – Tipica funzione SIL



Componenti del sistema GuardLogix

Nelle tabelle riportate in questa sezione sono elencati i componenti GuardLogix Certificati SIL 3 ed i componenti privi di certificazione SIL 3 che possono essere utilizzati con i sistemi GuardLogix SIL 3.

Per un elenco aggiornato delle serie e delle versioni del firmware certificate dei controllori GuardLogix e dei dispositivi I/O CIP Safety, visitare il sito http://www.rockwellautomation.com/products/certification/safety/. Le versioni del firmware sono disponibili all'indirizzo http://support.rockwellautomation.com/ControlFLASH™/.

Tabella 2 – Componenti GuardLogix certificati SIL 3

Tipo di dispositivo	Num. di Cat.	Descrizione	Documentazione attinente[3]	
			Istruzioni per l'installazione	Manuale utente
Controllore primario GuardLogix 1756 (ControlLogix5570S)	1756-L71S	Controllore con 2 MB di memoria standard, 1 MB di memoria di sicurezza	N/A[4]	• Con ambiente Studio 5000, versione 21 o successiva: 1756-UM022 • Con software RSLogix 5000, versione 20 o precedente: 1756-UM020
	1756-L72S	Controllore con 4 MB di memoria standard, 2 MB di memoria di sicurezza		
	1756-L73S	Controllore con 8 MB di memoria standard, 4 MB di memoria di sicurezza		
	1756-L73SXT	Controllore (XT) con 8 MB di memoria standard, 4 MB di memoria di sicurezza		
Coprocessore di sicurezza GuardLogix 1756 (ControlLogix557SP)	1756-L7SP	Coprocessore di sicurezza		
	1756-L7SPXT	Coprocessore di sicurezza (XT)		
Controllore primario GuardLogix 1756 (ControlLogix5560S)[1]	1756-L61S	Controllore con 2 MB di memoria standard, 1 MB di memoria di sicurezza	N/A[4]	1756-UM020
	1756-L62S	Controllore con 4 MB di memoria standard, 1 MB di memoria di sicurezza		
	1756-L63S	Controllore con 8 MB di memoria standard, 3,75 MB di memoria di sicurezza		
Coprocessore di sicurezza GuardLogix 1756 (ControlLogix55SP)[1]	1756-LSP	Coprocessore di sicurezza		
Controllore Compact GuardLogix 1768 (CompactLogix4xS)[2]	1768-L43S	Controllore compatibile con due moduli 1768	N/A[4]	1768-UM002
	1768-L45S	Controllore compatibile con quattro moduli 1768		
Moduli I/O CIP Safety su reti DeviceNet	Per un elenco aggiornato delle serie e delle versioni del firmware certificate, visitare il sito http://www.rockwellautomation.com/products/certification/safety/		1791DS-IN001 1791DS-IN002 1732DS-IN001	1791DS-UM001
Moduli I/O CIP Safety su reti EtherNet/IP			1791ES-IN001	1791ES-UM001
Moduli POINT Guard I/O			N/A[4]	1734-UM013
Servoazionamenti Kinetix 5500 (numeri di catalogo che terminano con -ERS2)	Per un elenco aggiornato delle serie e delle versioni del firmware certificate, visitare il sito http://www.rockwellautomation.com/products/certification/safety/		2198-IN001	2198-UM001

(1) Certificati per l'uso con il software RSLogix 5000, versione 14, versione 16 e successiva.
(2) Certificati per l'uso con il software RSLogix 5000, versione 18 e successiva.
(3) Queste pubblicazioni sono disponibili sul sito Web di Rockwell Automation all'indirizzo http://www.rockwellautomation.com/literature.
(4) Per le istruzioni per l'installazione, vedere il manuale dell'utente.

Tabella 3 – Componenti adatti all'uso con sistemi di controllo di sicurezza GuardLogix 1756

Tipo di dispositivo	Num. di Cat.	Descrizione	Serie[1]	Versione[1]	Documentazione attinente[3]	
					Istruzioni per l'installazione	Manuale utente
Chassis	1756-A4 1756-A7 1756-A10 1756-A13 1756-A17	Chassis a 4 slot Chassis a 7 slot Chassis a 10 slot Chassis a 13 slot Chassis a 17 slot	B	N/A	1756-IN005	N/A
	1756-A4LXT 1756-A5XT 1756-A7XT 1756-A7LXT	Chassis XT a 4 slot Chassis XT a 5 slot Chassis XT a 7 slot Chassis XT a 7 slot	B	N/A		
Alimentatore	1756-PA72	Alimentatore CA	C	N/A	1756-IN005	N/A
	1756-PB72	Alimentatore CC	C			
	1756-PA75	Alimentatore CA	B			
	1756-PB75	Alimentatore CC	B			
	1756-PAXT	Alimentatore XT, CA	B			
	1756-PBXT	Alimentatore XT, CC	B			
Moduli di comunicazione	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR	Bridge EtherNet/IP	A A A C B	3.006 2.005 2.005 10.007 10.007	ENET-IN002	ENET-UM001
	1756-EN2TXT 1756-EN2TRXT	Bridge EtherNet/IP XT (rame)	C C	5.007 10.006		
	1734-AENT	Scheda Ethernet POINT I/O	A	3.001	1734-IN590	1734-UM011
	1756-DNB	Bridge DeviceNet	A	6.002	DNET-IN001	DNET-UM004
	1756-CN2	Bridge ControlNet	A	12.001	CNET-IN005	CNET-UM001
	1756-CN2R	Bridge ControlNet, supporti ridondanti	A	12.001		
	1756-CN2RXT	Bridge ControlNet XT, supporti ridondanti	B	20.020		
Software di programmazione	9324-*xxxx*	Software RSLogix 5000 per controllori GuardLogix 5560	N/A	14[2]	N/A	Consultare la guida in linea.
		Software RSLogix 5000 per controllori GuardLogix 5570 (XT)		20		
	9324-*xxxx*	Ambiente Studio 5000 per controllori GuardLogix 5570 (XT)		21		
Schede di memoria	1784-CF128	Scheda CompactFlash da 128 MB per controllori GuardLogix 5560	N/A	N/A	N/A	N/A
	1784-SD1	Scheda SD (Secure Digital) da 1 GB per controllori GuardLogix 5570				
	1784-SD2	Scheda SD (Secure Digital) da 2 GB per controllori GuardLogix 5570				

(1) La presente versione o successiva.
(2) Il software RSLogix 5000 versione 15 non supporta i controllori di sicurezza GuardLogix.
(3) Queste pubblicazioni sono disponibili sul sito Web di Rockwell Automation all'indirizzo http://www.rockwellautomation.com/literature.

È possibile riempire gli slot dello chassis di un sistema SIL 3 non utilizzati dal sistema GuardLogix SIL 3 con altri moduli ControlLogix (1756) certificati in base alle direttive Bassa tensione e Compatibilità elettromagnetica.

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

Per trovare i certificati relativi a "Controllo programmabile – Famiglia di prodotti ControlLogix" consultare http://www.rockwellautomation.com/products/certification/ce/.

Certificazioni di GuardLogix

I dati tecnici ControlLogix Controllers, pubblicazione 1756-TD001, includono le specifiche dei prodotti e le certificazioni di terza parte per cui i prodotti sono approvati. Se un prodotto ha ottenuto una certificazione di terza parte, il marchio viene riportato nell'etichetta del prodotto. Per informazioni sulle dichiarazioni di conformità, i certificati ed altre informazioni sui certificati, vedere http://www.rockwellautomation.com/products/certification/.

Specifiche relative a PFD e PFH per GuardLogix

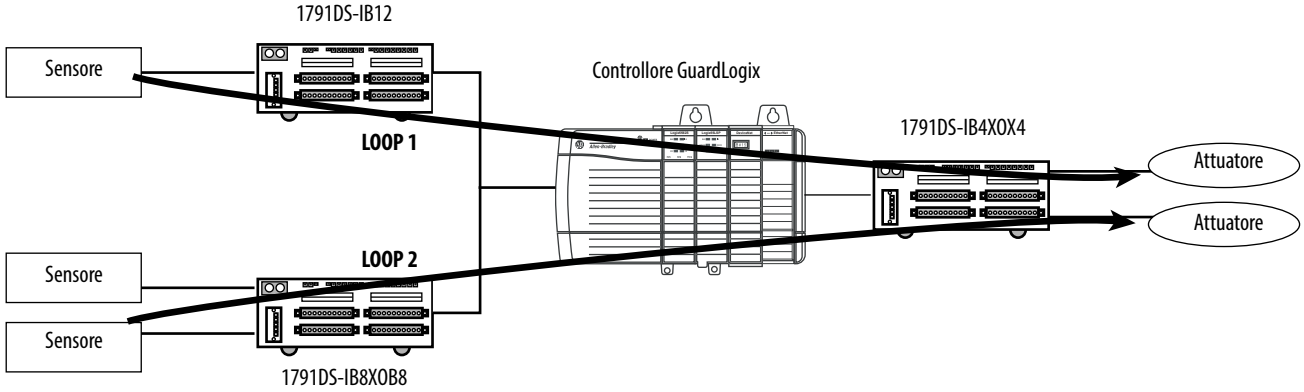
I sistemi di sicurezza possono essere classificati come funzionanti sia in una modalità a bassa percentuale di requisiti che in una modalità ad alta percentuale di requisiti o continua. La norma IEC 61508 quantifica questa classificazione impostando la frequenza delle richieste per il funzionamento del sistema di sicurezza su un valore non superiore ad una volta l'anno nella modalità a bassa percentuale di requisiti e superiore ad una volta l'anno nella modalità ad alta percentuale di requisirti o continua.

Il valore del livello di integrità della sicurezza (SIL) per un sistema di sicurezza a bassa percentuale di requisiti è direttamente correlato all'ordine di grandezza della sua probabilità media di guasto di eseguire in modo conforme la funzione di sicurezza quando richiesto o, semplicemente, la probabilità di guasto su domanda (PFD). Il valore SIL per un sistema di sicurezza a alta percentuale di requisiti è direttamente correlato alla probabilità di guasto pericoloso all'ora (PFH).

I valori PFD e PFH sono associati a ciascuno dei tre elementi primari che costituiscono un sistema di sicurezza (i sensori, la logica e gli attuatori). La logica include gli ingressi, il processore e le uscite.

Per i valori PFD e PFH e gli intervalli delle prove funzionali per i moduli Guard I/O, vedere l'Appendice E, Dati di sicurezza dei sistemi GuardLogix.

Figura 2 – Esempio di PFH



Per determinare il valore PHF della logica per ogni loop di sicurezza nel semplice sistema mostrato nell'esempio di PFH, sommare i valori PFH di ogni componente presente nel loop. La tabella Equazioni PFH per loop di sicurezza fornisce un esempio semplificato di calcoli del valore PFH per ogni loop di sicurezza presente nella figura dell'esempio di PFH.

Tabella 4 – Equazioni PFH per loop di sicurezza

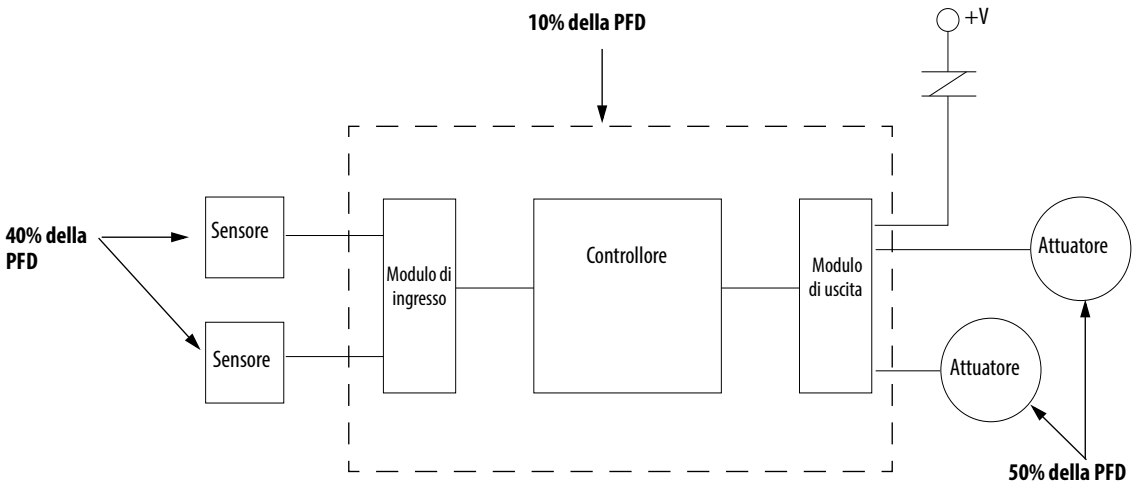
Per questo loop	Sommare i valori PFH di questi componenti
PFH totale per loop 1 =	1791DS-IB12 + controllore GuardLogix + 1791DS-IB4XOX4
PFH totale per loop 2 =	1791DS-IB8XOB8 + controllore GuardLogix + 1791DS-IB4XOX4

Durante il calcolo dei valori di PFH, si deve tenere conto dei requisiti specifici dell'applicazione, inclusi gli intervalli di tempo per i test.

Peso e distribuzione della conformità al livello di integrità della sicurezza (SIL)

Si può supporre che il controllore GuardLogix ed il sistema I/O contribuiscano al 10% del livello di affidabilità. È possibile che un sistema SIL 3 debba incorporare ingressi multipli per sensori e dispositivi di ingresso critici oltre ad uscite doppie collegate in serie ad attuatori doppi che dipendono dalle valutazioni SIL per il sistema di sicurezza.

Figura 3 – Livello di affidabilità



Tempo di risposta del sistema

Il tempo di risposta del sistema corrisponde al tempo che intercorre tra un evento connesso con la sicurezza come ingresso al sistema ed il momento in cui il sistema imposta le uscite corrispondenti sullo stato di sicurezza. Anche gli errori di sistema possono incidere sul tempo di risposta del sistema. Il tempo di risposta del sistema corrisponde alla somma dei seguenti tempi di risposta:

Tempo di risposta sensore + Tempo di risposta ingresso + Tempo di risposta task di sicurezza + Tempo di risposta uscita + Tempo di risposta attuatore

Ciascuno dei tempi di risposta dipende in modo variabile da fattori quali il tipo di dispositivo I/O e le istruzioni utilizzate nel programma.

Tempo di risposta task di sicurezza

Il tempo di risposta del task di sicurezza è il ritardo massimo che può intercorrere tra qualsiasi cambiamento dell'ingresso applicato al controllore ed il momento in cui l'uscita elaborata è disponibile. È inferiore o pari alla somma del periodo del task di sicurezza e del watchdog del task di sicurezza.

Periodo del task di sicurezza e watchdog del task di sicurezza

Il periodo del task di sicurezza è l'intervallo in cui viene eseguito il task di sicurezza.

Il tempo del watchdog del task di sicurezza corrisponde al tempo massimo consentito per l'elaborazione del task di sicurezza. Se il tempo di elaborazione del task di sicurezza supera il tempo del watchdog del task di sicurezza, si verifica un errore di sicurezza irreversibile nel controllore e la transizione automatica delle uscite allo stato di sicurezza (off).

Il tempo del watchdog del task di sicurezza è definito dall'utente e deve essere inferiore o pari a quello del periodo del task di sicurezza.

Il tempo del watchdog del task di sicurezza è impostato nella finestra delle proprietà del task dell'applicazione Logix Designer. Questo valore può essere modificato online, indipendentemente dalla modalità del controllore ma non può essere cambiato quando il controllore è in blocco di sicurezza oppure dopo che è stata creata una firma del task di sicurezza.

Informazioni di contatto per i casi di guasto ai dispositivi

Nel caso in cui si verifichi un guasto in qualsiasi dispositivo certificato SIL 3, contattare il distributore Allen-Bradley di zona e procedere come segue:

- Restituire il dispositivo a Rockwell Automation in modo che il guasto sia opportunamente registrato per il numero di catalogo interessato e che venga creato un record del guasto.
- Richiedere un'analisi del guasto (se necessario) per determinarne la causa.

Sistema di controllo GuardLogix

Per un breve elenco dei componenti utilizzabili in applicazioni SIL 3, consultare la tabella riportata a pagina 16. Per informazioni più dettagliate ed aggiornate, visitare il sito http://www.rockwellautomation.com/products/certification/safety/.

Quando si installa un controllore GuardLogix 5570, attenersi alle istruzioni riportate nel manuale dell'utente GuardLogix 5570 Controllers, pubblicazione 1756-UM022.

Hardware del controllore GuardLogix 5570

Il controllore GuardLogix è costituito da un controllore primario (ControlLogix 557*x*S) e da un coprocessore di sicurezza (ControlLogix 557SP). Questi due moduli lavorano in un'architettura 1oo2 per creare un controllore SIL 3. Sono descritti nelle sezioni che seguono.

Sia il controllore primario sia il coprocessore di sicurezza eseguono test diagnostici funzionali all'accensione e durante il funzionamento su tutti i componenti di sicurezza presenti nel controllore.

Per informazioni dettagliate sul funzionamento degli indicatori di stato, consultare il manuale dell'utente GuardLogix 5570 Controllers, pubblicazione 1756-UM022.

IMPORTANTE	Gli indicatori di stato non sono affidabili per le funzioni di sicurezza. Utilizzarli soltanto per operazioni di diagnostica generale durante la messa in servizio o la ricerca guasti. Non cercare di utilizzare gli indicatori di stato per determinare lo stato di funzionamento.

Per un elenco dei numeri di catalogo dei controllori di sicurezza GuardLogix, vedere la Tabella 2 a pagina 16. Per un elenco dei componenti ControlLogix standard adatti ad applicazioni di sicurezza, vedere la Tabella 3 a pagina 17.

Controllore primario

Il controllore primario è il processore che esegue funzioni di controllo standard e di sicurezza e comunica con il coprocessore di sicurezza per le funzioni di sicurezza nel sistema di controllo GuardLogix. Il controllore primario è composto da un processore centrale, un'interfaccia I/O ed una memoria.

Coprocessore di sicurezza

Per soddisfare i requisiti SIL 3, nello slot immediatamente a destra del controllore primario deve essere installato un coprocessore di sicurezza. Il coprocessore di sicurezza garantisce la ridondanza per le funzioni connesse con la sicurezza nel sistema.

Il controllore primario configura il coprocessore di sicurezza. È sufficiente un unico download del programma utente nel controllore primario. La modalità operativa del coprocessore di sicurezza è controllata dal controllore primario.

Chassis

Lo chassis fornisce le connessioni fisiche tra i moduli ed il sistema GuardLogix 1756. Qualsiasi guasto, sebbene improbabile, verrebbe rilevato come tale da uno o più componenti attivi del sistema. Pertanto lo chassis non è rilevante per il tema della sicurezza.

I controllori GuardLogix-XT™ devono usare uno chassis ControlLogix-XT per ottenere la classificazione per ambiente estremo.

Alimentatori

Non è necessaria alcuna configurazione o cablaggio aggiuntivo per il funzionamento SIL 3 degli alimentatori ControlLogix. Qualsiasi guasto verrebbe rilevato come tale da uno o più componenti attivi del sistema GuardLogix. Pertanto l'alimentatore non è rilevante per il tema della sicurezza.

I controllori GuardLogix-XT devono usare un alimentatore ControlLogix-XT per ottenere la classificazione per ambiente estremo.

Protocollo CIP Safety

La comunicazione di sicurezza tra i controllori GuardLogix avviene tramite tag di sicurezza prodotti (inviati) e consumati (ricevuti). Questi tag di sicurezza utilizzano il protocollo CIP Safety che è progettato per conservare l'integrità dei dati durante la comunicazione.

Per maggiori informazioni sui tag di sicurezza, vedere Capitolo 5, Caratteristiche dei tag di sicurezza, del task di sicurezza e dei programmi di sicurezza.

Dispositivi I/O di sicurezza

Per informazioni sui dispositivi I/O CIP Safety compatibili con i controllori GuardLogix, consultare il Capitolo 3.

Bridge di comunicazione

La Tabella 5 elenca i moduli interfaccia di comunicazione disponibili per facilitare la comunicazione sulle reti EtherNet/IP, DeviceNet e ControlNet tramite il protocollo CIP Safety.

Tabella 5 – Moduli interfaccia di comunicazione per sistema

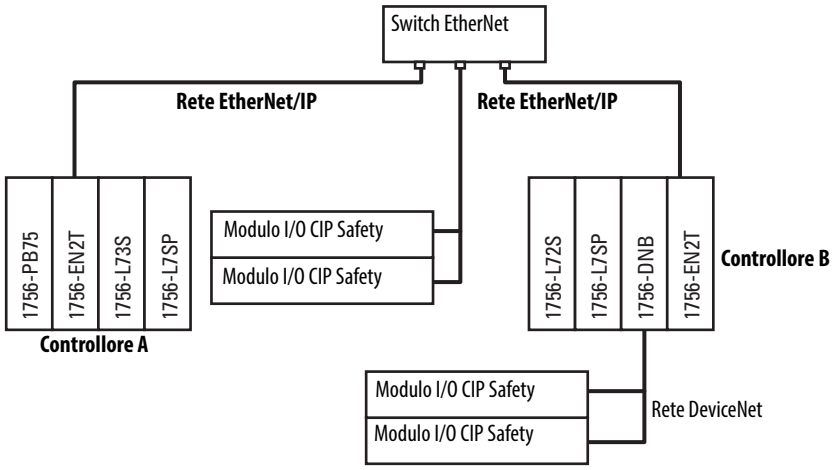
Sistema GuardLogix	Moduli di comunicazione
1756	• Bridge EtherNet/IP 1756-ENBT, 1756-EN2T(R), 1756-EN2F o 1756-EN3TR • Scheda Ethernet POINT I/O 1734-AENT • Bridge DeviceNet 1756-DNB • Bridge ControlNet 1756-CN2 • Bridge ControlNet ridondante 1756-CN2R
1756 -XT	• Bridge EtherNet/IP XT 1756-EN2TXT, 1756-EN2TRXT (rame) • Bridge ControlNet XT ridondante 1756-CN2RXT
1768	• 1768-ENBT • Scheda Ethernet POINT I/O 1734-AENT • 1768-CNB • 1768-CNBR

IMPORTANTE Vista la struttura del sistema di controllo CIP Safety, non è necessario che i dispositivi bridge CIP Safety come i bridge elencati in tabella siano certificati SIL 3.

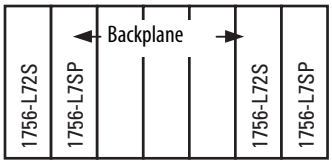
Rete EtherNet/IP

La comunicazione di sicurezza peer-to-peer tra controllori GuardLogix è possibile tramite la rete EtherNet/IP grazie all'uso dei bridge EtherNet/IP. Il bridge EtherNet/IP consente al controllore GuardLogix di controllare e scambiare dati di sicurezza con i dispositivi I/O CIP Safety su una rete EtherNet/IP.

Figura 4 – Comunicazione peer-to-peer tramite bridge EtherNet/IP su rete EtherNet/IP



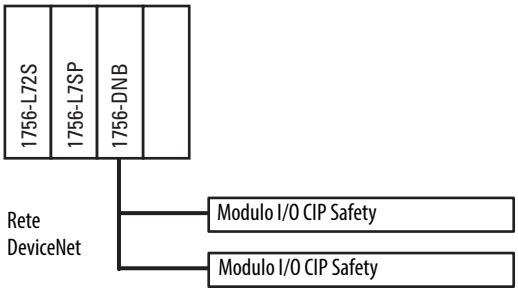
SUGGERIMENTO La comunicazione di sicurezza peer-to-peer tra due controllori GuardLogix nello stesso chassis è possibile anche mediante il backplane.



Rete DeviceNet Safety

I bridge DeviceNet permettono al controllore GuardLogix di controllare e scambiare dati di sicurezza con i moduli I/O CIP Safety su una rete DeviceNet.

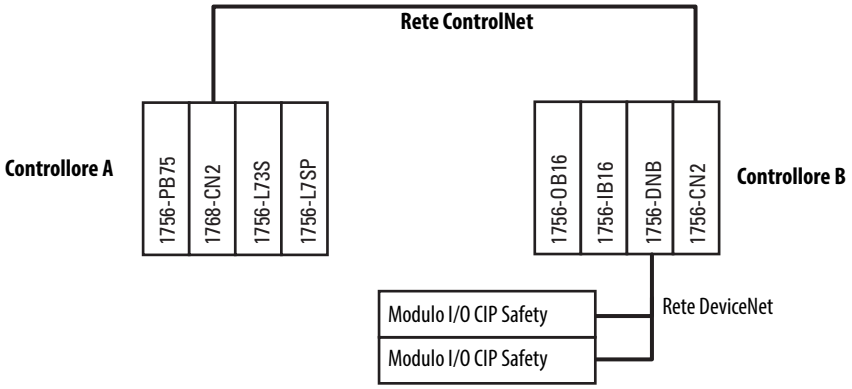
Figura 5 – Comunicazione mediante un bridge DeviceNet



Rete ControlNet

I bridge ControlNet permettono al controllore GuardLogix di produrre e consumare tag di sicurezza su reti ControlNet con altri controllori GuardLogix o reti I/O CIP Safety remote.

Figura 6 – Comunicazione mediante un bridge ControlNet



Cenni generali sulla programmazione

Programmare i controllori GuardLogix 5570 utilizzando l'applicazione Logix Designer Studio 5000.

Usare l'applicazione Logix Designer per definire posizione, proprietà e configurazione di dispositivi I/O e controllori, oltre che per creare, testare ed eseguire il debug della logica del programma. Soltanto la logica ladder è supportata dal task di sicurezza GuardLogix.

Per informazioni sul set di istruzioni logiche disponibili per i progetti di sicurezza, consultare l'Appendice A.

Il personale autorizzato può modificare un programma di sicurezza solamente utilizzando uno dei processi descritti in Modifica dell'applicazione di sicurezza a pagina 59.

Note:

I/O CIP Safety per il sistema di controllo GuardLogix

Panoramica

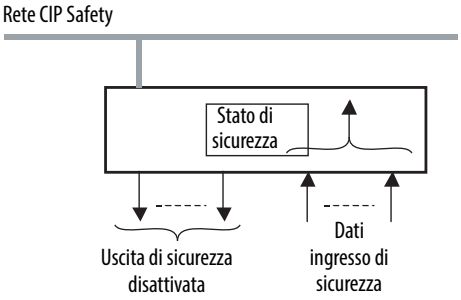
Prima di utilizzare un sistema di sicurezza GuardLogix 5570 con dispositivi I/O CIP Safety, è necessario leggere, comprendere e seguire le informazioni per l'installazione, il funzionamento e la sicurezza fornite nelle pubblicazioni elencate nelle tabelle Componenti GuardLogix certificati SIL 3 a pagina 16.

I dispositivi I/O CIP Safety possono essere collegati a dispositivi di ingresso e di uscita di sicurezza, come sensori ed attuatori, consentendone il monitoraggio ed il controllo da parte del controllore GuardLogix. Nel caso dei dati di sicurezza, la comunicazione I/O viene eseguita attraverso connessioni di sicurezza utilizzando il protocollo CIP Safety; la logica di sicurezza è elaborata nel controllore GuardLogix.

Tipiche funzioni di sicurezza dei dispositivi I/O CIP Safety

Quanto segue è trattato come stato di sicurezza dai dispositivi I/O CIP Safety:

- Uscite di sicurezza: OFF
- Dati ingresso di sicurezza al controllore: OFF



Usare i dispositivi I/O CIP Safety per applicazioni che si trovano nello stato di sicurezza quando l'uscita di sicurezza viene disattivata.

Diagnostica

I dispositivi I/O CIP Safety eseguono un'autodiagnosi all'accensione e periodicamente durante il funzionamento. Se viene rilevato un errore diagnostico, i dati di ingresso di sicurezza (inviati al controllore) e le uscite di sicurezza locali vengono impostate nel rispettivo stato di sicurezza (OFF).

Dati di stato

Oltre ai dati di ingresso e di uscita di sicurezza, alcuni dispositivi I/O CIP Safety supportano i dati di stato per monitorare lo stato generale del dispositivo e del circuito I/O. Per informazioni sulle funzioni di un prodotto specifico, consultare la documentazione fornita con il dispositivo.

Indicatori di stato

I dispositivi I/O CIP Safety sono provvisti di indicatori di stato. Per informazioni dettagliate sul funzionamento degli indicatori di stato, fare riferimento alla documentazione del proprio dispositivo specifico.

Funzione di ritardo all'eccitazione ed alla diseccitazione

È possibile che alcuni dispositivi I/O CIP Safety supportino le funzioni di ritardo all'eccitazione ed alla diseccitazione dei segnali di ingresso. A seconda dell'applicazione utilizzata, potrebbe essere necessario includere il ritardo all'eccitazione, il ritardo alla diseccitazione o entrambi quando si calcola il tempo di risposta del sistema.

Per informazioni sul tempo di risposta del sistema, consultare l'Appendice C.

Tempo di risposta

Il tempo di risposta di ingresso corrisponde al tempo che intercorre tra il momento in cui il segnale si modifica su un morsetto di ingresso ed il momento in cui i dati di sicurezza vengono inviati al controllore GuardLogix.

Il tempo di risposta di uscita corrisponde al tempo che intercorre tra il momento in cui i dati di sicurezza vengono ricevuti dal controllore GuardLogix ed il momento in cui viene modificato lo stato del morsetto di uscita.

Per informazioni sulla determinazione dei tempi di risposta di ingresso e di uscita, fare riferimento alla documentazione prodotto per il dispositivo I/O CIP Safety specifico.

Per informazioni sul calcolo del tempo di risposta del sistema, consultare l'Appendice C.

Considerazioni sulla sicurezza dei dispositivi I/O CIP Safety

Tutti i dispositivi devono essere messi in servizio con un indirizzo di nodo o indirizzo IP ed una velocità di comunicazione, se necessario, prima della loro installazione nella rete di sicurezza.

Proprietà

Ciascun dispositivo I/O CIP Safety in un sistema GuardLogix è di proprietà di un controllore GuardLogix. È possibile utilizzare più controllori GuardLogix e dispositivi I/O CIP Safety negli chassis o sulle reti, senza restrizioni. Se un controllore è proprietario di un dispositivo I/O, memorizza i dati di configurazione del dispositivo, come definito dall'utente. Questa configurazione consente di controllare il funzionamento dei dispositivi nel sistema.

Dal punto di vista del controllo, i dispositivi di uscita di sicurezza possono essere gestiti da un solo controllore. Anche ogni dispositivo di ingresso di sicurezza è di proprietà di un unico controllore ma i dati di ingresso di sicurezza possono essere condivisi (consumati) da diversi controllori GuardLogix.

Firma della configurazione degli I/O di sicurezza

Questa autenticazione definisce la configurazione del dispositivo. Può essere letta e monitorata. L'autenticazione di configurazione viene utilizzata per identificare univocamente la configurazione di un dispositivo. Quando si utilizza un controllore GuardLogix, non è necessario monitorare questa firma. Il controllore GuardLogix monitora la firma automaticamente.

Sostituzione dei dispositivi I/O di sicurezza

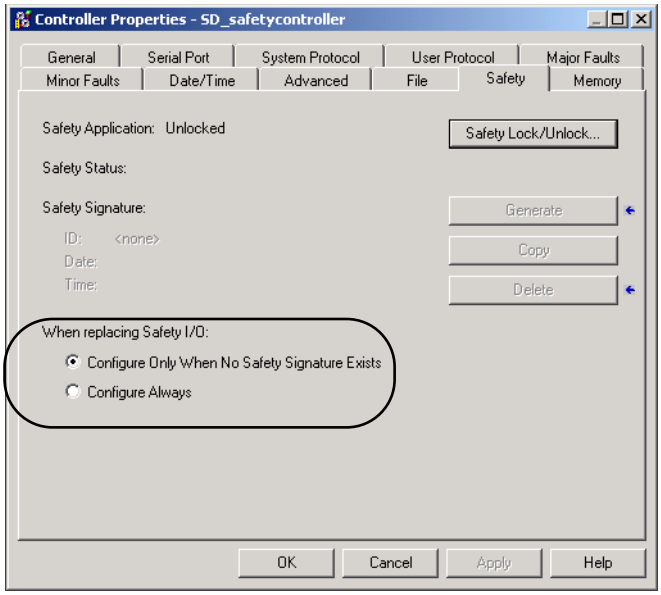
La sostituzione dei dispositivi di sicurezza prevede che il dispositivo sostitutivo sia configurato in modo opportuno e che il funzionamento del dispositivo sostitutivo venga verificato dall'utente.

ATTENZIONE: Durante la sostituzione o il collaudo funzionale di un dispositivo, la sicurezza del sistema non deve basarsi su alcuna parte del dispositivo interessato.

Nella scheda Safety della finestra di dialogo Controller Properties dell'applicazione Logix Designer sono disponibili due opzioni per la sostituzione dei dispositivi I/O:

- Configure Only When No Safety Signature Exists
- Configure Always

Figura 7 – Opzioni di sostituzione dei moduli I/O di sicurezza



Configure Only When No Safety Signature Exists

Questa impostazione richiede al controllore GuardLogix di configurare un dispositivo di sicurezza solo se il task di sicurezza non dispone di firma del task di sicurezza ed il dispositivo sostitutivo si trova nella condizione predefinita in fabbrica, cioè all'interno del dispositivo di sicurezza non è presente un numero della rete di sicurezza.

Se il task di sicurezza ha una firma, il controllore GuardLogix configura il dispositivo I/O CIP Safety sostitutivo solo in presenza delle seguenti condizioni:

- Il dispositivo ha già il corretto numero di rete di sicurezza.
- La codifica elettronica del dispositivo è corretta.
- L'indirizzo del nodo o IP è corretto.

Configure Always

Il controllore GuardLogix tenta di configurare un dispositivo I/O CIP Safety sostitutivo se questo si trova nella condizione predefinita in fabbrica, cioè all'interno di esso non è presente un numero della rete di sicurezza ed il numero del nodo e la codifica del dispositivo I/O corrispondono alla configurazione del controllore.

ATTENZIONE: Abilitare l'opzione Configure Always soltanto se non ci si basa su nessuna parte del sistema di controllo CIP Safety instradabile per mantenere il livello SIL 3 durante la sostituzione ed il collaudo funzionale di un dispositivo.

Se ci si basa su altre parti del sistema di controllo CIP Safety per mantenere il livello SIL 3, assicurarsi che l'opzione Configure Always del controllore sia disabilitata.

Sarà cura dell'utente adottare un processo tale da garantire il mantenimento di un livello funzionale di sicurezza appropriato durante la sostituzione del dispositivo.

ATTENZIONE: Non installare alcun dispositivo, così come fornito, su una rete CIP Safety quando è abilitata la funzione Configure Always, se non seguendo la procedura di sostituzione dei dispositivi riportata nel manuale dell'utente Controllori GuardLogix 5570, pubblicazione 1756-UM022.

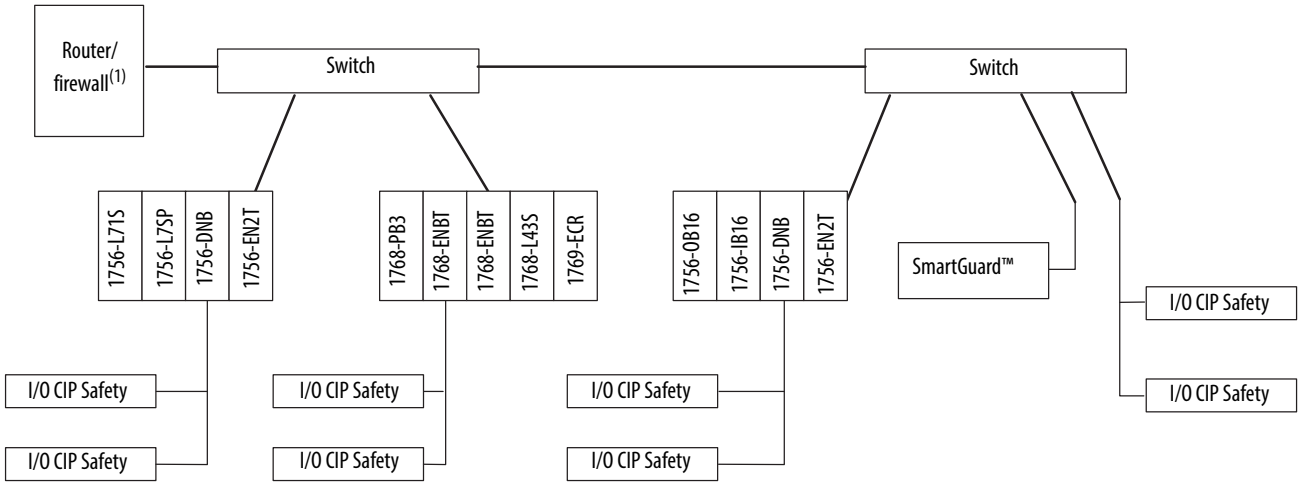
Note:

CIP Safety e numero della rete di sicurezza

Sistema di controllo CIP Safety instradabile

Per comprendere i requisiti di sicurezza di un sistema di controllo CIP Safety, incluso il numero della rete di sicurezza (SNN), si deve innanzitutto comprendere il modo in cui avviene la comunicazione nei sistemi di controllo CIP. Il sistema di controllo CIP Safety è un insieme di dispositivi di sicurezza CIP Safety interconnessi. Il sistema instradabile rappresenta l'ambito della potenziale deviazione (misrouting) di pacchetti da un dispositivo di origine ad un dispositivo di destinazione nell'ambito del sistema di controllo CIP Safety. Il sistema è isolato in modo tale che non vi siano altri collegamenti all'interno del sistema. Ad esempio, poiché il sistema illustrato nella Figura 8 non può essere interconnesso con un altro sistema CIP Safety per mezzo di una dorsale Ethernet di impianto di grandi dimensioni, esso illustra l'ambito di un sistema CIP Safety instradabile.

Figura 8 – Esempio di sistema CIP Safety



(1) Il router o il firewall servono a limitare il traffico.

Riferimento univoco del nodo

Il protocollo CIP Safety è un protocollo di sicurezza da nodo terminale a nodo terminale. Il protocollo CIP Safety permette l'instradamento dei messaggi CIP Safety verso e dai dispositivi CIP Safety per mezzo di ponti, switch e router non certificati.

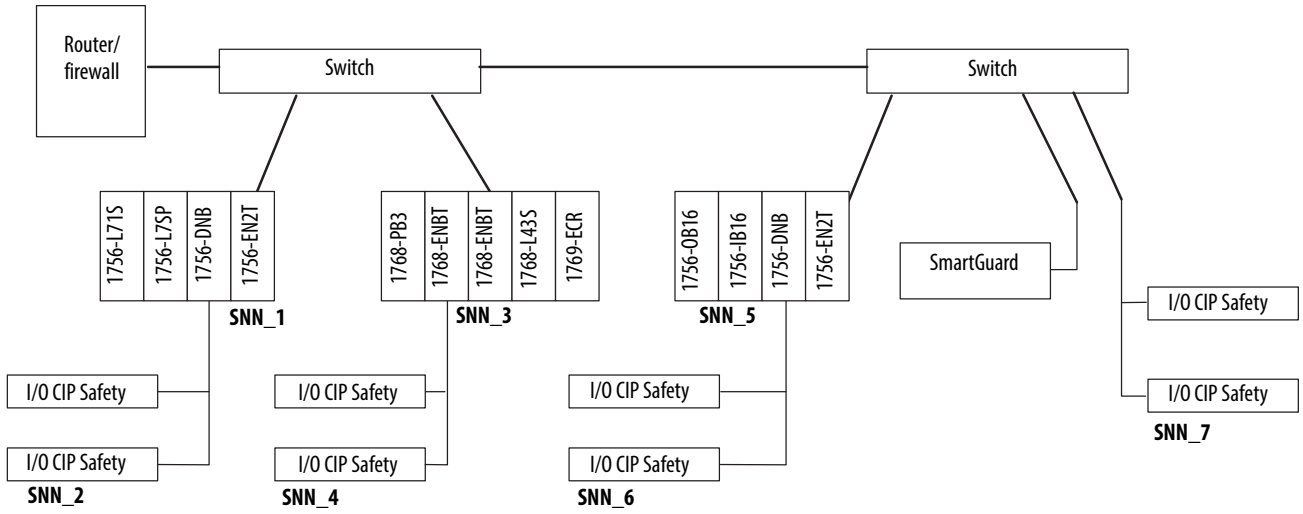
Per impedire che errori in ponti, switch o router non certificati diventino pericolosi, ogni nodo terminale di un sistema di controllo CIP Safety instradabile deve avere un riferimento univoco per i nodi. Il riferimento univoco del nodo è una combinazione composta da un numero della rete di sicurezza (SNN) e dall'indirizzo del nodo.

Numero della rete di sicurezza

Il numero della rete di sicurezza (SNN) è assegnato automaticamente da un software oppure manualmente dall'utente. Ogni rete CIP Safety che contiene nodi I/O di sicurezza deve avere almeno un SNN univoco. Ogni chassis che contiene uno o più dispositivi di sicurezza deve avere almeno un SNN univoco. I numeri di rete di sicurezza assegnati ad ogni rete o sottorete di sicurezza devono essere univoci.

SUGGERIMENTO A una sottorete CIP Safety o ad uno chassis che contiene diversi dispositivi di sicurezza, è possibile assegnare diversi SNN. Per semplicità, tuttavia, è consigliabile che ogni sottorete CIP Safety abbia un solo SNN univoco. Questa raccomandazione vale anche per gli chassis.

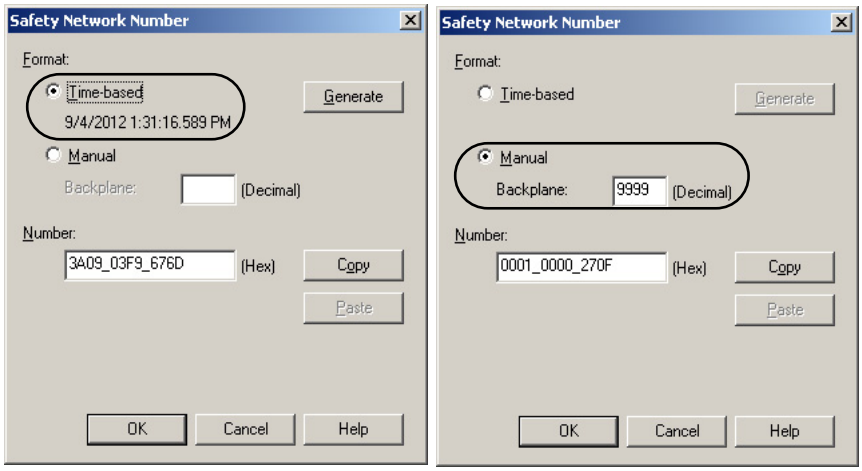
Figura 9 – Esempio di CIP Safety con più di un SNN



Ogni dispositivo CIP Safety deve essere configurato con un SNN. Qualunque dispositivo che dà origine ad una connessione di sicurezza ad un altro dispositivo di sicurezza deve essere configurato con l'SNN del dispositivo di destinazione. Se il sistema CIP Safety si trova nella fase di avvio prima del test di sicurezza funzionale del sistema, il dispositivo di origine può essere utilizzato per impostare il riferimento univoco per i nodi nel dispositivo.

L'SNN utilizzato dal sistema è un numero esadecimale a sei byte. L'SNN può essere impostato e visualizzato in uno dei due formati: in base al tempo o manuale. Quando viene selezionato il formato basato sul tempo, l'SNN rappresenta una data ed un'ora localizzate. Quando viene selezionato il formato manuale, l'SNN rappresenta un tipo di rete ed un valore decimale compreso tra 1 e 9999.

Figura 10 – Formati di SNN



L'assegnazione di un SNN basato sul tempo è automatica mentre si crea un progetto con un controllore di sicurezza GuardLogix e si aggiungono nuovi dispositivi I/O CIP Safety.

L'assegnazione manuale del numero SNN è necessaria nelle seguenti situazioni:

- se si utilizzano tag di sicurezza consumati
- se il progetto consuma dati di ingresso di sicurezza da un dispositivo la cui configurazione è di proprietà di qualche altro dispositivo di sicurezza
- se un progetto di sicurezza viene copiato in una diversa installazione hardware nell'ambito dello stesso sistema CIP Safety instradabile

IMPORTANTE	Se si assegna l'SNN manualmente, verificare che l'ampliamento del sistema non determini una duplicazione delle combinazioni del numero SNN e dell'indirizzo di nodo. Se il progetto contiene combinazioni di SNN ed indirizzo di nodo duplicati, viene generato un errore di verifica.

Considerazioni sull'assegnazione del numero della rete di sicurezza (SNN)

L'assegnazione del numero SNN dipende da vari fattori, tra cui la configurazione del controllore o del dispositivo I/O CIP Safety.

Numero della rete di sicurezza (SNN) per tag di sicurezza consumati

Quando un controllore di sicurezza contenente tag di sicurezza prodotti viene aggiunto alla struttura di configurazione I/O, deve essere inserito l'SNN del controllore produttore. È possibile copiare l'SNN dal progetto del controllore produttore ed incollarlo nel nuovo controllore che viene aggiunto alla struttura di configurazione I/O.

Consultare il manuale dell'utente Controllori GuardLogix 5570, pubblicazione 1756-UM022, per informazioni su come copiare ed incollare un numero SNN.

Numero della rete di sicurezza (SNN) per dispositivi con impostazioni predefinite

I dispositivi I/O CIP Safety con impostazioni predefinite non hanno SNN. L'SNN viene impostato all'invio di una configurazione al dispositivo da parte del controllore GuardLogix proprietario del dispositivo.

IMPORTANTE	Per aggiungere un dispositivo I/O CIP Safety ad un sistema GuardLogix configurato (il controllore GuardLogix ha un SNN), il dispositivo sostitutivo CIP Safety deve disporre del corretto SNN prima dell'aggiunta alla rete CIP Safety.

Numero della rete di sicurezza (SNN) per un dispositivo di sicurezza con un diverso proprietario della configurazione

Quando un dispositivo I/O CIP Safety è di proprietà di un controllore GuardLogix diverso (controllore B) e viene aggiunto ad un altro progetto GuardLogix (progetto controllore A), l'applicazione Logix Designer assegna l'SNN in base al progetto corrente. Poiché il progetto corrente (progetto controllore A) non è il reale proprietario della configurazione, è necessario copiare l'SNN originario (progetto controllore B) nella configurazione del progetto del controllore A. Questa operazione può essere facilmente eseguita con i normali comandi copia ed incolla. Di conseguenza, il dispositivo I/O CIP Safety produce i dati per due controllori GuardLogix contemporaneamente. L'operazione di copia ed incolla può essere eseguita per un massimo di 16 controllori.

Consultare il manuale dell'utente Controllori GuardLogix 5570, pubblicazione 1756-UM022, per informazioni su come modificare, copiare ed incollare i numeri di rete di sicurezza.

Numero della rete di sicurezza (SNN) quando si copia un progetto di sicurezza

ATTENZIONE: Se si sta copiando un progetto di sicurezza per utilizzarlo in un altro progetto con hardware differente o in una diversa posizione fisica ed il nuovo progetto si trova all'interno dello stesso sistema CIP Safety instradabile, è necessario modificare tutti gli SNN del secondo sistema. I valori SNN non devono essere ripetuti.

Consultare il manuale dell'utente Controllori GuardLogix 5570, pubblicazione 1756-UM022, per informazioni sulla modifica del numero SNN.

Caratteristiche dei tag di sicurezza, del task di sicurezza e dei programmi di sicurezza

Distinzione tra componenti standard e di sicurezza

Trattandosi di un controllore della serie Logix, nel sistema di controllo GuardLogix è possibile utilizzare sia componenti standard (non di sicurezza) che componenti di sicurezza.

Il controllo dell'automazione standard può essere eseguito utilizzando task standard all'interno di un progetto GuardLogix. I controllori GuardLogix hanno la stessa funzionalità degli altri controllori della serie ControlLogix. Ciò che differenzia i controllori GuardLogix dai controllori standard è che permettono di avere un task di sicurezza SIL 3.

Tuttavia, si deve effettuare una distinzione logica ed evidente tra la parte standard dell'applicazione e la parte relativa alla sicurezza. L'applicazione Logix Designer determina questa distinzione tramite il task di sicurezza, i programmi di sicurezza, le routine di sicurezza, i tag di sicurezza ed i dispositivi I/O di sicurezza. Con il task di sicurezza del controllore GuardLogix è possibile implementare sia il livello di controllo di sicurezza SIL 2 che SIL 3.

Applicazioni di sicurezza SIL 2

Il controllo di sicurezza SIL 2 può essere eseguito utilizzando il task di sicurezza del controllore GuardLogix.

Dal momento che i controllori GuardLogix appartengono alla serie di processori ControlLogix, il controllo di sicurezza SIL 2 nel caso di un controllore GuardLogix può essere eseguito utilizzando task standard o il task di sicurezza. In questo modo, si hanno a disposizione opzioni di controllo di sicurezza uniche e versatili, dal momento che la maggior parte delle applicazioni ha una maggiore percentuale di funzioni di sicurezza SIL 2 rispetto a SIL 3.

Controllo di sicurezza SIL 2 nel task di sicurezza

Il task di sicurezza GuardLogix può essere utilizzato per funzioni di sicurezza SIL 2 e SIL 3. Se le funzioni di sicurezza SIL 3 devono essere eseguite in contemporanea alle funzioni di sicurezza SIL 2, è necessario soddisfare i requisiti indicati nelle sezioni Sicurezza SIL 3 – il task di sicurezza, Programmi di sicurezza e Routine di sicurezza del presente capitolo, oltre i che requisiti SIL 2 elencati in questa sezione.

Logica di sicurezza SIL 2

Se si esamina il controllo di sicurezza GuardLogix, la differenza maggiore tra i dispositivi SIL 2 e SIL 3 sta nel fatto che SIL 2 generalmente è monocanale, mentre SIL 3 generalmente è a doppio canale. Quando si utilizzano moduli Guard I/O di sicurezza (moduli rossi), indispensabili nel task di sicurezza, gli ingressi di sicurezza SIL 2 possono essere monocanale e ciò riduce la complessità ed il numero di moduli necessari.

Compete al progettista del sistema di sicurezza implementare correttamente tutte le funzioni di sicurezza. Occorre considerare quanto segue:

- selezione dei dispositivi di campo (scegliere il dispositivo corretto, identificare e risolvere tutti gli eventuali errori)
- considerare i requisiti di sicurezza (bassi – IEC 61511 o alti – ISO 13849)
- considerare gli intervalli di prova (diagnostica e prove funzionali necessarie a soddisfare i requisiti dell'applicazione)
- identificare e giustificare con la documentazione adeguata ogni esclusione errori utilizzata

IMPORTANTE	Se si utilizza una combinazione di funzioni di sicurezza SIL 2 e SIL 3 all'interno del task di sicurezza, bisogna impedire che i segnali di ingresso SIL 2 controllino direttamente le funzioni di sicurezza SIL 3. Per separare le funzioni di sicurezza SIL 2 e SIL 3, utilizzare programmi o routine specifici per i task di sicurezza.

Nel task di sicurezza, l'applicazione Logix Designer include un set di istruzioni in logica ladder relative alla sicurezza. I controllori GuardLogix prevedono l'uso di istruzioni di sicurezza in classe SIL 3 specifiche per applicazione. Tutte queste istruzioni logiche possono essere utilizzate in funzioni di sicurezza di Cat 1...4 e SIL 1...3.

Nel caso specifico di sicurezza SIL 2, non è richiesta una firma del task di sicurezza. Tuttavia, se si utilizzano funzioni di sicurezza SIL 3 all'interno del task di sicurezza, la firma del task di sicurezza è richiesta.

Per le applicazioni SIL 2 si consiglia di attivare il blocco di sicurezza per il task di sicurezza una volta terminati i test. Bloccando il task di sicurezza si abilitano delle funzioni di sicurezza aggiuntive. Per limitare l'accesso alla logica di sicurezza, è possibile utilizzare anche FactoryTalk® Security e la funzione di protezione del sorgente delle routine di Logix Designer.

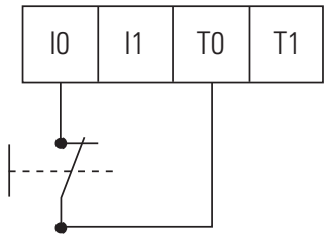
Per ulteriori informazioni sulla generazione della firma del task di sicurezza e sul blocco del task di sicurezza, consultare il manuale dell'utente Controllori GuardLogix 5570, pubblicazione 1756-UM022.

Ingressi di sicurezza SIL 2

I moduli di ingresso di sicurezza CompactBlock™ Guard I/O™ (serie 1791), ArmorBlock® Guard I/O™ (serie 1732) e POINT Guard I/O (serie 1734) supportano circuiti di ingresso di sicurezza monocanale SIL 2. Questi moduli sono certificati anche SIL 3, pertanto è consentito abbinare circuiti SIL 2 e SIL 3 sullo stesso modulo, a patto che le presenti regole generali vengano rispettate.

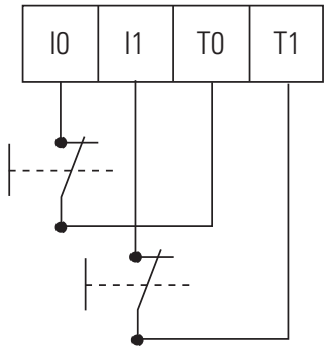
Nei due esempi seguenti sono illustrate le procedure di cablaggio dei circuiti di sicurezza SIL 2 su moduli di ingresso di sicurezza Guard I/O. In questi esempi vengono utilizzate sorgenti di test integrate (T0...T*x*) residenti su tutti i moduli di ingresso di sicurezza 1791 e 1732.

Figura 11 – Cablaggio ingressi



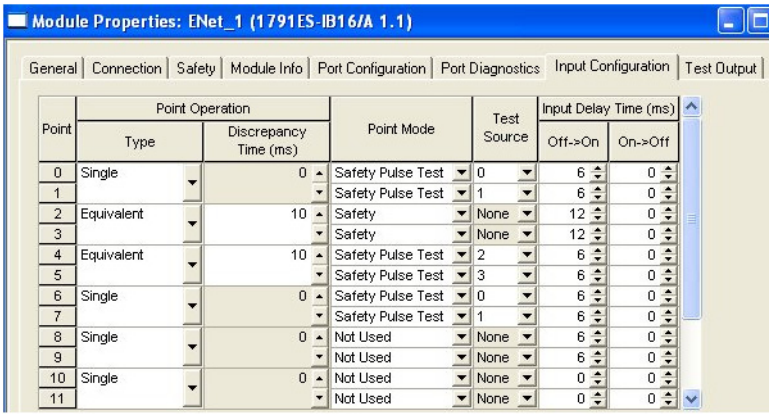
I moduli Guard I/O raggruppano gli ingressi a coppie per facilitare le funzioni di sicurezza Cat 3, Cat 4 e SIL 3. Nel caso delle funzioni di sicurezza Cat 1, Cat 2 e SIL 2, gli ingressi del modulo devono essere comunque utilizzati a coppie come illustrato. Sono inoltre rappresentate due funzioni di sicurezza SIL 2 cablate agli ingressi I0 e I1 che utilizzano rispettivamente le sorgenti di test T0 e T1.

Figura 12 – Cablaggio ingressi a coppie



Nel caso delle funzioni di sicurezza Cat 1, Cat 2 e SIL 2, i moduli di sicurezza Guard I/O richiedono configurazioni specifiche nell'ambito del progetto GuardLogix. In questo esempio, gli ingressi 0, 1, 6, 7, 8, 9, 10 e 11 fanno parte di una funzione di sicurezza Cat 1, 2 o SIL 2. Gli ingressi 2 e 3, così come gli ingressi 4 e 5, fanno parte di una funzione di sicurezza Cat 3, Cat 4 o SIL 3.

Figura 13 – Configurazione degli ingressi



Campo	Valore
Tipo	Single
Discrepancy Time	N/A
Point Mode	Safety Pulse Test
Test Source	Impostare i valori in base alle modalità con cui il dispositivo di campo è fisicamente cablato al modulo. Per essere certi che la sorgente di test sia abilitata correttamente, aprire e visualizzare le impostazioni della scheda Test Output.
Input Delay Time	Valori immessi dall'utente in base alle caratteristiche del dispositivo di campo.

IMPORTANTE Generalmente, con i dispositivi di campo provvisti di contatti meccanici vengono utilizzate le uscite di test ad impulsi integrate (T0…Tx). Se si utilizza un dispositivo di sicurezza provvisto di uscite elettroniche (per alimentare gli ingressi di sicurezza), queste ultime dovranno possedere il livello di sicurezza appropriato.

IMPORTANTE Se si utilizzano istruzioni per applicazioni di sicurezza GuardLogix, si raccomanda di configurare i moduli di ingresso di sicurezza come singoli, non equivalenti o complementari. Queste istruzioni consentono di ottenere tutte le funzionalità a doppio canale necessarie per le funzioni di sicurezza PLd (Cat. 3) o PLe (Cat. 4).

Consultare il manuale di riferimento GuardLogix Safety Application Instruction Set, pubblicazione 1756-RM095

Controllo di sicurezza SIL 2 nei task standard

I controllori della serie ControlLogix, grazie alla qualità ed alla disponibilità di innumerevoli funzioni diagnostiche integrate, consentono di eseguire le funzioni di sicurezza SIL 2 da task standard. Vale anche per i controllori GuardLogix.

Per eseguire il controllo di sicurezza SIL 2 da un task standard GuardLogix, è necessario rispettare i requisiti definiti nel manuale di riferimento per la sicurezza Using ControlLogix in SIL 2 Applications, pubblicazione 1756-RM001.

Sicurezza SIL 3 – il task di sicurezza

La creazione di un progetto GuardLogix genera automaticamente un unico task di sicurezza. Il task di sicurezza ha le seguenti caratteristiche aggiuntive.

- I controllori GuardLogix sono gli unici compatibili con il task di sicurezza.
- Il task di sicurezza non può essere eliminato.
- I controllori GuardLogix permettono l'uso di un task di sicurezza singolo.
- All'interno del task di sicurezza, è possibile utilizzare diversi programmi di sicurezza, costituiti da più routine di sicurezza.
- Non si possono pianificare o eseguire routine standard nel task di sicurezza.

Il task di sicurezza è un task periodico temporizzato con un watchdog ed una priorità di task selezionabile dall'utente. Nella maggior parte dei casi, rappresenta la priorità massima del controllore ed il watchdog del programma definito dall'utente deve essere impostato per adattarsi alle variazioni dell'esecuzione del task di sicurezza.

Limitazioni relative al task di sicurezza

L'utente deve specificare sia il periodo del task di sicurezza che il watchdog del task di sicurezza. Il periodo del task di sicurezza è l'intervallo con cui viene eseguito il task di sicurezza. Il watchdog del task di sicurezza è il tempo massimo consentito dall'avvio dell'esecuzione pianificata del task di sicurezza fino al suo completamento.

Per maggiori informazioni sul watchdog del task di sicurezza, vedere l'Appendice C, Tempi di risposta.

Il periodo del task di sicurezza è limitato ad un massimo di 500 ms e non può essere modificato in modalità online. Assicurarsi che il task di sicurezza disponga del tempo necessario per terminare prima di essere nuovamente avviato. Il timeout del watchdog del task di sicurezza, un errore di sicurezza irreversibile nel controllore GuardLogix, si verifica se il task di sicurezza viene avviato mentre è ancora in corso l'esecuzione precedente.

Per ulteriori informazioni vedere Capitolo 7, Monitoraggio dello stato e gestione degli errori.

Dettagli sull'esecuzione del task di sicurezza

Il task di sicurezza viene eseguito allo stesso modo dei task periodici standard, ad eccezione di quanto segue.

- Il task di sicurezza non inizia ad essere eseguito fino a quando il controllore primario ed il coprocessore di sicurezza hanno stabilito la loro partnership di controllo ed il tempo di sistema coordinato (CST) è sincronizzato. Tuttavia i task standard iniziano ad essere eseguiti non appena il controllore passa in modalità Esecuzione.

- Sebbene il campo configurabile dell'intervallo di pacchetto richiesto (RPI) per gli ingressi di sicurezza ed i tag di sicurezza consumati sia 6...500 ms, i tag di ingresso di sicurezza ed i tag di sicurezza consumati vengono aggiornati solo all'inizio dell'esecuzione del task di sicurezza. Significa che sebbene l'RPI degli I/O possa essere più rapido del periodo del task di sicurezza, i dati non vengono modificati nel corso dell'esecuzione di quest'ultimo. I dati vengono letti una sola volta all'inizio dell'esecuzione del task di sicurezza.

- I valori degli ingressi di sicurezza rimangono fissi all'avvio dell'esecuzione del task di sicurezza. Conseguentemente le istruzioni che utilizzano il timer, come TON e TOF, non saranno aggiornate nel corso dell'esecuzione di un singolo task di sicurezza. Esse manterranno una temporizzazione precisa tra l'esecuzione di un task e l'altra ma il tempo accumulato non cambierà durante l'esecuzione del task di sicurezza.

ATTENZIONE: Questo comportamento è diverso dall'esecuzione del task Logix standard ma è simile a quello del PLC o SLC™.

- Per i tag standard che sono mappati nei tag di sicurezza, i valori dei tag standard vengono copiati nella memoria di sicurezza all'avvio del task di sicurezza e non cambiano durante l'esecuzione del task di sicurezza.

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

- Il task di sicurezza risponde alle modifiche della modalità (ad esempio, da esecuzione a programmazione o da programmazione ad esecuzione) ad intervalli temporizzati. Conseguentemente è possibile che il task di sicurezza possa impiegare più del periodo di un task ma sempre meno di due per eseguire una transizione di modalità.

IMPORTANTE	In una condizione senza blocco di sicurezza e senza la firma del task di sicurezza, il controllore impedisce un accesso di scrittura simultaneo alla memoria di sicurezza da parte del task di sicurezza e dei comandi di comunicazione. Conseguentemente il task di sicurezza può essere ritardato fino al completamento dell'aggiornamento della comunicazione. Il tempo necessario per l'aggiornamento varia in base alle dimensioni dei tag. Pertanto potrebbero verificarsi timeout del watchdog di sicurezza e di una connessione di sicurezza. (ad esempio se si eseguono modifiche online con il periodo del task di sicurezza impostato su 1 ms, potrebbe verificarsi un timeout del watchdog di sicurezza). Per compensare il ritardo dovuto all'aggiornamento della comunicazione, aggiungere 2 ms al tempo del watchdog di sicurezza. Quando il controllore è in blocco di sicurezza o è presente una firma del task di sicurezza, la situazione descritta in questa nota non può verificarsi.

Uso delle interfacce operatore

Per utilizzare dispositivi di interfaccia operatore in sistemi GuardLogix classificati SIL, attenersi alle istruzioni ed alle precauzioni che seguono.

Precauzioni

Con i dispositivi di interfaccia operatore, adottare tutte le necessarie precauzioni ed implementare tecniche specifiche. Tali precauzioni includono, tra l'altro, le seguenti:

- limitazione degli accessi e sicurezza
- specifiche, test e validazione
- restrizioni su dati ed accesso
- limiti su dati e parametri.

Per ulteriori informazioni sull'utilizzo dei dispositivi di interfaccia operatore in un tipico loop SIL, vedere Figura 1 a pagina 15.

Utilizzare tecniche sicure nel software applicativo all'interno dell'interfaccia operatore e del controllore.

Accesso ai sistemi di sicurezza

Le funzioni dell'interfaccia operatore possono essere raggruppate in due attività principali: lettura e scrittura dei dati.

Lettura dei parametri nei sistemi di sicurezza

Non influendo sul comportamento del sistema di sicurezza, la lettura dei dati non prevede restrizioni. Tuttavia, il numero, la frequenza e le dimensioni dei dati che vengono letti possono incidere sulla disponibilità del controllore. Per evitare interventi di protezione indesiderati di sicurezza, ricorrere a valide pratiche di comunicazione per limitare l'impatto dell'elaborazione delle comunicazioni sul controllore. Non impostare le frequenze di lettura al massimo valore possibile.

Modifica dei parametri nei sistemi SIL

La modifica di un parametro in un loop di sicurezza attraverso un dispositivo esterno (esterno al loop di sicurezza) come, ad esempio, un'interfaccia operatore è ammessa solo con i vincoli di seguito.

- Solo personale autorizzato e qualificato (operatori) può modificare i parametri dei sistemi di sicurezza attraverso le interfacce operatore.
- L'operatore che effettua modifiche in un sistema di sicurezza attraverso un'interfaccia operatore è responsabile dell'effetto di tali modifiche sul loop di sicurezza.
- È necessario documentare chiaramente le variabili che devono essere modificate.
- È necessario usare una procedura chiara, completa ed esplicita per apportare modifiche al sistema di sicurezza attraverso un'interfaccia operatore.
- In un sistema di sicurezza, le modifiche possono essere accettate solo in presenza della seguente sequenza di eventi:

  a. La nuova variabile deve essere inviata due volte a due tag differenti; ovvero, entrambi i valori non devono essere scritti con un solo comando.
  b. Il codice di sicurezza eseguito nel controllore deve controllare l'equivalenza di entrambi i tag e verificare che rientrino nel campo previsto (controlli di limite).
  c. Entrambe le nuove variabili devono essere rilette e visualizzate sul dispositivo di interfaccia operatore.
  d. Operatori qualificati devono controllare visivamente che le variabili siano uguali e che il valore sia corretto.
  e. Operatori qualificati devono confermare manualmente la correttezza dei valori visualizzati sulla schermata dell'interfaccia operatore che invia alla logica di sicurezza il comando che permette di utilizzare i nuovi valori nella funzione di sicurezza.

In ogni caso, l'operatore deve verificare la validità delle modifiche, prima che possano essere accettate ed applicate nel loop di sicurezza.

- Testare tutte le modifiche nell'ambito della procedura di validazione di sicurezza.
- Documentare adeguatamente tutte le modifiche apportate al sistema di sicurezza attraverso l'interfaccia operatore, incluse le seguenti:
  - autorizzazione
  - analisi dell'impatto
  - esecuzione
  - informazioni sul test
  - informazioni sulla versione.
- Le modifiche al sistema di sicurezza devono conformarsi alla norma IEC 61511 sulla sicurezza dei processi, sezione 11.7.1 Requisiti dell'interfaccia operatore.
- Le modifiche al sistema di sicurezza devono conformarsi alla norma IEC 62061 per la sicurezza delle macchine.
- Lo sviluppatore deve seguire le procedure e le tecniche di sviluppo utilizzate anche per lo sviluppo di altri software applicativi, tra cui la verifica ed il collaudo dell'interfaccia operatore ed il suo accesso ad altre parti del programma. Nel software applicativo del controllore, creare una tabella che sia accessibile dall'interfaccia operatore e limitare l'accesso esclusivamente ai dati necessari.
- Come il programma del controllore, anche il software dell'interfaccia operatore ha bisogno di essere protetto e manutenuto per garantire la conformità al livello SIL dopo la validazione ed il test del sistema.

Programmi di sicurezza

Un programma di sicurezza è dotato di tutti gli attributi di un programma standard, ad eccezione del fatto che può essere pianificato soltanto nel task di sicurezza. Un programma di sicurezza può anche definire tag di sicurezza in ambito programma. Un programma di sicurezza può essere pianificato o non pianificato.

Un programma di sicurezza può contenere soltanto componenti di sicurezza. Tutte le routine contenute in un programma di sicurezza sono routine di sicurezza. Un programma di sicurezza non può contenere routine standard o tag standard.

Routine di sicurezza

Una routine di sicurezza è dotata di tutti gli attributi di una routine standard, ad eccezione del fatto che può esistere solo nei programmi di sicurezza. Una routine di sicurezza può essere designata come routine principale. Un'altra routine di sicurezza può essere designata come routine di errore. Soltanto le istruzioni certificate di sicurezza possono essere utilizzate in routine di sicurezza.

Per un elenco delle istruzioni di sicurezza, vedere l'Appendice A.

ATTENZIONE: Per mantenere il livello SIL 3, accertarsi che la propria logica di sicurezza non cerchi di leggere o scrivere i tag standard.

Tag di sicurezza

Il sistema di controllo GuardLogix supporta l'utilizzo sia dei tag standard sia di quelli di sicurezza nello stesso progetto. Tuttavia, il software di programmazione distingue funzionalmente tra tag standard e tag di sicurezza.

I tag di sicurezza sono dotati di tutti gli attributi dei tag standard con l'aggiunta di meccanismi per garantire l'integrità dei dati secondo SIL 3.

Tabella 6 – Tipi di dati validi per i tag di sicurezza

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

L'applicazione Logix Designer previene la creazione diretta di tag non validi in un programma di sicurezza. I tag non validi importati non possono essere verificati.

IMPORTANTE L'uso di alias tra tag standard e tag di sicurezza è vietato nelle applicazioni di sicurezza.

I tag classificati come tag di sicurezza possono essere definiti nell'ambito del controllore o nell'ambito del programma. I tag di sicurezza nell'ambito del controllore possono essere letti dalla logica standard o di sicurezza o da altri dispositivi di comunicazione ma possono essere scritti unicamente dalla logica di sicurezza o da un altro controllore di sicurezza GuardLogix. I tag di sicurezza nell'ambito del programma sono accessibili solo da routine di sicurezza locali. Si tratta di routine che si trovano all'interno del programma di sicurezza.

I tag associati agli I/O di sicurezza ed ai dati di sicurezza prodotti o consumati devono essere tag di sicurezza nell'ambito del controllore.

IMPORTANTE I tag di sicurezza nell'ambito del controllore sono leggibili da qualsiasi routine standard, ma la frequenza di aggiornamento si basa sull'esecuzione del task di sicurezza. Pertanto i tag di sicurezza vengono aggiornati alla frequenza periodica del task di sicurezza, che è diversa dal comportamento del tag standard.

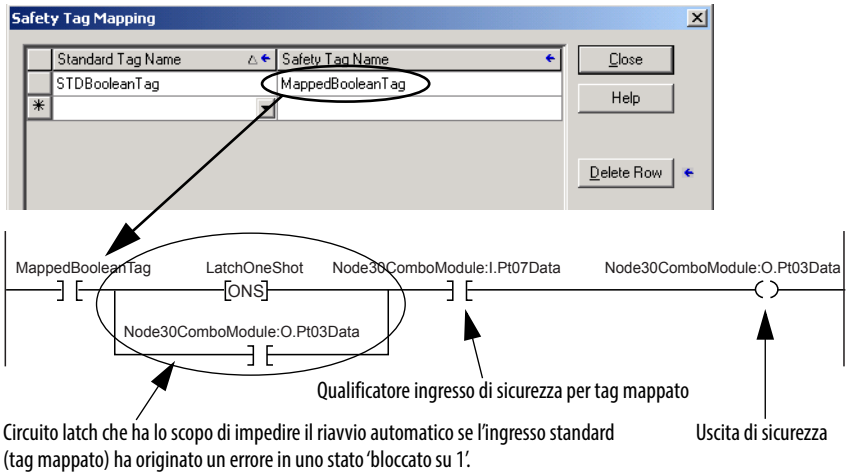
Tag standard in routine di sicurezza (mappatura dei tag)

I tag standard nell'ambito del controllore possono essere mappati in tag di sicurezza fornendo in tal modo un meccanismo per sincronizzare azioni standard ed azioni di sicurezza.

ATTENZIONE: Se si utilizzano dati standard in una routine di sicurezza, si è responsabili di fornire uno strumento affidabile per assicurare che i dati vengano utilizzati nel modo corretto. L'uso i dati standard in un tag di sicurezza non equivale a renderli dati di sicurezza. Non controllare un'uscita di sicurezza direttamente con i dati dei tag standard.

Questo esempio mostra come qualificare i dati standard con i dati di sicurezza.

Figura 14 – Qualificazione dei dati standard con dati di sicurezza



Note:

Sviluppo dell'applicazione di sicurezza

Presupposti del concetto di sicurezza

Il concetto di sicurezza presuppone che:

- i responsabili dello sviluppo, del funzionamento e della manutenzione dell'applicazione siano rappresentati da personale debitamente qualificato, specificamente addestrato e con esperienza nei sistemi di sicurezza
- l'utente applichi la logica in modo corretto intendendo con ciò che gli errori di programmazione possano essere rilevati; gli errori di programmazione possono essere rilevati attenendosi rigorosamente alle specifiche tecniche, alle regole di programmazione e denominazione
- l'utente esegua un'analisi critica dell'applicazione e utilizzi tutte le misure possibili per rilevare i guasti
- l'utente confermi tutti i download dell'applicazione attraverso un controllo manuale della firma del task di sicurezza
- prima dell'avviamento iniziale del sistema di sicurezza, l'intero sistema venga controllato con un test funzionale completo.

Tabella 7 – Modalità del controllore

Modalità del controllore	Stato del task di sicurezza	Sicurezza[1] (fino a ed incluso)	Commenti (nel controllore è stato scaricato un programma valido)
Programma	Sbloccato Senza firma		• Connessioni I/O stabilite. • Logica del task di sicurezza non in fase di scansione.
Esecuzione	Sbloccato Senza firma	(solo a fini di sviluppo)	• Forzature ammesse. • Modifiche online ammesse. • Memoria di sicurezza isolata ma non protetta (lettura/scrittura). • Logica del task di sicurezza in fase di scansione. Controllore primario e coprocessore elaborano la logica ed eseguono il controllo incrociato delle uscite logiche. Uscite logiche scritte sulle uscite di sicurezza.
Esecuzione	Bloccato Senza firma	PLd/Cat. 3 Controllo affidabile SIL CL2	• Non sono ammesse nuove forzature. Forzature esistenti mantenute. • Modifiche online non ammesse. • Memoria di sicurezza protetta (solo lettura). • Logica del task di sicurezza scandita. • Controllore primario e coprocessore elaborano la logica ed eseguono il controllo incrociato delle uscite logiche. Uscite logiche scritte sulle uscite di sicurezza.
Esecuzione	Sbloccato Con firma	Ple/Cat. 4 Controllo affidabile SIL CL3	• Forzature non ammesse (devono essere rimosse per generare la firma del task di sicurezza). • Modifiche online non ammesse. • Memoria di sicurezza protetta (solo lettura). • Logica del task di sicurezza scandita. • Controllore primario e coprocessore elaborano la logica ed eseguono il controllo incrociato delle uscite logiche. Uscite logiche scritte sulle uscite di sicurezza. • Firma del task di sicurezza non protetta e cancellabile da chiunque acceda al controllore.
Esecuzione	Bloccato Con firma	Ple/Cat. 4 Controllo affidabile SIL CL3	• Forzature non ammesse (devono essere rimosse per generare la firma del task di sicurezza). • Modifiche online non ammesse. • Memoria di sicurezza protetta (solo lettura). • Logica del task di sicurezza scandita. • Controllore primario e coprocessore elaborano la logica ed eseguono il controllo incrociato delle uscite logiche. Uscite logiche scritte sulle uscite di sicurezza. • La firma del task di sicurezza è protetta. Prima di poter cancellare la firma del task di sicurezza, gli utenti devono inserire la password di sblocco del controllore.

(1) Per ottenere questo livello, è necessario attenersi ai requisiti di sicurezza definiti in questa pubblicazione.

Concetti base per lo sviluppo ed il test dell'applicazione

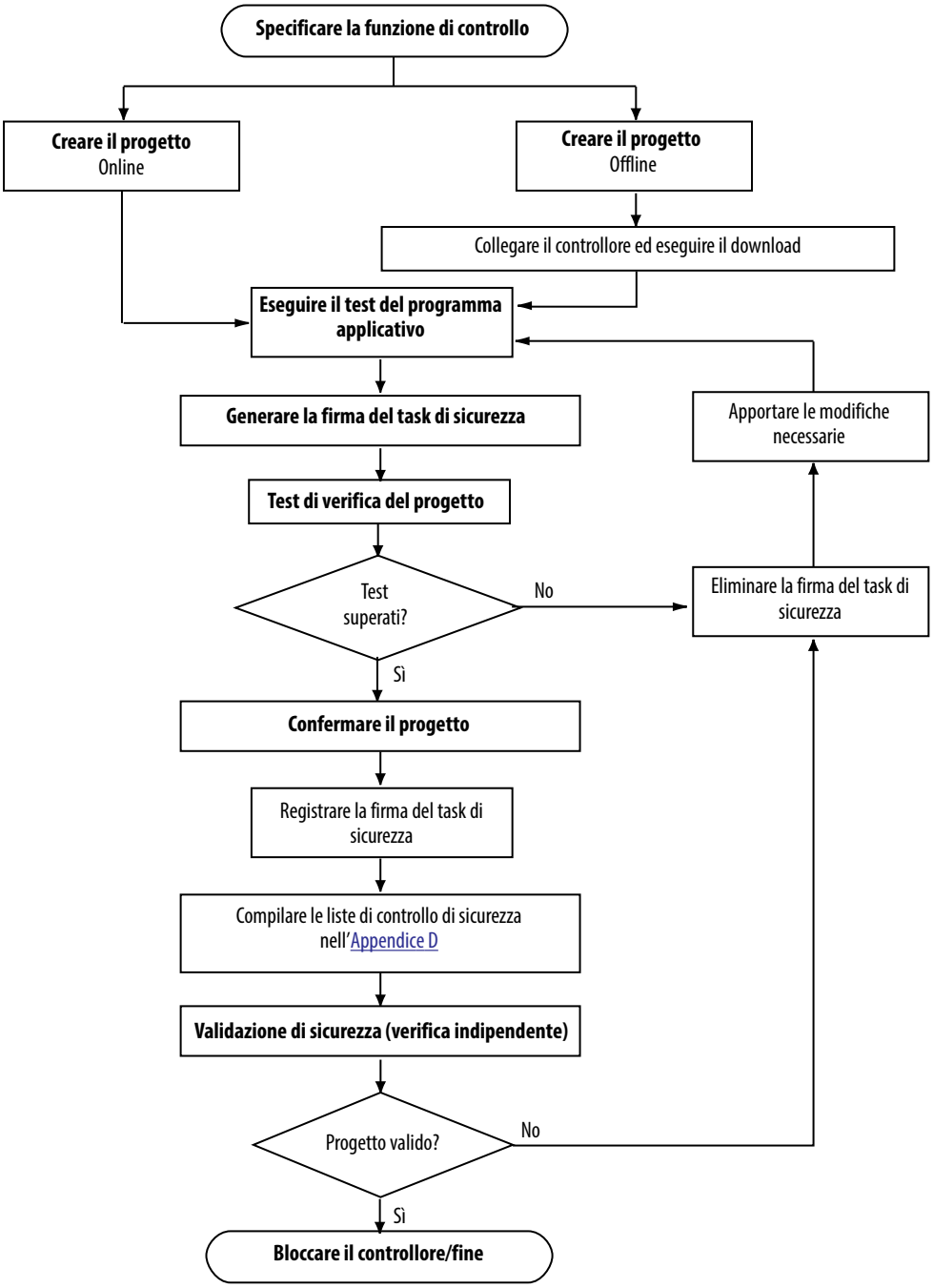
È consigliabile che il programma applicativo per il sistema SIL CL3 previsto sia sviluppato dall'integratore di sistemi o da un utente in possesso di formazione ed esperienza nelle applicazioni di sicurezza. Lo sviluppatore deve seguire tecniche di progettazione valide.

- Utilizzare specifiche funzionali, tra cui diagrammi di flusso, diagrammi dei tempi e diagrammi sequenziali.
- Eseguire l'analisi della logica del task di sicurezza.
- Eseguire la validazione dell'applicazione.

Procedura per la messa in servizio

Il diagramma di flusso sottoriportato mostra i passi necessari per la messa in servizio di un sistema GuardLogix. Le voci in grassetto sono spiegate nelle sezioni che seguono.

Figura 15 – Messa in servizio del sistema



Specifica della funzione di controllo

Si deve creare una specifica per la propria funzione di controllo. Utilizzare questa specifica per verificare che la logica del programma soddisfi correttamente e completamente i requisiti funzionali e di controllo della sicurezza della propria applicazione. La specifica può essere presentata in numerosi formati in base alla propria applicazione. Tuttavia la specifica deve essere una descrizione dettagliata che include quanto segue (se applicabile):

- Sequenza operativa
- Diagrammi di flusso e dei tempi
- Diagrammi sequenziali
- Descrizione del programma
- Stampa del programma
- Descrizioni scritte dei punti con le relative condizioni e gli attuatori da controllare, compreso quanto segue:
  - Definizioni ingressi
  - Definizioni uscite
  - Schemi di cablaggio I/O e riferimenti
  - Principio di funzionamento
- Matrice o tabella delle condizioni dei punti e degli attuatori da controllare, inclusi i diagrammi sequenziali e dei tempi
- Definizione delle condizioni limite, ad esempio, modalità operative e ARRESTO D'EMERGENZA

La parte relativa agli I/O della specifica tecnica deve contenere l'analisi dei circuiti di campo, ossia, il tipo di sensori ed attuatori.

- Sensori (digitali o analogici)
  - Segnale di funzionamento standard (principio della corrente a riposo per sensori digitali, sensori OFF significa nessun segnale)
  - Determinazione delle ridondanze necessarie per i livelli SIL
  - Monitoraggio e visualizzazione di discrepanze, inclusa la logica diagnostica dell'utente
- Attuatori
  - Posizione ed attivazione nel funzionamento standard (normalmente OFF)
  - Reazione/posizionamento di sicurezza in caso di spegnimento o di interruzione dell'alimentazione
  - Monitoraggio e visualizzazione di discrepanze, inclusa la logica diagnostica dell'utente

Creare il progetto

La logica e le istruzioni utilizzate nella programmazione dell'applicazione devono essere:

- facili da comprendere
- facili da tracciare
- facili da modificare
- facili da testare

Esaminare e testare tutta la logica. Tenere separate la logica connessa con la sicurezza e la logica standard.

Identificazione del programma

Il programma applicativo è chiaramente identificato da uno dei seguenti elementi:

- Nome
- Data
- Versione
- Qualsiasi altra identificazione utente

Test del programma applicativo

Questo passo include qualsiasi combinazione delle modalità Esecuzione e Programmazione, delle modifiche online ed offline, dell'upload e del download e del test informale necessari perché un'applicazione funzioni correttamente, in preparazione del test di verifica del progetto.

Generazione della firma del task di sicurezza

La firma del task di sicurezza identifica univocamente ciascun progetto, inclusi la logica, i dati e la configurazione. La firma del task di sicurezza è composta da ID (numero di identificazione), data e ora.

La firma del task di sicurezza può essere generata se sono soddisfatte tutte le seguenti condizioni:

- l'applicazione Logix Designer è online con il controllore
- il controllore è in modalità Programmazione
- il controllore non è in blocco di sicurezza
- il controllore non ha forzature di sicurezza o modifiche di sicurezza online in sospeso
- lo stato del task di sicurezza è OK.

Una volta completato il test del programma applicativo, si deve generare la firma del task di sicurezza. Il software di programmazione carica automaticamente la firma del task di sicurezza, dopo che è stata generata.

IMPORTANTE	Per verificare l'integrità di ciascun download, è necessario annotare manualmente la firma del task di sicurezza dopo la creazione iniziale e verificare la firma del task di sicurezza dopo ogni download per assicurarsi che corrisponda all'originale.

La firma del task di sicurezza può essere eliminata solo se il controllore GuardLogix non è in blocco di sicurezza e, se online, se il selettore a chiave è in posizione REM o PROG.

Quando esiste una firma del task di sicurezza, le seguenti azioni non sono ammesse nell'ambito del task di sicurezza:

- programmazione o modifica online o offline dei componenti di sicurezza
- forzatura degli I/O di sicurezza
- manipolazione dati (eccetto mediante logica di una routine o di un altro controllore GuardLogix)

Test di verifica del progetto

Per verificare che il programma applicativo sia conforme alla specifica, si deve generare un insieme idoneo di test case che coprono l'applicazione. L'insieme di test case deve essere archiviato e conservato come la specifica del test.

Per comprovare la validità dei calcoli (formule) utilizzati nella logica della propria applicazione si deve includere un insieme di test. Sono accettabili test con intervalli equivalenti. Si tratta di test eseguiti negli intervalli definiti dei valori, ai limiti o in intervalli non validi di valori. Il numero necessario di test case dipende dalle formule utilizzate e deve comprendere coppie di valori critici.

Deve essere inclusa anche la simulazione attiva con sorgenti (dispositivi di campo) poiché è l'unico modo per verificare che i sensori e gli attuatori nel sistema siano cablati correttamente. Verificare il funzionamento delle funzioni programmate manipolando manualmente i sensori e gli attuatori.

È necessario inoltre prevedere test per verificare la reazione agli errori di cablaggio ed agli errori di comunicazione della rete.

La verifica del progetto include test per routine di errore e canali di ingresso e di uscita, al fine di assicurare che il sistema di sicurezza funzioni correttamente.

Per eseguire un test di verifica del progetto sul controllore GuardLogix, è necessario eseguire un test completo dell'applicazione. È necessario alternare ciascun sensore ed attuatore coinvolti nelle funzioni di sicurezza. Dal punto di vista del controllore, significa ciclare il punto I/O nello stesso controllore, non necessariamente gli attuatori reali. Assicurarsi di verificare tutte le funzioni di spegnimento, poiché non vengono di solito utilizzate durante il funzionamento normale. Ricordare inoltre che un test di verifica del progetto è valido unicamente per la specifica applicazione testata. Se il controllore viene trasferito ad un'altra applicazione, è necessario eseguirne il test di avviamento e di verifica del progetto all'interno del nuovo programma applicativo.

Confermare il progetto

Si deve stampare o visualizzare il progetto e confrontare gli I/O di sicurezza caricati e le configurazioni del controllore, i dati di sicurezza e la logica del programma del task di sicurezza per assicurarsi che i componenti di sicurezza corretti siano stati scaricati, testati e mantenuti nel programma applicativo di sicurezza.

Se il programma applicativo contiene un'istruzione Add On di sicurezza sigillata con una firma dell'istruzione, è inoltre necessario confrontare la firma dell'istruzione, data/e ora e firma dell'istruzione di sicurezza con i valori che sono stati registrati quando è stata sigillata l'istruzione Add On.

Per informazioni sulla creazione e l'uso di istruzioni Add On di sicurezza in applicazioni SIL 3, vedere l'Appendice B, Istruzioni Add-On di sicurezza.

I punti sotto riportati illustrano un metodo per confermare il progetto.

1. Con il controllore in modalità Programmazione salvare il progetto.
2. Rispondere "Yes (Sì)" alla richiesta Upload tag Values (Carica valori tag).
3. Con l'applicazione Logix Designer offline, salvare il progetto con un nuovo nome, ad esempio "Offlineprojectname.ACD", dove projectname è il nome del proprio progetto.

   Questo è il nuovo file di progetto master testato.
4. Chiudere il progetto.
5. Spostare il file di archivio del progetto originale dalla directory attuale. Il file può essere eliminato o memorizzato in una posizione dell'archivio. Questo passo è necessario perché se l'applicazione Logix Designer trova projectname.ACD in questa directory, lo collega al progetto del controllore e non esegue un vero e proprio upload.
6. Con il controllore ancora in modalità Programmazione, caricare il progetto dal controllore.
7. Salvare il progetto caricato come "Onlineprojectname.ACD", dove projectname è il nome del proprio progetto.
8. Rispondere "Yes (Sì)" alla richiesta Upload tag Values (Carica valori tag).
9. Usare la funzione Program Compare di Logix Designer per i seguenti confronti:
   - confrontare tutte le proprietà del controllore GuardLogix e dei dispositivi I/O CIP Safety
   - confrontare tutte le proprietà del task di sicurezza, dei programmi di sicurezza e delle routine di sicurezza
   - confrontare l'intera logica nelle routine di sicurezza.

Validazione di sicurezza

È possibile che sia necessaria una verifica indipendente di terza parte del sistema di sicurezza, prima che il sistema venga approvato per il funzionamento. La normativa IEC 61508 SIL 3 richiede una certificazione indipendente eseguita da terze parti.

Blocco del controllore GuardLogix

Il blocco di sicurezza del sistema di controllo GuardLogix può essere impostato per contribuire a proteggere i componenti di controllo di sicurezza da eventuali modifiche. Tuttavia, il blocco di sicurezza del controllore non è un requisito delle applicazioni SIL 3. 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, i tag di sicurezza, le istruzioni Add On di sicurezza, l'I/O di sicurezza e la firma del task di sicurezza. Tuttavia il blocco di sicurezza da solo non soddisfa i requisiti SIL 3.

Nessun aspetto della sicurezza può essere modificato mentre il controllore si trova nello stato di blocco di sicurezza. Quando il controllore è in blocco di sicurezza, nel task di sicurezza non sono ammesse le seguenti azioni:

- programmazione o modifica online/offline
- forzatura degli I/O di sicurezza
- manipolazione dati (eccetto mediante logica di una routine o di un altro controllore GuardLogix)
- creazione o modifica di istruzioni Add On di sicurezza
- generazione o eliminazione della firma del task di sicurezza.

Lo stato di default del controllore è quello sbloccato. Si può portare l'applicazione di sicurezza in uno stato di blocco di sicurezza indipendentemente dal fatto che l'utente sia online o meno e che si disponga del sorgente originale del programma. Tuttavia non possono essere presenti forzature di sicurezza o modifiche di sicurezza in sospeso. Gli stati di blocco o sblocco di sicurezza non possono essere modificati quando il selettore a chiave si trova nella posizione RUN.

Per garantire un ulteriore livello di protezione, è possibile utilizzare password separate per il blocco di sicurezza e lo sblocco di sicurezza del controllore. Le password sono opzionali.

Download del programma applicativo di sicurezza

Durante il download, è richiesto il test dell'applicazione, a meno che non esista una firma del task di sicurezza.

IMPORTANTE	Per verificare l'integrità di ciascun download, è necessario annotare manualmente la firma del task di sicurezza dopo la creazione iniziale e verificare la firma del task di sicurezza dopo ogni download per assicurarsi che corrisponda all'originale.

I download in un controllore GuardLogix in blocco di sicurezza sono ammessi soltanto se la firma del task di sicurezza, le serie hardware e la versione del sistema operativo del progetto offline corrispondono tutte a quelle contenute nel controllore GuardLogix di destinazione e se lo stato del task di sicurezza del controllore è OK.

IMPORTANTE Se la firma del task di sicurezza non corrisponde ed il controllore è in blocco di sicurezza, per eseguire il download si deve sbloccare il controllore. In tal caso, il download sul controllore cancella la firma del task di sicurezza. Di conseguenza si deve validare di nuovo l'applicazione.

ATTENZIONE: La porta USB è adatta solo per la programmazione locale temporanea e non è previsto che sia collegata in modo permanente.

Upload del programma per applicazioni di sicurezza

Se il controllore GuardLogix contiene una firma del task di sicurezza, quest'ultima verrà caricata con il progetto. Significa che qualsiasi modifica ai dati di sicurezza offline sarà sovrascritta come conseguenza dell'upload.

Modifiche online

Se non è presente alcuna firma del task di sicurezza ed il controllore è in sblocco di sicurezza, è possibile apportare modifiche online alle proprie routine di sicurezza.

SUGGERIMENTO Non è possibile modificare le istruzioni Add On standard o di sicurezza mentre si è online.

Le modifiche in sospeso non possono essere presenti quando il controllore è in blocco di sicurezza oppure quando esiste una firma del task di sicurezza. Le modifiche online possono essere presenti quando il controllore è in blocco di sicurezza. Tuttavia non possono essere assemblate o annullate.

SUGGERIMENTO Le modifiche online nelle routine standard non sono interessate dallo stato di blocco o di sblocco di sicurezza.

Vedere pagina 59 per maggiori informazioni sulle modifiche al programma applicativo.

Memorizzazione e caricamento di un progetto dalla memoria non volatile

I controllori GuardLogix 5570 supportano gli aggiornamenti firmware e la memorizzazione o il recupero dei programmi utente tramite una scheda di memoria. In un sistema GuardLogix, solo il controllore primario utilizza una scheda di memoria per la memoria non volatile.

Quando si memorizza un progetto di sicurezza su una scheda di memoria, Rockwell Automation consiglia di selezionare Remote Program come modalità di caricamento, ossia la modalità a cui passa il controllore in seguito al caricamento. Prima dell'entrata in funzione effettiva della macchina è richiesto l'intervento dell'operatore, che deve avviarla.

Il caricamento può essere avviato dalla memoria non volatile solo:

- se il tipo di controllore specificato dal progetto memorizzato nella memoria non volatile corrisponde al tipo di controllore in uso
- se le versioni principali e secondarie del progetto nella memoria non volatile corrispondono alle versioni principali e secondarie del controllore in uso
- se il controllore non è in modalità Esecuzione.

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. Se le firme non corrispondono o se il controllore è in blocco di sicurezza senza firma del task di sicurezza, è necessario sbloccare preventivamente il controllore prima di cercare di eseguirne l'aggiornamento tramite la memoria non volatile.

IMPORTANTE	Se 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.

Dati forzati

Tutti i dati contenuti in un I/O, in un tag di sicurezza prodotto o consumato, incluso CONNECTION_STATUS possono essere forzati mentre il progetto è in sblocco di sicurezza e se non esiste una firma del task di sicurezza. Tuttavia le forzature devono essere disinstallate, non solo disabilitate, su tutti i tag di sicurezza prima che il progetto di sicurezza possa essere in blocco di sicurezza o che possa essere generata una firma del task di sicurezza. I tag di sicurezza non possono essere forzati mentre il progetto è in blocco di sicurezza o quando esiste una firma del task di sicurezza.

SUGGERIMENTO	È possibile installare e disinstallare le forzature su tag standard indipendentemente dallo stato di blocco o di sblocco di sicurezza.

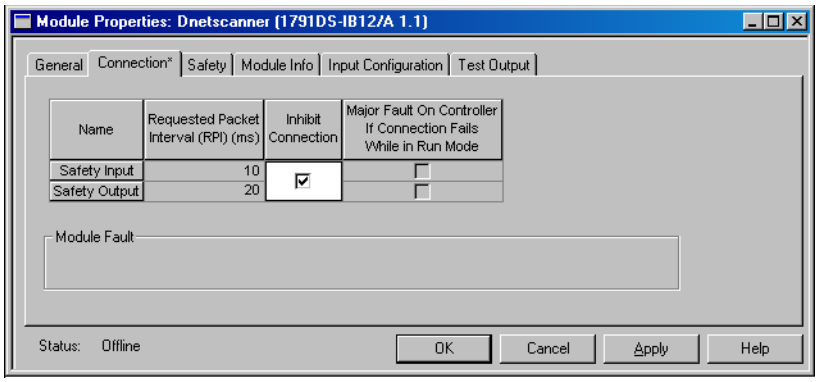
Inibizione di un dispositivo

Non è possibile inibire o abilitare i dispositivi I/O CIP Safety o i controllori produttori se il programma applicativo è in blocco di sicurezza oppure se esiste una firma del task di sicurezza.

Seguire questi passi per inibire uno specifico dispositivo I/O di sicurezza.

1. Nell'applicazione Logix Designer, fare clic con il pulsante destro del mouse sul dispositivo e selezionare Properties.

2. Fare clic sulla scheda Connection nella finestra di dialogo Module Properties.
3. Selezionare Inhibit Connection e fare clic su Apply.



Quando la casella di controllo è selezionata, il dispositivo è inibito. Se un dispositivo di comunicazione è inibito, lo saranno anche tutti i dispositivi a valle.

Modifica dell'applicazione di sicurezza

Per modificare il programma applicativo di sicurezza nell'applicazione Logix Designer, attenersi alle seguenti regole:

- Soltanto personale autorizzato specificamente addestrato può apportare modifiche al programma. Questo personale dovrebbe utilizzare tutti i metodi di supervisione disponibili, ad esempio, utilizzando il selettore a chiave del controllore e le protezioni mediante password del software.
- Apportando modifiche al programma il personale autorizzato specificamente addestrato si assume la responsabilità della sicurezza centrale mentre queste modifiche sono in corso. Questo personale deve anche mantenere sicuro il funzionamento dell'applicazione.
- Eseguendo le modifiche online, si deve utilizzare un meccanismo di protezione alternativo per mantenere la sicurezza del sistema.
- Si devono documentare tutte le modifiche apportate al programma, incluse le seguenti:
  - autorizzazione
  - analisi dell'impatto
  - esecuzione
  - informazioni sul test
  - informazioni sulla versione.
- Se esistono modifiche online soltanto nelle routine standard, non è necessario che queste modifiche vengano validate prima di ritornare al funzionamento normale.
- È necessario assicurarsi che le modifiche alla routine standard, per quanto riguarda la temporizzazione e la mappatura dei tag, siano valide per la propria applicazione di sicurezza.
- È **possibile** modificare la parte logica del proprio programma mentre si è offline oppure online, come descritto nelle sezioni che seguono.

Esecuzione di modifiche offline

Quando vengono apportate modifiche offline soltanto agli elementi del programma standard e la firma del task di sicurezza corrisponde dopo un download, è possibile riprendere il funzionamento.

Quando le modifiche offline influiscono sul programma di sicurezza, è necessario riconvalidare tutti gli elementi interessati dell'applicazione, secondo quanto determinato dall'analisi di impatto, prima di riprendere il normale funzionamento.

Il diagramma di flusso a pagina 61 illustra il processo per le modifiche offline.

Esecuzione di modifiche online

Quando le modifiche online influiscono sul programma di sicurezza, è necessario riconvalidare tutti gli elementi interessati dell'applicazione, secondo quanto determinato dall'analisi di impatto, prima di riprendere il normale funzionamento. Il diagramma di flusso a pagina 61 illustra il processo per le modifiche online.

SUGGERIMENTO Applicare modifiche online che siano soltanto di minore portata, ad esempio modifiche al setpoint o aggiunte, eliminazioni e modifiche secondarie alla logica.

Le modifiche online sono influenzate dal blocco di sicurezza e dalla firma del task di sicurezza del controllore GuardLogix.

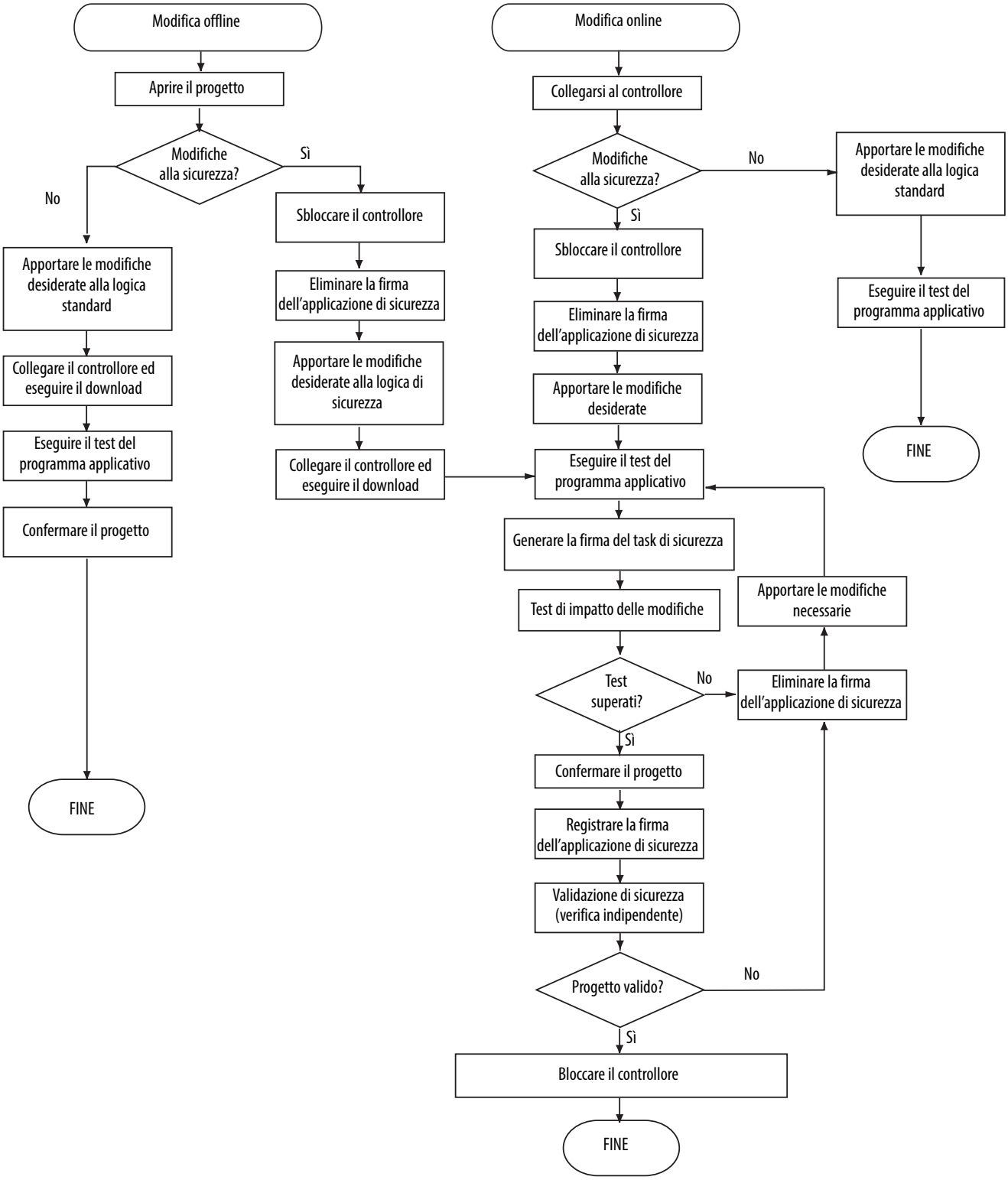
Per maggiori informazioni, vedere Generazione della firma del task di sicurezza a pagina 53 e Blocco del controllore GuardLogix a pagina 56.

Per maggiori informazioni sulle modifiche online alla logica ladder nell'applicazione Logix Designer, consultare Logix5000 Controllers Quick Start, pubblicazione 1756-QS001.

Test di impatto delle modifiche

Eventuali operazioni di modifica, miglioramento o adattamento del software convalidato devono essere pianificate ed analizzate per verificarne l'impatto sul sistema di sicurezza funzionale. Tutte le corrispondenti fasi del ciclo di vita di sicurezza del software devono essere realizzate come indicato dall'analisi di impatto. Come minimo, deve essere realizzato il collaudo funzionale di tutto il software interessato. Tutte le modifiche alle specifiche del software devono essere documentate. Anche i risultati dei test devono essere documentati. Per informazioni dettagliate, far riferimento alla norma IEC 61508-3, sezione 7.8 Modifiche software.

Figura 16 – Processo di modifica online ed offline



Note:

Monitoraggio dello stato e gestione degli errori

L'architettura GuardLogix fornisce all'utente molte possibilità per rilevare gli errori presenti nel sistema e per gestire gli stessi. Il primo modo in cui gli utenti possono gestire gli errori è accertarsi di avere completato le checklist per l'applicazione (vedere l'Appendice D).

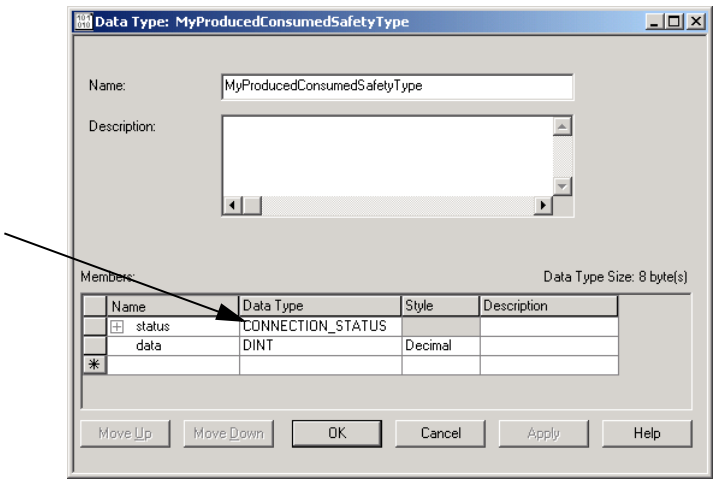
Monitoraggio dello stato del sistema

Lo stato delle connessioni del tag di sicurezza può essere visualizzato. Si può anche determinare lo stato di funzionamento corrente interrogando vari oggetti dei dispositivi. È responsabilità dell'utente determinare quali dati sono più opportuni per iniziare una sequenza di spegnimento.

Dati CONNECTION_STATUS

Il primo membro della struttura di tag associata con i dati di ingresso di sicurezza ed i dati dei tag di sicurezza prodotti/consumati contiene lo stato del collegamento. Questo membro è costituito da un tipo di dati predefinito denominato CONNECTION_STATUS.

Figura 17 – Finestra di dialogo Data Type



I primi due bit del tipo di dati CONNECTION_STATUS contengono i bit di stato RunMode e ConnectionFaulted di un dispositivo. La seguente tabella descrive le combinazioni degli stati RunMode e ConnectionFaulted.

Tabella 8 – Stato della connessione di sicurezza

Stato RunMode	Stato ConnectionFaulted	Funzionamento del collegamento di sicurezza
1 = Run	0 = Valid	I dati vengono attivamente controllati dal dispositivo produttore. Il dispositivo produttore è in modalità Esecuzione.
0 = Idle	0 = Valid	Il collegamento è attivo ed il dispositivo produttore è in stato di riposo. I dati di sicurezza vengono azzerati.
0 = Idle	1 = Faulted	Il collegamento di sicurezza è in errore. Lo stato del dispositivo produttore non è noto. I dati di sicurezza vengono azzerati.
1	1	Stato non valido.

ATTENZIONE: I collegamenti degli I/O di sicurezza ed i collegamenti prodotti/consumati non possono essere configurati automaticamente per generare un errore del controllore se un collegamento è perso ed il sistema passa allo stato di sicurezza. Pertanto, se è necessario rilevare un errore del dispositivo per assicurarsi che il sistema mantenga il livello SIL 3, si devono monitorare i bit CONNECTION_STATUS degli I/O di sicurezza ed inizializzare l'errore attraverso la logica del programma.

Diagnostica ingressi ed uscite

I moduli Guard I/O comprendono funzioni di monitoraggio e test ad impulsi. Se il modulo rileva un guasto, imposta l'ingresso o l'uscita che causa il problema nello stato di sicurezza e comunica il guasto al controllore. L'indicazione di guasto viene comunicata attraverso lo stato dell'ingresso o dell'uscita e conservata per un arco di tempo configurabile dopo che il guasto è stato riparato.

IMPORTANTE L'utente è responsabile dello sviluppo della logica di ritenuta (latch) degli errori I/O e deve assicurarsi che il riavvio del sistema avvenga in modo corretto.

Stato della connessione dei dispositivi I/O

Il protocollo CIP Safety fornisce lo stato di ogni dispositivo I/O nel sistema di sicurezza. Se viene rilevato un errore del collegamento di ingresso, il sistema operativo imposta tutti gli ingressi dei dispositivi sullo stato diseccitato (di sicurezza) e l'ingresso associato sullo stato di errore. Se viene rilevato un errore del collegamento di uscita, il sistema operativo imposta l'uscita associata sullo stato di errore. Le uscite vengono diseccitate dal dispositivo di uscita.

IMPORTANTE L'utente è responsabile dello sviluppo della logica di ritenuta (latch) degli errori I/O e deve assicurarsi che il riavvio del sistema avvenga in modo corretto.

Sistema di diseccitazione all'intervento

I controllori GuardLogix fanno parte di un sistema con diseccitazione all'intervento, vale a dire che zero è lo stato di sicurezza. Alcuni errori dei dispositivi I/O di sicurezza, ma non tutti, provocano l'impostazione a zero (stato di sicurezza) di tutti gli ingressi/uscite del modulo. Gli errori associati ad uno specifico canale di ingresso comportano l'impostazione a zero di quel canale; ad esempio, un errore del test ad impulsi specifico del canale 0 comporta l'impostazione in stato di sicurezza (0) dei dati di ingresso del canale 0. Se l'errore riguarda tutto il dispositivo e non uno specifico canale, il bit Combined Status visualizza lo stato di errore e tutti i dati del dispositivo vengono impostati in stato di sicurezza (0).

Per informazioni su come usare le istruzioni dell'applicazione di sicurezza GuardLogix, vedere l'Appendice F di questo manuale ed il manuale di riferimento per la sicurezza Set di istruzioni per l'applicazione di sicurezza GuardLogix, pubblicazione 1756-RM095.

Istruzioni Get System Value (GSV) e Set System Value (SSV)

Le istruzioni GSV e SSV permettono di ottenere (GSV) ed impostare (SSV) i dati del sistema di controllo memorizzati negli oggetti dei dispositivi. Inserendo un'istruzione GSV/SSV, il software di programmazione visualizza le classi di oggetti validi, i nomi degli oggetti ed i nomi degli attributi per ciascuna istruzione. Per l'utilizzo delle istruzioni GSV e SSV con i componenti di sicurezza esistono delle limitazioni.

IMPORTANTE	Il task di sicurezza non può eseguire operazioni GSV o SSV su attributi standard. Gli attributi degli oggetti di sicurezza che possono essere scritti dal task standard sono concepiti soltanto per scopi diagnostici. Non riguardano l'esecuzione del task di sicurezza.

Per ulteriori informazioni su quali attributi di sicurezza sono accessibili tramite le istruzioni GSV ed SSV, consultare il manuale dell'utente GuardLogix 5570 Controllers, pubblicazione 1756-UM022.

Per informazioni generali sull'uso delle istruzioni GSV ed SSV, consultare il manuale di riferimento Istruzioni generali per controllori Logix5000, pubblicazione 1756-RM003.

Errori del sistema GuardLogix

Gli errori nel sistema GuardLogix rientrano nelle seguenti tre categorie:

- errori irreversibili del controllore
- errori di sicurezza irreversibili
- errori reversibili

Per informazioni sulla gestione degli errori, consultare il manuale dell'utente GuardLogix 5570 Controllers, pubblicazione 1756-UM022.

Errori irreversibili del controllore

Un errore irreversibile del controllore si verifica se la diagnostica interna del controllore va in errore. La partnership viene persa quando si verifica un errore irreversibile del controllore nel controllore primario o nel coprocessore di sicurezza, facendo sì che l'altro generi un errore irreversibile di timeout del watchdog. L'esecuzione del task standard e del task di sicurezza si arresta e gli I/O di sicurezza passano allo stato di sicurezza.

Il ripristino da un errore irreversibile del controllore richiede di eseguire nuovamente il download del programma applicativo.

Errori di sicurezza irreversibili

In caso di un errore di sicurezza irreversibile, il controllore registra l'errore nel gestore degli errori nell'ambito del controllore e disattiva il task di sicurezza, inclusi gli I/O di sicurezza e la logica di sicurezza.

Per il ripristino da un errore di sicurezza irreversibile, la memoria di sicurezza viene reinizializzata dalla firma del task di sicurezza (avviene automaticamente quando si cancella l'errore) oppure, se non esiste una firma del task di sicurezza, attraverso un download del progetto di sicurezza.

Si può annullare l'errore di sicurezza eliminando la voce del registro errori per mezzo del gestore degli errori di sicurezza nell'ambito del controllore. Permette ai task standard di continuare a funzionare.

ATTENZIONE: Annullare un errore di sicurezza non significa cancellarlo. Se si annulla un errore di sicurezza, è responsabilità dell'utente dimostrare che così facendo si mantiene il livello SIL 3.

Errori reversibili

Gli errori del controllore causati da errori di programmazione dell'utente in un programma di sicurezza attivano il controllore che inizia ad elaborare la logica contenuta nel gestore degli errori del programma di sicurezza del progetto. Il gestore degli errori del programma di sicurezza fornisce all'applicazione l'opportunità di eliminare la condizione di errore e quindi di correggerla.

ATTENZIONE: L'utente deve dimostrare al proprio ente certificatore che il ripristino automatico degli errori reversibili mantiene il livello SIL 3.

Quando non esiste un gestore degli errori del programma di sicurezza oppure l'errore non viene ripristinato dal gestore stesso, il controllore elabora la logica nel gestore degli errori nell'ambito del controllore, terminando l'esecuzione della logica del programma di sicurezza e lasciando attive, ma a riposo, le connessioni degli I/O di sicurezza.

IMPORTANTE Quando l'esecuzione della logica del programma di sicurezza viene terminata in seguito ad un errore reversibile non ripristinato dal gestore degli errori di sicurezza, le connessioni degli I/O di sicurezza sono chiuse e riaperte per inizializzare nuovamente le connessioni di sicurezza.

Se la logica utente è terminata in seguito ad un errore reversibile non ripristinato, le uscite di sicurezza vengono portate nello stato di sicurezza e il produttore dei tag di sicurezza consumati comanda ai consumatori di portarli in uno stato di sicurezza.

SUGGERIMENTO Quando si utilizzano gli I/O di sicurezza per applicazioni standard, gli I/O di sicurezza saranno impostati sullo stato di sicurezza se la logica utente viene terminata in seguito ad un errore reversibile non ripristinato.

Se un errore di sicurezza reversibile viene annullato nel gestore degli errori nell'ambito del controllore, continua solo l'esecuzione dei task standard. Se l'errore non viene annullato, anche i task standard vengono chiusi.

ATTENZIONE: Annullare un errore di sicurezza non significa cancellarlo. Se si annulla un errore di sicurezza, è responsabilità dell'utente dimostrare che così facendo si mantiene il livello SIL 3.

Note:

Istruzioni di sicurezza

Per informazioni aggiornate, consultare i certificati di sicurezza sul sito http://www.rockwellautomation.com/products/certification/safety/.

La Tabella 9 e la Tabella 10 elencano le istruzioni per le applicazioni di sicurezza certificate per l'uso in applicazioni SIL 3.

Tabella 9 – Istruzioni generali per le applicazioni di sicurezza

Mnemonico	Nome	Scopo	Certificazione
CROUT	Configurable Redundant Output	Controlla e monitora le uscite ridondanti.	• BG • TÜV
DCA	Dual Channel Input – Analog (interi)	Monitora due valori analogici per la deviazione e la tolleranza del campo.	TÜV
DCAF	Dual Channel Input – Analog (virgola mobile)		
DCS	Dual Channel Input – Stop	Monitora i dispositivi di sicurezza a doppio ingresso il cui obiettivo principale è quello di fornire una funzione di arresto, ad esempio un pulsante di emergenza, una barriera fotoelettrica o un interruttore di interblocco porte.	• BG • TÜV
DCST	Dual Channel Input – Stop With Test	Monitora i dispositivi di sicurezza a doppio ingresso il cui obiettivo principale è quello di fornire una funzione di arresto, ad esempio un pulsante di emergenza, una barriera fotoelettrica o un interruttore di interblocco porte. Inoltre può avviare un collaudo funzionale del dispositivo di arresto.	• BG • TÜV
DCSTL	Dual Channel Input – Stop With Test and Lock	Monitora i dispositivi di sicurezza a doppio ingresso il cui obiettivo principale è quello di fornire una funzione di arresto, ad esempio un pulsante di emergenza, una barriera fotoelettrica o un interruttore di interblocco porte. Inoltre può avviare un collaudo funzionale del dispositivo di arresto. Può monitorare un segnale di feedback proveniente da un dispositivo di sicurezza e generare una richiesta di blocco destinata ad un dispositivo di sicurezza.	• BG • TÜV
DCSTM	Dual Channel Input – Stop With Test and Mute	Monitora i dispositivi di sicurezza a doppio ingresso il cui obiettivo principale è quello di fornire una funzione di arresto, ad esempio un pulsante di emergenza, una barriera fotoelettrica o un interruttore di interblocco porte. Può inoltre avviare un collaudo funzionale del dispositivo di arresto ed il muting del dispositivo di sicurezza.	TÜV
DCM	Dual Channel Input – Monitor	Monitora i dispositivi di sicurezza a doppio ingresso.	• BG • TÜV
DCSRT	Dual Channel Input – Start	Mette in tensione i dispositivi di sicurezza a doppio ingresso la cui funzione principale è quella di avviare una macchina in sicurezza, ad esempio un interruttore a fune.	• BG • TÜV
SMAT	Safety Mat	Indica se la pedana di sicurezza è occupata.	TÜV
THRSe	Two-Hand Run Station – Enhanced	Monitora due diversi ingressi di sicurezza, uno per il pulsante destro ed uno per il pulsante sinistro, per controllare un'unica uscita. Consente di configurare il tempo di discrepanza da canale a canale ed inoltre di bypassare un comando a due mani.	• BG • TÜV
TSAM	Two Sensor Asymmetrical Muting	Disabilita automaticamente, per un certo periodo di tempo, la funzione di protezione di una barriera fotoelettrica utilizzando due sensori di muting disposti in modo asimmetrico.	TÜV
TSSM	Two Sensor Symmetrical Muting	Disabilita automaticamente, per un certo periodo di tempo, la funzione di protezione di una barriera fotoelettrica utilizzando due sensori di muting disposti in modo simmetrico.	TÜV
FSBM	Four Sensor Bidirectional Muting	Disabilita automaticamente, per un certo periodo di tempo, la funzione di protezione di una barriera fotoelettrica utilizzando quattro sensori disposti in sequenza a monte ed a valle del campo di rilevamento della barriera fotoelettrica.	TÜV

Tabella 10 – Istruzioni per le applicazioni di sicurezza nella formatura lamiera

Mnemonico	Nome	Scopo	Certificazione
CBCM	Clutch Brake Continuous Mode	Utilizzata per applicazioni relative alle presse, quando si richiede un funzionamento continuo.	• BG • TÜV
CBIM	Clutch Brake Inch Mode	Utilizzata per applicazioni relative alle presse, quando si richiedono piccole regolazioni della slitta, ad esempio durante la configurazione della pressa.	• BG • TÜV
CBSSM	Clutch Brake Single Stoke Mode	Utilizzata per applicazioni relative a presse a ciclo singolo.	• BG • TÜV
CPM	Crankshaft Position Monitor	Utilizzata per determinare la posizione della slitta della pressa.	• BG • TÜV
CSM	Camshaft Monitor	Monitora il movimento per le operazioni di avviamento, arresto e marcia di un albero a camme.	• BG • TÜV
EPMS	Eight-position Mode Selector	Monitora otto ingressi di sicurezza per controllare una delle otto uscite corrispondenti all'ingresso attivo.	• BG • TÜV
AVC	Auxiliary Valve Control	Controlla una valvola ausiliaria utilizzata con una valvola principale.	TÜV
MVC	Main Valve Control	Controlla e monitora una valvola principale.	• BG • TÜV
MMVC	Maintenance Manual Valve Control	Utilizzata per azionare manualmente una valvola durante operazioni di manutenzione.	• BG • TÜV

Le routine del task di sicurezza possono utilizzare queste istruzioni di sicurezza in logica ladder.

Tabella 11 – Istruzioni di sicurezza in logica ladder

Tipo	Mnemonico	Nome	Scopo
Array (File)	FAL[(1)]	File Arithmetic and Logic	Esegue operazioni di copia, aritmetiche, logiche e di funzione sui dati memorizzati in una matrice
	FLL[(1)]	File Fill	Popola l'elemento di una matrice con il valore sorgente, lasciando quest'ultimo invariato
	FSC[(1)]	File Search and Compare	Confronta il valore in una matrice, elemento per elemento
	SIZE[(1)]	Size In Elements	Trova la dimensione di una matrice
Bit	XIC	Examine If Closed	Abilita le uscite quando viene impostato un bit
	XIO	Examine If Open	Abilita le uscite quando viene azzerato un bit
	OTE	Output Energize	Imposta un bit
	OTL	Output Latch	Imposta un bit (ritentivo)
	OTU	Output Unlatch	Azzera un bit (ritentivo)
	ONS	One shot	Attiva un evento in modo che si verifichi una sola volta
	OSR	One Shot Rising	Attiva un evento in modo che si verifichi una sola volta sul fronte da FALSE a TRUE (in salita) del cambiamento di stato
	OSF	One Shot Falling	Attiva un evento in modo che si verifichi una sola volta sul fronte da TRUE a FALSE (in discesa) del cambiamento di stato
Timer	TON	Timer On Delay	Ritardo di attivazione del temporizzatore
	TOF	Timer Off Delay	Ritardo di disattivazione del temporizzatore
	RTO	Retentive Timer On	Accumula il tempo
	CTU	Conteggio ad incremento	Conteggio ad incremento
	CTD	Conteggio a decremento	Conteggio a decremento
	RES	Reset	Azzera un temporizzatore o un contatore

Tabella 11 – Istruzioni di sicurezza in logica ladder

Tipo	Mnemonico	Nome	Scopo
Compare	CMP[1][2]	Compare	Esegue un confronto sulle operazioni aritmetiche specificate nell'espressione
	EQU	Equal To	Verifica se due valori sono uguali
	GEQ	Greater Than Or Equal To	Verifica se un valore è maggiore o uguale ad un secondo valore
	GRT	Greater Than	Verifica se un valore è maggiore di un secondo valore
	LEQ	Less Than Or Equal To	Verifica se un valore è inferiore a o uguale ad un secondo valore
	LES	Less Than	Verifica se un valore è inferiore ad un secondo valore
	MEQ	Masked Comparison for Equal	Filtra la sorgente confrontando i valori attraverso una maschera e verifica se sono uguali
	NEQ	Not Equal To	Verifica se un valore è diverso da un secondo valore
	LIM	Limit Test	Verifica se un valore rientra in un intervallo specificato
Move	CLR	Clear	Azzera un valore
	COP[3]	Copy	Copia un valore
	MOV	Move	Copia un valore
	MVM	Masked Move	Copia una parte specifica di un numero intero
	SWPB[1]	Swap Byte	Riordina i byte di un valore
Logical	AND	Bitwise AND	Esegue l'operazione AND bit per bit
	NOT	Bitwise NOT	Esegue l'operazione NOT bit per bit
	OR	Bitwise OR	Esegue l'operazione OR bit per bit
	XOR	Bitwise Exclusive OR	Esegue l'operazione OR esclusivo bit per bit
Program Control	JMP	Jump To Label	Salta una sezione di logica che non sempre è necessario eseguire (salta all'istruzione con l'etichetta a cui si fa riferimento)
	LBL	Label	Etichetta un'istruzione in modo tale che vi possa fare riferimento un'istruzione JMP
	JSR	Jump to Subroutine	Salta ad una routine separata
	RET	Return	Restituisce i risultati di una subroutine
	SBR	Subroutine	Inoltra i dati ad una subroutine
	TND	Temporary End	Contrassegna una fine temporanea che arresta l'esecuzione della routine
	MCR	Master Control Reset	Disabilita ogni ramo in una sezione di logica
	AFI	Always False Instruction	Disabilita un ramo
	NOP	No Operation	Inserisce un marcatore di posizione nella logica
	EVENT	Trigger Event Task	Attiva l'esecuzione di un task evento[5]
Math/ Compute	ADD	Add	Somma due valori
	CPT[1]	Compute	Esegue l'operazione aritmetica definita nell'espressione
	SUB	Subtract	Sottrae due valori
	MUL	Multiply	Moltiplica due valori
	DIV	Divide	Divide due valori
	MOD	Modulo	Determina il resto dopo avere diviso un valore per un secondo valore
	SQR	Square Root	Calcola la radice quadrata di un valore
	NEG	Negate	Determina il segno opposto di un valore
	ABS	Absolute Value	Determina il valore assoluto di un valore
I/O	GSV[4]	Get System Value	Ottiene informazioni sullo stato del controllore
	SSV[4]	Set System Value	Imposta le informazioni sullo stato del controllore

(1) Supportata solo sui controllori 1756-L7*x*S e 1756-L7*x*SXT. Per il tipo di dati REAL, è supportato un formato a virgola mobile per le routine di sicurezza sui controllori 1756-L7*x*S e 1756-L7*x*SXT.
(2) Operandi avanzati come SIN, COS e TAN non sono supportati nelle routine di sicurezza.
(3) L'operando della lunghezza deve essere una costante quando l'istruzione COP viene utilizzata in una routine di sicurezza. La lunghezza della sorgente e della destinazione devono essere uguali.
(4) Per considerazioni speciali relative all'uso delle istruzioni GSV ed SSV, fare riferimento al manuale dell'utente Controllori GuardLogix 5570, pubblicazione 1756-UM022.
(5) L'istruzione EVENT attiva una scansione del task standard.

IMPORTANTE Se si utilizza Motion Direct Commands con un servoazionamento Kinetix 5500, fare riferimento al manuale dell'utente Servoazionamenti Kinetix 5500, pubblicazione 2198-UM001, per informazioni su come utilizzare questa funzione nelle applicazioni di sicurezza.

Per ulteriori informazioni, consultare le seguenti pubblicazioni.

Tabella 12 – Altre risorse

Risorsa	Descrizione
Manuale di riferimento Set di istruzioni per l'applicazione di sicurezza GuardLogix, pubblicazione 1756-RM095	Fornisce ulteriori informazioni sulle istruzioni per applicazioni di sicurezza
Logix5000 Controllers General Instructions Reference Manual, pubblicazione 1756-RM003	Contiene informazioni dettagliate sul set di istruzioni Logix

Istruzioni Add-On di sicurezza

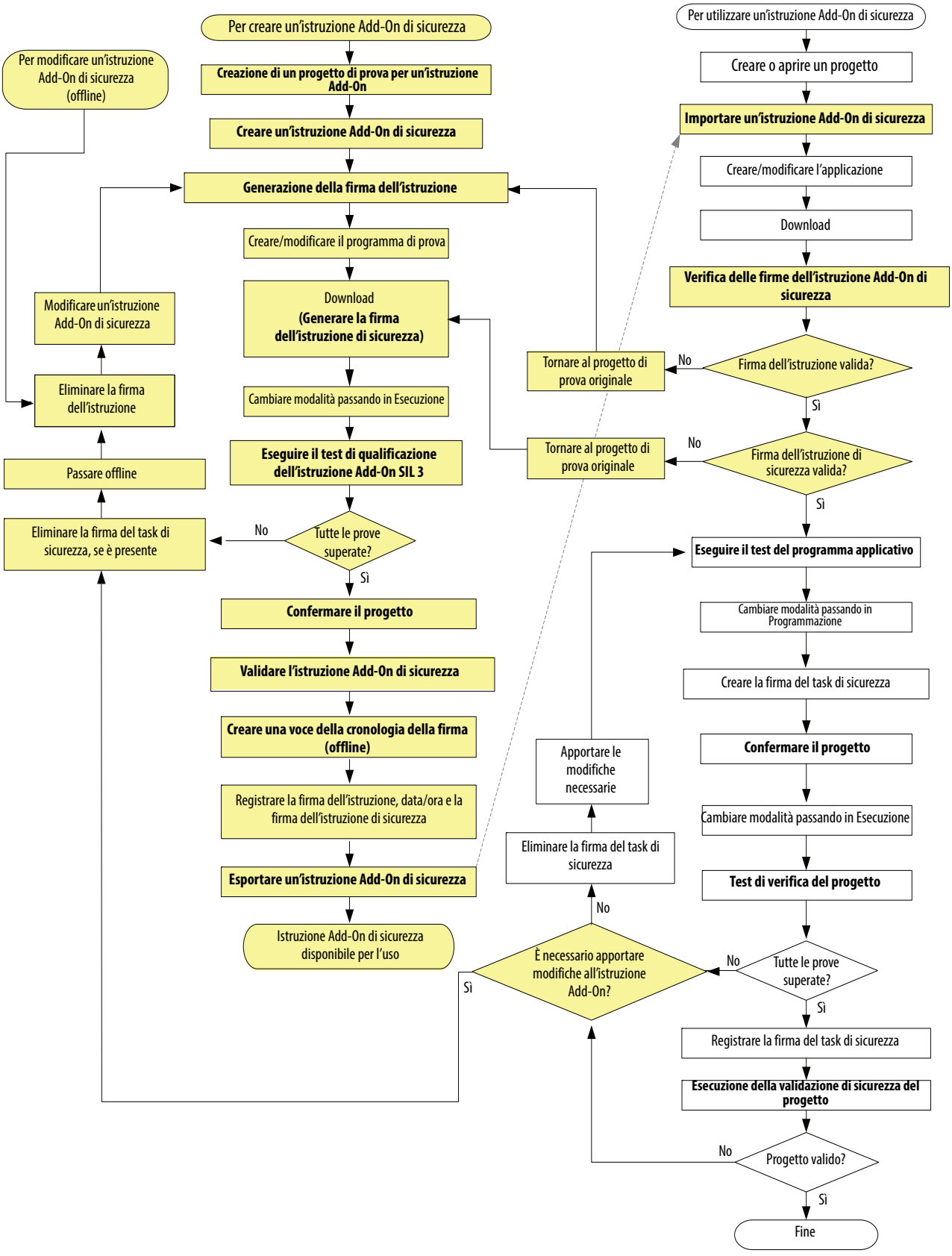
Con l'applicazione Logix Designer, è possibile creare istruzioni Add-On di sicurezza che permettono di integrare logica di sicurezza di uso comune in un'istruzione unica. In questo modo le istruzioni risultano modulari e facilmente riutilizzabili.

Le istruzioni Add-On di sicurezza utilizzano la firma dell'istruzione per le istruzioni Add-On ad alta integrità ed inoltre una firma dell'istruzione di sicurezza SIL 3, che vengono impiegate nelle funzioni inerenti alla sicurezza fino al livello SIL 3 compreso.

Creazione ed utilizzo di un'istruzione Add-On di sicurezza

Nel diagramma di flusso riportato a pagina 74 sono indicati i passi richiesti per la creazione di un'istruzione Add-On di sicurezza e l'utilizzo di tale istruzione in un programma applicativo di sicurezza SIL 3. Le voci ombreggiate sono passi esclusivi delle istruzioni Add-On. Le voci in grassetto sono spiegate nelle pagine successive al diagramma di flusso.

Figura 18 – Diagramma di flusso relativo alla creazione ed all'uso delle istruzioni Add-On di sicurezza



Creazione di un progetto di prova per un'istruzione Add-On

È necessario creare un progetto di prova univoco, specifico per la creazione dell'istruzione Add-On di sicurezza e le relative prove. Il progetto deve essere separato e dedicato per ridurre al minimo eventuali interazioni impreviste.

Seguire le regole generali relative ai progetti descritte in Creare il progetto a pagina 53.

Creazione di un'istruzione Add-On di sicurezza

Per ulteriori indicazioni relative alla creazione di istruzioni Add-On, consultare il manuale di programmazione Logix5000 Controllers Add-On Instruction, pubblicazione 1756-PM010.

Generazione della firma dell'istruzione

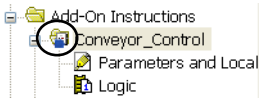
La firma dell'istruzione consente di verificare rapidamente se l'istruzione è stata modificata. Ogni istruzione Add-On può avere la propria firma. La firma dell'istruzione è richiesta quando un'istruzione Add-On viene impiegata per funzioni relative alla sicurezza e può talvolta essere obbligatoria nei settori soggetti a norme specifiche. La firma dell'istruzione deve essere utilizzata quando l'applicazione richiede un livello di integrità superiore.

La firma dell'istruzione è costituita da un numero ID e dalla registrazione cronologica, che associa i contenuti dell'istruzione Add-On ad una determinata ora e data.

Una volta generata, la firma dell'istruzione "sigilla" l'istruzione Add-On, impedendo che venga modificata fintanto che è presente la firma. Questa restrizione riguarda i commenti al ramo, le descrizioni dei tag ed eventuale altra documentazione creata relativamente all'istruzione. Quando l'istruzione è sigillata, è possibile eseguire solo le seguenti azioni:

- Copiare la firma dell'istruzione
- Creare o copiare una voce della cronologia della firma
- Creare istanze dell'istruzione Add-On
- Scaricare l'istruzione
- Rimuovere la firma dell'istruzione
- Stampare dei report

In seguito alla generazione della firma dell'istruzione, l'applicazione Logix Designer visualizza la definizione dell'istruzione con l'icona del sigillo.



IMPORTANTE	Se si intende proteggere l'istruzione Add-On con la funzione di protezione del sorgente dell'applicazione Logix Designer, è necessario abilitare tale funzione prima di generare la firma dell'istruzione.

Download e generazione della firma dell'istruzione di sicurezza

Quando si scarica per la prima volta un'istruzione Add-On di sicurezza sigillata, viene generata automaticamente una firma dell'istruzione di sicurezza SIL 3. La firma dell'istruzione di sicurezza è un numero ID che identifica le caratteristiche di esecuzione dell'istruzione Add On di sicurezza.

Test di qualificazione dell'istruzione Add-On SIL 3

I test relativi alle istruzioni Add-On di sicurezza SIL 3 devono essere eseguiti in un'applicazione separata dedicata, al fine di ridurre al minimo le influenze impreviste. È necessario attenersi ad un piano di prova ben progettato e testare l'istruzione Add-On di sicurezza sull'unità provando tutti i percorsi di esecuzione possibili tramite la logica, ivi compresi i campi di impostazione validi e non validi di tutti i parametri di ingresso.

Durante lo sviluppo di tutte le istruzioni Add-On di sicurezza occorre rispettare la normativa IEC 61508, "Requisiti per le prove relative ai moduli software", in cui sono specificati i requisiti dettagliati per le prove relative alle unità.

Conferma del progetto

Si deve stampare o visualizzare il progetto e confrontare manualmente le configurazioni caricate degli I/O di sicurezza e del controllore, i dati di sicurezza, le definizioni dell'istruzione Add-On di sicurezza e la logica del programma del task di sicurezza per assicurarsi che nel programma applicativo di sicurezza siano stati scaricati, testati e mantenuti i componenti di sicurezza corretti.

In Confermare il progetto a pagina 55 è riportata la descrizione di un metodo di conferma di un progetto.

Validazione di sicurezza delle istruzioni Add-On

È possibile che sia necessaria una verifica indipendente dell'istruzione Add-On di sicurezza eseguita da terze parti, prima che l'istruzione possa essere approvata per l'uso. La normativa IEC 61508 SIL 3 richiede una validazione indipendente eseguita da terze parti.

Creazione di una voce nella cronologia della firma

La cronologia della firma è un documento utile per consultazioni future. Ciascuna voce della cronologia della firma comprende: la firma dell'istruzione, il nome dell'utente, il valore della registrazione cronologica di ora e data ed una descrizione definita dall'utente. È possibile memorizzare fino a sei voci della cronologia. Per creare una voce nella cronologia della firma occorre essere offline.

SUGGERIMENTO Il report Signature Listing dell'applicazione Logix Designer consente di stampare la firma dell'istruzione, la registrazione cronologica di ora e data e la firma dell'istruzione di sicurezza. Per stampare il report, fare clic con il pulsante destro del mouse sull'istruzione Add-On nell'organizer del controllore e selezionare Print>Signature Listing.

Esportazione ed importazione dell'istruzione Add-On di sicurezza

Durante l'esportazione di un'istruzione Add-On di sicurezza, scegliere l'opzione che consente di includere tutte le istruzioni Add-On referenziate ed i tipi definiti dall'utente nello stesso file di esportazione. Includendo le istruzioni Add-On referenziate, è più facile conservare le firme.

Durante l'importazione delle istruzioni Add-On, tenere presente le seguenti regole generali:

- Non è possibile importare un'istruzione Add-On di sicurezza in un progetto standard.
- Non è possibile importare un'istruzione Add-On di sicurezza in un progetto di sicurezza che si trova in blocco di sicurezza o è provvisto di una firma del task di sicurezza.
- Non è possibile importare un'istruzione Add-On di sicurezza mentre si è online.
- Se si importa un'istruzione Add-On con firma dell'istruzione in un progetto in cui non sono disponibili istruzioni Add-On referenziate o tipi definiti dall'utente, potrebbe essere necessario rimuovere la firma.

Verifica delle firme dell'istruzione Add-On di sicurezza

Dopo aver eseguito il download del progetto applicativo contenente l'istruzione Add-On di sicurezza importata, è necessario confrontare il valore della firma dell'istruzione, la data, la registrazione cronologica di ora e data ed i valori della firma dell'istruzione di sicurezza con i valori originali registrati prima dell'esportazione dell'istruzione Add-On di sicurezza. Se corrispondono, l'istruzione Add-On di sicurezza è valida ed è possibile proseguire con la validazione dell'applicazione.

Esecuzione del test del programma applicativo

Questo passo include qualsiasi combinazione di modalità Esecuzione e Programmazione, modifiche al programma online o offline, upload e download e test informali necessari perché un'applicazione funzioni correttamente.

Test di verifica del progetto

Eseguire un test funzionale dell'applicazione, comprendente il sistema di sicurezza.

Per ulteriori informazioni sui requisiti, vedere Test di verifica del progetto a pagina 54.

Esecuzione della validazione di sicurezza del progetto

È possibile che sia necessaria una verifica indipendente di terza parte del sistema di sicurezza, prima che il sistema venga approvato per il funzionamento. La normativa IEC 61508 SIL 3 richiede una validazione indipendente eseguita da terze parti.

Altre risorse

Per ulteriori informazioni sull'uso delle istruzioni Add-On, consultare le seguenti pubblicazioni:

Risorsa	Descrizione
Manuale di programmazione Istruzioni add-on per controllori Logix5000, pubblicazione 1756-PM010	Fornisce informazioni su come pianificare, creare, utilizzare, importare ed esportare istruzioni Add-On nelle applicazioni RSLogix 5000
Manuale di programmazione Importazione/esportazione di componenti del progetto, pubblicazione 1756-PM019	Contiene informazioni dettagliate su come importare ed esportare componenti del progetto

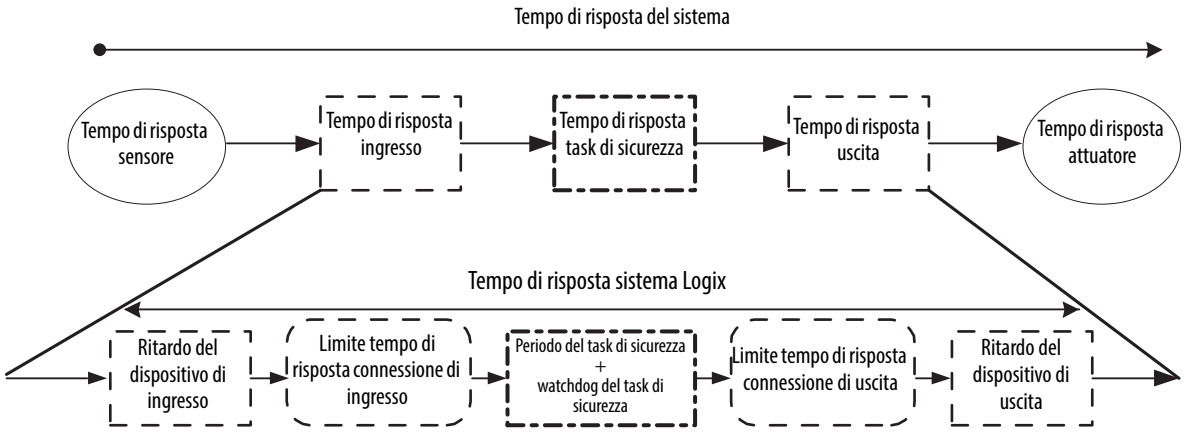
Tempi di risposta

Tempo di risposta del sistema

Per determinare il tempo di risposta del sistema di qualsiasi catena di controllo, è necessario sommare i tempi di risposta di tutti i componenti della catena di sicurezza.

Tempo di risposta del sistema = tempo di risposta sensore + tempo di risposta del sistema Logix + tempo di risposta attuatore

Figura 19 – Tempo di risposta del sistema

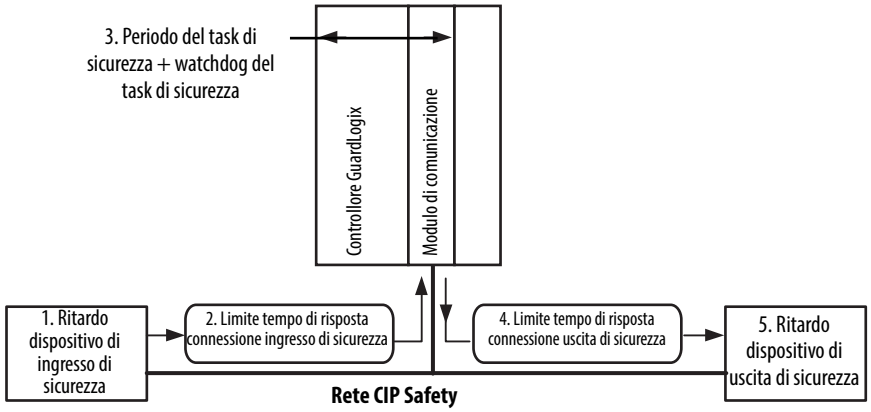


Tempo di risposta del sistema Logix

Le sezioni che seguono forniscono informazioni sui metodi di calcolo del tempo di risposta del sistema Logix per una semplice catena ingresso-logica-uscita e per un'applicazione più complessa che utilizza tag di sicurezza prodotti/consumati nella catena logica.

Semplice catena ingresso-logica-uscita

Figura 20 – Tempo di risposta massimo del sistema Logix per una catena semplice di ingresso-logica-uscita



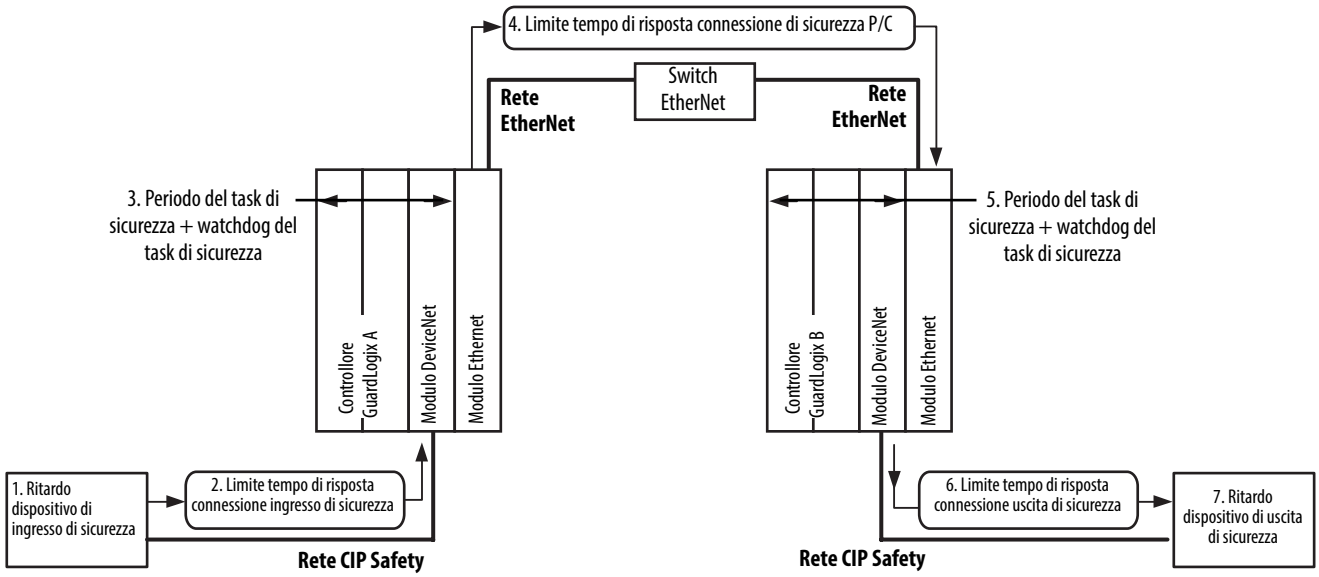
Il tempo di risposta del sistema Logix per qualunque catena semplice di ingresso-logica-uscita dipende dai cinque componenti che seguono:

1. Tempo di risposta del dispositivo di ingresso di sicurezza (+ tempo di ritardo di ingresso, se applicabile)
2. Limite tempo di risposta connessione ingresso di sicurezza (da leggere nella finestra di dialogo Module Properties dell'applicazione Logix Designer, questo valore è un multiplo dell'RPI della connessione del dispositivo di ingresso di sicurezza).
3. Periodo del task di sicurezza + tempo di watchdog del task di sicurezza
4. Limite tempo di risposta connessione uscita di sicurezza (da leggere nella finestra di dialogo Module Properties dell'applicazione Logix Designer, questo valore è un multiplo del periodo del task di sicurezza).
5. Tempo di risposta del dispositivo di uscita di sicurezza

Per determinare il tempo di risposta del proprio loop di controllo, è disponibile un foglio di calcolo elettronico Microsoft Excel nella cartella Tools del DVD dell'ambiente Studio 5000.

Catena logica che utilizza tag di sicurezza prodotti/consumati

Figura 21 – Tempo di risposta del sistema Logix per la catena ingresso-logica controllore A-logica controllore B-uscita



Il tempo di risposta del sistema Logix per la catena ingresso-logica controllore A-logica controllore B-uscita dipende dai sette componenti che seguono:

1. Tempo di risposta del dispositivo di ingresso di sicurezza (+ tempo di ritardo di ingresso, se applicabile)
2. Limite tempo di risposta connessione ingresso di sicurezza
3. Periodo del task di sicurezza + tempo di watchdog del task di sicurezza per il controllore A
4. Limite tempo di risposta connessione di sicurezza P/C (prodotta/consumata)
5. Periodo del task di sicurezza + tempo di watchdog del task di sicurezza per il controllore B
6. Limite tempo di risposta connessione uscita di sicurezza
7. Tempo di risposta del dispositivo di uscita di sicurezza

Per determinare il tempo di risposta del proprio loop di controllo, è disponibile un foglio di calcolo elettronico Microsoft Excel nella cartella Tools del DVD dell'ambiente Studio 5000.

Elementi che influiscono sui componenti del tempo di risposta Logix

I componenti del tempo di risposta Logix descritti nelle sezioni precedenti possono essere influenzati da diversi fattori.

Tabella 13 – Elementi che influiscono sul tempo di risposta del sistema Logix

Questi componenti del tempo di risposta	Sono influenzati dai seguenti elementi
Ritardo del dispositivo di ingresso	Tempo di risposta del dispositivo di ingresso
	Impostazioni di ritardo On-Off e Off-On di ogni canale di ingresso, se applicabile
Limite tempo di risposta connessione ingresso di sicurezza	Impostazioni dispositivo di ingresso per: • Intervallo di pacchetto richiesto (RPI) • Moltiplicatore di timeout • Moltiplicatore di ritardo
	Il traffico di comunicazione di rete
	L'ambiente EMC del sistema
Periodo del task di sicurezza e watchdog del task di sicurezza	Impostazione del periodo del task di sicurezza
	Impostazione del watchdog del task di sicurezza
	Il numero ed il tempo di esecuzione delle istruzioni del task di sicurezza
	Qualsiasi task di priorità superiore che può ostacolare l'esecuzione del task di sicurezza
Limite tempo di risposta connessione di sicurezza P/C (prodotta/consumata)	Impostazioni dei tag consumati per: • RPI • Moltiplicatore di timeout • Moltiplicatore di ritardo
	Il traffico di comunicazione di rete
	L'ambiente EMC del sistema
Limite tempo di risposta connessione di uscita	Impostazione del periodo del task di sicurezza
	Impostazioni del dispositivo di uscita per: • Moltiplicatore di timeout • Moltiplicatore di ritardo
	Il traffico di comunicazione di rete
	L'ambiente EMC del sistema
Ritardo modulo di uscita	Tempo di risposta modulo di uscita

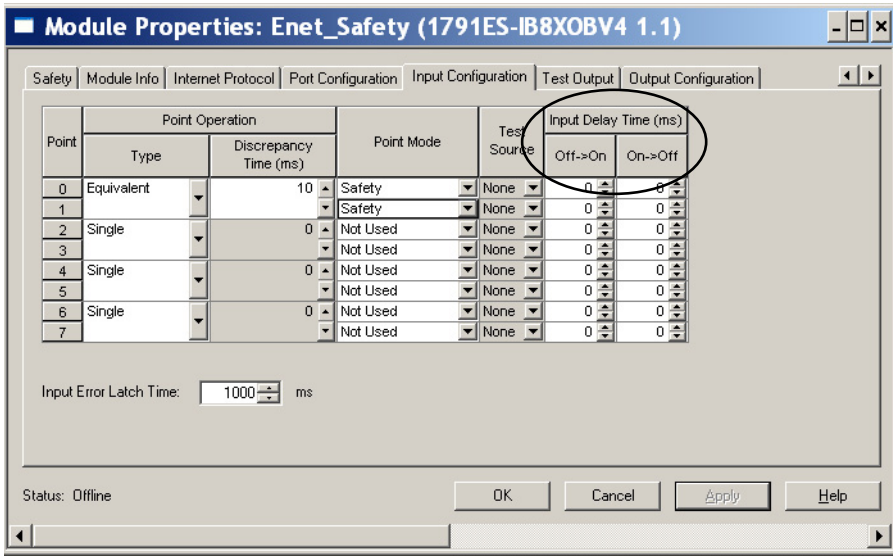
Le sezioni che seguono spiegano come accedere ai dati o alle impostazioni di una serie di questi fattori.

Accesso alle impostazioni di ritardo del modulo di ingresso Guard I/O

Per configurare il tempo di ritardo del modulo di ingresso nell'applicazione Logix Designer, procedere come segue.

1. Nell'albero di configurazione, fare clic con il pulsante destro del mouse sul modulo Guard I/O e selezionare Properties.
2. Fare clic sulla scheda Input Configuration.

3. Modificare il tempo di ritardo di ingresso come desiderato per l'applicazione.



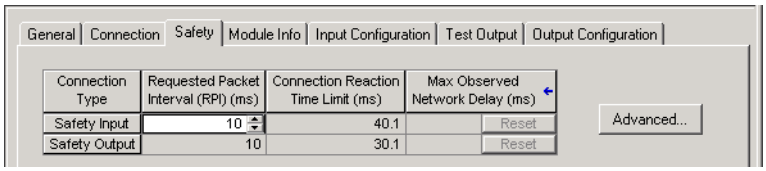
Accesso al limite del tempo di risposta delle connessioni di sicurezza di ingresso ed uscita

Il limite del tempo di risposta delle connessioni è definito da tre valori:

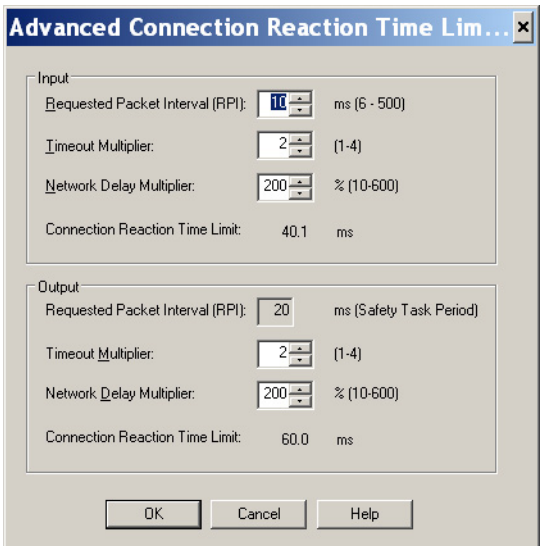
Valore	Descrizione
Intervallo di pacchetto richiesto (RPI)	Frequenza alla quale i pacchetti di ingresso e di uscita vengono trasmessi sul cavo (rete).
Moltiplicatore di timeout	Il moltiplicatore di timeout è essenzialmente il numero di tentativi prima del timeout.
Moltiplicatore ritardo rete	Il moltiplicatore di ritardo rete considera qualunque ritardo conosciuto sul cavo. Quando si verificano questi ritardi, i timeout possono essere evitati tramite questo parametro.

Modificando questi valori, è possibile cambiare il limite del tempo di risposta delle connessione. Per visualizzare o configurare queste impostazioni, procedere come segue.

1. Nell'albero di configurazione, fare clic con il pulsante destro del mouse sul dispositivo I/O di sicurezza e selezionare Properties.
2. Fare clic sulla scheda Safety.



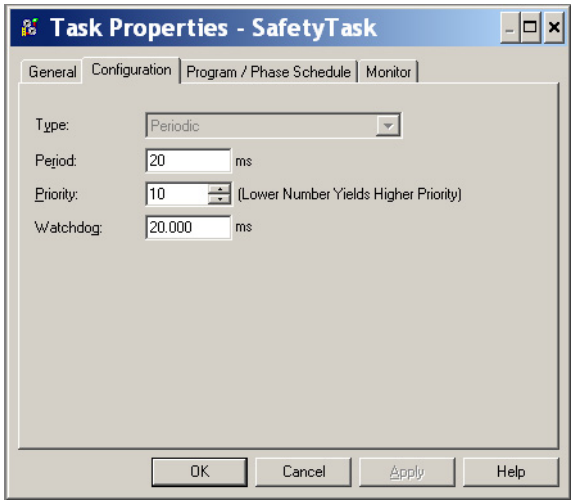
3. Fare clic su Advanced per aprire la finestra di dialogo Advanced Connection Reaction Time Limit.



Configurazione del periodo del task di sicurezza e del watchdog

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 del progetto Logix Designer.

Per accedere alle impostazioni del periodo del task di sicurezza e del tempo di watchdog, fare clic con il pulsante destro del mouse su Safety Task e selezionare Properties.

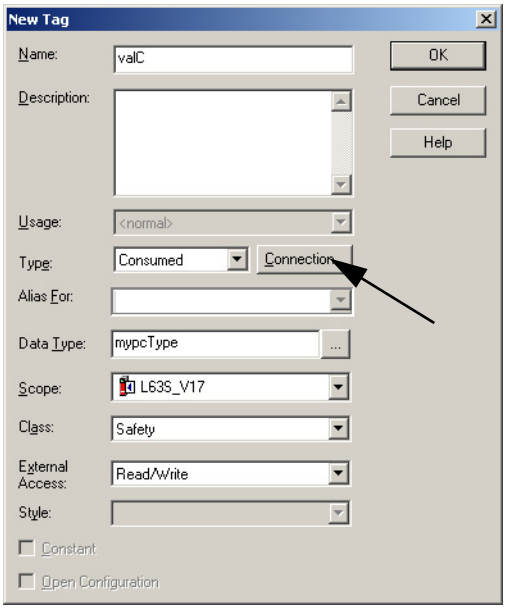


La priorità del task di sicurezza non è un problema di sicurezza, dato che il watchdog del task di sicurezza controlla se il task viene interrotto da task di priorità superiore.

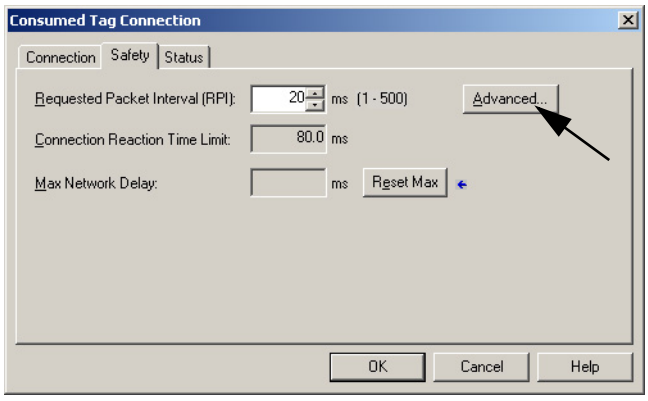
Accesso ai dati dei tag prodotti/consumati

Per visualizzare o configurare i dati di connessione dei tag di sicurezza, procedere come segue.

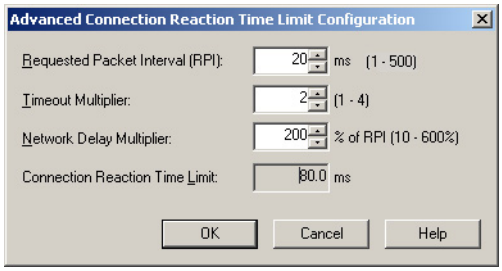
1. Nell'albero di configurazione, fare clic con il pulsante destro del mouse su Controller Tags e selezionare Edit tags.
2. In Tag Editor, fare clic con il pulsante destro del mouse sul nome del tag e selezionare Edit Properties.
3. Fare clic su Connection.



4. Fare clic sulla scheda Safety.



5. Fare clic su Advanced per visualizzare o modificare le impostazioni attuali.



Per ulteriori informazioni, consultare il manuale dell'utente controllori GuardLogix 5570, pubblicazione 1756-UM022.

Checklist per le applicazioni di sicurezza GuardLogix

Le checklist presenti in questa appendice sono necessarie per la progettazione, la programmazione e l'avvio di un'applicazione GuardLogix certificata SIL 3. Possono essere utilizzate come guide di pianificazione e durante il test di verifica del progetto. Se utilizzate come guide di pianificazione, le checklist possono essere salvate come registrazione del piano.

Le checklist presenti nelle seguenti pagine forniscono un esempio di considerazioni sulla sicurezza e non intendono essere un elenco completo di voci da verificare. Ciascuna applicazione di sicurezza specifica potrebbe avere ulteriori requisiti di sicurezza, per i quali è stato previsto uno spazio nelle checklist.

SUGGERIMENTO Eseguire delle copie delle checklist e conservarle per un eventuale utilizzo futuro.

Checklist del sistema di controllo GuardLogix

Checklist del sistema GuardLogix				
Azienda				
Sito				
Definizione della funzione di sicurezza				
Numero	**Requisiti di sistema**	**Realizzato**		**Commento**
		Sì	**No**	
1	Si stanno utilizzando esclusivamente i componenti elencati in Componenti GuardLogix certificati SIL 3 a pagina 16 e sul sito http://www.rockwellautomation.com/products/certification/safety/ con le corrispondenti versioni firmware?	☐	☐	
2	Si è calcolato il tempo di risposta di sicurezza del sistema per ogni catena di sicurezza?	☐	☐	
3	Il tempo di risposta del sistema include sia il tempo di watchdog del programma del task di sicurezza definito dall'utente (watchdog software) che la frequenza/il periodo del task di sicurezza?	☐	☐	
4	Il tempo di risposta del sistema è relazionato correttamente con il tempo di tolleranza del processo?	☐	☐	
5	I valori di probabilità (PFD/PFH) sono stati calcolati in base alla configurazione del sistema?	☐	☐	
6	Sono stati eseguiti tutti gli opportuni test di verifica del progetto?	☐	☐	
7	Si è determinato il modo in cui il proprio sistema gestirà gli errori?	☐	☐	
8	Ogni rete nel sistema di sicurezza è dotata di un SNN univoco?	☐	☐	
9	Ogni dispositivo di sicurezza CIP è configurato con l'SNN corretto?	☐	☐	
10	È stata generata una firma del task di sicurezza?	☐	☐	
11	La firma del task di sicurezza è stata caricata e registrata per un confronto futuro?	☐	☐	
12	Dopo un download, si è verificato che la firma del task di sicurezza presente nel controllore corrisponda alla firma del task di sicurezza registrata?	☐	☐	
13	Si dispone di un meccanismo alternativo per preservare l'integrità della sicurezza del sistema mentre si eseguono modifiche online?	☐	☐	
14	Sono state considerate le checklist per l'utilizzo degli ingressi e delle uscite SIL elencati nelle pagine 89 e 90?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Checklist per gli ingressi di sicurezza

Per la programmazione o l'avvio, può essere compilata una checklist individuale per ogni canale di ingresso SIL di un sistema. Questo è l'unico modo per essere certi che i requisiti siano implementati in modo completo e chiaro. Questa checklist può essere utilizzata anche come documentazione relativa al collegamento del cablaggio esterno al programma applicativo.

Checklist degli ingressi del sistema GuardLogix				
Azienda				
Sito				
Definizione della funzione di sicurezza				
Canali di ingresso SIL				
Numero	**Requisiti dei dispositivi di ingresso**	**Realizzato**		**Commento**
		Sì	**No**	
1	Sono state seguite le istruzioni per l'installazione e le precauzioni in modo da soddisfare gli standard di sicurezza applicabili?	☐	☐	
2	Sono stati eseguiti test di verifica del progetto sul sistema e sui dispositivi?	☐	☐	
3	Nella logica dell'applicazione vengono eseguite in sequenza funzioni di controllo, diagnostica ed allarme?	☐	☐	
4	È stata caricata e confrontata la configurazione di ogni dispositivo con la configurazione inviata dallo strumento di configurazione?	☐	☐	
5	I dispositivi sono cablati in conformità con PLe/Cat. 4 secondo la normativa ISO 13849-1?(1)	☐	☐	
6	Si è verificato che le specifiche tecniche elettriche del sensore e quelle dell'ingresso siano compatibili?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) Per informazioni sul cablaggio del dispositivo I/O CIP Safety in uso, fare riferimento alla documentazione del prodotto per il dispositivo specifico.

Checklist per le uscite di sicurezza

Per la programmazione o l'avvio, deve essere compilata una checklist individuale dei requisiti per ogni canale di ingresso SIL di un sistema. Questo è l'unico modo per essere certi che i requisiti siano implementati in modo completo e chiaro. Questa checklist può essere utilizzata anche come documentazione relativa al collegamento del cablaggio esterno al programma applicativo.

Checklist delle uscite del sistema GuardLogix				
Azienda				
Sito				
Definizione della funzione di sicurezza				
Canali di uscita SIL				
Numero	**Requisiti dei dispositivi di uscita**	**Realizzato**		**Commento**
		Sì	**No**	
1	Sono state seguite le istruzioni per l'installazione e le precauzioni in modo da soddisfare gli standard di sicurezza applicabili?	☐	☐	
2	Sono stati eseguiti i test di verifica del progetto sui dispositivi?	☐	☐	
3	È stata caricata e confrontata la configurazione di ogni dispositivo con la configurazione inviata dallo strumento di configurazione?	☐	☐	
4	Si è verificato che le uscite per i test non siano utilizzate come uscite di sicurezza?	☐	☐	
5	I dispositivi sono cablati in conformità con PLe/Cat. 4 secondo la normativa ISO 13849-1?(1)	☐	☐	
6	Si è verificato che le specifiche tecniche elettriche dell'uscita e dell'attuatore siano compatibili?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) Per informazioni sul cablaggio del dispositivo I/O di sicurezza in uso, fare riferimento alla documentazione del prodotto per il dispositivo specifico.

Checklist per sviluppare un programma di un'applicazione di sicurezza

Utilizzare la seguente checklist per contribuire a mantenere la sicurezza mentre si crea o si modifica un programma di un'applicazione di sicurezza.

Checklist per lo sviluppo del programma applicativo GuardLogix				
Azienda				
Sito				
Definizione progetto				
Numero	**Requisiti del programma applicativo**	**Realizzato**		**Commento**
		Sì	**No**	
1	Si sta utilizzando la versione 21 o successiva dell'applicazione Logix Designer, lo strumento di programmazione del sistema GuardLogix?	☐	☐	
2	Sono state seguite le linee guida di programmazione del Capitolo 6 durante lo sviluppo del programma applicativo di sicurezza?	☐	☐	
3	Il programma applicativo di sicurezza contiene soltanto logica ladder?	☐	☐	
4	Il programma applicativo di sicurezza contiene soltanto le istruzioni elencate nell'Appendice A in quanto idonee per la programmazione delle applicazioni di sicurezza?	☐	☐	
5	Il programma applicativo di sicurezza distingue chiaramente tra tag di sicurezza e tag standard?	☐	☐	
6	Per le routine di sicurezza vengono utilizzati soltanto i tag di sicurezza?	☐	☐	
7	Si è verificato che le routine di sicurezza non tentino di leggere dai tag standard o scrivere su di essi?	☐	☐	
8	Si è verificato che nessun tag di sicurezza sia stato definito come alias di tag standard e viceversa?	☐	☐	
9	Ogni tag di uscita di sicurezza è stato configurato correttamente e collegato ad un canale di uscita fisico?	☐	☐	
10	Si è verificato che tutti i tag mappati siano stati condizionati nella logica dell'applicazione di sicurezza?	☐	☐	
11	Sono stati definiti i parametri di processo che sono monitorati dalle routine di errore?	☐	☐	
12	Le istruzioni Add-On di sicurezza sono state sigillate con una firma dell'istruzione e la firma dell'istruzione di sicurezza è stata registrata?	☐	☐	
13	Il programma è stato controllato da un revisore di sicurezza indipendente (se necessario)?	☐	☐	
14	La revisione è stata documentata e firmata?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Note:

Dati di sicurezza dei sistemi GuardLogix

I seguenti esempi mostrano i valori della probabilità di guasto su domanda (PFD) e probabilità di guasto all'ora (PFH) per i sistemi GuardLogix 1oo2 SIL 3 che utilizzano moduli Guard I/O.

Il ciclo di vita previsto per i controllori GuardLogix ed i moduli Guard I/O è di 20 anni.

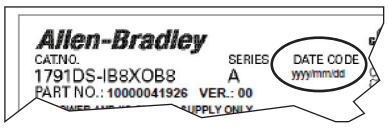
Valori di PFD

Tabella 14 – PFD calcolata per intervallo tra prove funzionali

Num. di Cat.	Descrizione	PFD calcolata			
		2 anni (17.520 ore)	5 anni (43.800 ore)	10 anni (87.600 ore)	20 anni (175.200 ore)
1756-L7xS e 1756-L7SP	Controllore GuardLogix	5,7E-06	1,5E-05	3,5E-05	8,9E-05
1756-L73SXT e 1756-L7SPXT	Controllore GuardLogix XT	5,7E-06	1,5E-05	3,5E-05	8,9E-05
1791DS-IB12	Modulo di ingresso a 12 punti CIP Safety	4,73E-07	1,18E-06	2,35E-06	4,71E-06(2)
1791DS-IB16	Modulo di ingresso a 16 punti CIP Safety	4,11E-06	1,03E-05	2,06E-05	4,11E-05
1791DS-IB8XOB8	Modulo di ingresso/uscita a 8 punti CIP Safety	4,73E-07	1,18E-06	2,35E-06	4,71E-06(2)
1791DS-IB4XOW4	Modulo di ingresso/uscita a relè a 4 punti CIP Safety	2,21E-05	7,05E-05	1,92E-04	5,88E-04(2)
1791DS-IB8XOBV4	Modulo di ingresso a 8 punti e 4 uscite bipolari CIP Safety	4,16E-06	1,04E-05	2,08E-05	4,16E-05
1732DS-IB8XOBV4					
1732DS-IB8	Modulo di ingresso a 8 punti CIP Safety	4,11E-06	1,03E-05	2,06E-05	4,11E-05
1791ES-IB16	Modulo di ingresso a 16 punti CIP Safety	4,13E-06	1,03E-05	2,06E-05	—
1791ES-IB8XOBV4	Modulo di ingresso a 8 punti e 4 uscite bipolari CIP Safety	4,17E-06	1,04E-05	2,09E-05	—
1734-IB8S, serie A	Modulo di ingresso a 8 punti CIP Safety	4,23E-06	1,06E-05	2,11E-05	4.23-05
1734-IB8S, serie B(1)	Modulo di ingresso a 8 punti CIP Safety	4,36E-06	1,09E-05	2,18E-05	4,36E-05
1734-OB8S, serie A	Modulo di uscita a 8 punti CIP Safety	4,27E-06	1,07E-05	2,13E-05	4,27E-05
1734-OB8S, serie B	Modulo di uscita a 8 punti CIP Safety	4,32E-06	1,08E-05	2,16E-05	4,32E-05
1734-IE4S	Modulo di ingresso analogico a 4 punti CIP Safety, funzionamento monocanale	4,7E-07	1,2E-06	2,4E-06	4,8E-06
1734-IE4S	Modulo di ingresso analogico a 4 punti CIP Safety, funzionamento a doppio canale	3,2E-07	8,1E-07	1,6E-06	3,3E-06

(1) Questi dati si riferiscono al funzionamento monocanale ed a doppio canale.

(2) I dati relativi alla probabilità PFD su 20 anni valgono soltanto per i prodotti con codice data di produzione 2009/01/01 (1° gennaio 2009) o successivo. Per informazioni sul codice data, fare riferimento all'etichetta del prodotto.



Valori di PFH

I dati sotto riportati si riferiscono ad un intervallo tra test funzionali minore o pari a 20 anni.

Tabella 15 – Calcolo PFH

Num. di Cat.	Descrizione	PFH (1/ora)
1756-L7xS e 1756-L7SP	Controllore GuardLogix	1,2E-09
1756-L7xSXT e 1756-L7SPXT	Controllore GuardLogix-XT	1,2E-09
1791DS-IB12	Modulo di ingresso a 12 punti CIP Safety	5,77E-11(1)
1791DS-IB16	Modulo di ingresso a 16 punti CIP Safety	4,96E-10
1791DS-IB8XOB8	Modulo di ingresso/uscita a 8 punti CIP Safety	5,77E-11(1)
1791DS-IB4XOW4	Modulo di ingresso/uscita a relè a 4 punti CIP Safety	9,03E-09(1)
1791DS-IB8XOBV4	Modulo di ingresso a 8 punti e 4 uscite bipolari CIP Safety	5,02E-10
1732DS-IB8XOBV4		
1732DS-IB8	Modulo di ingresso a 8 punti CIP Safety	4,96E-10
1791ES-IB16	Modulo di ingresso a 16 punti CIP Safety	4,98E-10
1791ES-IB8XOBV4	Modulo di ingresso a 8 punti e 4 uscite bipolari CIP Safety	5,04E-10
1734-IB8S, serie A	Modulo di ingresso a 8 punti CIP Safety	5,10E-10
1734-IB8S, serie B	Modulo di ingresso a 8 punti CIP Safety	5,27E-10
1734-OB8S, serie A	Modulo di uscita a 8 punti CIP Safety	5,14E-10
1734-OB8S, serie B	Modulo di uscita a 8 punti CIP Safety	5,20E-10
1734-IE4S	Modulo di ingresso analogico a 4 punti CIP Safety, funzionamento monocanale Modulo di ingresso analogico a 4 punti CIP Safety, funzionamento a doppio canale	5,6E-11 3,9E-11

(1) I dati relativi alla probabilità PFH valgono soltanto per i prodotti con codice di data di produzione 2009/01/01 (1° gennaio 2009) o successivo. Per informazioni sul codice data, fare riferimento all'etichetta del prodotto.

Software RSLogix 5000, versione 14 e successiva, istruzioni per applicazioni di sicurezza

Sistema di diseccitazione all'intervento

Quando si utilizzano istruzioni per applicazioni di sicurezza tramite il software RSLogix 5000, versione 14, al rilevamento di un errore tutti gli ingressi e le uscite vengono impostati a zero. Conseguentemente, gli ingressi monitorati da una tra le istruzioni per ingressi diversificati (Diverse Inputs o Two-hand Run Station) dovrebbero essere normalmente chiusi, condizionati da una logica simile a quella del ramo 4 di Logica ladder: esempio 2 e Logica ladder: esempio 3 alle pagine 98 e 99. La logica esatta richiesta dipende sia dall'applicazione che dal dispositivo di ingresso. Tuttavia, la logica deve creare uno stato di sicurezza 1 per l'ingresso normalmente chiuso delle istruzioni degli ingressi diversificati.

Utilizzare i dati sullo stato della connessione per inizializzare un errore tramite il programma

I diagrammi che seguono forniscono esempi della logica applicativa necessaria per il latch ed il reset degli errori I/O. Gli esempi mostrano la logica necessaria sia per i moduli di solo ingresso sia per i moduli combinati di ingresso ed uscita. Tali esempi usano la funzione Combined Status dei moduli I/O, che indica lo stato di tutti i canali di ingresso in un'unica variabile booleana. Una seconda variabile booleana rappresenta lo stato di tutti i canali di uscita. Questo approccio riduce la quantità di logica di condizionamento degli I/O richiesta e forza la logica stessa a disattivare tutti i canali di ingresso ed uscita sul modulo interessato.

Utilizzare il Diagramma di flusso di latch e reset degli errori di ingresso a pagina 96 per determinare quali rami della logica sono necessari nelle diverse situazioni applicative. Logica ladder: esempio 1 mostra la logica che sovrascrive le variabili correnti dei tag di ingresso in presenza di una condizione di errore.
Se per la ricerca guasti è richiesto lo stato effettivo dell'ingresso mentre il guasto all'ingresso è in latch, utilizzare la logica riportata in Logica ladder: esempio 2. Questa logica utilizza tag interni che rappresentano gli ingressi da utilizzare nella logica dell'applicazione. Quando il guasto all'ingresso è in latch, i tag interni sono impostati sullo stato di sicurezza. Quando il guasto dell'ingresso non è in latch, i valori di ingresso correnti vengono copiati nei tag interni.

Utilizzare il Diagramma di flusso per latch e reset degli errori di uscita per determinare quali rami della logica dell'applicazione in Logica ladder: esempio 3 a pagina 99 sono richiesti.

Figura 22 – Diagramma di flusso di latch e reset degli errori di ingresso

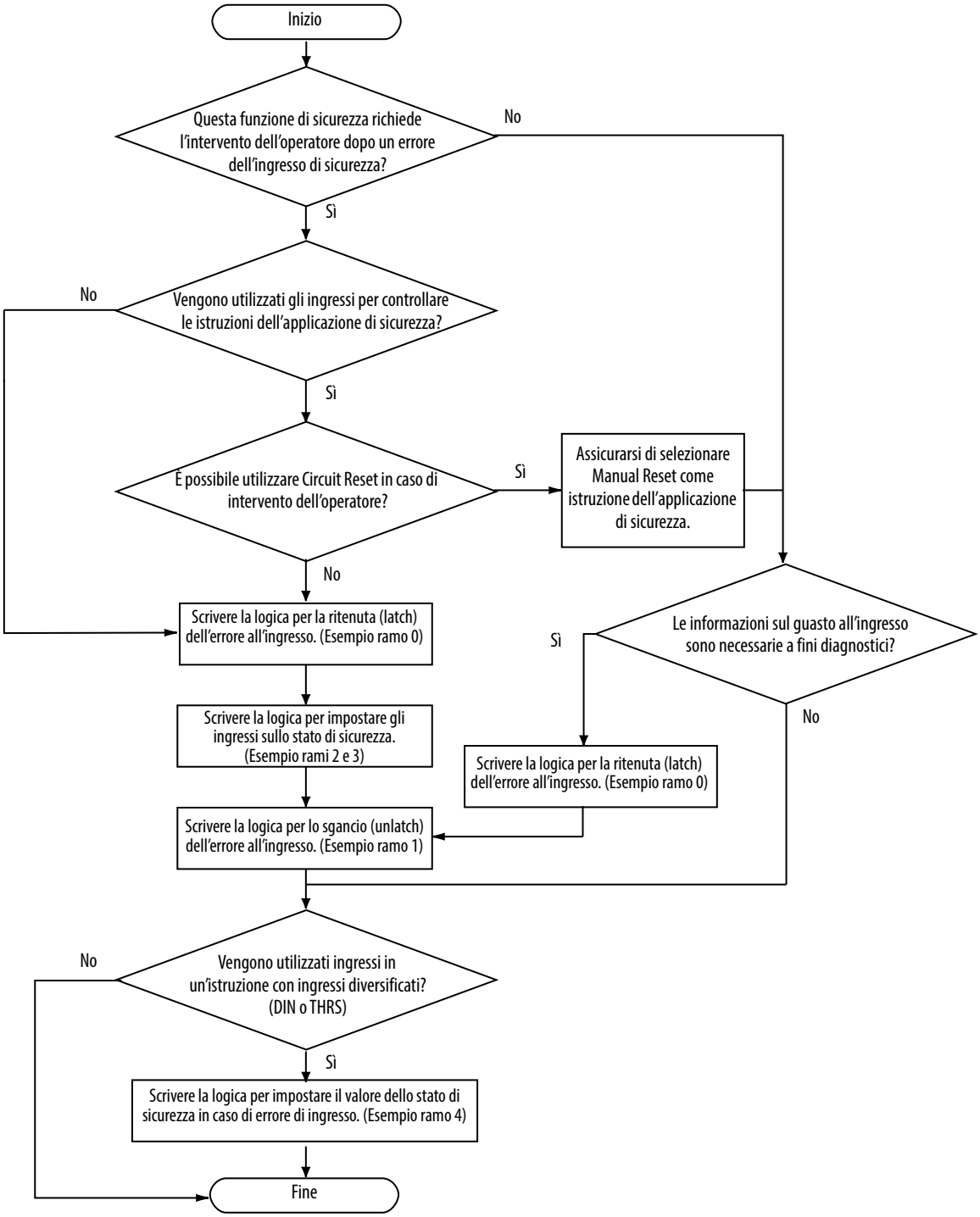


Figura 23 – Logica ladder: esempio 1

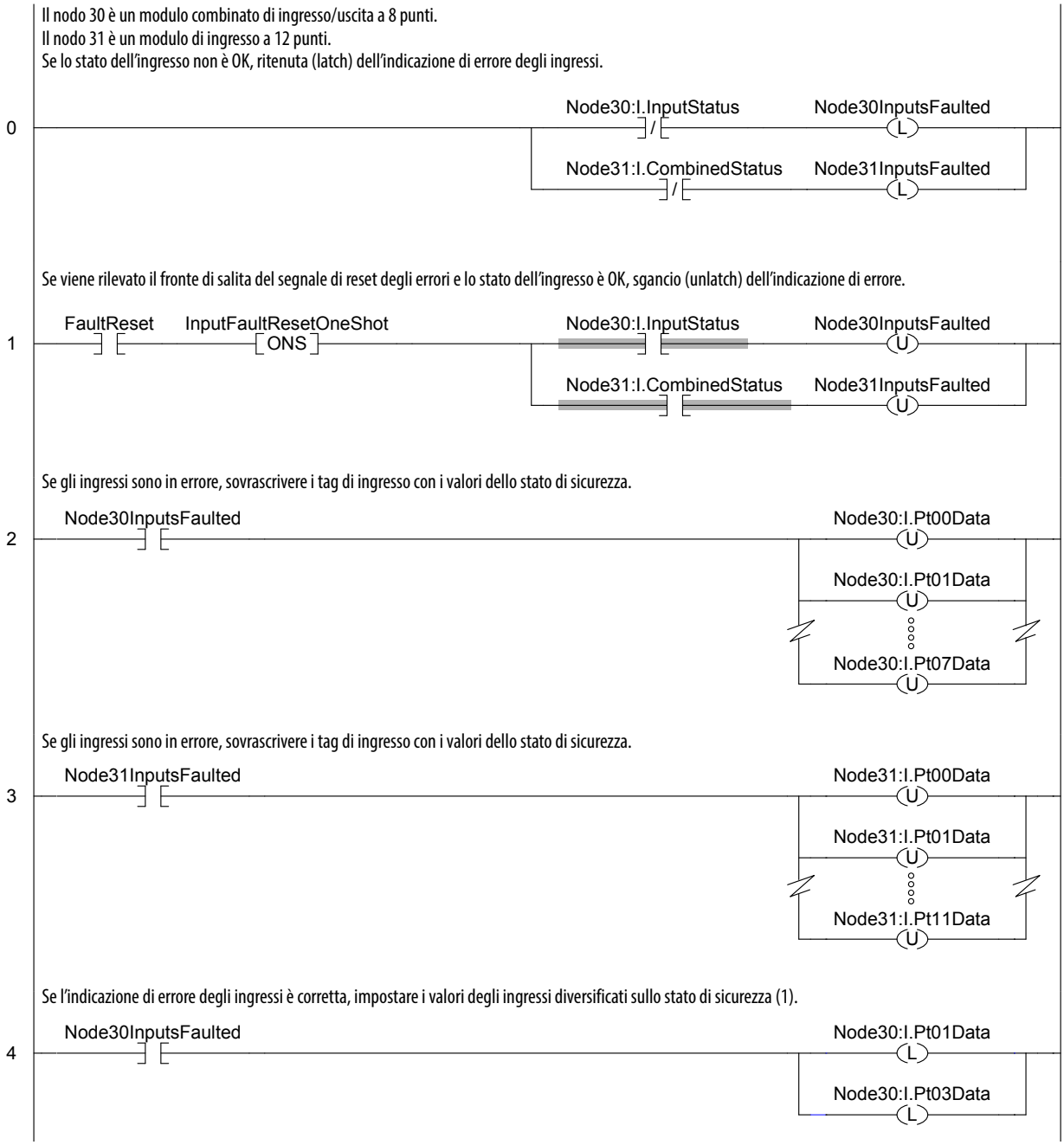


Figura 24 – Logica ladder: esempio 2

Figura 25 – Diagramma di flusso per latch e reset degli errori di uscita

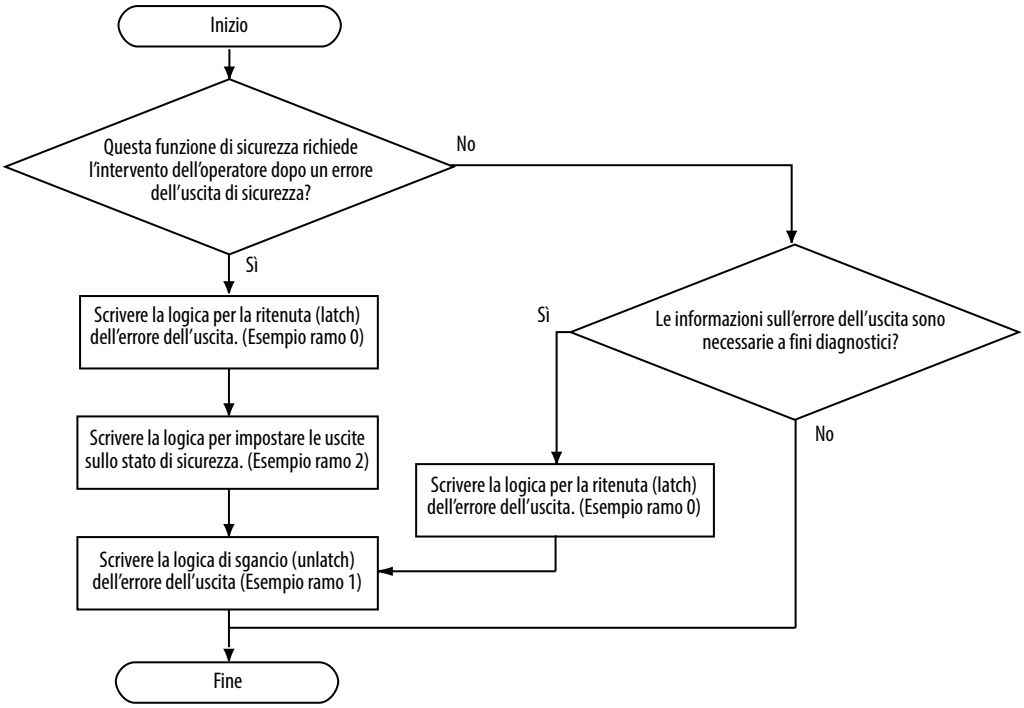
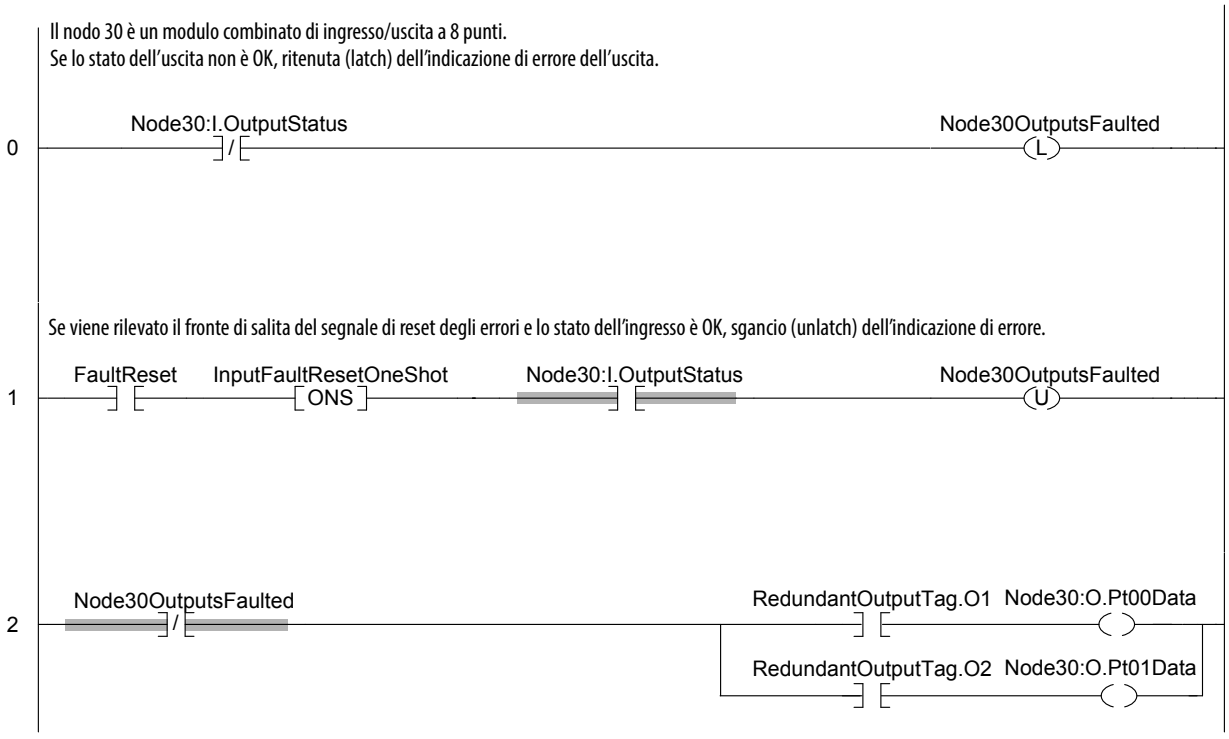


Figura 26 – Logica ladder: esempio 3



Note:

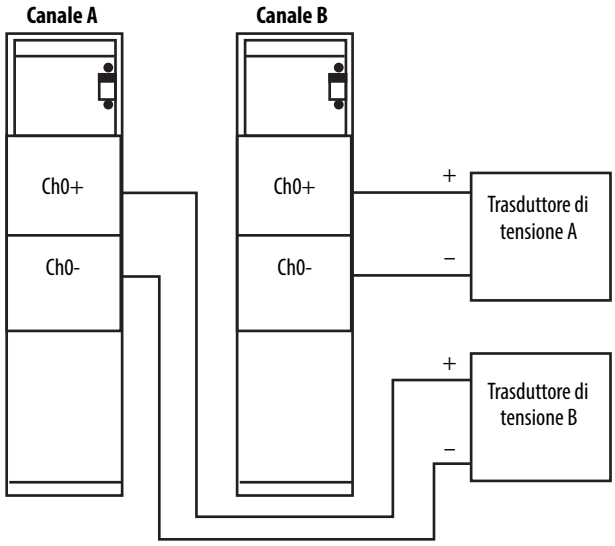
Utilizzo dei moduli FLEX I/O 1794 e degli ingressi/uscite SIL 2 1756 con controllori GuardLogix 1756 per la conformità alla norma EN 50156

Per garantire la conformità in determinate applicazioni di sicurezza, ivi comprese le funzioni di sicurezza relative ai bruciatori, è richiesta la configurazione a doppio canale. Questi esempi forniscono indicazioni per la conformità ai requisiti della norma EN50156 per il funzionamento a doppio canale SIL 2 con intervalli tra prove funzionali di 1 e 2 anni.

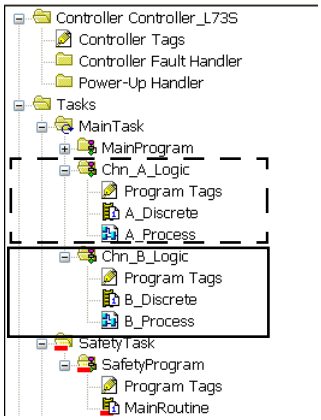
Ingressi a doppio canale SIL 2 (lato standard dei controllori GuardLogix)

Si deve prevedere una separazione chiara e facilmente identificabile tra i due canali di ingresso ed ottemperare a tutti i requisiti SIL 2 definiti in Using ControlLogix in SIL 2 Applications, pubblicazione 1756-RM001.

Figura 27 – Ingressi a doppio canale SIL 2 – Esempio F



Dati di ingresso SIL 2



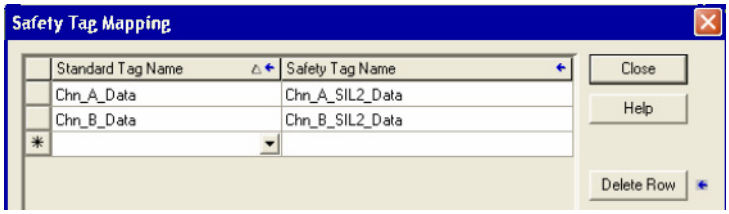
I dati di ingresso del canale A e del canale B devono essere mantenuti costantemente separati. In questo esempio è illustrato un metodo che si può adottare per separare i dati del canale A dai dati del canale B nell'applicazione.

Attenersi a tutte le regole per i moduli I/O 1756 ed i moduli FLEX™ I/O 1794 come definite nel manuale di riferimento per la sicurezza Using ControlLogix in SIL 2 Applications Safety, pubblicazione 1756-RM001.

IMPORTANTE Non eseguire funzioni specifiche di sicurezza all'interno di queste routine. La valutazione di sicurezza deve essere gestita all'interno del task di sicurezza GuardLogix 1756.

Trasferimento di dati SIL 2 nel task di sicurezza

Per trasferire i dati di sicurezza SIL 2 del canale A e del canale B nel task di sicurezza GuardLogix, utilizzare la funzionalità di mappatura dei tag di sicurezza dell'applicazione Logix Designer. I nomi dei tag utilizzati qui sono solo degli esempi. Adottare delle convenzioni di attribuzione dei nomi adatte all'applicazione specifica.



SUGGERIMENTO Per utilizzare la funzionalità di mappatura dei tag di sicurezza, selezionare Map Safety Tags dal menu Logic dell'applicazione Logix Designer.

Uscite SIL 2 che utilizzano moduli di uscita SIL 3 Guard I/O

Per le uscite SIL 2, attenersi alle seguenti regole generali:

- I moduli di uscita Guard I/O utilizzati per le uscite di sicurezza SIL 2 devono essere configurati per il funzionamento a doppio canale.
- Tutti i moduli di uscita Guard I/O sono omologati per l'uso in applicazioni SIL 2.
  - 1732DS-IB8XOBV4
  - 1791ES-IB8XOBV4
  - 1791DS-IB8XOBV4, 1791ES-IB8XOBV4
  - 1791DS-IB4XOW4
  - 1791DS-IB8XOB8
  - 1734-OB8S

Uscite SIL 2 che utilizzano moduli di uscita 1756 o 1794 SIL 2

Quando si utilizzano questi moduli di uscita SIL 2, è necessario configurare le uscite di sicurezza SIL 2 come tag di sicurezza prodotti da GuardLogix, per la conformità ai requisiti di funzionamento a doppio canale della norma EN 50156.

Creare i tag di sicurezza prodotti con le uscite SIL 2 che l'applicazione richiede. I tag di sicurezza GuardLogix prodotti/consumati richiedono che il primo membro venga assegnato alla diagnostica. Il primo membro di una connessione di sicurezza prodotta/consumata deve essere un tipo di dati denominato CONNECTION_STATUS. Questo esempio mostra un tag SIL 2 con due membri INT e due membri BOOL. Usare questi tag di sicurezza SIL 2 per controllare direttamente le uscite 1756 o 1794 SIL 2.

Name	Alias For	Base Tag	Data Type	Class	Description	External Access	Constant	Style
-SIL2_Outputs			SIL_2_Produced	Safety		Read/Write	☐	
+SIL2_Outputs.Connection_Status			CONNECTION_STA	Safety		Read/Write		
+SIL2_Outputs.SIL2_TempA			INT	Safety		Read/Write		Decimal
+SIL2_Outputs.SIL2_TempB			INT	Safety		Read/Write		Decimal
SIL2_Outputs.SIL2_Valve1			BOOL	Safety		Read/Write		Binary
SIL2_Outputs.SIL2_Valve2			BOOL	Safety		Read/Write		Binary

SUGGERIMENTO In questo esempio, non esiste un consumatore del tag prodotto. Lo stato della connessione passa in errore se non si configura un consumatore. Tuttavia, in questo tipo di configurazione, non è necessario monitorare lo stato della connessione del tag prodotto e quindi l'errore non rappresenta un problema.

Attenersi a tutte le regole per i moduli I/O 1756 ed i moduli FLEX I/O 1794 come definite nel manuale di riferimento per la sicurezza Using ControlLogix in SIL 2 Applications Safety, pubblicazione 1756-RM001.

Funzioni di sicurezza nel task di sicurezza GuardLogix 1756

Per utilizzare le funzioni di sicurezza SIL 2 e SIL 3 all'interno del task di sicurezza, attenersi alle seguenti regole generali.

- È possibile utilizzare tutte le istruzioni per applicazioni di sicurezza disponibili.
- I moduli di ingresso di sicurezza SIL CL3 (ossia, i moduli Guard I/O) possono essere utilizzati con la configurazione monocanale per funzioni di sicurezza SIL 2.
- Si consiglia di utilizzare la firma del task di sicurezza e di attivare il blocco di sicurezza dell'applicazione.

IMPORTANTE Non utilizzare i dati SIL 2 per controllare direttamente un'uscita SIL 3.

Di seguito sono riportati termini ed abbreviazioni che vengono utilizzati all'interno di questo manuale. Per le definizioni dei termini non riportati qui, consultare il glossario di automazione industriale di Allen-Bradley, pubblicazione AG-7.1.

Annullare le modifiche Azione eseguita per rifiutare le modifiche online non assemblate.

Assemblare le modifiche Questa azione viene eseguita dopo aver apportato delle modifiche online al programma del controllore e se si desidera che esse diventino permanenti dal momento che è possibile testarle, non testarle o cancellarle.

Collegamento valido Il collegamento di sicurezza è aperto ed attivo e non presenta errori.

Componente di sicurezza Qualsiasi oggetto, task, programma, routine, tag o modulo contrassegnato come elemento relativo alla sicurezza.

Componente standard Qualsiasi oggetto, task, tag, programma e così via **non** contrassegnato come elemento relativo alla sicurezza.

Controllore primario Il processore di un controllore a due processori che esegue le funzioni standard del controllore e comunica con il coprocessore di sicurezza per eseguire le funzioni di sicurezza.

Controllore standard In base all'utilizzo che ne viene fatto nel presente documento, il controllore standard si riferisce genericamente ad un controllore ControlLogix.

Coprocessore di sicurezza Il processore in un controllore a due processori che lavora con il controllore primario per eseguire le funzioni di sicurezza.

Errore di sicurezza irreversibile Un errore che, anche se gestito correttamente dai sistemi di gestione errori forniti dal controllore di sicurezza ed implementati dall'utente, interrompe l'intera elaborazione del task di sicurezza e richiede l'intervento esterno dell'utente per riavviare il task di sicurezza.

Errore irreversibile del controllore Un errore che determina l'interruzione di tutta l'elaborazione e che richiede lo spegnimento e la riaccensione del controllore. Il programma utente non viene conservato e va ricaricato.

Errore reversibile Un errore che, se trattato correttamente implementando i meccanismi di gestione errori del controllore, non determina l'interruzione dell'esecuzione della logica utente.

Firma del task di sicurezza Un valore calcolato dal firmware che rappresenta univocamente la logica e la configurazione del sistema di sicurezza. Viene utilizzata per verificare l'integrità del programma applicativo di sicurezza durante i download nel controllore.

Firma dell'istruzione La firma dell'istruzione è costituita da un numero ID e dalla registrazione cronologica, che associa la definizione dell'istruzione Add On ad una determinata ora e data.

Firma dell'istruzione di sicurezza La firma dell'istruzione di sicurezza è un numero ID che identifica le caratteristiche di esecuzione dell'istruzione Add On di sicurezza. Viene utilizzata per verificare l'integrità dell'istruzione Add On di sicurezza durante i download nel controllore.

Firma della configurazione Un numero univoco che identifica la configurazione di un dispositivo. L'autenticazione di configurazione è composta da numero ID, data ed ora.

I/O di sicurezza Gli I/O di sicurezza hanno le stesse caratteristiche degli I/O standard, ad eccezione del fatto che dispongono dei meccanismi certificati SIL 3 per l'integrità dei dati.

Indirizzamento simbolico Un metodo di indirizzamento che fornisce una codifica ASCII del nome di un tag.

Intervallo di pacchetto richiesto (RPI) Nella comunicazione su una rete, questo valore indica il tempo massimo che intercorre tra produzioni successive di dati di ingresso.

Istruzione Add-On Istruzione creata come istruzione aggiuntiva per il set di istruzioni Logix. In seguito alla loro definizione, le istruzioni Add-On possono essere utilizzate come tutte le altre istruzioni di Logix e possono essere impiegate in vari progetti. Ciascuna istruzione Add-On è composta da parametri, tag locali, routine logiche e routine delle modalità di scansione opzionali.

Istruzione Add-On di sicurezza Istruzione Add-On che può utilizzare istruzioni per applicazioni di sicurezza. Oltre alla firma dell'istruzione utilizzata per istruzioni Add-On ad alta integrità, le istruzioni Add-On di sicurezza sono caratterizzate da una firma dell'istruzione di sicurezza SIL 3 da utilizzare nelle funzioni di sicurezza.

Istruzioni per applicazioni di sicurezza Istruzioni di sicurezza che garantiscono la funzionalità connessa con la sicurezza. Sono state certificate SIL 3 per l'utilizzo in routine di sicurezza.

Modifica in sospeso Un cambiamento ad una routine apportato nell'applicazione Logix Designer ma che non è ancora stato comunicato al controllore accettando la modifica.

Moltiplicatore di timeout Questo valore determina il numero di messaggi che possono essere persi prima che venga dichiarato un errore di collegamento.

Numero della rete di sicurezza (SNN) Identifica univocamente una rete tra tutte le reti presenti del sistema di sicurezza. L'utente è responsabile dell'assegnazione di un numero univoco per ogni rete o sottorete di sicurezza nell'ambito di un sistema. Il numero della rete di sicurezza fa parte dell'identificatore univoco dei nodi (UNID).

Online Situazione in cui l'utente monitora/modifica il programma del controllore.

Partnership Il controllore primario ed il coprocessore di sicurezza devono essere entrambi presenti e l'hardware ed il firmware devono essere compatibili affinché la partnership venga stabilita.

Periodo del task di sicurezza Periodicità di esecuzione del task di sicurezza.

Programma di sicurezza Un programma di sicurezza è dotato di tutti gli attributi di un programma standard, ad eccezione del fatto che può soltanto essere pianificato in un task di sicurezza. Il programma di sicurezza è composto da zero o più routine di sicurezza. Non può contenere routine standard o tag standard.

Protocollo CIP Safety Un protocollo di comunicazione in rete progettato e certificato per trasportare dati ad elevata integrità.

Routine Un insieme di istruzioni logiche in un unico linguaggio di programmazione, per esempio il linguaggio ladder. Le routine forniscono un codice eseguibile per il progetto in un controllore. Ogni programma ha una routine principale. Si possono anche specificare routine di sicurezza opzionali.

Routine di sicurezza Una routine di sicurezza ha tutti gli attributi di una routine standard, ad eccezione del fatto che è valida solo in un programma di sicurezza e che è costituita da una o più istruzioni adatte ad applicazioni di sicurezza (vedere l'Appendice A per un elenco delle istruzioni per applicazioni di sicurezza e delle istruzioni standard Logix che possono essere utilizzate nella logica di una routine di sicurezza).

Sovrapposizione Quando un task (periodico o ad evento) viene attivato mentre è ancora in corso il task attivato precedentemente.

Tag di sicurezza Un tag di sicurezza è dotato di tutti gli attributi di un tag standard ad eccezione del fatto che il controllore GuardLogix fornisce meccanismi certificati SIL 3 per contribuire a proteggere l'integrità dei dati associati. Possono essere dell'ambito del programma o dell'ambito del controllore.

Task Un meccanismo di pianificazione per l'esecuzione di un programma. Un task fornisce informazioni sulla pianificazione e sulla priorità di un insieme di uno o più programmi che vengono eseguiti sulla base di determinati criteri. Una volta attivato un task, tutti i programmi assegnati al task (schedulati) vengono eseguiti nell'ordine in cui vengono visualizzati nell'organizer del controllore.

Task di sicurezza Un task di sicurezza è dotato di tutti gli attributi di un task standard ad eccezione del fatto che è valido soltanto in un controllore GuardLogix e che può pianificare soltanto programmi di sicurezza. In un controllore GuardLogix può essere presente un solo task di sicurezza. Il task di sicurezza deve essere un task periodico/a tempo.

Task periodico Un task che viene attivato dal sistema operativo periodicamente. Trascorso questo periodo, viene attivato il task e vengono eseguiti i suoi programmi. I dati e le uscite stabiliti dai programmi del task conservano i loro valori fino all'esecuzione successiva del task o fino a quando vengono elaborati da un altro task. I task periodici interrompono sempre il task continuo.

Tempo di risposta del sistema Il tempo massimo che può intercorrere tra un evento connesso con la sicurezza come un ingresso al sistema oppure come errore nel sistema ed il tempo impiegato dal sistema a raggiungere lo stato di sicurezza. Il tempo di risposta del sistema include i tempi di risposta dei sensori e degli attuatori ed il tempo di risposta del controllore.

Tempo di risposta task di sicurezza La somma del periodo del task di sicurezza più il watchdog del task di sicurezza. Questo tempo è il ritardo massimo che può intercorrere tra qualsiasi cambiamento in ingresso applicato al controllore GuardLogix ed il momento in cui l'uscita elaborata è disponibile per il collegamento produttore.

Watchdog del task di sicurezza Il tempo massimo ammesso dall'avvio del task di sicurezza fino al suo completamento. Il superamento del watchdog del task di sicurezza attiva un errore di sicurezza irreversibile.

Note:

Numerici

A

B

C

D

E

F

R

S

T

V

W

Assistenza Rockwell Automation

Rockwell Automation fornisce informazioni tecniche sul Web per assistere i clienti nell'utilizzo dei suoi prodotti. All'indirizzo http://www.rockwellautomation.com/support, è possibile trovare note tecniche ed applicative, codici di esempio e collegamenti ai service pack software. Inoltre, è possibile visitare il nostro Support Center all'indirizzo https://rockwellautomation.custhelp.com/ per aggiornamenti software, chat e forum di supporto, informazioni tecniche, FAQ e sottoscrizione di news riguardanti i prodotti.

Vengono proposti anche numerosi programmi di supporto alle operazioni di installazione, configurazione e ricerca guasti. Per ulteriori informazioni, contattare il proprio distributore di zona o il rappresentante Rockwell Automation, oppure visitare il sito http://www.rockwellautomation.com/services/online-phone.

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 Worldwide Locator sul sito http://www.rockwellautomation.com/rockwellautomation/support/overview.page, oppure contattare il rappresentante Rockwell Automation di zona.

Restituzione di nuovi prodotti non funzionanti

Rockwell Automation testa tutti i propri prodotti per garantire che siano perfettamente funzionanti al momento della spedizione dalla fabbrica. Tuttavia, se il prodotto non funziona e deve essere restituito, procedere come segue:

Stati Uniti	Contattare il proprio distributore. Per completare la procedura di reso è necessario fornire al distributore il numero di pratica attribuito dall'Assistenza Clienti (chiamare il numero telefonico sopra indicato per ottenerne uno).
Al di fuori degli Stati Uniti	Si prega di contattare il proprio rappresentante Rockwell Automation di zona per la procedura di restituzione.

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/.

Informazioni ambientali aggiornate sui prodotti sono disponibili sul sito web di Rockwell Automation, all'indirizzo http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

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
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

Pubblicazione 1756-RM099B-IT-P – Novembre 2014