Benutzerhandbuch

Allen-Bradley

GuardLogix-Steuerungen

Bestellnummern 1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP, 1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT

Wichtige Hinweise für den Anwender

Die Betriebseigenschaften elektronischer Geräte unterscheiden sich von denen elektromechanischer Geräte. In der Publikation SGI-1.1, „Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls“ (erhältlich bei Ihrem Rockwell Automation-Vertriebsbüro oder online unter http://www.rockwellautomation.com/literature/) werden einige wichtige Unterschiede zwischen elektronischen und festverdrahteten elektromechanischen Geräten beschrieben. Aufgrund dieser Unterschiede und der vielfältigen Einsatzbereiche elektronischer Geräte müssen die für die Anwendung dieser Geräte verantwortlichen Personen sicherstellen, dass die Geräte zweckgemäß eingesetzt werden.

Rockwell Automation ist in keinem Fall verantwortlich oder haftbar für indirekte Schäden oder Folgeschäden, die durch den Einsatz oder die Anwendung dieses Geräts entstehen.

Die in diesem Handbuch aufgeführten Beispiele und Abbildungen dienen ausschließlich zur Veranschaulichung. Aufgrund der unterschiedlichen Anforderungen der jeweiligen Anwendung kann Rockwell Automation keine Verantwortung oder Haftung für den tatsächlichen Einsatz der Produkte auf der Grundlage dieser Beispiele und Abbildungen übernehmen.

Rockwell Automation übernimmt keine patentrechtliche Haftung in Bezug auf die Verwendung von Informationen, Schaltkreisen, Geräten oder Software, die in dieser Publikation beschrieben werden.

Die Vervielfältigung des Inhalts dieser Publikation, ganz oder auszugsweise, bedarf der schriftlichen Genehmigung von Rockwell Automation.

In dieser Publikation werden folgende Hinweise verwendet, um Sie auf bestimmte Sicherheitsaspekte aufmerksam zu machen.

	**WARNUNG:** Dieser Hinweis macht Sie auf Vorgehensweisen und Zustände aufmerksam, die in explosionsgefährdeten Umgebungen zu einer Explosion und damit zu Verletzungen oder Tod, Sachschäden oder wirtschaftlichen Verlusten führen können.
	**ACHTUNG:** Dieser Hinweis macht Sie auf Vorgehensweisen und Zustände aufmerksam, die zu Verletzungen oder Tod, Sachschäden oder wirtschaftlichen Verlusten führen können. Die Achtungshinweise helfen Ihnen, eine Gefahr zu erkennen, die Gefahr zu vermeiden und die Folgen abzuschätzen.
	**STROMSCHLAGGEFAHR:** An der Außenseite oder im Inneren des Geräts (z. B. eines Antriebs oder Motors) kann ein Etikett dieser Art angebracht sein, das Sie auf das mögliche Anliegen gefährlicher Spannungen aufmerksam macht.
	**VERBRENNUNGSGEFAHR:** An der Außenseite oder im Inneren des Geräts (z. B. eines Antriebs oder Motors) kann ein Etikett dieser Art angebracht sein, das Sie auf eventuell gefährliche Temperaturen der Oberflächen hinweist.
WICHTIG	Dieser Hinweis enthält Informationen, die für den erfolgreichen Einsatz und das Verstehen des Produkts besonders wichtig sind.

Die nachfolgenden Informationen enthalten eine Zusammenfassung der Änderungen, die sich seit der letzten Veröffentlichung an diesem Handbuch ergeben haben.

Thema	Seiten
Informationen zu 1756-L71S-Steuerungen	11, 18, 21, 27, 49
Praktische Anleitung zur Installation des Energiespeichermoduls (ESM)	48

Notizen:

Vorwort

Kapitel 1

Systemüberblick

Kapitel 2

Installation der Steuerung

Kapitel 3

Konfiguration der Steuerung

Kapitel 4

Kommunikation über Netzwerke

Kapitel 5

Hinzufügen, Konfigurieren, Überwachen und Ersetzen von CIP Safety-E/A-Modulen

Kapitel 6

Entwicklung von Sicherheitsanwendungen

Kapitel 7

Schalten der Steuerung in den Online-Modus

Kapitel 8

Speichern und Laden von Projekten mithilfe des nichtflüchtigen Speichers

Kapitel 9

Zustandsüberwachung und Fehlerbehebung

Anhang A

Statusanzeigen

Anhang B

Warten der Batterie

Anhang C

Wechsel des Steuerungstyps in RSLogix 5000-Projekten

Anhang D

Änderungshistorie

Index

Dieses Handbuch ist eine Anleitung zur Verwendung von GuardLogix™-Steuerungen. Es enthält eine Beschreibung der GuardLogix-spezifischen Verfahren, die zum Konfigurieren und Bedienen der Steuerung sowie zur Fehlerbehebung eingesetzt werden.

Das Handbuch richtet sich an Personen, die für die Konzeption, Installation, Programmierung und Wartung von Steuerungssystemen mit GuardLogix-Steuerungen verantwortlich sind.

Grundlegende Kenntnisse im Umgang mit elektrischen Schaltungen und Relaislogik werden vorausgesetzt. Weitere Anforderungen sind eine Ausbildung und Erfahrung in Erstellung, Betrieb und Wartung von Sicherheitssystemen.

Ausführliche Informationen zu weiterführenden Themen wie z. B. zur Programmierung Ihrer GuardLogix-Steuerung, zu den SIL 3-/PLe-Anforderungen oder Informationen zu Logix-Standardkomponenten finden Sie in der Liste Weitere Informationen auf Seite 13.

Informationen über 1756 GuardLogix-Steuerungen

Es stehen zwei Produktreihen von GuardLogix™-Steuerungen der Serie 1756 zur Verfügung. Diese Steuerungen weisen viele ähnliche Leistungsmerkmale auf, unterscheiden sich jedoch auch in einigen Eigenschaften. In Tabelle 1 sind die Unterschiede kurz zusammengefasst.

Tabelle 1 – Unterschiede zwischen den Steuerungen 1756-L7*x*S und 1756-L6*x*S

Funktion	**1756-L7*x*S** (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	**1756-L6*x*S** (1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP)
Unterstützung einer Uhr und Backup zur Absicherung des Speichers beim Herunterfahren	Energiespeichermodul (ESM)	Batterie
Kommunikationsanschlüsse (integriert)	USB	Seriell
Anschlüsse, Steuerung	500	250
Speicherung, nichtflüchtig	SD-Karte	CompactFlash-Karte
Statusanzeigen/-leuchten	Bildlauf-Statusanzeige und LED-Statusleuchten	LED-Statusleuchten

Die GuardLogix-Steuerungen für extreme Umgebungsbedingungen, Bestellnummern 1756-L73SXT und 1756-L7SPXT, bieten dieselbe Funktionalität wie die Steuerung 1756-L73S, sind jedoch zusätzlich für Temperaturen von –25 bis +70 °C (–13 bis +158 °F) ausgelegt.

WICHTIG	Logix-XT-Systemkomponenten sind nur für den Betrieb unter extremen Umgebungsbedingungen ausgelegt, wenn sie ordnungsgemäß mit anderen Logix-XT-Systemkomponenten eingesetzt werden. Bei Verwendung von Logix-XT-Komponenten mit herkömmlichen Logix-Systemkomponenten gelten die Nennwerte für extreme Umgebungen nicht mehr.

Verwendete Begriffe

In der folgenden Tabelle werden die in diesem Handbuch verwendeten Begriffe definiert.

Tabelle 2 – Begriffe und Definitionen

Abkürzung	Vollständiger Begriff	Definition
1oo2	One Out of Two/Einer von zweien	Bezieht sich auf die Arbeitsweise eines Multiprozessor-Sicherheitsystems.
CIP	Common Industrial Protocol	Ein Kommunikationsprotokoll, das für industrielle Automatisierungsanwendungen konzipiert ist.
CIP Safety	Common Industrial Protocol – Sicherheitszertifizierung	SIL 3/PLe-Versionen von CIP.
DC	Diagnostic Coverage/Diagnoseabdeckung	Das Verhältnis zwischen erkannter Ausfallrate und Gesamtausfallrate.
EN	Europäische Norm	Die offizielle europäische Industrienorm.
ESM	Energiespeichermodul	Zur Unterstützung der Uhr und als Backup zur Absicherung des Speichers beim Herunterfahren der 1756-L7xS- und 1756-L73SXT-Steuerungen.
GSV	Get System Value/Systemwert abrufen	Ein Befehl, mit dem spezifizierte Steuerungsstatusinformationen abgerufen und in einem Ziel-Tag abgelegt werden.
–	Multicast	Die Übermittlung von Informationen von einem Sender zu mehreren Empfängern.
PFD	Probability of Failure on Demand/Ausfallwahrscheinlichkeit auf Anforderung	Die mittlere Wahrscheinlichkeit, dass ein System seine vorgegebene Funktion auf Anforderung nicht ausführt.
PFH	Probability of Failure per Hour/Ausfallwahrscheinlichkeit pro Stunde	Die Wahrscheinlichkeit eines gefährlichen Ausfalls in einem System pro Stunde.
PL	Performance Level (Leistungsstufe)	ISO 13849-1 (Sicherheitsklassifizierung).
RPI	Angefordertes Paketintervall (RPI)	Die erwartete Zeitspanne für die Produktion der Daten beim Kommunizieren über ein Netzwerk.
SNN	Sicherheitsnetzwerknummer	Eine eindeutige Nummer, die einen Abschnitt eines Sicherheitsnetzwerks identifiziert.
SSV	Set System Value/Systemwert einstellen	Ein Befehl zur Konfiguration von Steuerungssystemdaten.
–	Standard	Objekte, Tasks, Tags, Programme oder Komponenten in Ihrem Projekt, die nicht sicherheitsrelevant sind.
–	Unicast	Die Übermittlung von Informationen von einem Sender zu einem Empfänger.

Weitere Informationen

Die folgenden Dokumente enthalten zusätzliche Informationen zu verwandten Produkten von Rockwell Automation.

Tabelle 3 – Publikationen zu GuardLogix-Steuerungen und -Systemen

Weitere Informationen zu	Finden Sie hier	Beschreibung
(Sicherheits-) Anwendungsanforderungen	Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch, Publikation 1756-RM093	Ausführliche Anforderungen zum Erreichen und Erhalten von SIL 3/PLe mit dem GuardLogix-Steuerungssystem.
Batterien	Guidelines for Handling Lithium Batteries, Publikation AG-5.4	Informationen zu Lagerung, Handhabung, Transport und Entsorgung von Lithiumbatterien.
	Website zu den Batterien für speicherprogrammierbare Steuerungen: http://www.ab.com/programmablecontrol/batteries.html	Bietet Materialsicherheitsdatenblätter (Material Safety Data Sheets, MSDS) zu individuellen Ersatzbatterien.
CIP Sync (Zeitsynchronisation)	Integrated Architecture and CIP Sync Configuration Application Technique, Publikation IA-AT003	Ausführliche Informationen zur Anwendung von CIP Sync-Technologie zur Synchronisation von Uhren in einem Logix-Steuerungssystem.
Design und Auswahl	Logix5000 Controllers Design Considerations Reference Manual, Publikation 1756-RM094	Bietet erfahrenen Anwendern Leitlinien zu Systemoptimierung sowie weitere Systeminformationen, um sie bei Entscheidungen zum Systemdesign zu unterstützen.
	ControlLogix Selection Guide, Publikation 1756-SG001	Ermöglicht eine erste ungefähre Auswahl der ControlLogix®-Systemkomponenten und enthält Informationen zu kritischen Spezifikationen sowie Links zu umfassenden Spezifikationsinformationen.
Guard I/O	Guard I/O DeviceNet Safety Modules User Manual, Publikation 1791DS-UM001	Informationen zur Verwendung von Guard I/O DeviceNet-Sicherheitsmodulen.
	Guard I/O EtherNet/IP-Sicherheitsmodule – Benutzerhandbuch, Publikation 1791ES-UM001	Informationen zur Verwendung von Guard I/O EtherNet/IP-Sicherheitsmodulen.
	POINT Guard I/O-Sicherheitsmodule – Installations- und Benutzerhandbuch, Publikation 1734-UM013	Informationen zur Installation, Konfiguration und Verwendung von POINT Guard I/O™-Modulen.
Hardware-Installation	ControlLogix Chassis and Power Supplies Installation Instructions, Publikation 1756-IN005	Informationen zur Installation und Erdung von ControlLogix-Chassis und -Netzteilen.
	Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Publikation 1770-4.1	Detaillierte Informationen zum Erden und Verdrahten speicherprogrammierbarer Steuerungen
Befehle (Programmierung)	Befehlssatz für GuardLogix-Sicherheitsanwendungen – Referenzhandbuch, Publikation 1756-RM095	Informationen zum Befehlssatz für GuardLogix-Sicherheitsanwendungen.
	Logix5000-Steuerungen – Allgemeine Befehle – Referenzhandbuch, Publikation 1756-RM003	Bietet Programmierern detaillierte Informationen zu jedem für eine Logix5000-Steuerung verfügbaren Befehl.
	Logix5000 Controllers Motion Instructions Reference Manual, Publikation MOTION-RM002	Bietet Programmierern detaillierte Informationen zu den für eine Logix5000-Steuerung verfügbaren Achssteuerungsbefehlen.
Achssteuerung	SERCOS Motion Configuration and Startup User Manual, Publikation MOTION-UM001	Einzelheiten zum Konfigurieren eines Anwendungssystems mit SERCOS-Achssteuerung.
	Motion Coordinated Systems User Manual, Publikation MOTION-UM002	Einzelheiten zum Erstellen und Konfigurieren eines Anwendungssystems zur koordinierten Achssteuerung.
	Integrated Motion über EtherNet/IP-Netzwerk – Konfiguration und Inbetriebnahme – Benutzerhandbuch, Publikation MOTION-UM003	Einzelheiten zum Konfigurieren eines Anwendungssystems mit Integrated Motion über EtherNet/IP-Netzwerke.
	CIP Motion Reference Manual, Publikation MOTION-RM003	Ausführliche Informationen zu Achssteuerungsbetriebsarten und -attributen für Integrated Motion über EtherNet/IP-Netzwerke.
Netzwerke (ControlNet, DeviceNet, EtherNet/IP)	EtherNet/IP Modules in Logix5000 Control Systems User Manual, Publikation ENET-UM001	Informationen zur Konfiguration und Verwendung von EtherNet/IP-Modulen in einem Logix5000™-Steuerungssystem.
	ControlNet Modules in Logix5000 Control Systems User Manual, Publikation CNET-UM001	Informationen zur Konfiguration und Verwendung von ControlNet-Modulen in einem Logix5000-Steuerungssystem.
	DeviceNet Modules in Logix5000 Control Systems User Manual, Publikation DNET-UM004	Informationen zur Konfiguration und Verwendung von DeviceNet-Modulen in einem Logix5000-Steuerungssystem.
PhaseManager™	PhaseManager User Manual, Publikation LOGIX-UM001	Schrittweise Anleitungen und Beispiele zur Konfiguration und Programmierung einer Logix5000-Steuerung im Hinblick auf die Verwendung von Gerätephasen.

Tabelle 3 – Publikationen zu GuardLogix-Steuerungen und -Systemen

Weitere Informationen zu	Finden Sie hier	Beschreibung
Programmieraufgaben und -verfahren	Logix5000 Controllers Common Procedures Programming Manual, Publikation 1756-PM001	Ermöglicht den Zugriff auf die Programmierhandbücher der Logix5000-Steuerungen, in denen Sie Informationen zum Verwalten von Projektdateien, zum Organisieren von Tags, zur Kontaktplanprogrammierung, zum Testen von Routinen, zum Erstellen von Add-On-Befehlen, zu Steuerungsstatusdaten, zu Handhabungsfehlern, zum Importieren und Exportieren von Projektkomponenten und vieles mehr finden.
	Logix5000 Controllers Execution Time and Memory Use Reference Manual, Publikation 1756-RM087	Unterstützung beim Abschätzen der Speicherbelegung und Ausführungszeit programmierter Logik und bei der Auswahl der verschiedenen Programmieroptionen.
Redundanz	ControlLogix Redundancy System User Manual, Publikation 1756-UM523	Bietet Unterstützung bei Design, Entwicklung und Realisierung eines standardmäßigen ControlLogix-Redundanzsystems.
	ControlLogix Enhanced Redundancy System User Manual, Publikation 1756-UM535	Bietet Unterstützung bei Design, Entwicklung und Realisierung eines erweiterten ControlLogix-Redundanzsystems.

Die Publikationen stehen unter http://www.rockwellautomation.com/literature zur Ansicht oder zum Download bereit. Wenn Sie eine gedruckte Version der technischen Dokumentation benötigen, wenden Sie sich an den für Sie zuständigen Allen-Bradley®-Distributor oder Vertriebsbeauftragten von Rockwell Automation.

Systemüberblick

Anforderungen an Sicherheitsanwendungen

Das GuardLogix -Steuerungssystem ist für die Verwendung in Sicherheitsanwendungen bis zu und einschließlich Safety Integrity Level (SIL) 3 und Performance Level (PL) e zertifiziert, wobei der abgeschaltete Zustand der sichere Zustand ist. Die Anforderungen an Sicherheitsanwendungen umfassen die Einschätzung der Wahrscheinlichkeit von Ausfallraten (PFD und PFH), die Einstellung von Systemreaktionszeiten und funktionelle Verifizierungsprüfungen gemäß SIL 3-/PLe-Kriterien.

Weitere Informationen zu den Anforderungen an Sicherheitssysteme nach SIL 3 und PLe, einschließlich der Intervalle der funktionellen Validierungsprüfungen, der Berechnungen von Systemreaktionszeiten und Ausfallwahrscheinlichkeiten (PFD/PFH), sind der Publikation 1756-RM093, „Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch“, zu entnehmen. Sie müssen diese Anforderungen gelesen, verstanden und erfüllt haben, bevor Sie mit einem auf einer GuardLogix-Steuerung basierenden SIL 3-, PLe-Sicherheitssystem arbeiten.

Für auf GuardLogix basierende SIL 3-/PLe-Sicherheitsanwendungen müssen mindestens eine Sicherheitsnetzwerknummer (SNN) und eine Sicherheits-Task-Signatur verwendet werden. Beide beeinflussen die Konfiguration von Steuerung und E/A sowie die Netzwerkkommunikation.

Weitere Informationen enthält die Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch.

Sicherheitsnetzwerknummer

Die Sicherheitsnetzwerknummer (SNN) muss eine eindeutige Nummer sein, welche die Sicherheitsteilnetze kennzeichnet. Jedes Sicherheitsteilnetz, das die Steuerung für die Sicherheitskommunikation verwendet, muss über eine

eindeutige SNN verfügen. Jedes CIP Safety-Gerät muss auch mit einer SNN des Sicherheitsteilnetzes konfiguriert werden. Die SNN kann automatisch oder manuell zugeordnet werden.

Informationen zum Festlegen der SNN finden Sie unter Verwalten der Sicherheitsnetzwerknummer auf Seite 55.

Sicherheits-Task-Signatur

Die Sicherheits-Task-Signatur besteht aus einer Identifikationsnummer (ID-Nummer), Datum und Zeit, die in eindeutiger Weise den Sicherheitsteil eines Projekts kennzeichnen. Dies beinhaltet die Sicherheitslogik, die Daten sowie die Konfiguration. Das GuardLogix-System verwendet die Sicherheits-Task-Signatur, um die Integrität des Projekts festzulegen und gibt Ihnen die Möglichkeit zu prüfen, ob das richtige Projekt auf die Zielsteuerung heruntergeladen wird. Das Erstellen, Aufzeichnen und Prüfen der Sicherheits-Task-Signatur ist ein obligatorischer Bestandteil des Entwicklungsprozesses einer Sicherheitsanwendung.

Weitere Informationen finden Sie unter Erstellen einer Sicherheits-Task-Signatur auf Seite 110.

Unterscheiden zwischen Standard- und Sicherheitskomponenten

Steckplätze eines GuardLogix-Systemchassis, die nicht für die Sicherheitsfunktion verwendet werden, können mit anderen ControlLogix-Modulen besetzt werden, die gemäß der Niederspannungs- und der EMV-Richtlinie zertifiziert sind. Die CE-Zertifizierung für die speicherprogrammierbare Steuerung der ControlLogix-Produktfamilie und Informationen dazu, welche Module zertifiziert sind, finden Sie unter http://ab.com/certification/ce.

Sie müssen eine klare, logische und sichtbare Unterscheidung zwischen den Sicherheits- und Standardteilen der Anwendung vornehmen. Um Sie beim Festlegen dieser Unterscheidung zu unterstützen, bietet die Programmiersoftware RSLogix 5000 Sicherheitsidentifikationssymbole, mit denen Sie die Sicherheits-Task, Sicherheitsprogramme, Sicherheitsroutinen und Sicherheitskomponenten kennzeichnen können. Darüber hinaus verwendet die Software RSLogix 5000 ein Sicherheitsklassenattribut, das immer dann sichtbar ist, wenn die Eigenschaften von Sicherheits-Tasks, Sicherheitsprogrammen, Sicherheitsroutinen, Sicherheits-Tags oder Sicherheits-Add-On-Befehlen angezeigt werden.

Die Steuerung gestattet nicht, dass Sicherheits-Tag-Daten von externen Bedienerschnittstellengeräten oder über Nachrichtenbefehle von Peer-Steuerungen überschrieben werden. Die Software RSLogix 5000 kann Sicherheits-Tags schreiben, wenn die GuardLogix-Steuerung sicherheitsentriegelt ist, über keine Sicherheits-Task-Signatur verfügt und keine Sicherheitsfehler aufweist.

Publikation 1756-UM001, „ControlLogix-System – Benutzerhandbuch“, enthält Informationen zur Verwendung von ControlLogix-Geräten in nicht sicherheitsrelevanten Standardanwendungen.

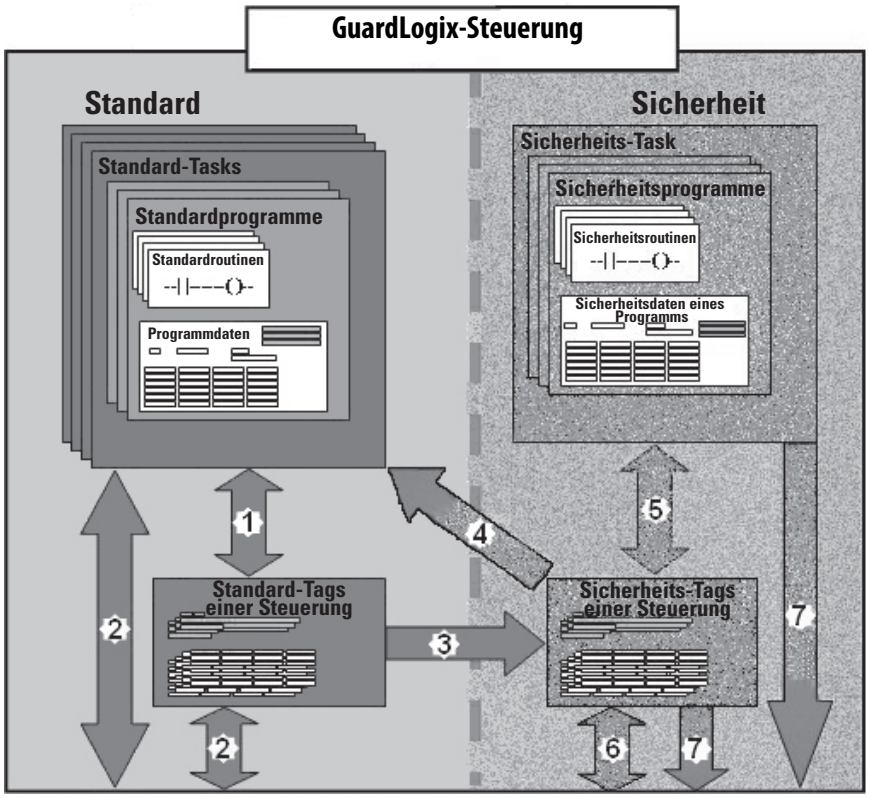
Bedienerschnittstellengeräte

Bedienerschnittstellengeräte (HMI-Geräte) können mit GuardLogix-Steuerungen verwendet werden. Mit Bedienerschnittstellengeräten kann auf Standard-Tags zugegriffen werden, wie mit einer Standardsteuerung. Sie können allerdings nicht auf Sicherheits-Tags schreiben, da diese für Bedienerschnittstellengeräte schreibgeschützt sind (Nur-Lese-Status).

Datenflussfunktionen der Steuerung

Diese Abbildung veranschaulicht die Flussfunktionen für Standard- und Sicherheitsdaten der GuardLogix-Steuerung.

Abbildung 1 – Datenflussfunktionen



Nr.	Beschreibung	
1	Standard-Tags und Logik verhalten sich genau so wie in der Logix-Standardplattform.	
2	Standard-Tag-Daten, programm- sowie steuerungsbezogen, können mit externen Bedienerschnittstellengeräten, PCs und anderen Steuerungen ausgetauscht werden.	
3	GuardLogix-Steuerungen sind integrierte Steuerungen, die in der Lage sind, Standard-Tag-Daten in Sicherheits-Tags zu verlagern (Zuordnung), damit sie in der Sicherheits-Task verwendet werden können.	
	⚠	**ACHTUNG:** Diese Daten dürfen nicht verwendet werden, um einen SIL 3/PLe-Ausgang direkt zu steuern.
4	Steuerungsbezogene Sicherheits-Tags können direkt von der Standardlogik gelesen werden.	
5	Sicherheits-Tags können von der Sicherheitslogik gelesen oder geschrieben werden.	
6	Sicherheits-Tags können zwischen Sicherheitssteuerungen über Ethernet- oder ControlNet-Netzwerke ausgetauscht werden (einschließlich 1756- und 1768-GuardLogix-Steuerungen).	
7	Sicherheits-Tag-Daten, programm- oder steuerungsbezogen, können von externen Geräten, wie HMI-Geräten, PCs oder anderen Standardsteuerungen, gelesen werden.	
	WICHTIG	Sobald diese Daten gelesen wurden, gelten sie als Standarddaten, nicht als SIL 3/PLe-Daten.

Auswählen der Systemhardware

Das GuardLogix-System unterstützt SIL 3- und PLe-Sicherheitsanwendungen. Die GuardLogix-Steuerung besteht aus einer Primärsteuerung und einem Sicherheitspartner, die gemeinsam in einer 1oo2-Architektur verwendet werden können. In Tabelle 4 finden Sie Bestellnummern für Primärsteuerungen und Sicherheitspartner.

Der Sicherheitspartner muss im Steckplatz unmittelbar rechts neben der Primärsteuerung installiert werden. Die Haupt- und Nebenversionen der Firmware der Primärsteuerung und des Sicherheitspartners müssen exakt übereinstimmen, damit sie eine für Sicherheitsanwendungen erforderliche Steuerungspartnerschaft aufbauen können.

Tabelle 4 – Bestellnummern für Primärsteuerung und entsprechenden Sicherheitspartner

Primärsteuerung	Sicherheitspartner
1756-L61S, 1756-L62S, 1756-L63S	1756-LSP
1756-L71S, 1756-L72S, 1756-L73S	1756-L7SP
1756-L73SXT	1756-L7SPXT

Primärsteuerung

Die Primärsteuerung ist der Prozessor, der Standard- und Sicherheitsfunktionen ausführt und der bei sicherheitsrelevanten Funktionen mit dem Sicherheitspartner im GuardLogix-Steuerungssystem kommuniziert. Folgende Funktionen zählen zu den Standardfunktionen:

- E/A-Steuerung
- Logik
- Zeitmessung
- Zählung
- Berichtserstellung
- Kommunikation
- Arithmetische Berechnungen
- Datenfile-Bearbeitung

Die Primärsteuerung besteht aus einem zentralen Prozessor, einer E/A-Schnittstelle und einem Speicher.

Tabelle 5 – Speicherkapazität

Bestellnummer	Anwenderspeicher (RAM-Kapazität)	
	Standard-Tasks und -komponenten	Sicherheits-Tasks und -komponenten
1756-L61S	2 MB	1 MB
1756-L62S	4 MB	1 MB
1756-L63S	8 MB	3,75 MB
1756-L71S	2 MB	1 MB
1756-L72S	4 MB	2 MB
1756-L73S, 1756-L73SXT	8 MB	4 MB

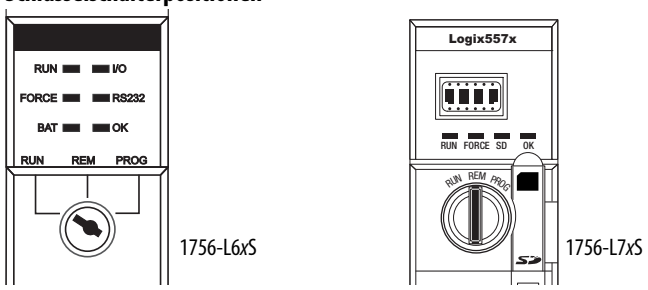
In der Software RSLogix 5000 ab Version 18 unterstützt die GuardLogix-Steuerung Betriebssystemaktualisierungen oder die Speicherung bzw. das Abrufen von Anwenderprogrammen mithilfe einer Speicherkarte. In Version 16 und 17 der Software RSLogix 5000 hatten Sie dagegen nur die Möglichkeit, den Inhalt einer Speicherkarte einzusehen, sofern eine in der Primärsteuerung installiert war. Vor Version 16 wurden noch keine Speicherkarten unterstützt.

Weitere Informationen finden Sie unter Kapitel 8, Speichern und Laden von Projekten mithilfe des nichtflüchtigen Speichers.

Ein Drei-Positionen-Schlüsselschalter auf der Vorderseite der Primärsteuerung regelt die Betriebsmodi der Steuerung. Folgende Modi stehen zur Verfügung:

- RUN
- PROGram
- REMote – dieser softwareaktivierte Modus kann Program, Run oder Test sein

Abbildung 2 – Schlüsselschalterpositionen



Sicherheitspartner

Der Sicherheitspartner ist ein Coprozessor, der für einen isolierten zweiten Kanal (Redundanz) für sicherheitsrelevante Funktionen im System sorgt.

Der Sicherheitspartner verfügt über keinen Schlüsselschalter oder Kommunikationsanschluss. Seine Konfiguration und sein Betrieb werden durch die Primärsteuerung geregelt.

Chassis

Das ControlLogix-Chassis stellt die physische Verbindung zwischen den Modulen und der GuardLogix-Steuerung bereit.

Netzteil

Die ControlLogix-Netzteile, die auf Seite 28 aufgeführt sind, eignen sich für den Einsatz in SIL 3-Anwendungen. Für den SIL 3-Betrieb des Netzteils ist keine zusätzliche Konfiguration oder Verkabelung erforderlich.

Auswählen von Sicherheits-E/A-Modulen

Sicherheitseingangs- und -ausgangsgeräte können an die CIP Safety-E/A in DeviceNet- oder EtherNet/IP-Netzwerken angeschlossen werden und ermöglichen die Steuerung von Ausgangsgeräten durch das GuardLogix-Steuerungssystem per DeviceNet- oder EtherNet/IP-Kommunikation.

Aktuelle Informationen zu den verfügbaren Bestellnummern, zertifizierten Serien und Firmwareversionen für CIP Safety-E/A finden Sie unter http://www.ab.com/certification/safety.

Auswählen von Kommunikationsnetzwerken

Die GuardLogix-Steuerung unterstützt Kommunikation, die ihr Folgendes ermöglicht:

- Verteilen und Steuern von Sicherheits-E/A in DeviceNet- oder EtherNet/IP-Netzwerken.
- Verteilen und Steuern von dezentralen Sicherheits-E/A in DeviceNet-, EtherNet/IP- oder ControlNet-Netzwerken.
- Produzieren und Konsumieren von Sicherheits-Tag-Daten zwischen 1756- und 1768 GuardLogix-Steuerungen über EtherNet/IP- oder ControlNet-Netzwerke oder innerhalb desselben ControlLogix-Chassis.
- Verteilen und Steuern von Standard-E/A in EtherNet-, ControlNet- oder DeviceNet-Netzwerken.

Verwenden dieser Kommunikationsmodule zum Bereitstellen einer Schnittstelle zwischen GuardLogix-Steuerungen und Netzwerkgeräten.

Tabelle 6 – Kommunikationsmodule

Als Schnittstelle zwischen	Verwenden Sie dieses Modul	Siehe Installationsanleitung
GuardLogix-Steuerung und DeviceNet-Geräten	1756-DNB	DNET-IN001
GuardLogix-Steuerung und EtherNet/IP-Geräten	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR, 1756-EN3TR 1756-EN2TXT	ENET-IN002
Steuerungen im ControlNet-Netzwerk	1756-CN2, 1756-CN2R 1756-CN2RXT	CNET-IN005

Die GuardLogix-Steuerung kann über eine serielle oder eine USB-Verbindung, ein EtherNet-Modul oder ein ControlNet-Modul mit der Programmiersoftware RSLogix 5000 verbunden werden.

Die 1756-L6*x*S-Steuerungen verfügen über eine serielle Schnittstelle. Die 1756-L7*x*S-Steuerungen verfügen über einen USB-Anschluss.

Weitere Informationen zur Verwendung von Netzwerkkommunikationsmodulen siehe Weitere Informationen auf Seite 13.

Programmieranforderungen

Die Software RSLogix 5000 ist das Programmierwerkzeug für die Anwendungen der GuardLogix-Steuerung.

Schlagen Sie in Tabelle 7 nach, um festzustellen, welche Software-Versionen Sie mindestens für Ihre GuardLogix-Steuerungen benötigen. Die Software RSLogix 5000, Version 15, unterstützt Safety Integrity Level (SIL) 3 nicht.

Tabelle 7 – Softwareversionen

Bestellnummer	Version Software RSLogix 5000(1)	Version Software RSLinx® Classic(1)
1756-L61S, 1756-L62S	14	Beliebige Version
1756-L63S	16	
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	20	2.59

(1) Diese Version oder höher.

Sicherheitsroutinen umfassen Sicherheitsbefehle, die eine Untermenge des Standardbefehlssatzes für Kontaktplanlogik sind, sowie Befehle für Sicherheitsanwendungen. Unter der Sicherheits-Task geplante Programme unterstützen nur Kontaktplanlogik.

Tabelle 8 – Von der RSLogix 5000-Softwareversion unterstützte Funktionen

Funktion	Version 14		Version 16		Version 17		Version 18		Version 19		Version 20	
	Sicherheits-Task	Standard-Task	Sicherheits-Task	Standard-Task	Sicherheits-Task	Standard-Task	Sicherheits-Task	Standard-Task	Sicherheits-Task	Standard-Task	Sicherheits-Task	Standard-Task
Add-On-Befehle				X		X	X	X	X	X	X	X
Alarmmeldungen und Ereignisse				X		X		X		X		X
Steuerungsprotokollierung					X	X	X	X	X	X	X	X
Datenzugriffssteuerung							X	X	X	X	X	X
Routinen der Gerätephase				X		X		X		X		X
Ereignisgesteuerte Tasks				X		X		X		X		X
Firmware Supervisor				X		X	X	X	X	X	X	X
Funktionsblockdiagramme (FBD)				X		X		X		X		X
Integrierte Achssteuerung				X		X		X		X		X
Kontaktplanlogik	X	X	X	X	X	X	X	X	X	X	X	X
Sprachenwechsel					X	X	X	X	X	X	X	X
Speicherkarte							X	X	X	X	X	X
Online-Import und -Export von Programmkomponenten						X		X		X		X
Routinen in sequenzieller Ablaufsprache (SFC)				X		X		X		X		X
Strukturierter Text				X		X		X		X		X
Unicast-Verbindungen für produzierte und konsumierte Sicherheits-Tags									X	X	X	X
Unicast-Verbindungen für Sicherheits-E/A-Module auf EtherNet/IP-Netzwerken											X	X

Informationen zur Verwendung dieser Funktionen finden Sie in Publikation 1756-PM001, „Logix5000 Controllers Common Procedures Programming Manual“, in den im Abschnitt Weitere Informationen auf Seite 13 genannten Publikationen und in der Online-Hilfe zur Software RSLogix 5000.

Notizen:

Installation der Steuerung

Vorsichtsmaßnahmen

Lesen und befolgen Sie diese Vorsichtsmaßnahmen beim Einsatz der Ausrüstung.

Informationen über Umgebung und Gehäuse

ACHTUNG: Dieses Gerät wurde für den Einsatz in einer industriellen Umgebung mit einer Verschmutzung des Grades 2, in Anwendungen mit Überspannungskategorie II (gemäß IEC-Publikation 60664-1) und in Höhen von bis zu 2000 m ohne Minderung der Betriebswerte entwickelt.

Gemäß IEC/CISPR-Publikation 11 entspricht dieses Produkt einem industriellen Gerät der Gruppe 1, Klasse A. Bei Nichtbeachtung der entsprechenden Vorsichtsmaßnahmen kann die elektromagnetische Verträglichkeit in Wohnbereichen und anderen Umgebungen aufgrund von leitungsgeführten und abgestrahlten Störungen eventuell nicht gewährleistet werden.

Dieses Gerät wird als „offenes" Gerät geliefert. Es muss in ein Gehäuse eingebaut werden, das für diese speziellen Umgebungsbedingungen zugelassen ist und den Zugriff auf leitfähige Teile und damit das Risiko von Verletzungen verhindert. Das Gehäuse muss über geeignete flammhemmende Eigenschaften verfügen, um die Ausbreitung von Flammen zu verhindern oder zu minimieren, und dabei die Flammenausbreitungsklassifizierung 5VA erfüllen. Sofern es nicht aus Metall besteht, muss das Gehäuse für die Anwendung genehmigt werden. Das Innere des Gehäuses darf nur unter Zuhilfenahme eines Werkzeugs zugänglich sein. Nachfolgende Abschnitte dieser Publikation können zusätzliche Informationen bezüglich der spezifischen Gehäuseschutzklassen enthalten, die erforderlich sind, um bestimmte Produktsicherheits-Zertifizierungen einzuhalten.

Lesen Sie zusätzlich zu dieser Publikation auch folgende Publikationen:

- Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Publikation 1770-4.1, für zusätzliche Installationsanforderungen
- NEMA-Norm 250 und IEC 60529, sofern zutreffend, für Erklärungen zur Schutzklasse der verschiedenen Gehäuse

Programmierbare Elektroniksysteme (PES)

ACHTUNG: Personal, das für die Anwendung sicherheitsrelevanter programmierbarer Elektroniksysteme (PES) verantwortlich ist, muss mit den Sicherheitsanforderungen bei der Anwendung des Systems vertraut sein und für die Verwendung des Systems geschult sein.

Ziehen und Stecken unter Spannung

WARNUNG: Wenn Sie das Modul bei aktivierter Backplane einsetzen oder entfernen, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden.

Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten. Wiederholte elektrische Lichtbogenbildung führt an den Kontakten des Moduls und des entsprechenden Anschlusses zu übermäßigem Verschleiß. Verschlissene Kontakte können einen elektrischen Widerstand verursachen und den Modulbetrieb beeinträchtigen.

Zulassung für explosionsgefährdete Standorte – Nordamerika

The following information applies when operating this equipment in hazardous locations:	**Informations sur l'utilisation de cet équipement en environnements dangereux:**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Les produits marqués « CL I, DIV 2, GP A, B, C, D » ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**AVERTISSEMENT :** RISQUE D'EXPLOSION • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

Die folgenden Informationen gelten, wenn dieses Gerät an explosionsgefährdeten Standorten eingesetzt wird:

Produkte, die mit „CL I, DIV 2, GP A, B, C, D“ gekennzeichnet sind, eignen sich nur für den Einsatz an explosionsgefährdeten Standorten der Klasse I, Division 2, Gruppe A, B, C, D, und an nicht explosionsgefährdeten Standorten. Bei allen Produkten ist auf dem Typenschild der Temperaturcode für den explosionsgefährdeten Standort angegeben. Werden Produkte innerhalb eines Systems kombiniert, kann anhand des ungünstigsten Temperaturcodes (niedrigste „T“-Zahl) der Temperaturcode für das gesamte System bestimmt werden. Kombinationen der Geräte in Ihrem System müssen bei der Installation durch die für Sie zuständige Behörde überprüft werden.

WARNUNG: EXPLOSIONSGEFAHR

- Geräte dürfen erst dann vom System getrennt werden, wenn die Stromversorgung unterbrochen wurde oder wenn es sich um einen bekanntermaßen nicht explosionsgefährdeten Bereich handelt.
- Verbindungen zu den Geräten dürfen erst dann getrennt werden, wenn die Stromversorgung unterbrochen wurde oder wenn es sich um einen bekanntermaßen nicht explosionsgefährdeten Bereich handelt. Sichern Sie alle externen Verbindungen zu diesem Gerät mit Schrauben, Schiebeverriegelungen, Gewindeanschlüssen oder anderen Vorrichtungen, die mit diesem Produkt geliefert werden.
- Ein Austausch von Komponenten kann die Eignung für Klasse I, Division 2, beeinträchtigen.
- Falls das Produkt Batterien enthält, dürfen diese nur in einem Bereich ausgetauscht werden, der bekanntermaßen nicht explosionsgefährdet ist.

Zulassung für explosionsgefährdete Standorte Europa

Wenn das Produkt die Ex-Kennzeichnung trägt, gilt Folgendes.

Dieses Gerät ist für die Verwendung an explosionsgefährdeten Standorten gemäß der EU-Richtlinie 94/9/EG vorgesehen und wurde als konform mit den grundlegenden Gesundheits- und Sicherheitsanforderungen hinsichtlich des Designs und Aufbaus von Geräten der Kategorie 3 bewertet, die für die Verwendung an potenziell explosionsgefährdeten Standorten der Zone 2 gemäß Anhang II dieser Richtlinie vorgesehen sind.

Die Übereinstimmung mit den grundlegenden Gesundheits- und Sicherheitsanforderungen wurde durch die Konformität mit EN 60079-15 und EN 60079-0 versichert.

ACHTUNG: Dieses Gerät darf nicht direktem Sonnenlicht oder anderen Quellen mit UV-Strahlung ausgesetzt werden.

WARNUNG:

- Dieses Gerät muss in einem Gehäuse installiert werden, das mindestens der Schutzart IP54 entspricht, wenn das Gerät in Umgebungen der Zone 2 eingesetzt wird.
- Dieses Gerät muss innerhalb der von Rockwell Automation angegebenen Leistungsbereiche verwendet werden.
- Dieses Gerät darf nur mit ATEX-zertifizierten Backplanes von Rockwell Automation verwendet werden.
- Sichern Sie alle externen Verbindungen zu diesem Gerät mit Schrauben, Schiebeverriegelungen, Gewindeanschlüssen oder anderen Vorrichtungen, die mit diesem Produkt geliefert werden.
- Geräte dürfen erst dann vom System getrennt werden, wenn die Stromversorgung unterbrochen wurde oder wenn es sich um einen bekanntermaßen nicht explosionsgefährdeten Bereich handelt.

Verhindern elektrostatischer Entladung

ACHTUNG: Dieses Gerät ist empfindlich gegen elektrostatische Entladung, die interne Schäden verursachen und die normale Funktionsweise beeinträchtigen kann. Befolgen Sie beim Umgang mit diesem Gerät die folgenden Richtlinien:

- Berühren Sie einen geerdeten Gegenstand, um eventuelle elektrische Ladung abzuleiten.
- Tragen Sie ein zugelassenes Erdungsband am Handgelenk.
- Berühren Sie keine Anschlüsse oder Stifte auf den Komponentenplatinen.
- Berühren Sie keine Schaltkreiskomponenten im Innern des Geräts.
- Verwenden Sie möglichst einen vor statischen Entladungen sicheren Arbeitsplatz.
- Lagern Sie das Gerät in einer geeigneten antistatischen Verpackung, wenn Sie es nicht verwenden.

Sicherstellen der Verfügbarkeit aller Komponenten

Stellen Sie sicher, dass Sie über alle benötigten Komponenten verfügen, bevor Sie mit der Arbeit beginnen.

WICHTIG Sie müssen eine Primärsteuerung **und** einen Sicherheitspartner verwenden, um SIL 3/PLe zu erreichen.

1756-L6*x*S-Steuerungen

Ein 1747-KY-Schlüssel und eine 1756-BA2-Batterie sind im Lieferumfang der 1756-L6*x*S-Steuerung enthalten, während der 1756-LSP-Sicherheitspartner mit einer 1756-BA2-Batterie ausgeliefert wird.

Um ein Gerät (z. B. einen Computer) an die serielle Schnittstelle der Steuerung anzuschließen, verwenden Sie ein serielles Kabel der Serie 1756-CP3.

Als nichtflüchtigen Speicher können Sie eine CompactFlash-Karte 1784-CF128 mit den 1756-L6*x*S GuardLogix-Steuerungen ab Firmwareversion 18 verwenden.

1756-L7*x*S-Steuerungen

Diese Teile sind im Lieferumgang von Primärsteuerung und Sicherheitspartner enthalten.

Bestellnummer	Beschreibung	Im Lieferumfang enthalten
1756-L71S 1756-L72S 1756-L73S	Primärsteuerung	• 1756-ESMCAP – Kondensator-basiertes Energiespeichermodul (ESM) • 1784-SD1 – SD-Speicherkarte, 1 GB • 1747-KY – Schlüssel
1756-L7SP	Sicherheitspartner	• 1756-SPESMNSE – Energiespeichermodul (ESM)
1756-L73SXT	Für extreme Temperaturen ausgelegte Primärsteuerung	• 1756-ESMCAPXT – Kondensator-basiertes Energiespeichermodul (ESM) • 1747-KY – Schlüssel
1756-L7SPXT	Für extreme Temperaturen ausgelegter Sicherheitspartner	• 1756-SPESMNSEXT – Kondensator-basiertes Energiespeichermodul (ESM)

Die folgende Ausrüstung kann optional eingesetzt werden.

Anforderung der Anwendung	Zu verwendendes Teil
Nichtflüchtiger Speicher	1784-SD1 (1 GB) oder 1784-SD2 (2 GB)
Abbau der gespeicherten Restenergie des installierten ESM auf 200 µJoule oder weniger, bevor es in Ihre Anwendung integriert oder aus ihr ausgebaut werden kann(1)	1756-ESMNSE für die Primärsteuerung 1756-SPESMNSE für den Sicherheitspartner(2) Dieses ESM verfügt über keine Backupleistung für die Uhrzeit. Zudem können Sie dieses ESM nur mit der Steuerung 1756-L73S (8 MB) oder mit einer Steuerung mit kleinerem Speicher verwenden.
Absicherung der Steuerung durch das ESM, das die Verwendung der USB-Verbindung und der SD-Karte verhindert(1)	1756-ESMNRM für die Primärsteuerung 1756-SPESMNRM für den Sicherheitspartner(3) Dieses ESM bietet Ihrer Anwendung verbesserte Sicherheit.

(1) Informationen zur Haltezeit der ESMs finden Sie im Abschnitt Abschätzen der ESM-Unterstützung für die Uhrzeit auf Seite 128.

(2) Für den Einsatz bei extremen Temperaturen ist 1756-ESMNSEXT für die Primärsteuerung und 1756-SPESMNSEXT für den Sicherheitspartner einzusetzen.

(3) Für den Einsatz bei extremen Temperaturen ist 1756-ESMNRMXT für die Primärsteuerung und 1756-SPESMNRMXT für den Sicherheitspartner einzusetzen.

Installieren eines Chassis und eines Netzteils

Sie müssen ein Chassis und ein Netzteil installieren, bevor Sie eine Steuerung einbauen.

1. Installieren Sie ein ControlLogix-Chassis gemäß der entsprechenden Installationsanleitung.

Bestellnummer	Verfügbare Steckplätze	Serie	Siehe Installationsanleitung
1756-A4	4	B	1756-IN005
1756-A7	7		
1756-A10	10		
1756-A13	13		
1756-A17	17		
1756-A4LXT	4	B	
1756-A5XT	5	B	
1756-A7XT	7	B	
1756-A7LXT	7	B	

Steuerungen für den Einsatz unter extremen Umgebungsbedingungen (XT) benötigen ein XT-Chassis.

2. Installieren Sie ein ControlLogix-Netzteil gemäß der entsprechenden Installationsanleitung.

Bestellnummer	Beschreibung	Serie	Siehe Installationsanleitung
1756-PA72	Netzteil, AC	C	1756-IN005
1756-PB72	Netzteil, DC		
1756-PA75	Netzteil, AC	B	
1756-PB75	Netzteil, DC		
1756-PAXT	XT-Netzteil, AC	B	
1756-PBXT	XT-Netzteil, DC		

Steuerungen für den Einsatz unter extremen Umgebungsbedingungen (XT) erfordern ein XT-Netzteil.

Anschließen der Batterie (nur 1756-L6*x*S-Steuerungen)

Die 1756-L6*x*S-Steuerungen und der 1756-LSP-Sicherheitspartner enthalten eine Lithiumbatterie, die während der Lebensdauer des Produktes ausgetauscht werden muss.

WARNUNG: Beim Anschließen oder Trennen der Batterie kann es zur Bildung eines elektrischen Lichtbogens kommen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden. Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

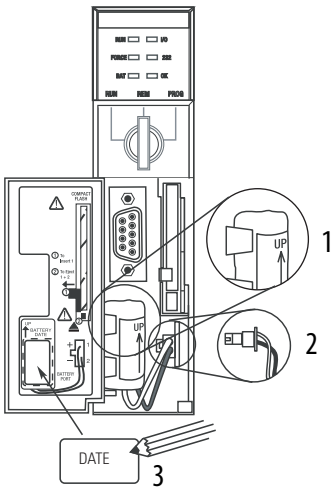
Informationen zur Sicherheit bei der Handhabung von Lithiumbatterien sowie zur Handhabung und Entsorgung von undichten Batterien finden Sie in den Richtlinien zur Handhabung von Lithiumbatterien, Publikation AG 5-4.

Schließen Sie eine Batterie an, um sicherzustellen, dass die im Speicher der Steuerung enthaltenen Daten nicht verloren gehen, wenn die Betriebsspannung der Steuerung ausgeschaltet wird. Befolgen Sie die nachstehend beschriebenen Schritte für die 1756-L6*x*S-Steuerung und den 1756-LSP-Sicherheitspartner.

WICHTIG Schließen Sie nur Batterien des Typs 1756-BA2 an die Steuerung an. Bei Verwendung anderer Batterien kann die Steuerung beschädigt werden.

Gehen Sie wie im Folgenden beschrieben vor, um eine neue 1756-BA2-Batterie zu installieren.

1. Installieren Sie die Batterie wie dargestellt.
2. Schließen Sie die Batterie an:
   + Rot
   – Schwarz
3. Schreiben Sie das Installationsdatum der Batterie auf das Etikett der Batterie und befestigen Sie dieses auf der Innenseite der Steuerungsabdeckung.



Nähere Informationen zur Wartung der Batterie finden Sie in Anhang B.

Einsetzen der Steuerung in das Chassis

Sie können eine Steuerung bei eingeschalteter Chassisspannungsversorgung und bei laufendem System ein- oder ausbauen.

WARNUNG: Wenn ein Modul bei anliegender Backplane-Spannung installiert bzw. entfernt wird, kann ein elektrischer Lichtbogen auftreten. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden.

Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten. Wiederholte elektrische Lichtbogenbildung führt an den Kontakten des Moduls und des entsprechenden Anschlusses zu übermäßigem Verschleiß. Abgenutzte Kontakte können einen elektrischen Widerstand verursachen und den Steuerungsbetrieb beeinträchtigen.

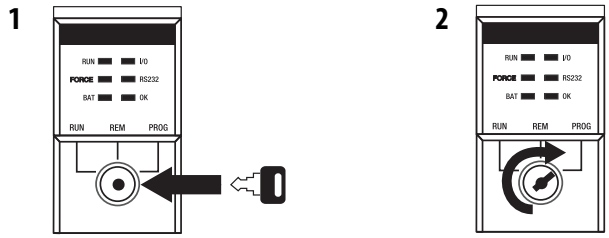
WICHTIG

Bei den 1756-L7*x*S-Steuerungen und den 1756-L7SP-Sicherheitspartnern beginnt das ESM mit dem Ladevorgang, sobald eine der folgenden Situationen eintritt:

- Die Steuerung und das ESM werden in ein an die Stromversorgung angeschlossenes Chassis installiert.
- Das Chassis, das die Steuerung mit dem installierten ESM enthält, wird eingeschaltet.
- Ein ESM wird in eine an die Stromversorgung angeschlossene Steuerung eingebaut.

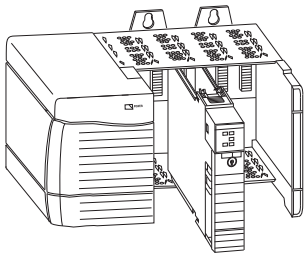
Nach dem Einschalten lädt das ESM etwa zwei Minuten lang, was durch die Meldung „CHRG“ (Aufladen) oder „ESM Charging“ (ESM aufladen) in der Statusanzeige bestätigt wird.

1. Führen Sie den Schlüssel in die Primärsteuerung ein.
2. Drehen Sie den Schlüssel in die Position „PROG“.



Der Sicherheitspartner verfügt über keinen Schlüsselschalter.

3. Richten Sie die Leiterplatte an den oberen und unteren Führungen im Chassis aus.



4. Schieben Sie die Steuerung in das Chassis.

Die Steuerung ist vollständig eingebaut, wenn sie bündig mit dem Netzteil und den anderen installierten Modulen ausgerichtet ist sowie die oberen und unteren Verriegelungen eingerastet sind.

WICHTIG Der Sicherheitspartner muss im Steckplatz unmittelbar rechts neben der Primärsteuerung installiert werden. Führen Sie die oben beschriebenen Schritte 3 und 4 aus, um den Sicherheitspartner zu installieren.

Wenn Sie die Steuerung in das Chassis eingesetzt haben, lesen Sie den Abschnitt Kapitel 9, der weitere Informationen zur Interpretation der Statusleuchten der Primärsteuerung und des Sicherheitspartners enthält.

Einbauen oder Ausbauen einer Speicherkarte

WARNUNG: Wenn Sie die Speicherkarte bei eingeschaltetem System einsetzen oder herausnehmen, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden. Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

ACHTUNG: Wenn Sie **nicht** sicher sind, ob Inhalte auf der Speicherkarte gespeichert sind, drehen Sie **vor** der Installation der Karte den Schlüsselschalter der Steuerung in die Position „PROG“. Abhängig vom Inhalt der Karte kann das Aus- und Einschalten der Versorgungsspannung oder ein Fehler dazu führen, dass die Karte ein anderes Projekt oder Betriebssystem in die Steuerung lädt.

Die 1756-L7*x*S-Steuerungen verwenden Secure Digital (SD)-Karten.
Siehe Seite 32.

Die 1756-L6*x*S-Steuerungen verwenden CompactFlash (CF)-Karten.
Siehe Seite 34.

SD-Karte (1756-L7*x*S-Steuerungen)

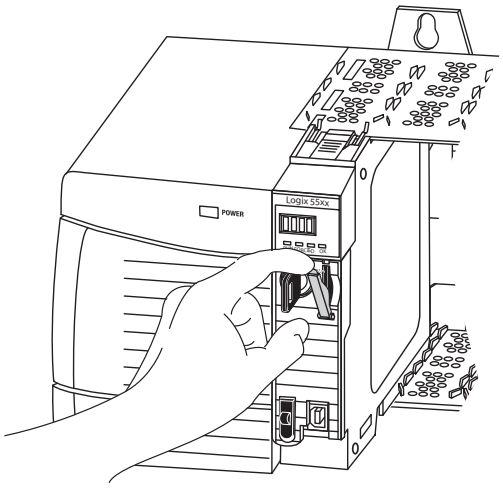
Im Lieferumfang der 1756-L7*x*S-Steuerung ist eine bereits installierte SD-Karte enthalten. Es wird empfohlen, die SD-Karte installiert zu lassen.

Ausbauen der SD-Karte

Gehen Sie wie folgt vor, um die SD-Karte aus der 1756-L7*x*S-Steuerung auszubauen.

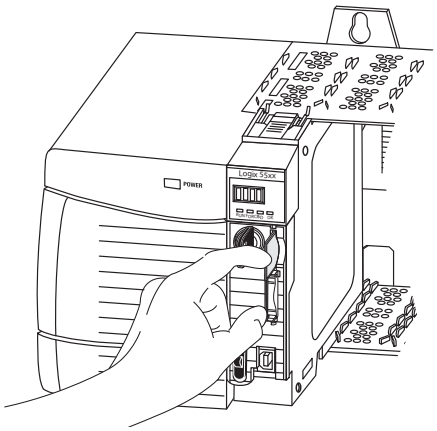
WICHTIG	Stellen Sie vor dem Ausbau der Karte sicher, dass die Statusleuchte der SD-Karte deaktiviert ist und dass die Karte nicht verwendet wird.

1. Drehen Sie die Schlüsselschalter in die Position „PROG“.
2. Öffnen Sie die Klappe, um auf die SD-Karte zugreifen zu können.



32015-M

3. Drücken Sie kurz auf die SD-Karte, um sie auszuwerfen.



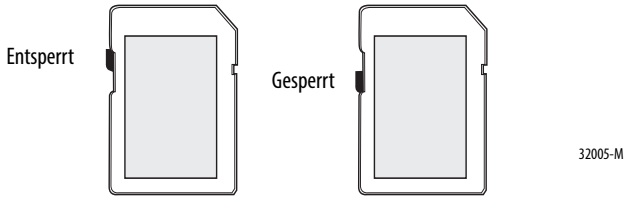
32004-M

4. Nehmen Sie die SD-Karte heraus und schließen Sie die Klappe.

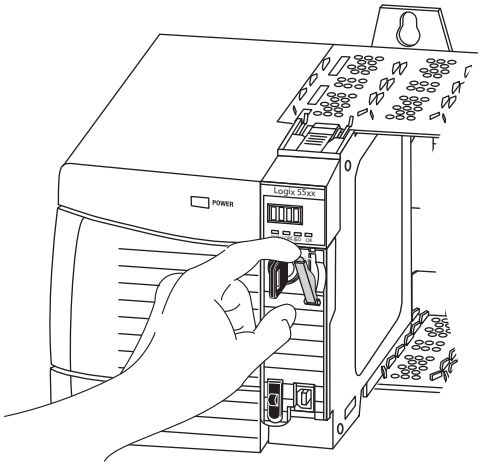
Einbauen der SD-Karte

Gehen Sie wie folgt vor, um die SD-Karte in die 1756-L7*x*S-Steuerung einzubauen.

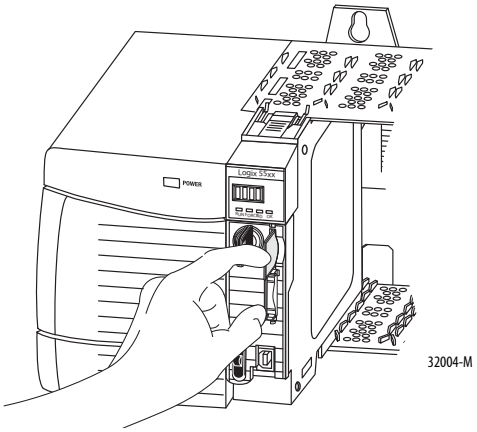
1. Vergewissern Sie sich, dass die SD-Karte, abhängig von Ihren Anforderungen, gesperrt oder entsperrt ist.



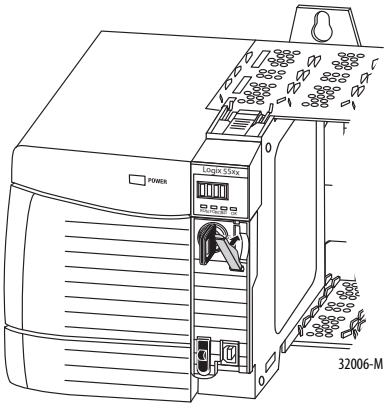
2. Öffnen Sie die Klappe für die SD-Karte.



3. Setzen Sie die SD-Karte in den SD-Kartensteckplatz ein.
4. Drücken Sie die Karte vorsichtig in den Steckplatz, bis sie einrastet.



5. Schließen Sie die Klappe für die SD-Karte.



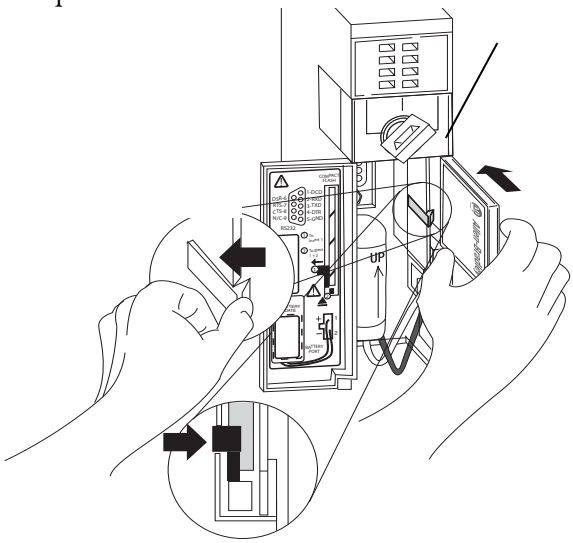
CompactFlash-Karte (1756-L6xS-Steuerungen)

Bei Auslieferung der 1756-L6xS-Steuerungen ist keine CompactFlash-Karte installiert.

Einbauen der CF-Karte

Gehen Sie wie folgt vor, um die Speicherkarte einzubauen.

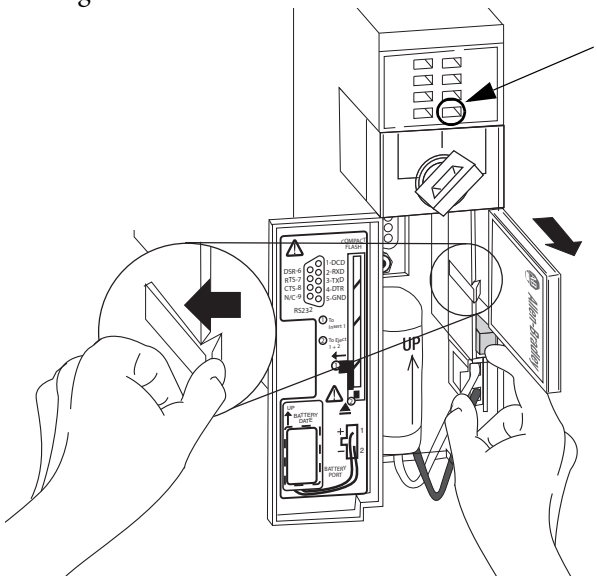
1. Drehen Sie die Schlüsselschalter in die Position „PROG“.
2. Öffnen Sie die Tür der Steuerung.
3. Drücken Sie die Verriegelung nach links.
4. Setzen Sie die Speicherkarte so ein, dass das A-B-Logo nach links zeigt.
5. Lassen Sie die Verriegelung los, und stellen Sie sicher, dass sie sich über die Speicherkarte schiebt.



Ausbauen der CF-Karte

Gehen Sie wie folgt vor, um die Speicherkarte auszubauen.

1. Wenn die Statusleuchte „OK“ grün blinkt, warten Sie, bis sie dauerhaft grün leuchtet.



2. Öffnen Sie die Tür der Steuerung.
3. Drücken Sie die Verriegelung nach links, und halten Sie sie in dieser Position.
4. Drücken Sie die Auswurftaste, und entfernen Sie die Karte.
5. Lassen Sie die Verriegelung los.

Herstellen einer Kommunikationsverbindung

Die 1756-L7*x*S-Steuerungen verfügen über einen USB-Anschluss. Siehe Anschließen der Workstation an den USB-Anschluss der 1756-L7xS-Steuerung.

Die 1756-L6*x*S-Steuerungen verfügen über eine serielle Schnittstelle. Siehe Anschließen der Workstation an die serielle Schnittstelle der 1756-L6xS-Steuerung auf Seite 38.

Anschließen der Workstation an den USB-Anschluss der 1756-L7*x*S-Steuerung

Die Steuerung ist mit einem USB-Anschluss ausgestattet, der eine Buchse vom Typ B verwendet. Der Anschluss ist USB 2.0-kompatibel und überträgt Daten mit 12 Mbit/s.

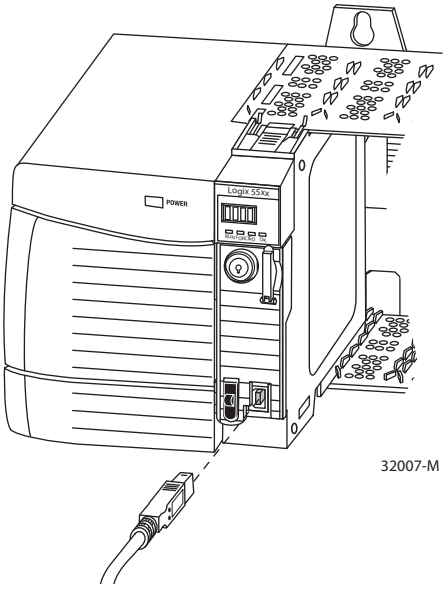
Wenn Sie den USB-Anschluss der Steuerung verwenden möchten, muss auf Ihrer Workstation die Software RSLinx, Version 2.59 oder höher, installiert sein. Verwenden Sie für den Anschluss Ihrer Workstation an den USB-Anschluss ein USB-Kabel. Mit dieser Verbindung können Sie direkt von der Workstation aus Firmware-Upgrades vornehmen und Programme auf die Steuerung herunterladen.

ACHTUNG: Der USB-Anschluss ist ausschließlich für die temporäre, lokale Programmierung vorgesehen und ist für einen dauerhaften Anschluss nicht geeignet.

Das USB-Kabel darf maximal 3,0 m lang sein und keine Hubs aufweisen.

WARNUNG: Verwenden Sie den USB-Anschluss nicht in explosionsgefährdeten Bereichen.

Abbildung 3 – USB-Anschluss



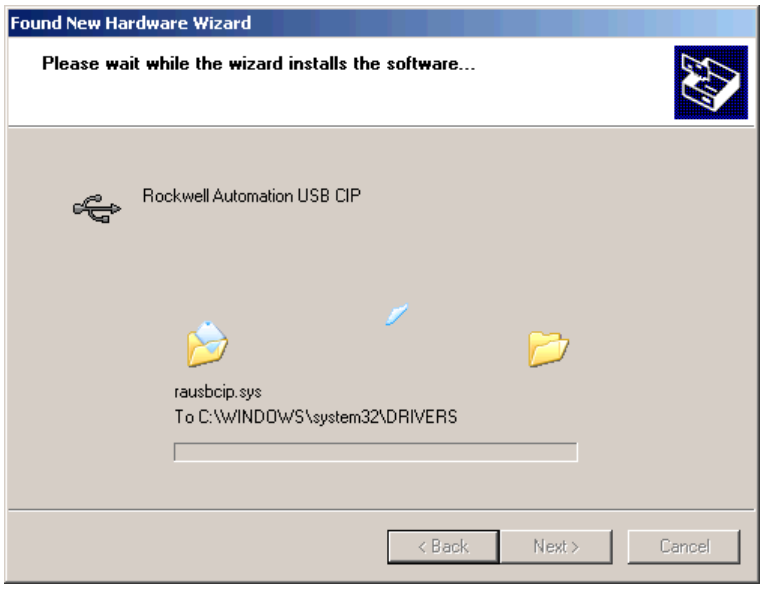
Wenn Sie die Software RSLinx so konfigurieren möchten, dass ein USB-Anschluss verwendet wird, müssen Sie zunächst einen USB-Treiber konfigurieren. Gehen Sie zum Konfigurieren eines USB-Treibers wie folgt vor.

1. Schließen Sie Ihre Steuerung und Workstation mithilfe eines USB-Kabels an.
2. Wählen Sie im Dialogfeld „Found New Hardware Wizard“ (Assistent für das Suchen neuer Hardware) eine der Optionen für Windows-Updates aus und klicken Sie auf „Next“ (Weiter).

TIPP Wenn die Software für den USB-Treiber nicht gefunden werden kann und die Installation abgebrochen wird, vergewissern Sie sich, dass die Software RSLinx Classic, Version 2.59 or höher, installiert ist.

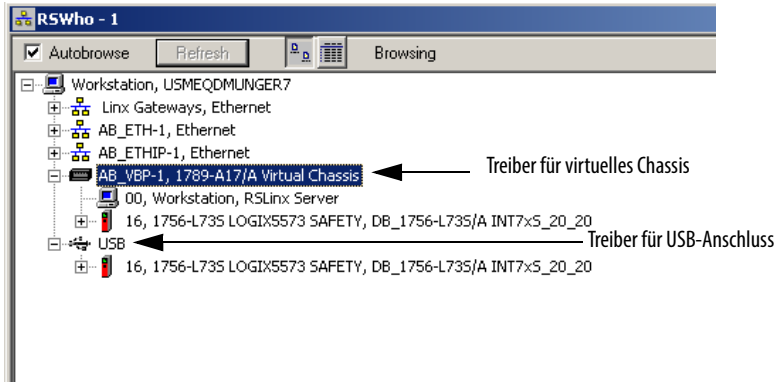
3. Klicken Sie auf „Install the software automatically (Recommended)“ (Software automatisch installieren (empfohlen)) und anschließend auf „Next“ (Weiter).

   Die Software wird installiert.



4. Klicken Sie auf „Finish“ (Fertigstellen), um Ihren USB-Treiber zu konfigurieren.
5. Um in der Software RSLinx direkt zu Ihrer Steuerung zu wechseln, klicken Sie auf das Symbol „RSWho“  .

Im RSLinx-Workstation-Organisator wird Ihre Steuerung unter zwei verschiedenen Treibern angezeigt: unter einem virtuellen Chassis und unter dem USB-Anschluss. Sie können über beide Treiber zu Ihrer Steuerung wechseln.



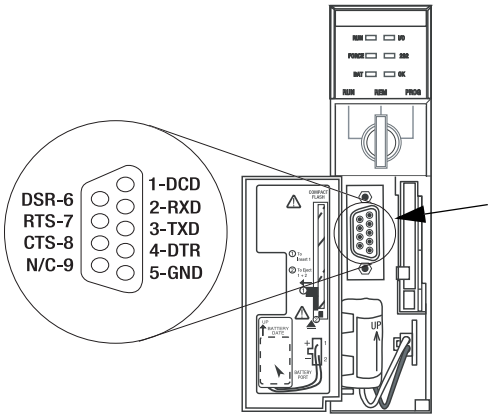
Anschließen der Workstation an die serielle Schnittstelle der 1756-L6xS-Steuerung

WARNUNG: Wenn Sie das serielle Kabel anschließen oder abziehen, solange dieses Modul oder das serielle Gerät am anderen Kabelende mit Strom versorgt wird, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden.

Stellen Sie sicher, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

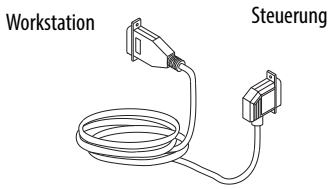
Verwenden Sie die serielle Schnittstelle auf der 1756-L6*x*S-Steuerung für die RS-232-Kommunikation.

Abbildung 4 – Serielle Schnittstelle



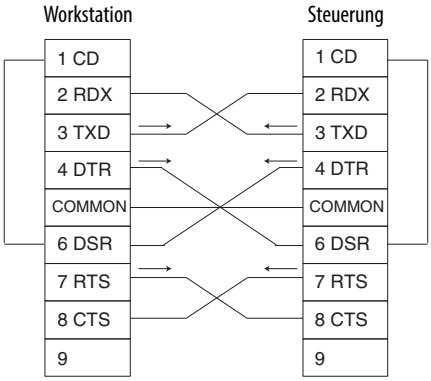
Verwenden Sie eines der folgenden Kabel, um eine Workstation an die serielle Schnittstelle anzuschließen:

- Serielles Kabel 1756-CP3
- Kabel 1747-CP3 aus der SLC-Produktfamilie (wenn Sie dieses Kabel verwenden, lässt sich die Klappe der Steuerung möglicherweise nicht mehr schließen)



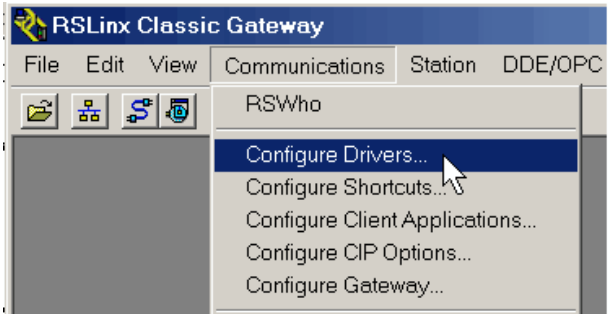
Falls Sie selbst ein Kabel herstellen, beachten Sie dabei bitte folgende Leitlinien.

- Beschränken Sie die Länge auf 15,2 m (50 ft).
- Verdrahten Sie die Anschlüsse wie abgebildet.
- Bringen Sie an beiden Steckverbindern die Abschirmung an.

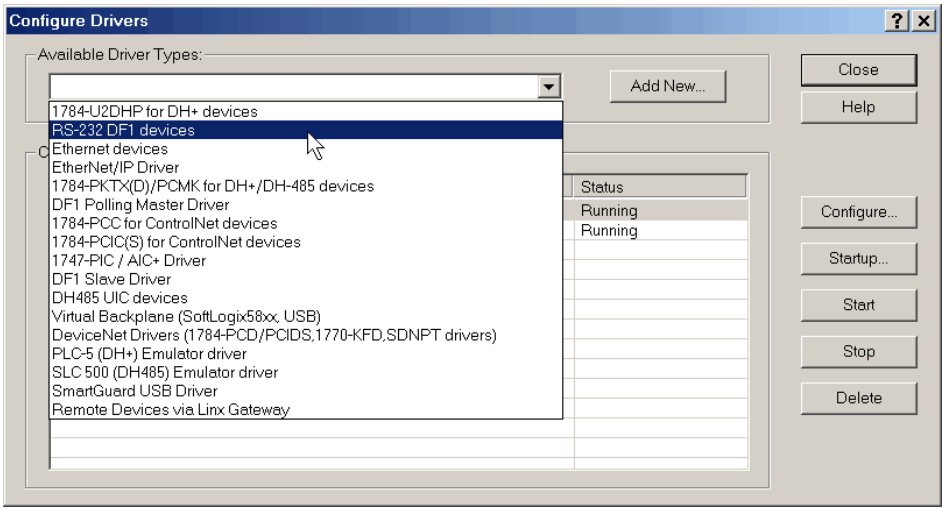


Gehen Sie wie folgt vor, um den RS-232-DF1-Gerätetreiber mithilfe der Software RSLinx für die serielle Kommunikation zu konfigurieren.

1. Wählen Sie in der RSLinx-Software im Menü „Communication“ (Kommunikation) die Option „Configure Drivers“ (Treiber konfigurieren).

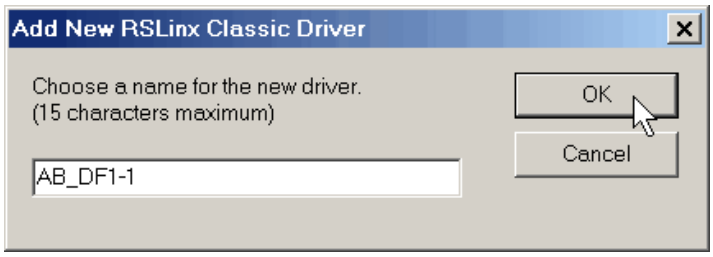


Das Dialogfeld „Configure Drivers“ wird angezeigt.



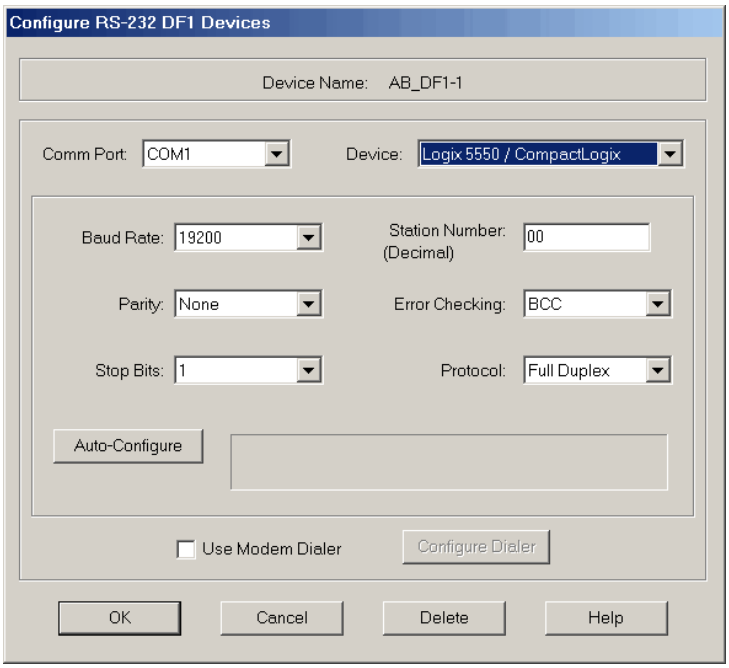
2. Wählen Sie im Pulldown-Menü „Available Driver Types“ (Verfügbare Treibertypen) den Treiber „RS-232 DF1 devices“ (RS-232-DF1-Geräte) aus.
3. Klicken Sie auf „Add New“ (Neue Treiber hinzufügen).

   Es öffnet sich das Dialogfeld „Add New RSLinx Driver“ (Neuen RSLinx-Treiber hinzufügen).



4. Geben Sie den Namen des Treibers ein, und klicken Sie auf „OK“.
5. Legen Sie die Einstellungen für die serielle Schnittstelle fest.
   a. Wählen Sie im Pulldown-Menü „Comm Port“ (Kommunikationsanschluss) die serielle Schnittstelle auf der Workstation aus, an die das Kabel angeschlossen ist.
   b. Wählen Sie im Pulldown-Menü „Device“ (Gerät) die Option „Logix 5550/CompactLogix“.

c. Klicken Sie auf „Auto-Configure“ (Automatisch konfigurieren).



6. Wenn die automatische Konfiguration erfolgreich verlaufen ist, klicken Sie auf „OK“.

   Ist die automatische Konfiguration fehlgeschlagen, prüfen Sie bitte, ob unter „Comm Port“ der korrekte Kommunikationsanschluss ausgewählt wurde.

7. Klicken Sie auf „Close“ (Schließen).

Update der Steuerung

Im Lieferumfang der Steuerungen ist keine Firmware enthalten. Die Steuerungsfirmware ist in einem Paket mit der Programmiersoftware RSLogix 5000 enthalten. Zudem kann die Steuerungsfirmware auch von der Rockwell Automation-Website für technischen Support unter http://www.rockwellautomation.com/support/ heruntergeladen werden.

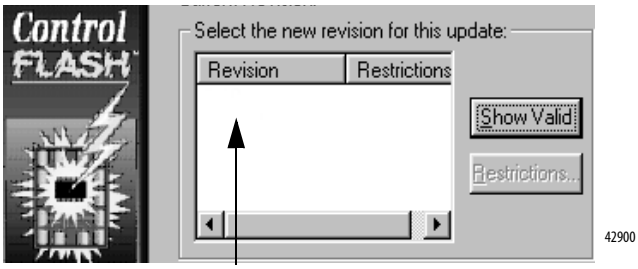
Sie können Ihre Firmware entweder mithilfe der ControlFLASH™-Software, die im Lieferumfang der Software RSLogix 5000 enthalten ist, oder mithilfe der AutoFlash-Funktion von RSLogix 5000 aufrüsten.

Verwenden der Software ControlFLASH zum Aktualisieren der Firmware

Wenn Sie die ControlFLASH-Software ab Version 8 (RSLogix 5000-Software ab Version 18) verwenden, wird der Sicherheitspartner automatisch aktualisiert, sobald die Primärsteuerung aktualisiert wird.

WICHTIG	Für 1756-L7*x*S-Steuerungen gilt: Wenn die SD-Karte gesperrt ist und die Option „Load Image" (Abbilddatei laden) des gespeicherten Projekts auf „On Power Up" (Beim Einschalten) gesetzt ist, wird die Steuerungsfirmware mit diesen Schritten nicht aktualisiert. Stattdessen werden die zuvor gespeicherte Firmware und das zuvor gespeicherte Projekt geladen.

1. Stellen Sie sicher, dass die entsprechende Netzwerkverbindung hergestellt wurde und dass der Netzwerktreiber in der Software RSLinx konfiguriert wurde.
2. Starten Sie die Software ControlFLASH.
3. Klicken Sie auf „Next" (Weiter).
4. Wählen Sie die Bestellnummer Ihrer Steuerung aus und klicken Sie auf „Next" (Weiter).
5. Erweitern Sie den Netzwerktreiber, bis Ihre Steuerung angezeigt wird.
6. Wählen Sie die Steuerung aus und klicken Sie auf „Next" (Weiter).



7. Wählen Sie die Firmwareversion aus, für die Sie das Update ausführen möchten, und klicken Sie auf „Next" (Weiter).
8. Zum Starten des Updates der Steuerung klicken Sie auf „Finish" (Fertigstellen) und anschließend auf „Yes" (Ja).

   Nach dem Update der Steuerung wird im Status-Dialogfeld „Update complete" (Update abgeschlossen) angezeigt.

WICHTIG	Warten Sie, bis die Firmware vollständig aktualisiert wurde, bevor Sie das System aus- und wieder einschalten, und unterbrechen Sie das Update auch nicht auf andere Weise.

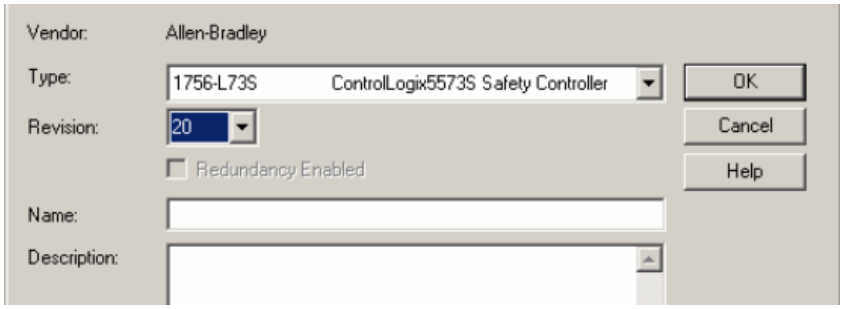
TIPP	Wenn das ControlFLASH-Update der Steuerung unterbrochen wird, kehrt die 1756-L7*x*S-Steuerung wieder zur Boot-Firmware zurück, also zu Firmwareversion 1.*xxx*.

9. Klicken Sie auf „OK".
10. Schließen Sie die Software ControlFLASH.

Verwenden von AutoFlash zum Aktualisieren der Firmware

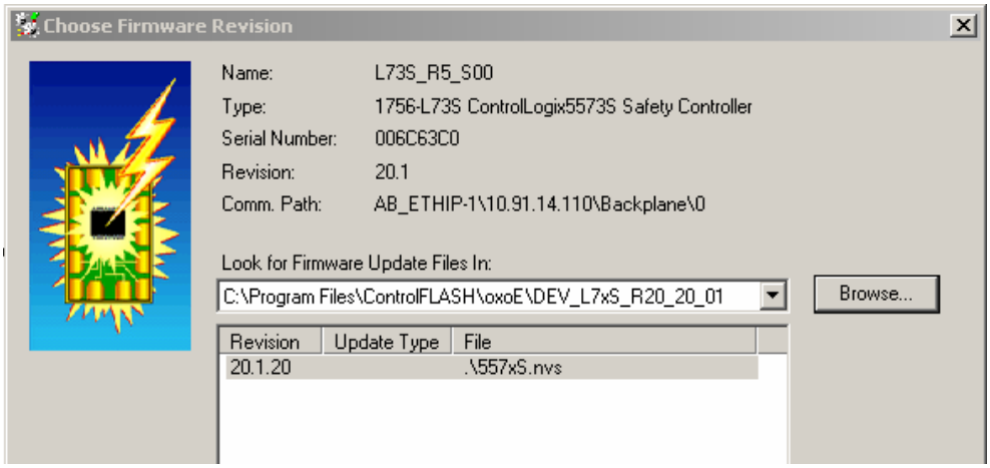
Gehen Sie wie folgt vor, wenn Sie Ihre Steuerungsfirmware mit der AutoFlash-Funktion der Software RSLogix 5000 aktualisieren möchten.

1. Vergewissern Sie sich, dass die entsprechende Netzwerkverbindung hergestellt wurde und dass der Netzwerktreiber in der Software RSLinx konfiguriert wurde.
2. Erstellen Sie mithilfe der Programmiersoftware RSLogix 5000 ein Steuerungsprojekt auf der von Ihnen benötigten Versionsstufe.



3. Klicken Sie auf „RSWho“, um den Steuerungspfad anzugeben.

4. Wählen Sie Ihre Steuerung aus und klicken Sie auf „Update Firmware“ (Firmware aktualisieren).
5. Wählen Sie die Firmwareversion aus, auf die aktualisiert werden soll.



6. Klicken Sie auf „Update“.
7. Klicken Sie auf „Yes“ (Ja).

Warten Sie, bis das Firmware-Update abgeschlossen wurde, ohne den Vorgang zu unterbrechen. Wenn das Firmware-Update abgeschlossen ist, wird das Dialogfeld „Who Active“ (Aktive Geräte) geöffnet. Sie können nun andere Aufgaben in der Software RSLogix 5000 durchführen.

Auswählen der Betriebsart der Steuerung

Bestimmen Sie anhand dieser Tabelle die Betriebsart Ihrer Steuerung.

Tabelle 9 – Betriebsarten der Steuerung

Gewünschte Funktionen	Wählen Sie eine dieser Betriebsarten aus				
	Run	Remote			Program
		Run	Test	Program	
Umschalten der Ausgänge in den von der Logik des Projekts vorgegebenen Zustand	X	X			
Umschalten der Ausgänge in ihren konfigurierten Zustand für den Programm-Modus			X	X	X
Ausführen (Abtasten) von Tasks	X	X	X		
Ändern der Betriebsart der Steuerung über die Anwendung Logix Designer		X	X	X	
Herunterladen eines Projekts		X	X	X	X
Planen eines ControlNet-Netzwerks				X	X
Bearbeiten des Projekts im Onlinezustand		X	X	X	X
Senden von Nachrichten	X	X	X		
Senden und Empfangen von Daten als Reaktion auf eine Nachricht von einer anderen Steuerung	X	X	X	X	X
Produzieren und Konsumieren von Tags	X	X	X	X	X

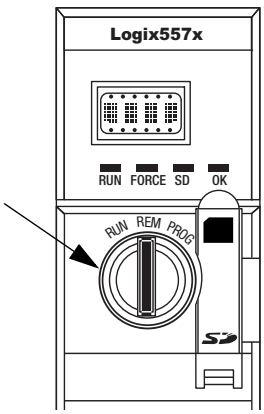
Ändern der Betriebsart über den Schlüsselschalter

Der Schlüsselschalter (Betriebsartschalter) an der Vorderseite der Steuerung kann zum Ändern der Betriebsart der Steuerung verwendet werden. Die folgenden Betriebsarten stehen zur Auswahl:

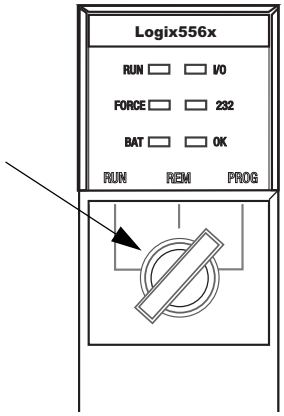
- Programmierung (PROG)
- Dezentral (REM)
- Aktiv (RUN)

Abbildung 5 – Schlüsselschalter

1756-L7*x*S



1756-L6*x*S



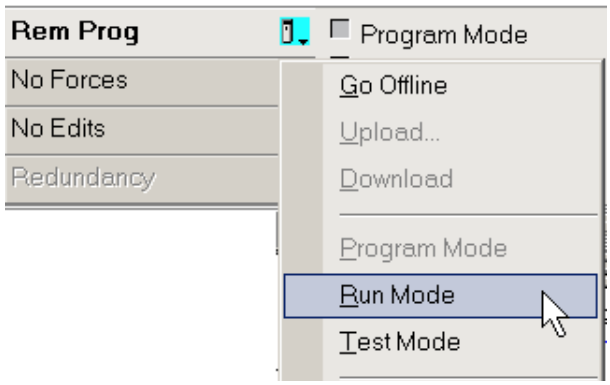
Betriebsartenwechsel über die Software RSLogix 5000

Abhängig von der Steuerungsbetriebsart, die Sie mithilfe des Schlüsselschalters angeben, können Sie die Betriebsart der Steuerung in der Software RSLogix 5000 ändern.

Wenn Sie die Steuerung auf online geschaltet haben und sich der Schlüsselschalter der Steuerung in der Position REM (mittlere Position) befindet, können Sie über das Menü „Controller Status“ (Steuerungsstatus) links oben im Fenster der Software RSLogix 5000 die folgenden Betriebsarten angeben:

- Remote Program
- Remote Run
- Remote Test

Abbildung 6 – Betriebsartenwechsel über die Software RSLogix 5000



TIPP Für dieses Beispiel wird der Schlüsselschalter der Steuerung in die dezentrale Betriebsart (REM-Modus) gebracht. Wenn für den Schlüsselschalter Ihrer Steuerung RUN oder PROG ausgewählt wird, ändern sich die Menüoptionen.

Deinstallieren eines Energiespeichermoduls (ESM)

Die 1756-L7*x*S-Steuerungen werden mit installiertem ESM ausgeliefert.

Steuerung	Bestellnummer des installierten ESM
1756-L7xS, Steuerung	1756-ESMCAP
1756-L7xSXT, Steuerung für extreme Temperatur	1756-ESMCAPXT
1756-L7SP, Sicherheitspartner	1756-SPESMNSE
1756-L7SPXT, Sicherheitspartner für extreme Temperatur	1756-SPESMNSEXT

Beachten Sie vor dem Ausbau des ESM folgende Punkte:

- Wenn die Spannungsversorgung der 1756-L7*x*S-Steuerung unterbrochen wird, entweder weil die Chassisspannung unterbrochen wurde oder die Steuerung aus einem eingeschalteten Chassis ausgebaut wurde, bauen Sie das ESM nicht sofort aus.

  Warten Sie, bis die Statusleuchte „OK“ der Steuerung von grün nach konstant rot wechselt und dann erlischt, bevor Sie das ESM ausbauen.

- Verwenden Sie das Modul 1756-ESMNSE, wenn für Ihre Anwendung das installierte ESM seine gespeicherte Restenergie auf 40 µJoule oder weniger abbauen muss, bevor es in Ihre Anwendung integriert oder aus ihr entfernt werden kann.

- Sobald es installiert ist, können Sie das Modul 1756-ESMNRM nicht aus der 1756-L7xS-Steuerung ausbauen.

WICHTIG Stellen Sie vor dem Ausbau eines ESM Ihr Programm so ein, dass die möglichen Änderungen am Attribut „WallClockTime“ (Uhrzeit) berücksichtigt werden.

Gehen Sie wie folgt vor, um das Modul 1756-ESMCAP(XT), 1756-ESMNSE(XT) oder 1756-SPESMNSE(XT) aus der Steuerung auszubauen.

WARNUNG: Wenn für Ihre Anwendung das ESM seine gespeicherte Restenergie auf 40 µJoule oder weniger abbauen muss, bevor es in Ihre Anwendung integriert oder aus ihr entfernt werden kann, verwenden Sie ausschließlich das Modul 1756-ESMNSE(XT) für die Primärsteuerung und das Modul 1756-SPESMNSE(XT) für den Sicherheitspartner. Gehen Sie in diesem Fall wie folgt vor, bevor Sie das ESM ausbauen.

a. Schalten Sie die Chassisspannung aus.

   Nach dem Ausschalten der Chassisspannung wechselt die Statusleuchte „OK“ der Steuerung von grün nach konstant rot und erlischt dann.

b. Warten Sie **mindestens 20 Minuten**, bis die verbleibende gespeicherte Energie auf 40 µJoule oder weniger abgebaut ist, bevor Sie das ESM ausbauen.

   Es erfolgt keine visuelle Anzeige, wenn die 20 Minuten abgelaufen sind. **Die Zeit muss von Ihnen selbst verfolgt werden**.

WARNUNG: Wenn Sie das Energiespeichermodul einsetzen oder herausnehmen, während die Backplane eingeschaltet ist, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden.

Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten. Wiederholte elektrische Lichtbogenbildung führt an den Kontakten des Moduls und des entsprechenden Anschlusses zu übermäßigem Verschleiß.

1. Ziehen Sie den Schlüssel vom Schlüsselschalter ab.

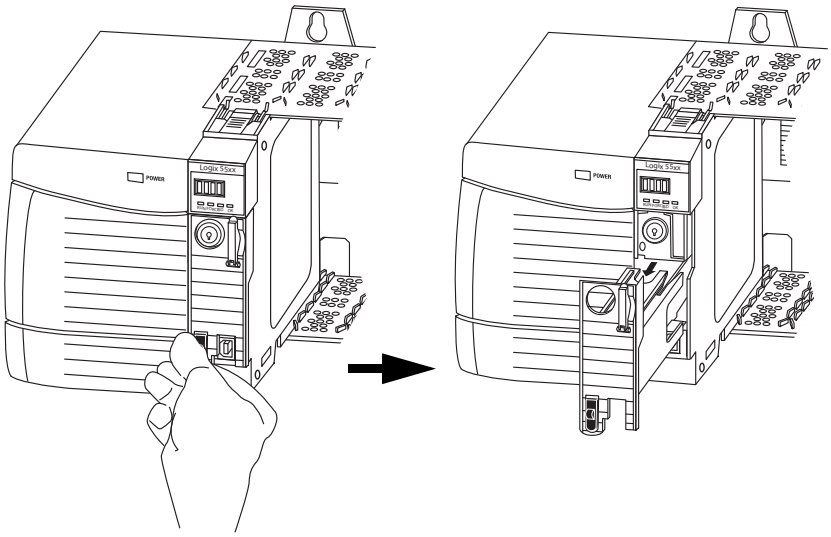
WICHTIG Der nächste Schritt hängt davon ab, welche der folgenden Bedingungen für Ihre Anwendung gilt:

- Wenn Sie das ESM aus einer eingeschalteten 1756-L7*x*S(XT)-Steuerung ausbauen, fahren Sie bitte mit Schritt 2 fort.
- Wenn Sie das ESM aus einer 1756-L7*x*S(XT)-Steuerung ausbauen, die nicht eingeschaltet ist – weil entweder die Chassisspannung ausgeschaltet ist oder die Steuerung aus einem eingeschalteten Chassis ausgebaut wurde – bauen Sie das ESM **nicht sofort** aus.

  Warten Sie, bis die Statusleuchte „OK“ der Steuerung von grün nach konstant rot wechselt und dann erlischt, bevor Sie das ESM ausbauen.

  Wenn die Statusleuchte „OK“ erlischt, fahren Sie mit Schritt 2 fort.

2. Drücken Sie mit Ihrem Daumen auf die schwarze Entriegelung und ziehen Sie das ESM von der Steuerung weg.



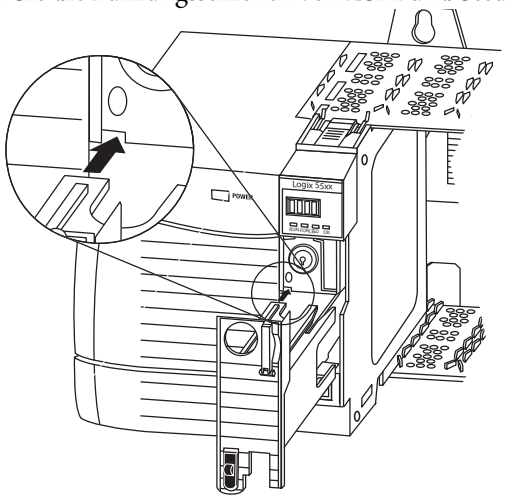
Installieren eines Energiespeichermoduls (ESM)

Tabelle 10 – Kompatible Energiespeichermodule

Bestellnummer	Kompatible ESMs
1756-L7*x*S	1756-ESMCAP, 1756-ESMNSE, 1756-ESMNRM
1756-L7*x*SXT	1756-ESMCAPXT, 1756-ESMNSEXT, 1756-ESMNRMXT
1756-L7SP	1756-SPESMNSE, 1756-SPESMNRM
1756-L7SPXT	1756-SPESMNSEXT, 1756-SPESMNRMXT

Gehen Sie bei der Installation eines ESM wie folgt vor. Für den Sicherheitspartner ist die gleiche Vorgehensweise anzuwenden.

1. Richten Sie die Führungsschienen von ESM und Steuerung aus.



2. Schieben Sie das ESM in das Chassis, bis es einrastet.

ACHTUNG: Um mögliche Schäden am Produkt zu vermeiden, wenn Sie das ESM einsetzen, richten Sie es in der Führungsschiene aus und schieben Sie es mit minimalem Kraftaufwand nach vorne, bis es einrastet.

Das ESM beginnt unmittelbar nach der Installation mit dem Aufladen. Der Ladestatus wird durch eine der folgenden Statusmeldungen angezeigt:

- ESM Charging (ESM lädt auf)
- CHRG (Aufladen)

Nach der Installation des ESM kann es bis zu 15 Sekunden dauern, bis Meldungen zum Ladestatus angezeigt werden.

WICHTIG Warten Sie, bis das ESM aufgeladen ist, bevor Sie die Spannungsversorgung der Steuerung unterbrechen. Das ESM ist vollständig aufgeladen, wenn in der Statusanzeige die Meldung „CHRG“ (Aufladen) oder „ESM charging“ (ESM lädt auf) nicht mehr angezeigt wird.

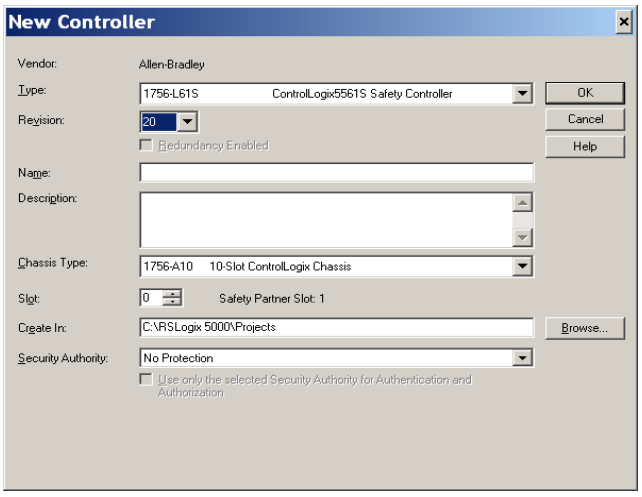
TIPP Überprüfen Sie nach der Installation eines ESM die Attribute des Objekts „WallClockTime“ (Uhrzeit), um sicherzustellen, dass die Uhrzeit der Steuerung korrekt eingestellt ist.

Konfiguration der Steuerung

Erstellen eines Steuerungsprojekts

Zur Konfiguration und Programmierung Ihrer Steuerung verwenden Sie die Software RSLogix 5000, mit der Sie ein Projekt für die Steuerung erstellen und verwalten können.

1. Erstellen Sie ein Projekt mit der Software RSLogix 5000, indem Sie in der Hauptsymbolleiste auf die Schaltfläche „New“ (Neu) klicken.
2. Wählen Sie im Pulldown-Menü „Type“ (Typ) eine GuardLogix-Steuerung aus.
   - 1756-L61S ControlLogix5561S Controller
   - 1756-L62S ControlLogix5562S Controller
   - 1756-L63S ControlLogix5563S Controller
   - 1756-L71S ControlLogix5571S Controller
   - 1756-L72S ControlLogix5572S Controller
   - 1756-L73S ControlLogix5573S Controller



3. Geben Sie die Hauptversion der Firmware für die Steuerung ein.

4. Geben Sie einen Namen für die Steuerung ein.

   Wenn Sie ein Projekt erstellen, ist der Projektname der gleiche wie der Name der Steuerung. Sie können jedoch entweder das Projekt oder die Steuerung umbenennen.

5. Wählen Sie die Chassisgröße.
6. Geben Sie die Steckplatznummer der Steuerung ein.

   Das Dialogfeld „New Controller“ (Neue Steuerung) zeigt die Steckplatzposition des Sicherheitspartners basierend auf der für die Primärsteuerung eingegebenen Steckplatznummer an.

   Falls Sie eine Steckplatznummer für die Primärsteuerung wählen, die keinen Platz für den Sicherheitspartner direkt rechts neben der Primärsteuerung bietet, werden Sie aufgefordert, erneut eine gültige Steckplatznummer einzugeben.

7. Geben Sie den Ordner an, in dem das Sicherheitssteuerungsprojekt gespeichert werden soll.
8. Wählen Sie für RSLogix 5000 ab Version 20 eine Security Authority-Option.

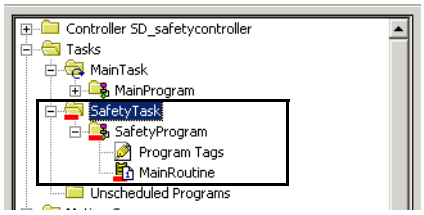
   Ausführliche Informationen zu Sicherheitsfunktionen finden Sie in der Publikation 1756-PM016, Logix5000-Steuerungen – Sicherheit – Programmierhandbuch.

9. Klicken Sie auf „OK“.

Die Software RSLogix 5000 generiert automatisch eine Sicherheits-Task und ein Sicherheitsprogramm.

Eine Hauptroutine in Kontaktplanlogik, „MainRoutine“ genannt, wird ebenfalls innerhalb des Sicherheitsprogramms erstellt.

Abbildung 7 – Sicherheits-Task im Controller Organizer (Steuerungsorganisator)



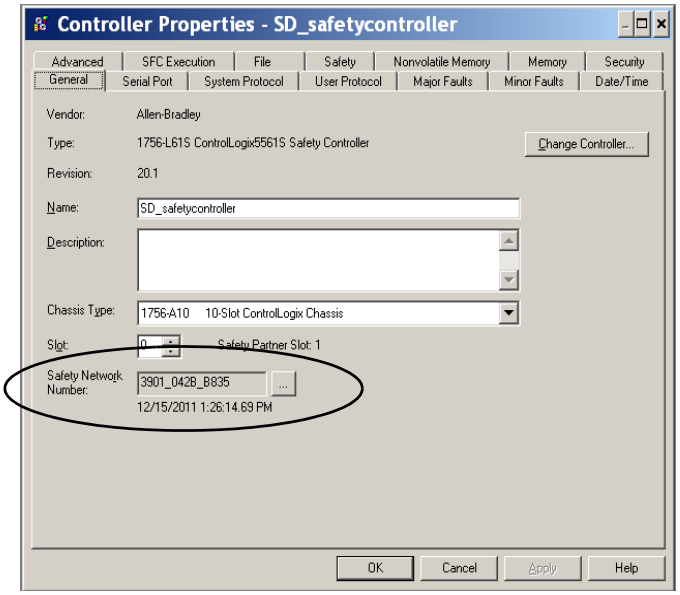
Ein roter Balken unter dem Ordnersymbol unterscheidet die Sicherheitsprogramme und -routinen von Standardkomponenten des Projekts im Controller Organizer von RSLogix 5000.

Wenn ein neues Sicherheitsprojekt angelegt wird, erstellt die Software RSLogix 5000 automatisch auch eine zeitbasierende Sicherheitsnetzwerknummer (SNN).

Diese SNN definiert die lokale Chassis-Backplane als Sicherheitsteilnetz. Sie kann über die Registerkarte „General“ (Allgemein) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) eingesehen und geändert werden.

Für die meisten Anwendungen ist diese automatische, zeitbasierende SNN ausreichend. Es gibt jedoch Fälle, in denen die Eingabe einer bestimmten SNN erforderlich ist.

Abbildung 8 – Sicherheitsnetzwerknummer



TIPP

Sie können das Dialogfeld „Controller Properties“ (Steuerungseigenschaften) verwenden, um die Steuerung von Standard auf Sicherheit oder umgekehrt umzuschalten. Klicken Sie dazu auf die Schaltfläche „Change Controller“ (Steuerung ändern). Standard- und Sicherheitsprojekte werden dadurch jedoch wesentlich beeinflusst.

Ausführliche Informationen zu den Auswirkungen von Änderungen an der Steuerung finden Sie in Anhang C, Wechsel des Steuerungstyps in RSLogix 5000-Projekten.

Tabelle 11 – Weitere Informationen

Quelle	Beschreibung
Kapitel 6, Entwicklung von Sicherheitsanwendungen.	Enthält weitere Informationen zu Sicherheits-Tasks, Sicherheitsprogrammen und Sicherheitsroutinen
Kapitel 4, Kommunikation über Netzwerke	Bietet weitere Informationen zum Verwalten der SNN

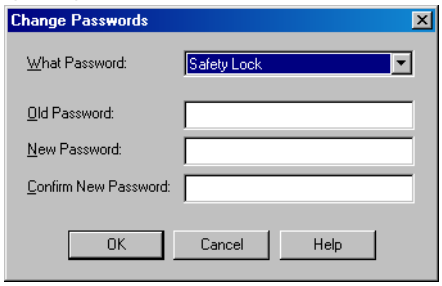
Festlegen von Kennwörtern für die Sicherheitsverriegelung und -entriegelung

Die Sicherheitsverriegelung der Steuerung schützt Sicherheits-Steuerungskomponenten vor Änderungen. Nur Sicherheitskomponenten wie die Sicherheits-Task, die Sicherheitsprogramme, die Sicherheitsroutinen und die Sicherheits-Tags sind davon betroffen. Standardkomponenten sind nicht betroffen. Sie können die Sicherheitsverriegelung oder -entriegelung des Steuerungsprojekts entweder online oder offline durchführen.

Die Funktion zur Sicherheitsverriegelung und -entriegelung verwendet zwei getrennte Kennwörter. Kennwörter sind optional.

Gehen Sie zum Festlegen von Kennwörtern wie folgt vor:

1. Wählen Sie „Tools“ (Extras) > „Safety“ (Sicherheit) > „Change Password“ (Kennwort ändern) aus.
2. Wählen Sie im Pulldown-Menü „What Password“ (Welches Kennwort) entweder „Safety Lock“ (Sicherheitsverriegelung) oder „Safety Unlock“ (Sicherheitsentriegelung) aus.

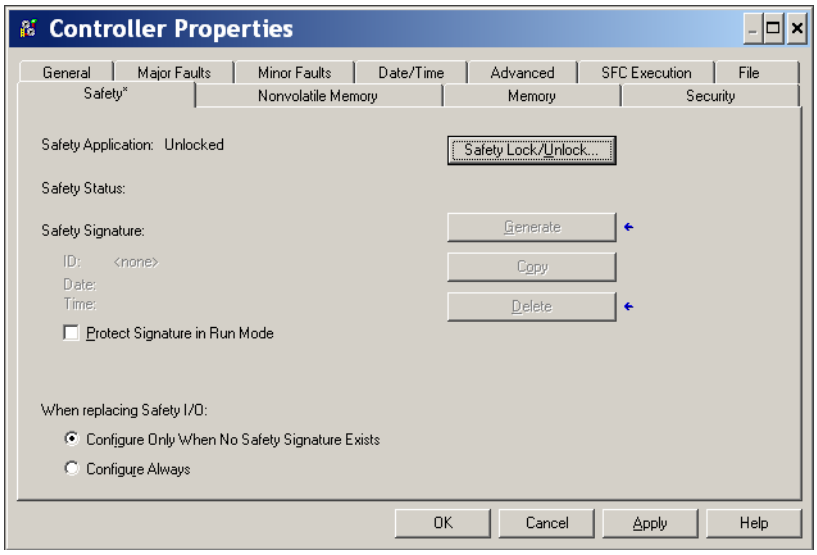


3. Geben Sie das alte Kennwort ein, falls vorhanden.
4. Geben Sie anschließend das neue Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf „OK“.

   Kennwörter können 1 bis 40 Zeichen lang sein und es wird nicht zwischen Klein- und Großbuchstaben unterschieden. Buchstaben, Ziffern und folgende Symbole können verwendet werden: ‘ ~ ! @ # $ % ^ & * ( ) _ + , – = { } | [ ] \ : ; ? / .

Schützen der Sicherheits-Task-Signatur im Run-Modus

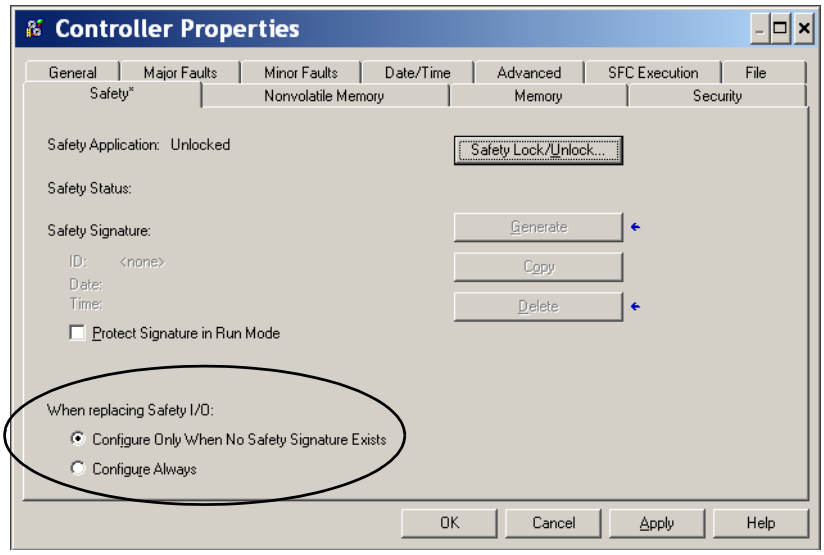
Sie können verhindern, dass die Sicherheits-Task-Signatur erstellt oder gelöscht wird, während sich die Steuerung im Run- oder Remote-Run-Modus befindet. Dies erfolgt unabhängig davon, ob die Sicherheitsanwendung verriegelt oder entriegelt ist, durch Auswählen der Option „Protect Signature in Run Mode“ (Signatur im Run-Modus schützen) auf der Registerkarte „Safety“ (Sicherheit) im Dialogfenster „Controller Properties“ (Steuerungseigenschaften).



Handhaben des Austauschs eines E/A-Moduls

Mithilfe der Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) können Sie definieren, wie die Steuerung den Austausch eines E/A-Moduls im System handhabt. Diese Option legt fest, ob die Steuerung die Sicherheitsnetzwerknummer (SNN) eines E/A-Moduls bestimmt, mit dem sie verbunden ist und für das sie Konfigurationsdaten besitzt, wenn eine Sicherheits-Task-Signatur(1) vorliegt.

Abbildung 9 – Optionen für den Austausch eines E/A-Moduls



ACHTUNG: Aktivieren Sie das Optionsfeld „Configure Always“ (Immer konfigurieren) nur, wenn die Beibehaltung von SIL 3 während des Austauschs und der Funktionstests eines Moduls nicht vom gesamten routbaren CIP Safety-Steuerungssystem abhängt.

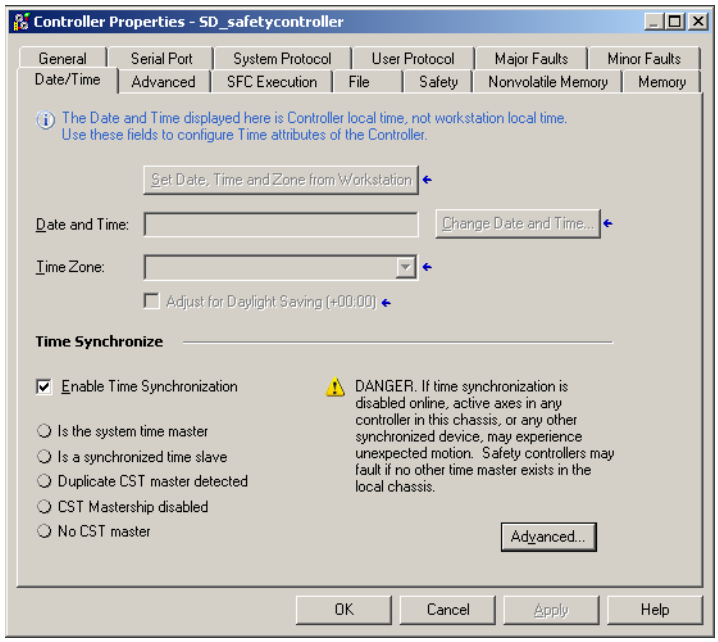
Weitere Informationen siehe Kapitel 5, Hinzufügen, Konfigurieren, Überwachen und Ersetzen von CIP Safety-E/A-Modulen.

Aktivieren der Zeitsynchronisierung

In einem GuardLogix-Steuerungssystem muss ein Gerät im lokalen Chassis als Master für die koordinierte Systemzeit (CST-Master) festgelegt werden. Damit die Steuerung als CST-Master definiert werden kann, müssen Sie im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) auf der Registerkarte „Date/Time“ (Datum/Uhrzeit) die Option „Time Synchronization“ (Zeitsynchronisierung) aktivieren. Mit der Option „Time Synchronization“ (Zeitsynchronisierung) steht ein Standardmechanismus zum Synchronisieren der Uhren in einem Netzwerk mit dezentralen Geräten zur Verfügung.

(1) Die Sicherheits-Task-Signatur ist eine Nummer, die ausschließlich dazu verwendet wird, um Logik, Daten und Konfiguration jedes Projekts zu kennzeichnen und dadurch die Safety Integrity Level (SIL) des Systems zu schützten. Weitere Informationen finden Sie unter Sicherheits-Task-Signatur auf Seite 16 und Erstellen einer Sicherheits-Task-Signatur auf Seite 110.

Abbildung 10 – Registerkarte „Date/Time“ (Datum/Uhrzeit)



Weitere Informationen zur Zeitsynchronisierung finden Sie in der Publikation IA-AT003, Integrated Architecture™ and CIP Sync Configuration Application Solution.

Konfigurieren einer Peer-Sicherheitssteuerung

Sie können eine Peer-Sicherheitssteuerung zum E/A-Konfigurationsordner Ihres Sicherheitsprojekts hinzufügen, um zuzulassen, dass Standard- oder Sicherheits-Tags konsumiert werden. Zum Austausch von Sicherheitsdaten zwischen Peer-Steuerungen produzieren und konsumieren Sie Steuerungsbereichs-Sicherheits-Tags.

Einzelheiten zum Konfigurieren der Peer-Sicherheitssteuerungen sowie zum Produzieren und Konsumieren von Sicherheits-Tags siehe Produzierte/konsumierte Sicherheits-Tags auf Seite 101.

Kommunikation über Netzwerke

Das Sicherheitsnetzwerk

Das CIP Safety-Protokoll ist ein Endknoten-zu-Endknoten-Sicherheitsprotokoll, welches das Routing von CIP Safety-Nachrichten zu und von CIP Safety-Geräten über Bridges, Switches und Router ermöglicht.

Um die hohe Integrität beizubehalten, wenn das Routing über Standard-Bridges, -Switches oder -Router erfolgt, muss jeder Endknoten innerhalb eines routingfähigen CIP Safety-Steuerungssystems eine eindeutige Referenz haben. Diese eindeutige Referenz ist eine Kombination aus Sicherheitsnetzwerknummer (SNN) und der Netzknotenadresse des Netzwerkgeräts.

Verwalten der Sicherheitsnetzwerknummer

Sicherheitsnetzwerknummern (SNN), die Sicherheitsgeräten in einem Netzwerksegment zugeordnet werden, müssen eindeutig sein. Es muss sichergestellt werden, dass eine eindeutige SNN folgenden Elementen zugewiesen wird:

- jedem CIP Safety-Netzwerk, das Sicherheitsgeräte enthält.
- jedem Chassis, das mindestens eine GuardLogix-Steuerung enthält.

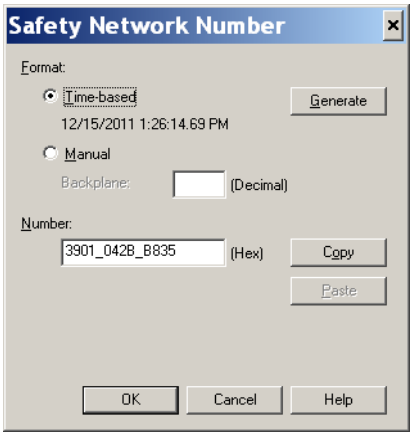
TIPP Mehrere Sicherheitsnetzwerknummern können einem CIP Safety-Teilnetz oder einem ControlBus-Chassis zugeordnet werden, das mehr als ein Sicherheitsgerät enthält. **Aus Gründen der Einfachheit wird jedoch empfohlen, jedem CIP Safety-Teilnetz nur eine eindeutige SNN zuzuweisen.**

Die SNN kann von der Software (zeitbasierend) oder vom Anwender (manuell) zugewiesen sein. Diese beiden Formate einer SNN werden in den nachfolgenden Abschnitten beschrieben.

Zeitbasierende Sicherheitsnetzwerknummer

Wenn das zeitbasierende Format gewählt wird, repräsentiert der generierte SNN-Wert Datum und Uhrzeit der Nummernerstellung, und zwar entsprechend dem PC, auf dem die Konfigurationssoftware ausgeführt wird.

Abbildung 11 – Zeitbasierendes Format



Manuelle Sicherheitsnetzwerknummer

Wird das manuelle Format gewählt, stellt die SNN eingegebene Werte von 1 bis 9999 dezimal dar.

Abbildung 12 – Manuelle Eingabe

Zuordnen der Sicherheitsnetzwerknummer (SNN)

Sie können zulassen, dass die Software RSLogix 5000 eine SNN automatisch zuordnet, oder Sie können die SNN manuell zuweisen.

Automatische Zuweisung

Wenn eine neue Steuerung oder ein neues Modul erstellt wird, wird eine zeitbasierende SNN automatisch über die Konfigurationssoftware zugewiesen. Werden zu einem späteren Zeitpunkt neue Sicherheitsmodule zum gleichen CIP Safety-Netzwerk hinzugefügt, wird ihnen die gleiche SNN zugeordnet, die innerhalb der niedrigsten Adresse auf diesem CIP Safety-Netzwerk definiert ist.

Manuelle Zuweisung

Die manuelle Option ist für routingfähige CIP Safety-Systeme vorgesehen, die nur über wenige Netzwerkteilnetze und zwischengeschaltete Netzwerke verfügen und bei denen die Anwender die SNN in einer logischen, der spezifischen Anwendung entsprechenden Art und Weise verwalten und zuweisen möchten.

Siehe Ändern der Sicherheitsnetzwerknummer (SNN) auf Seite 57.

WICHTIG	Wenn Sie eine SNN manuell zuordnen, vergewissern Sie sich, dass die Systemerweiterung nicht zu einer Verdoppelung der Kombinationen aus SNN und Netzknotenadresse führt.

Automatisch versus manuell

Für die meisten Anwender ist in der Regel die automatische Zuweisung einer SNN ausreichend. Allerdings ist eine manuelle Einstellung der SNN in den folgenden Situationen erforderlich:

- wenn konsumierte Sicherheits-Tags verwendet werden
- wenn das Projekt Sicherheitseingangsdaten von einem Modul konsumiert, dessen Konfiguration von einem anderen Gerät verwaltet wird
- wenn ein Sicherheitsprojekt in eine andere Hardwareinstallation innerhalb des gleichen routingfähigen CIP Safety-Systems kopiert wird

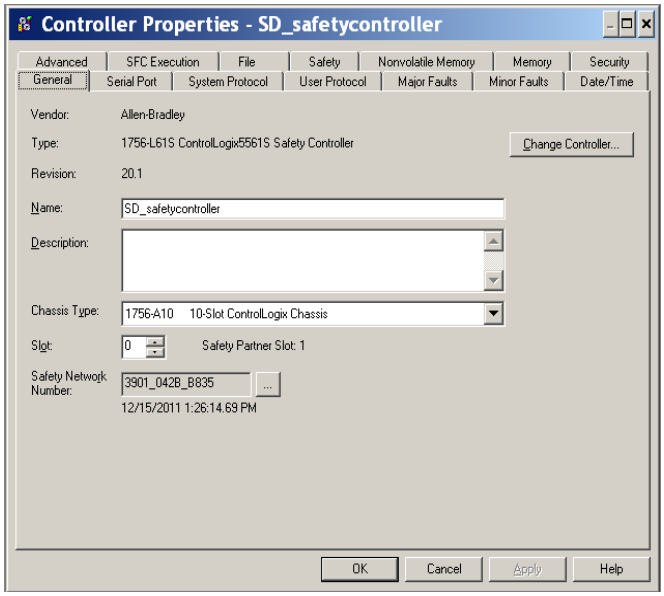
Ändern der Sicherheitsnetzwerknummer (SNN)

Bevor Sie die SNN ändern, müssen Sie folgende Maßnahmen durchführen:

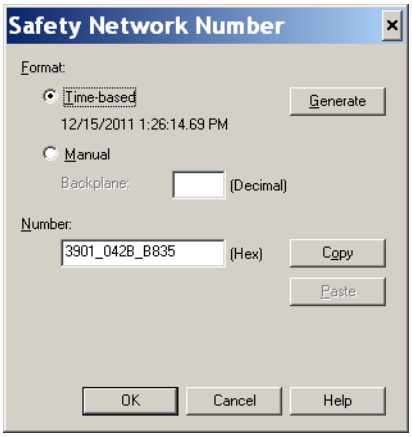
- das Projekt entriegeln, wenn es sicherheitsverriegelt ist.
  Siehe Sicherheitsverriegelung der Steuerung auf Seite 109.
- Die Sicherheits-Task-Signatur löschen, sofern eine solche vorliegt.
  Siehe Löschen der Sicherheits-Task-Signatur auf Seite 112.

Ändern der Sicherheitsnetzwerknummer der Steuerung

1. Klicken Sie im Controller Organizer (Steuerungsorganisator) mit der rechten Maustaste auf die Steuerung und wählen Sie „Properties“ (Eigenschaften) aus.
2. Klicken Sie auf der Registerkarte „General“ (Allgemein) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) auf die Schaltfläche ... rechts neben „Safety Network Number“ (Sicherheitsnetzwerknummer), um das Dialogfeld „Safety Network Number“ zu öffnen.



3. Klicken Sie auf „Time-based“ (Zeitbasierend) und anschließend auf „Generate“ (Generieren).

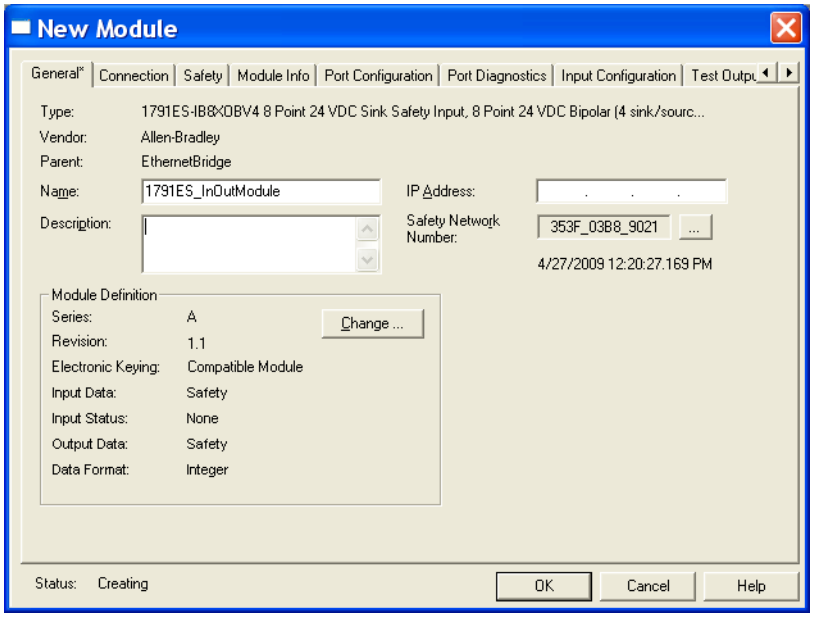


4. Klicken Sie auf „OK“.

Ändern der Sicherheitsnetzwerknummer eines Sicherheits-E/A-Moduls im CIP Safety-Netzwerk

In diesem Beispiel wird ein EtherNet/IP-Netzwerk verwendet.

1. Suchen Sie das erste EtherNet/IP-Kommunikationsmodul im E/A-Konfigurationsverzeichnis.
2. Erweitern Sie die über das EtherNet/IP-Kommunikationsmodul verfügbaren Sicherheits-E/A-Module.
3. Doppelklicken Sie auf das erste Sicherheits-E/A-Modul, um die Registerkarte „General“ (Allgemein) aufzurufen.



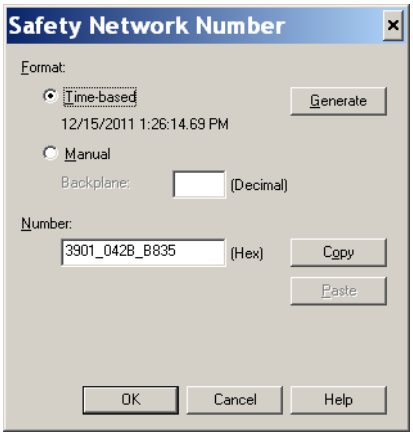
4. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.
5. Wählen Sie „Time-based“ (Zeitbasierend) und klicken Sie auf „Generate“ (Generieren), um eine neue SNN für dieses EtherNet/IP-Netzwerk zu erstellen.
6. Klicken Sie auf „OK“.
7. Klicken Sie auf die Schaltfläche „Copy“ (Kopieren), um die neue SNN in die Windows-Zwischenablage zu kopieren.
8. Öffnen Sie die Registerkarte „General“ (Allgemein) des Dialogfelds „Module Properties“ (Moduleigenschaften) des nächsten Sicherheits-E/A-Moduls unter diesem EtherNet/IP-Modul.
9. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.
10. Wählen Sie „Time-based“ (Zeitbasierend) und klicken Sie auf „Paste“ (Einfügen), um die SNN dieses EtherNet/IP-Netzwerks in dieses Gerät einzufügen.

11. Klicken Sie auf „OK“.
12. Wiederholen Sie die Schritte 8 bis 10 für die verbleibenden Sicherheits-E/A-Module unter diesem EtherNet/IP-Kommunikationsmodul.
13. Wiederholen Sie die Schritte 2 bis 10 für alle verbleibenden Netzwerkkommunikationsmodule im E/A-Konfigurationsverzeichnis.

Kopieren und Einfügen einer Sicherheitsnetzwerknummer (SNN)

Falls eine andere Steuerung die Konfiguration eines Moduls verwaltet, müssen Sie eventuell die SNN aus der diese Konfiguration verwaltenden Steuerung kopieren und in das Modul in Ihrem E/A-Konfigurationsverzeichnis einfügen.

1. Öffnen Sie im Konfigurationsverwalter des Moduls über das Software-Konfigurationswerkzeug das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) für das Modul.



2. Klicken Sie auf „Copy“ (Kopieren).
3. Klicken Sie auf die Registerkarte „General“ (Allgemein) im Dialogfeld „Module Properties“ (Moduleigenschaften) des E/A-Moduls im E/A-Konfigurationsverzeichnis des Projekts der konsumierenden Steuerung.
   Diese konsumierende Steuerung ist nicht der Konfigurationsverwalter.
4. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.
5. Klicken Sie auf „Paste“ (Einfügen).
6. Klicken Sie auf „OK“.

EtherNet/IP-Kommunikation

Für die EtherNet/IP-Netzwerkkommunikation in einem GuardLogix-System stehen mehrere Module zur Auswahl.Für die CIP Safety-Kommunikation – einschließlich Sicherheits-E/A-Modul-Steuerung – wählen Sie eines der in Tabelle 12 aufgeführten Module aus, mit Ausnahme des Moduls 1756-EWEB, das die CIP Safety-Kommunikation nicht unterstützt.

Tabelle 12 enthält eine Auflistung der Module und ihrer primären Leistungsmerkmale.

Tabelle 12 – EtherNet/IP-Kommunikationsmodule und ihre Leistungsmerkmale

Modul	Leistungsmerkmale
1756-ENBT	• Anschluss von Steuerungen an E/A-Module (erfordert einen Adapter für verteilte E/A). • Kommunikation mit anderen EtherNet/IP-Geräten (Nachrichten). • Dient als Übertragungspfad für die gemeinsame Nutzung von Daten zwischen Logix5000-Steuerungen (Produzieren/Konsumieren). • Überbrückung von EtherNet/IP-Netzknoten zur Weiterleitung von Nachrichten an Geräte in anderen Netzwerken.
1756-EN2T	• Ausführung derselben Funktionen wie das Modul 1756-ENBT mit der doppelten Kapazität für anspruchsvollere Anwendungen. • Bereitstellung einer vorübergehenden Konfigurationsverbindung über den USB-Anschluss. • Schnelles Konfigurieren der IP-Adressen mithilfe von Drehschaltern.
1756-EN2F	• Ausführen derselben Funktionen wie das Modul 1756-EN2T. • Anschließen von Glasfasermedien über einen LWL-Anschluss am Modul.
1756-EN2TXT	• Ausführen derselben Funktionen wie das Modul 1756-EN2T. • Betrieb unter extremen Umgebungsbedingungen bei Temperaturen von –25 bis +70 °C.
1756-EN2TR	• Ausführen derselben Funktionen wie das Modul 1756-EN2T. • Unterstützung der Kommunikation in einer Ringtopologie für ein DLR-Ringnetzwerk (Device Level Ring) mit Einzelfehlertoleranz.
1756-EN3TR	• Ausführen derselben Funktionen wie das Modul 1756-EN2TR. • Drei Anschlüsse für DLR-Verbindung.
1756-EWEB	• Bereitstellung anpassbarer Webseiten für den externen Zugriff auf Steuerungsinformationen. • Bereitstellung von dezentralem Zugriff über einen Internet-Browser auf Tags in einer lokalen ControlLogix-Steuerung. • Kommunikation mit anderen EtherNet/IP-Geräten (Nachrichten). • Überbrückung von EtherNet/IP-Netzknoten zur Weiterleitung von Nachrichten an Geräte in anderen Netzwerken. • Unterstützung von Ethernet-Geräten, die nicht auf EtherNet/IP mit einer Socket-Schnittstelle basieren. Dieses Modul bietet keine Unterstützung für E/A oder produzierte/konsumierte Tags und unterstützt auch nicht die CIP Safety-Kommunikation.

EtherNet/IP-Kommunikationsmodule bieten folgende Leistungsmerkmale:

- Unterstützung von Messaging, produzierten/konsumierten Tags, Bedienerschnittstellen und verteilten E/A.
- Möglichkeit zur Verkapselung von Nachrichten im TCP/UDP/IP-Standardprotokoll
- Eine gemeinsame Applikationsebene mit ControlNet- und DeviceNet-Netzwerken
- Netzwerkverbindungen über ein RJ45-Kabel, Kategorie 5, nicht abgeschirmtes Twisted-Pair-Kabel
- Unterstützung von Halb-/Vollduplexbetrieb mit 10 Mbit/s oder 100 Mbit/s
- Unterstützung von Standard-Switches
- Keine Netzwerkplanung erforderlich
- Keine Routing-Tabellen erforderlich

Diese Softwareprodukte stehen für EtherNet/IP-Netzwerke zur Verfügung.

Tabelle 13 – Software für EtherNet/IP-Module

Software	Aufgabe	Erforderlich
Programmiersoftware RSLogix 5000	Diese Software ist zum Konfigurieren des Steuerungsprojekts und zum Definieren der EtherNet/IP-Kommunikation erforderlich.	Ja
Dienstprogramm BOOTP/DHCP	Dieses Dienstprogramm ist im Lieferumfang der Software RSLogix 5000 enthalten. Sie können es verwenden, um den Geräten in einem EtherNet/IP-Netzwerk IP-Adressen zuzuordnen.	Nein
Software RSNetWorx™ for EtherNet/IP	Sie können diese Software zum Konfigurieren von EtherNet/IP-Geräten nach IP-Adressen und/oder Hostnamen verwenden.	Nein
Software RSLinx	Sie können diese Software zum Konfigurieren von Geräten, Definieren der Kommunikation zwischen Geräten und zum Bereitstellen von Diagnosefunktionen verwenden.	Ja

Produzieren und Konsumieren von Daten über ein EtherNet/IP-Netzwerk

Die Steuerung unterstützt die Möglichkeit, Tags über ein EtherNet/IP-Netzwerk zu produzieren (senden) und zu konsumieren (empfangen). Alle produzierten und konsumierten Tags benötigen eine Verbindung. Die Gesamtzahl der Tags, die produziert oder konsumiert werden kann, ist auf die Anzahl der verfügbaren Verbindungen beschränkt.

Verbindungen über das EtherNet/IP-Netzwerk

Sie bestimmen indirekt, wie viele Verbindungen die Sicherheitssteuerung verwendet, indem Sie die Steuerung so konfigurieren, dass sie mit anderen Geräten im System kommunizieren kann. Verbindungen sind Ressourcenzuordnungen, die im Vergleich zu Nachrichten ohne Verbindung (Nachrichtenbefehle) eine zuverlässigere Kommunikation zwischen Geräten ermöglichen.

EtherNet/IP-Verbindungen sind azyklisch. Eine azyklische Verbindung wird durch das angeforderte Paketintervall (RPI) für die E/A-Steuerung oder das Programm getriggert (z. B. ein MSG-Befehl). Azyklische Nachrichten ermöglichen Ihnen bei Bedarf das Senden und Empfangen von Daten.

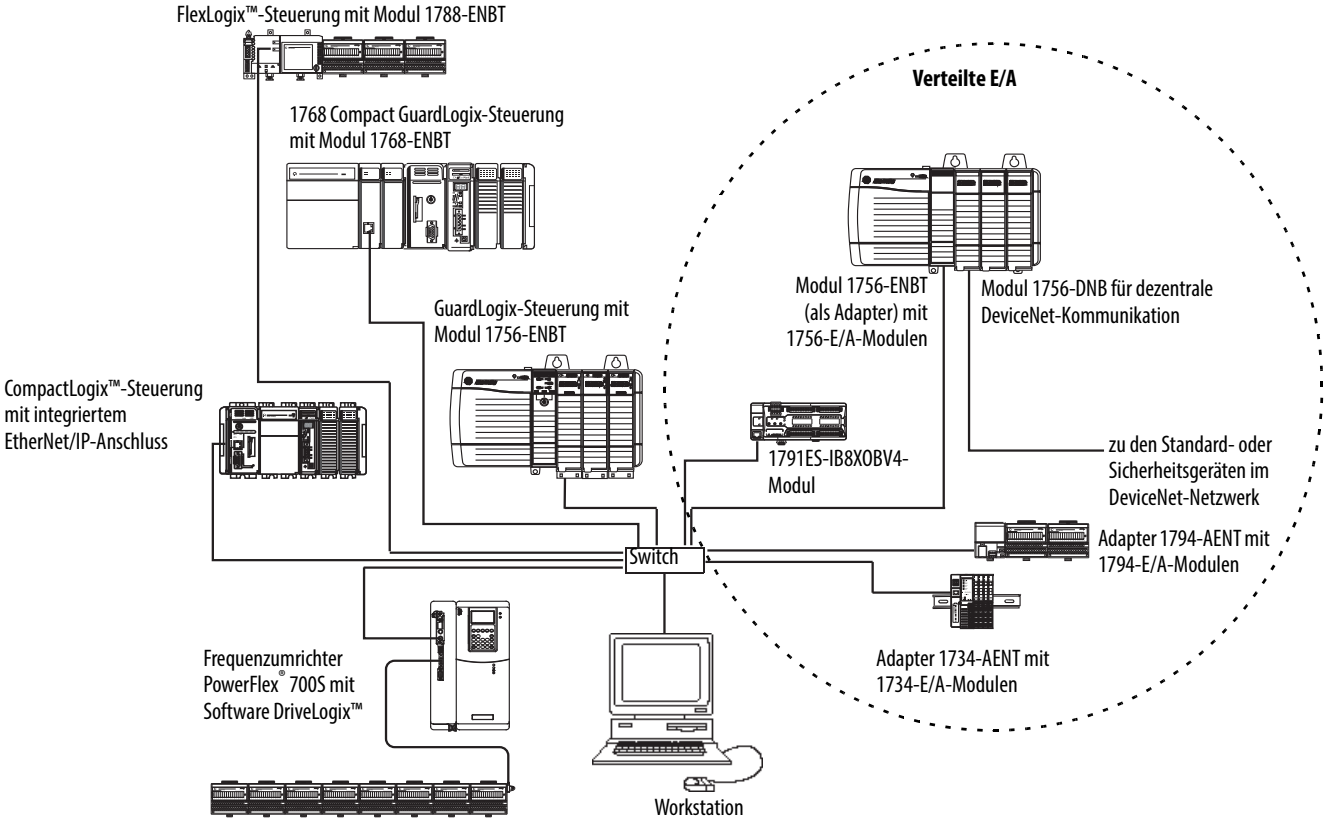
Die EtherNet/IP-Kommunikationsmodule unterstützen 128 CIP-Verbindungen (Common Industrial Protocol) über ein EtherNet/IP-Netzwerk.

Beispiel für die EtherNet/IP-Kommunikation

In diesem Beispiel:

- können die Steuerungen Standard- oder Sicherheits-Tags untereinander produzieren und konsumieren.
- können die Steuerungen MSG-Befehle initiieren, die Standarddaten senden/empfangen oder Geräte konfigurieren.(1)
- wird das EtherNet/IP-Kommunikationsmodul als Bridge verwendet und lässt die Sicherheitssteuerung Standard- und Sicherheitsdaten produzieren und konsumieren.
- kann der PC Projekte von den Steuerungen hochladen oder auf diese herunterladen.
- kann der PC Geräte auf dem EtherNet/IP-Netzwerk konfigurieren.

Abbildung 13 – Beispiel für die EtherNet/IP-Kommunikation

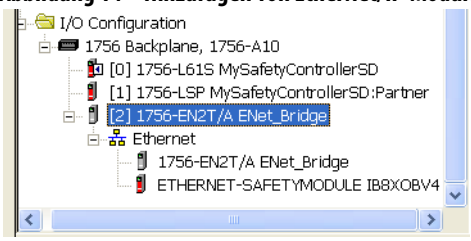


EtherNet/IP-Verbindungen für CIP Safety-E/A-Module

CIP Safety-E/A-Module auf EtherNet/IP-Netzwerken werden dem Projekt unter dem EtherNet/IP-Kommunikationsmodul hinzugefügt, wie in Kapitel 5, Hinzufügen, Konfigurieren, Überwachen und Ersetzen von CIP Safety-E/A-Modulen, beschrieben. Wenn Sie ein CIP Safety-E/A-Modul einfügen, erstellt die Software RSLogix 5000 für dieses Modul automatisch Sicherheitsdaten-Tags im Steuerungsbereich.

(1) GuardLogix-Steuerungen unterstützen keine MSG-Befehle für Sicherheitsdaten.

Abbildung 14 – Hinzufügen von EtherNet/IP-Modulen zum Projekt



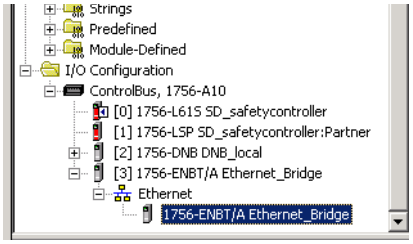
EtherNet/IP-Standardverbindungen

Wenn Sie ein Standard-EtherNet/IP-Modul mit der Sicherheitssteuerung verwenden möchten, fügen Sie das Modul dem Sicherheitssteuerungsprojekt hinzu, und laden Sie das Projekt in die GuardLogix-Steuerung.

1. Definieren Sie zum Konfigurieren des Moduls die IP-Adresse, die Subnet-Maske und das Gateway.

EtherNet/IP-Parameter	Beschreibung
IP-Adresse	Die IP-Adresse kennzeichnet das Modul auf eindeutige Weise. Die IP-Adresse hat das Format *xxx.xxx.xxx.xxx*. Dabei steht die Zeichenfolge *xxx* jeweils für eine Zahl zwischen 0 und 255. Allerdings dürfen einige Werte nicht als erstes Oktett in der Adresse verwendet werden: • 000.*xxx.xxx.xxx* • 127.*xxx.xxx.xxx* • 223 bis 255.*xxx.xxx.xxx*
Subnet-Maske	Die Teilnetz-Adressierung stellt eine Erweiterung des IP-Adressenschemas dar, durch das die Verwendung einer Netzwerk-ID für mehrere physische Netzwerke ermöglicht wird. Das Routing außerhalb des Standorts wird fortgesetzt, indem die IP-Adresse über die Klasse in eine Netz-ID und eine Host-ID aufgeteilt wird. Innerhalb eines Standorts wird die Subnet-Maske verwendet, um die IP-Adresse erneut in eine spezifische Netz-ID und eine Host-ID aufzuteilen. Dieses Feld wird standardmäßig auf den Wert 0.0.0.0 eingestellt. Falls Sie die Subnet-Maske eines bereits konfigurierten Moduls ändern, müssen Sie dieses aus- und wiedereinschalten, damit die Änderung wirksam wird.
Gateway	Ein Gateway verbindet individuelle physische Netzwerke zu einem System von Netzwerken. Wenn ein Netzknoten mit dem Netzknoten eines anderen Netzwerks kommunizieren muss, überträgt ein Gateway die Daten zwischen den beiden Netzwerken. Dieses Feld wird standardmäßig auf den Wert 0.0.0.0 eingestellt.

2. Nachdem Sie das EtherNet/IP-Modul physisch installiert und seine IP-Adresse festgelegt haben, müssen Sie das Modul dem Controller Organizer (Steuerungsorganisator) Ihres GuardLogix-Steuerungsprojekts hinzufügen.



3. Verwenden Sie die Software RSLogix 5000, um das Projekt herunterzuladen.

ControlNet-Kommunikation

Wählen Sie für die ControlNet-Kommunikation das Modul 1756-CNB oder 1756-CNBR für die Standardkommunikation oder das Modul 1756-CN2, 1756-CN2R oder 1756-CN2RXT für die Sicherheitskommunikation.

Tabelle 14 – ControlNet-Module

Wenn Ihre Anwendung	Wählen Sie
• Standard-E/A-Module steuert, • einen Adapter für verteilte E/A auf ControlNet-Verbindungen benötigt, • mit anderen ControlNet-Geräten kommuniziert (Nachrichten), • Standarddaten gemeinsam mit anderen Logix5000-Steuerungen verwendet (produziert/konsumiert), • ControlNet-Verbindungen überbrückt, um Nachrichten an Geräte in anderen Netzwerken weiterzuleiten,	1756-CNB
• dieselben Funktionen ausführt wie das Modul 1756-CNB, • auch redundant ausgelegte ControlNet-Medien unterstützt,	1756-CNBR
• dieselben Funktionen ausführt, die vom Modul 1756-CNB mit höherer Leistung unterstützt werden, • die CIP Safety-Kommunikation unterstützt,	1756-CN2
• dieselben Funktionen ausführt wie das Modul 1756-CN2, • auch redundant ausgelegte ControlNet-Medien unterstützt,	1756-CN2R
• dieselben Funktionen ausführt wie das Modul 1756-CN2R, • unter extremen Umgebungsbedingungen bei Temperaturen zwischen –25 bis +70 °C betrieben wird	1756-CN2RXT

Diese Softwareprodukte stehen für ControlNet-Netzwerke zur Verfügung.

Tabelle 15 – Software für ControlNet-Module

Software	Aufgabe	Erforderlich
Programmiersoftware RSLogix 5000	Diese Software ist erforderlich, um das GuardLogix-Projekt zu konfigurieren und ControlNet-Kommunikation zu definieren.	Ja
Software RSNetWorx for ControlNet	Diese Software ist erforderlich, um das ControlNet-Netzwerk zu konfigurieren, die Netzwerkaktualisierungszeit (NUT) zu definieren und das ControlNet-Netzwerk zu planen.	Ja
Software RSLinx	Sie können diese Software zum Konfigurieren von Geräten, Definieren der Kommunikation zwischen Geräten und zum Bereitstellen von Diagnosefunktionen verwenden.	Ja

Das ControlNet-Kommunikationsmodul bietet folgende Leistungsmerkmale:

- Es unterstützt das Messaging, produzierte/konsumierte Sicherheits- und Standard-Tags sowie verteilte E/A.
- Es unterstützt die Verwendung von Koax- und Glasfaser-Repeatern zur Isolierung und bei größeren Entfernungen.

Produzieren und Konsumieren von Daten über ein ControlNet-Netzwerk

Die GuardLogix-Steuerung unterstützt die Möglichkeit, Tags über ControlNet-Netzwerke zu produzieren (senden) und zu konsumieren (empfangen). Die Gesamtzahl der Tags, die produziert oder konsumiert werden kann, ist auf die Anzahl der verfügbaren Verbindungen in der GuardLogix-Steuerung beschränkt.

Verbindungen über das ControlNet-Netzwerk

Die Anzahl der von der Steuerung verwendeten Verbindungen wird dadurch bestimmt, wie Sie die Steuerung zum Kommunizieren mit anderen Geräten im System verwenden. Verbindungen sind Ressourcenzuordnungen, die im Vergleich zu Nachrichten ohne Verbindung (unconnected messages) eine zuverlässigere Kommunikation zwischen Geräten ermöglichen.

ControlNet-Verbindungen können zyklisch oder azyklisch sein.

Tabelle 16 – ControlNet-Verbindungen

Verbindungstyp	Beschreibung
Zyklisch (nur beim ControlNet-Netzwerk)	Eine zyklische Verbindung (scheduled connection) gibt es nur bei der ControlNet-Kommunikation. Eine zyklische Verbindung ermöglicht Ihnen das wiederholte Senden und Empfangen von Daten mit einem vordefinierten Intervall, dem angeforderten Paketintervall (RPI). Beispielsweise ist eine Verbindung zu einem E/A-Modul eine zyklische Verbindung, da Sie Daten von dem Modul wiederholt und mit einem festgelegten Intervall empfangen können. Weitere zyklische Verbindungen umfassen Verbindungen zu: • Kommunikationsgeräten • produzierten/konsumierten Tags In einem ControlNet-Netzwerk müssen Sie die Software RSNetWorx for ControlNet verwenden, um zyklische Verbindungen zu aktivieren und eine Netzwerkaktualisierungszeit (NUT) festzulegen. Beim Planen einer Verbindung wird Netzwerkbandbreite speziell für diese Verbindung reserviert.
Azyklisch	Eine azyklische Verbindung (unscheduled connection) ist eine Nachrichtenübertragung zwischen Steuerungen, die vom angeforderten Paketintervall (RPI) oder vom Programm getriggert wird (z. B. ein MSG-Befehl). Azyklische Nachrichten ermöglichen Ihnen bei Bedarf das Senden und Empfangen von Daten. Azyklische Verbindungen verwenden die Netzwerkbandbreite, die verbleibt, nachdem zyklische Verbindungen zugeordnet wurden. Produzierte/konsumierte Sicherheitsverbindungen sind azyklisch.

Die Kommunikationsmodule 1756-CNB und 1756-CNBR unterstützen 64 CIP-Verbindungen über ein ControlNet-Netzwerk. Für eine optimale Leistung sollten Sie jedoch maximal 48 Verbindungen pro Modul konfigurieren.

Das Modul 1756-CN2 unterstützt 128 CIP-Verbindungen über das ControlNet-Netzwerk.

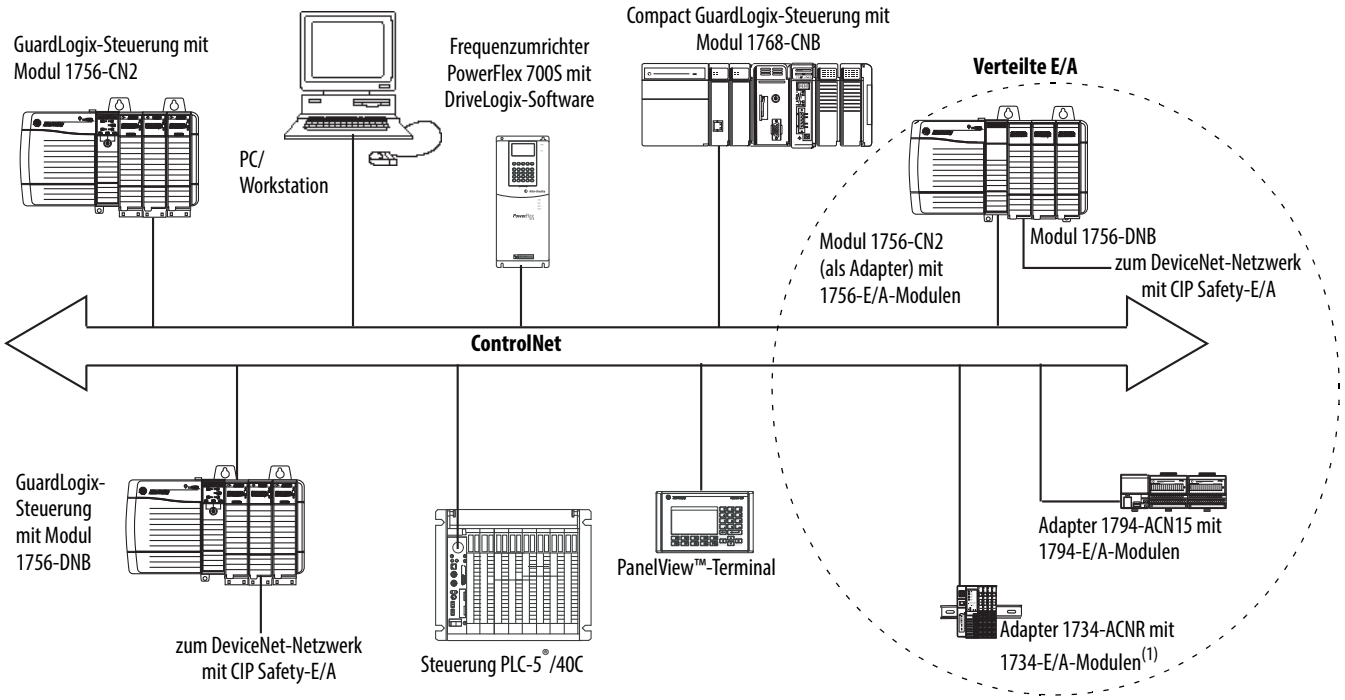
Beispiel für die ControlNet-Kommunikation

In diesem Beispiel:

- können GuardLogix-Steuerungen Standard- oder Sicherheits-Tags untereinander produzieren und konsumieren.
- können GuardLogix-Steuerungen MSG-Befehle initiieren, die Standarddaten senden/empfangen oder Geräte konfigurieren.(1)
- Das Modul 1756-CN2 kann als Bridge verwendet werden, wodurch die GuardLogix-Steuerung Standard- und Sicherheitsdaten von den E/A-Geräten konsumieren und für diese produzieren kann.
- kann der PC Projekte von den Steuerungen hochladen oder auf diese herunterladen.
- kann der PC Geräte im ControlNet-Netzwerk und das Netzwerk selbst konfigurieren.

(1) GuardLogix-Steuerungen unterstützten keine MSG-Befehle für Sicherheitsdaten.

Abbildung 15 – Beispiel für die ControlNet-Kommunikation



(1) Der Adapter 1734-ACN unterstützt keine POINT Guard-Sicherheits-E/A-Module.

ControlNet-Verbindungen für dezentrale E/A

Fügen Sie für die Kommunikation mit dezentralen E/A-Modulen über ein ControlNet-Netzwerk in den Ordner „I/O Configuration“ (E/A-Konfiguration) eine ControlNet-Bridge, einen ControlNet-Adapter sowie E/A-Module ein.

DeviceNet-Kommunikation

Für die Kommunikation und den Datenaustausch mit CIP Safety-E/A-Modulen in DeviceNet-Netzwerken benötigen Sie das Modul 1756-DNB im lokalen Chassis.

Informationen zum Installieren des Moduls 1756-DNB finden Sie in der Publikation 1756-IN566, ControlLogix DeviceNet Scanner Module Installation Instructions.

Das Modul 1756-DNB unterstützt die Kommunikation mit den DeviceNet-Safety-Geräten und den DeviceNet-Standardgeräten. Sie können beide Typen verwenden.

Die folgenden Softwareprodukte stehen für DeviceNet-Netzwerke und das Modul 1756-DNB zur Verfügung.

Tabelle 17 – Software für DeviceNet-Netzwerke

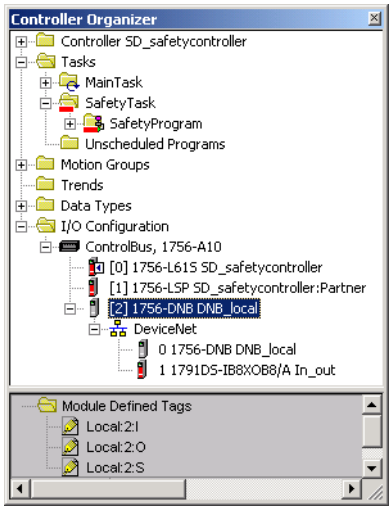
Software	Verwendungszweck	Erforderlich/optional
RSLogix 5000	• Konfigurieren von ControlLogix-Projekten. • Definieren der DeviceNet-Kommunikation.	Erforderlich
RSNetWorx™ for DeviceNet	• Konfigurieren von DeviceNet-Geräten. • Definieren der Abtastliste für diese Geräte.	
RSLinx Classic oder RSLinx Enterprise	• Konfigurieren von Kommunikationsgeräten. • Bereitstellen von Diagnosefunktionen. • Einrichten der Kommunikation zwischen Geräten.	

DeviceNet-Verbindungen für CIP Safety-E/A-Module

Zugriff auf CIP Safety-Geräte in DeviceNet-Netzwerken erhalten Sie, indem Sie das Modul 1756-DNB zum E/A-Konfigurationsverzeichnis des GuardLogix-Steuerungsprojekts hinzufügen.

CIP Safety-E/A-Module in DeviceNet-Netzwerken werden dem Projekt unter dem Modul 1756-DNB hinzugefügt, wie in Kapitel 5, Hinzufügen, Konfigurieren, Überwachen und Ersetzen von CIP Safety-E/A-Modulen beschrieben. Wenn Sie ein CIP Safety-E/A-Modul einfügen, erstellt die Software RSLogix 5000 für dieses Modul automatisch Sicherheitsdaten-Tags im Steuerungsbereich.

Abbildung 16 – DeviceNet-Modul in der Steuerung im E/A-Konfigurationsverzeichnis



Standard-DeviceNet-Verbindungen

Falls Sie Standard-DeviceNet-E/A mit Ihrer GuardLogix-Steuerung verwenden, müssen Sie jedem 1756-DNB-Modul zwei Verbindungen zuweisen. Eine Verbindung ist für den Modulstatus und die Konfiguration bestimmt. Die andere Verbindung ist eine Rack-optimierte Verbindung für die DeviceNet-E/A-Daten.

Wenn Sie das Modul 1756-DNB für den Zugriff auf Standarddaten über das DeviceNet-Netzwerk nutzen möchten, müssen Sie die Software RSNetWorx for DeviceNet verwenden, um:

- eine Konfigurationsdatei für das Netzwerk zu erstellen.
- jedes Standardgerät im Netzwerk zu konfigurieren.
- das Modul 1756-DNB zu konfigurieren.
- die Standard-E/A-Geräte in die 1756-DNB-Abtastliste einzufügen.

Wenn Sie das Modul 1756-DNB zur E/A-Konfiguration der Steuerung hinzufügen, erstellt die Software RSLogix 5000 automatisch einen Satz Standard-Tags für die Eingangs-, Ausgangs- und Zustandsdaten des Netzwerks.

Serielle Kommunikation

Zum Betrieb der GuardLogix-Steuerung in einem seriellen Netzwerk benötigen Sie:

- eine Workstation mit einer seriellen Schnittstelle.
- die Software RSLinx, um den seriellen Kommunikationstreiber zu konfigurieren.
- die Software RSLogix 5000, um die serielle Schnittstelle der Steuerung zu konfigurieren.

Damit die Steuerung mit einer Workstation oder einem anderen Gerät über das serielle Netzwerk kommunizieren kann, müssen Sie wie folgt vorgehen:

1. Konfigurieren Sie den seriellen Kommunikationstreiber für die Workstation.
2. Konfigurieren Sie die serielle Schnittstelle der Steuerung.

Tabelle 18 – Betriebsarten für serielle Kommunikation

Verwenden Sie diesen Modus:	für:
DF1-Punkt-zu-Punkt	Kommunikation zwischen der Steuerung und einem anderen mit dem DF1-Protokoll kompatiblen Gerät. Dies ist der Standardsystemmodus. Dieser Modus dient in der Regel zum Programmieren der Steuerung über ihre serielle Schnittstelle.
DF1-Master	Steuerung von Polling und Nachrichtenübertragungen zwischen den Master- und den Slave-Netzwerkknoten. Das Master-/Slave-Netzwerk umfasst eine als Master-Netzknoten konfigurierte Steuerung und bis zu 254 Slave-Netzknoten. Slave-Netzwerkknoten werden mithilfe von Modems oder Leitungstreibern verbunden. Ein Master/Slave-Netzwerk kann die Netzknotennummern 0 bis 254 aufweisen. Jeder Netzknoten muss über eine eindeutige Netzknotenadresse verfügen. Außerdem müssen zumindest 2 Netzknoten existieren, die Ihren Verbund als Netzwerk definieren (die beiden Netzknoten sind 1 Master-Station und 1 Slave-Station).
DF1-Slave	Eine Steuerung, die als Slave-Station in einem seriellen Master/Slave-Kommunikationsnetzwerk eingesetzt wird. Wenn es mehrere Slave-Stationen im Netzwerk gibt, verbinden Sie die Slave-Stationen mithilfe von Modems oder Leitungstreibern mit dem Master. Wenn Sie eine einzige Slave-Station im Netzwerk haben, benötigen Sie kein Modem, um die Slave-Station mit dem Master zu verbinden. Sie können die Steuerungsparameter für den No-Handshaking-Betrieb konfigurieren. Sie können 2 bis 255 Netzknoten mit einem Verbund verbinden. Im DF1-Slave-Modus verwendet die Steuerung ein DF1-Halbduplex-Protokoll. Ein Netzknoten wird als Master bestimmt und steuert, wer Zugriff auf den Verbund hat. Alle anderen Netzknoten sind Slave-Stationen und müssen vor dem Senden auf die Freigabe durch den Master warten.
DH-485	Kommunikation mit anderen DH-485-Geräten, Multi-Master, Token-Passing-Netzwerk, wodurch die Programmierung und die Peer-to-Peer-Nachrichtenübermittlung ermöglicht werden.

Weitere Informationen

Quelle	Beschreibung
EtherNet/IP Modules in Logix5000 Control Systems User Manual, Publikation ENET-UM001	Enthält ausführliche Informationen zu Konfiguration und Verwendung von EtherNet/IP-Kommunikationsmodulen in einem Logix5000-Steuerungssystem
ControlNet Modules in Logix5000 Control Systems User Manual, Publikation CNET-UM001	Enthält ausführliche Informationen zu Konfiguration und Verwendung von ControlNet-Kommunikationsmodulen in einem Logix5000-Steuerungssystem
DeviceNet Modules in Logix5000 Control Systems User Manual, Publikation DNET-UM004	Enthält ausführliche Informationen zur Konfiguration und Verwendung des Moduls 1756-DNB in einem Logix5000-Steuerungssystem

Hinzufügen, Konfigurieren, Überwachen und Ersetzen von CIP Safety-E/A-Modulen

Weitere Informationen zu Installation, Konfiguration und Betrieb der CIP Safety-E/A-Module finden Sie in den folgenden Informationsquellen:

- Guard I/O DeviceNet Safety Modules User Manual, Publikation 1791DS-UM001
- Guard I/O EtherNet/IP-Sicherheitsmodule – Benutzerhandbuch, Publikation 1791ES-UM001
- POINT Guard I/O™-Sicherheitsmodule – Installations- und Benutzerhandbuch, Publikation 1734-UM013
- Online-Hilfe der Software RSLogix 5000

Hinzufügen von CIP Safety-E/A-Modulen

Wenn Sie ein Modul in das System einfügen, müssen Sie eine Konfiguration für das Modul definieren, zu der unter anderem Folgendes gehört:

- Netzknotenadresse für DeviceNet-Netzwerke

  Die Netzknotenadresse eines CIP Safety-E/A-Moduls in DeviceNet-Netzwerken kann nicht über die Software RSLogix 5000 festgelegt werden. Modulnetzknotenadressen werden über Drehschalter an den Modulen festgelegt.

- IP-Adresse für EtherNet/IP-Netzwerke

  Zum Festlegen der IP-Adresse können Sie die Drehschalter am Modul entsprechend anpassen, die DHCP-Software verwenden, die Sie von Rockwell Automation erhalten, oder die Standardadresse aus dem nichtflüchtigen Speicher abrufen.

- Sicherheitsnetzwerknummer (SNN – Safety Network Number)

  Informationen zum Festlegen der SNN finden Sie auf Seite 73.

- Konfigurationssignatur

  Informationen darüber, wann die Konfigurationssignatur automatisch festgelegt wird und wann Sie die Signatur festlegen müssen, finden Sie auf Seite 78.

- Reaktionszeitgrenze

  Informationen zum Festlegen des Grenzwerts für die Reaktionszeit finden Sie auf Seite 73.

- Sicherheitseingangs-, Sicherheitsausgangs- und Testparameter

Sie können CIP Safety-E/A-Module über die GuardLogix-Steuerung mithilfe der Software RSLogix 5000 konfigurieren.

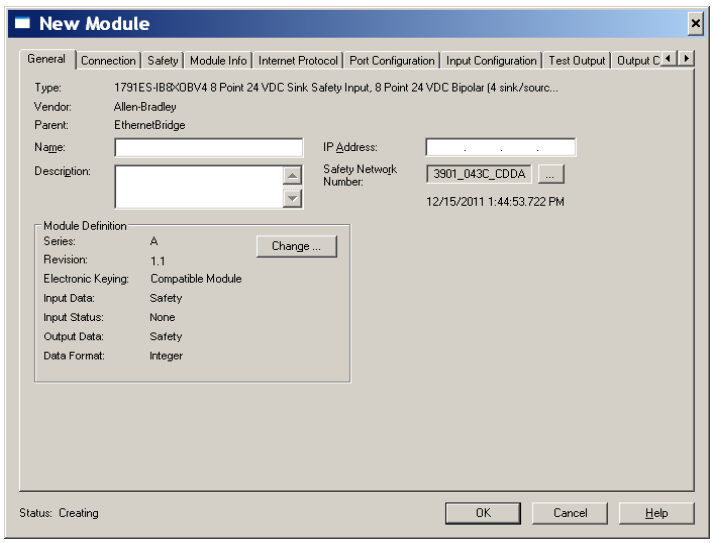
TIPP Sicherheits-E/A-Module unterstützen Standard- und Sicherheitsdaten. Die Modulkonfiguration definiert, welche Daten zur Verfügung stehen.

Konfigurieren von CIP Safety-E/A-Modulen über die Software RSLogix 5000

Fügen Sie dem Kommunikationsmodul die CIP Safety-E/A-Module unter dem Ordner „I/O Configuration“ (E/A-Konfiguration) des RSLogix 5000-Projekts hinzu.

TIPP Sie können ein CIP Safety-E/A-Modul weder hinzufügen noch löschen, solange Sie sich im Online-Modus befinden.

1. Klicken Sie mit der rechten Maustaste auf das entsprechende Netzwerk und wählen Sie „New Module“ (Neues Modul) aus.
2. Erweitern Sie die Kategorie „Safety“ (Sicherheit) und wählen Sie ein CIP Safety-E/A-Modul.
3. Spezifizieren Sie die Moduleigenschaften.



   a. Ändern Sie die Einstellungen unter „Module Definition“ (Moduldefinition), falls erforderlich, indem Sie auf „Change“ (Ändern) klicken.

   b. Geben Sie einen Namen für das neue Modul ein.

c. Geben Sie die Netzknotenadresse oder IP-Adresse des Moduls in seinem Verbindungsnetzwerk an.

   Das Pulldown-Menü enthält nur freie Netzknotennummern.

d. Ändern Sie die Sicherheitsnetzwerknummer (SNN), falls erforderlich, durch Anklicken der Schaltfläche ... .

   Ausführliche Informationen hierzu finden Sie auf Seite 73.

e. Legen Sie die Parameter der Modulkonfiguration mithilfe der Registerkarten „Input Configuration“ (Eingangskonfiguration), „Test Output“ (Ausgangsprüfung) und „Output Configuration“ (Ausgangskonfiguration) fest.

   Weitere Informationen zum Konfigurieren von CIP Safety-E/A-Modulen finden Sie in der Online-Hilfe der Software RSLogix 5000.

f. Legen Sie die Reaktionszeitgrenze der Verbindung mithilfe der Registerkarte „Safety“ (Sicherheit) fest.

   Ausführliche Informationen hierzu finden Sie auf Seite 73.

Festlegen der Sicherheitsnetzwerknummer (SNN)

Die Zuordnung einer zeitbasierenden SNN erfolgt automatisch, wenn neue Sicherheits-E/A-Module hinzugefügt werden. Werden zu einem späteren Zeitpunkt Sicherheitsmodule zum gleichen Netzwerk hinzugefügt, wird ihnen die gleiche SNN zugeordnet, die innerhalb der niedrigsten Adresse auf diesem CIP Safety-Netzwerk definiert ist.

Für die meisten Anwendungen ist diese automatische, zeitbasierende SNN ausreichend. Es gibt jedoch Fälle, in denen eine Änderung der SNNs erforderlich ist.

Siehe Zuordnen der Sicherheitsnetzwerknummer (SNN) auf Seite 57.

Verwenden von Unicast-Verbindungen auf EtherNet/IP-Netzwerken

In der Software RSLogix 5000 ab Version 20 können Sie festlegen, dass EtherNet/IP E/A-Module Unicast-Verbindungen verwenden sollen. Unicast-Verbindungen sind Punkt-zu-Punkt-Verbindungen zwischen einem Quell- und einem Zielknoten. Für diese Verbindungsart müssen Sie keinen minimalen oder maximalen RPI-Grenzwert oder Standardwert festlegen.

Wählen Sie zur Konfiguration von Unicast-Verbindungen die Registerkarte „Connection“ (Verbindung) und anschließend „Use Unicast Connection over Ethernet/IP“ (Unicast-Verbindung über Ethernet/IP verwenden) aus.

Festlegen der Reaktionszeitgrenze der Verbindung

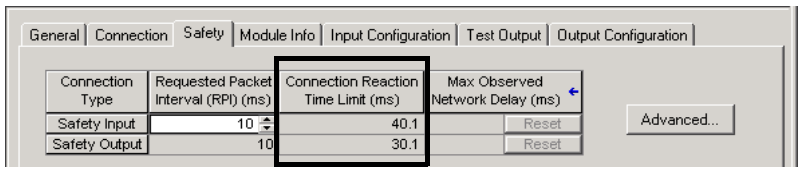
Die Reaktionszeitgrenze der Verbindung ist das maximale Alter der Sicherheitspakete auf der zugehörigen Verbindung. Falls das Alter der vom konsumierenden Gerät verwendeten Daten die Reaktionszeitgrenze der Verbindung überschreitet, tritt ein Verbindungsfehler ein. Die Reaktionszeitgrenze der Verbindung wird durch die folgenden Gleichungen bestimmt:

Reaktionszeitgrenze der Eingangsverbindung =
Eingang RPI x [Timeout-Multiplikator + Netzwerkverzögerungs-Multiplikator]

Reaktionszeitgrenze der Ausgangsverbindung =
Zeitspanne der Sicherheits-Task x [Timeout-Multiplikator + Netzwerkverzögerungs-Multiplikator – 1]

Die Reaktionszeitgrenze der Verbindung ist auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) angegeben.

Abbildung 17 – Reaktionszeitgrenze der Verbindung



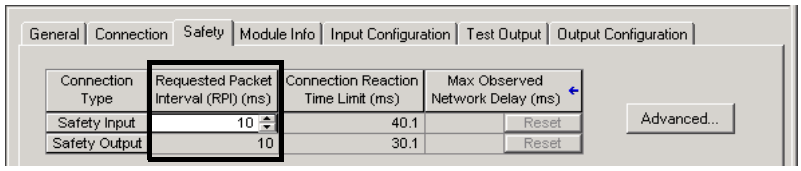
Spezifizieren des angeforderten Paketintervalls (RPI)

Das angeforderte Paketintervall (RPI) spezifiziert den Zeitraum, in dem die Daten über eine Verbindung aktualisiert werden. Ein Eingangsmodul erstellt beispielsweise Daten mit dem von Ihnen zugewiesenen RPI.

Für Sicherheits-Eingangsverbindungen können Sie das RPI auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) einstellen. Das angeforderte Paketintervall (RPI) wird in Schritten von 1 ms und innerhalb eines Bereichs von 1–100 ms eingegeben. Der Standardwert ist 10 ms.

Die Reaktionszeitgrenze der Verbindung wird sofort angepasst, wenn das RPI über die Software RSLogix 5000 geändert wird.

Abbildung 18 – Angefordertes Paketintervall (RPI)



Für Sicherheits-Ausgangsverbindungen wird das RPI anhand der Zeitspanne der Sicherheits-Task festgelegt. Falls eine entsprechende Reaktionszeitgrenze der Verbindung nicht zufriedenstellend ist, können Sie die Zeitspanne der Sicherheits-Task über das Dialogfeld „Safety Task Properties“ (Eigenschaften der Sicherheits-Task) anpassen.

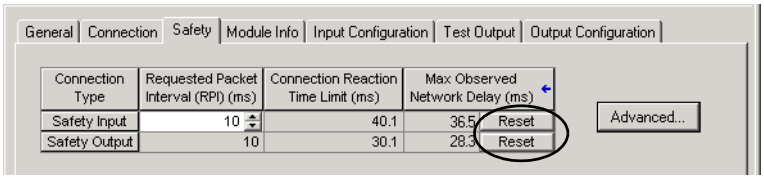
Unter Spezifizieren der Sicherheits-Task-Zeitspanne auf Seite 94 finden Sie weitere Informationen über die Zeitspanne der Sicherheits-Task.

Für die meisten Anwendungen ist das Standard-RPI in der Regel unzureichend. Für komplexere Anforderungen verwenden Sie die Schaltfläche „Advanced“ (Erweitert), um die Parameter der Reaktionszeitgrenze der Verbindung zu ändern, wie auf Seite 75 beschrieben.

Anzeigen der beobachteten maximalen Netzwerkverzögerung

Wenn die GuardLogix-Steuerung ein Sicherheitspaket empfängt, zeichnet die Software die beobachtete maximale Netzwerkverzögerung auf. Für Sicherheitseingänge zeigt die beobachtete maximale Netzwerkverzögerung die Verzögerung durch die Übertragung vom Eingangsmodul zur Steuerung und zurück sowie die Rückbestätigung zum Eingangsmodul an. Für Sicherheitsausgänge zeigt sie die Verzögerung durch die Übertragung von der Steuerung zum Ausgangsmodul und zurück sowie die Rückbestätigung zur Steuerung an. Die beobachtete maximale Netzwerkverzögerung wird auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) dargestellt. Im Online-Modus können Sie die beobachtete maximale Netzwerkverzögerung durch Klicken auf die Schaltfläche „Reset“ (Zurücksetzen) zurücksetzen.

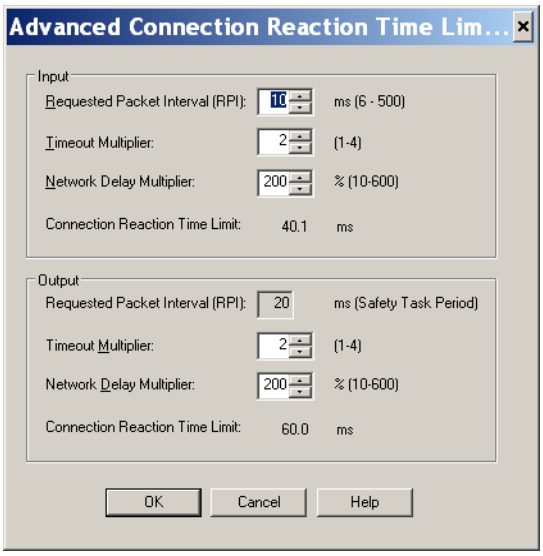
Abbildung 19 – Zurücksetzen der beobachteten maximalen Netzwerkverzögerung



WICHTIG Die tatsächliche maximale Netzwerkverzögerungszeit vom Producer zum Consumer ist kürzer als der auf der Registerkarte „Safety“ (Sicherheit) im Feld „Maximum Network Delay“ (Maximale Netzwerkverzögerung) angezeigte Wert. Im Allgemeinen beträgt die tatsächliche maximale Nachrichtenverzögerung etwa die Hälfte des Werts der angezeigten maximalen Netzwerkverzögerung.

Festlegen der erweiterten Parameter für die Reaktionszeitgrenze der Verbindung

Abbildung 20 – Erweiterte Konfiguration



Timeout Multiplier

Der Timeout Multiplier (Timeout-Multiplikator) bestimmt die Anzahl der RPIs, die auf ein Paket gewartet wird, bevor ein Verbindungs-Timeout erfolgt. Dies lässt sich durch die Anzahl der Nachrichten ausdrücken, die verloren gehen können, bevor ein Verbindungsfehler ausgewiesen wird.

Ein Timeout-Multiplikator von 1 zeigt beispielsweise an, dass Nachrichten während jedes RPI-Intervalls empfangen werden müssen. Ein Timeout-Multiplikator von 2 zeigt an, dass 1 Nachricht verloren gehen kann, solange mindestens 1 Nachricht innerhalb eines zweimaligen RPI (2 x RPI) empfangen wird.

Network Delay Multiplier

Der Network Delay Multiplier (Netzwerkverzögerungs-Multiplikator) definiert die Nachrichtentransportzeit, die durch das CIP Safety-Protokoll erzwungen wird. Der Netzwerkverzögerungs-Multiplikator spezifiziert die Verzögerung durch die Übertragung vom Producer zum Consumer und zurück und die Rückbestätigung zum Producer. Sie können den Netzwerkverzögerungs-Multiplikator verwenden, um die Reaktionszeitgrenze der Verbindung in solchen Fällen zu erhöhen oder zu verringern, in denen die erzwungene Nachrichtentransportzeit wesentlich geringer oder höher ist als das RPI. Das Einstellen des Netzwerkverzögerungs-Multiplikators kann beispielsweise hilfreich sein, wenn das RPI einer Ausgangsverbindung mit einer langen Sicherheits-Task-Zeitspanne übereinstimmt.

In Fällen, in denen das Eingangs-RPI oder das Ausgangs-RPI im Vergleich zur erzwungenen Nachrichtenverzögerungszeit relativ lang bzw. kurz ist, kann der Netzwerkverzögerungs-Multiplikator mithilfe einer der beiden Methoden angenähert werden.

Methode 1: Verwenden Sie das Verhältnis zwischen dem Eingangs-RPI und der Sicherheits-Task-Zeitspanne. Verwenden Sie diese Methode nur, wenn alle der nachfolgenden Bedingungen zutreffen:

- Der Pfad oder die Verzögerung sind ungefähr identisch mit dem Ausgangspfad oder der Ausgangsverzögerung und
- das Eingangs-RPI wurde so konfiguriert, dass die tatsächliche Eingangsnachrichten-Transportzeit kürzer ist als das Eingangs-RPI und
- die Sicherheits-Task-Zeitspanne im Vergleich zum Eingangs-RPI lang ist.

  Unter diesen Bedingungen kann der Ausgangs-Netzwerkverzögerungs-Multiplikator wie folgt angenähert werden:

  Eingangs-Netzwerkverzögerungs-Multiplikator x [Eingangs-RPI ÷ Sicherheits-Task-Zeitspanne]

BEISPIEL **Berechnung des angenäherten Ausgangs-Netzwerkverzögerungs-Multiplikators**

Wenn:

Eingangs-RPI = 10 ms
Eingangs-Netzwerkverzögerungs-Multiplikator = 200 %
Sicherheits-Task-Zeitspanne = 20 ms

dann ist der Ausgangs-Netzwerkverzögerungs-Multiplikator gleich:

200 % x [10 ÷ 20] = 100 %

Methode 2: Verwenden Sie die beobachtete maximale Netzwerkverzögerung. Wenn das System über einen längeren Zeitraum unter den schlechtesten Belastungsbedingungen betrieben wird, kann der Netzwerkverzögerungs-Multiplikator ausgehend von der beobachteten maximalen Netzwerkverzögerung festgelegt werden. Dieses Verfahren kann bei einer Eingangs- oder Ausgangsverbindung angewendet werden. Protokollieren Sie die beobachtete maximale Netzwerkverzögerung, nachdem das System über einen längeren Zeitraum unter den schlechtesten Belastungsbedingungen betrieben wurde.

Der Netzwerkverzögerungs-Multiplikator kann mit folgender Gleichung angenähert werden:

[Beobachtete maximale Netzwerkverzögerung + Toleranzfaktor] ÷ RPI

BEISPIEL **Berechnung des Netzwerkverzögerungs-Multiplikators aus der beobachteten maximalen Netzwerkverzögerung**

Wenn:

RPI = 50 ms
Beobachtete maximale Netzwerkverzögerung = 20 ms
Toleranzfaktor = 10

dann ist der Netzwerkverzögerungs-Multiplikator gleich:

[20 + 10] ÷ 50 = 60 %

Tabelle 19 – Weitere Informationen

Quelle	Beschreibung
Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch, Publikation 1756-RM093	Enthält Informationen zur Berechnung von Reaktionszeiten.
Guard I/O DeviceNet Safety Modules User Manual, Publikation 1791DS-UM001	
Guard I/O EtherNet/IP-Sicherheitsmodule – Benutzerhandbuch, Publikation 1791ES-UM001	

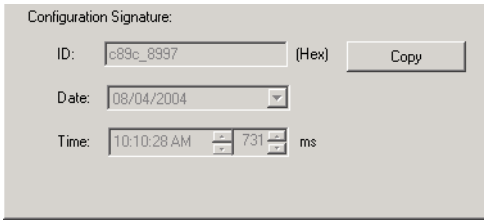
Verstehen der Konfigurationssignatur

Jedes Sicherheitsgerät hat eine eindeutige Konfigurationssignatur, die die Modulkonfiguration definiert. Die Konfigurationssignatur besteht aus einer Identifikationsnummer (ID-Nummer), Datum und Uhrzeit. Sie dient zur Verifizierung der Konfiguration eines Moduls.

Konfiguration über die Software RSLogix 5000

Beim Konfigurieren des E/A-Moduls mithilfe der Software RSLogix 5000 wird die Konfigurationssignatur automatisch generiert. Sie können die Konfigurationssignatur über die Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Module Properties“ (Moduleigenschaften) einsehen und kopieren.

Abbildung 21 – Einsehen und Kopieren der Konfigurationssignatur



Verschiedene Konfigurationsverwalter (Listen-only-Verbindung)

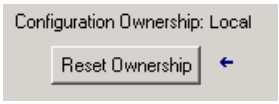
Wenn eine andere Steuerung die Verwaltungsrechte an der E/A-Modulkonfiguration hat, müssen Sie die Signatur der Modulkonfiguration aus dem Projekt der verwaltenden Steuerung kopieren und auf der Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Module Properties“ (Moduleigenschaften) einfügen.

TIPP Falls das Modul nur für Eingänge konfiguriert ist, können Sie die Konfigurationssignatur kopieren und einfügen. Verfügt das Modul über Sicherheitsausgänge, wird es von der Steuerung verwaltet, die die Verwaltungsrechte an der Konfiguration hat. Das Textfeld mit der Konfigurationssignatur steht in diesem Fall nicht zur Verfügung.

Zurücksetzen der Verwaltungsrechte an Sicherheits-E/A-Modulen

Wenn die Software RSLogix 5000 online geschaltet ist, zeigt die Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) die aktuellen Verwaltungsrechte an der Konfiguration an. Wenn das geöffnete Projekt die Verwaltungsrechte an der Konfiguration hat, wird „Local“ (Zentral) angezeigt. Wenn ein zweites Gerät die Konfiguration verwaltet, werden „Remote“ (Dezentral) sowie die Sicherheitsnetzwerknummer (SNN) und Netzknotenadresse oder Steckplatznummer des Konfigurationsverwalters angezeigt. „Communication error“ (Kommunikationsfehler) wird angezeigt, wenn das Auslesen des Moduls misslingt.

Wenn Sie online geschaltet sind, können Sie das Modul durch Klicken auf die Schaltfläche „Reset Ownership“ (Verwaltungsrechte zurücksetzen) auf seine werksseitige Konfiguration zurücksetzen.



TIPP Sie können die Verwaltungsrechte nicht zurücksetzen, wenn noch Änderungen an den Moduleigenschaften ausstehen oder eine Sicherheits-Task-Signatur bzw. eine Sicherheitsverriegelung vorliegt.

Adressieren von Sicherheits-E/A-Daten

Wenn Sie ein Modul zum E/A-Konfigurationsordner hinzufügen, erstellt die Software RSLogix 5000 automatisch Steuerungsbereichs-Tags für das Modul.

E/A-Informationen werden als Tag-Satz angezeigt. Jedes Tag verwendet eine Datenstruktur, die vom Typ und von den Leistungsmerkmalen des E/A-Moduls abhängt. Der Name eines Tags basiert auf dem Namen des Moduls im System.

Adressformat eines CIP Safety-E/A-Geräts:

Modulename:Type.Member

Tabelle 20 – Adressformat eines CIP Safety-E/A-Moduls

Wobei	Bedeutung	
Modulename	Name des CIP Safety-E/A-Moduls	
Typ	Datentyp	
	Eingang: I	
	Ausgang: O	
Member	Spezifische Daten des E/A-Moduls	
	Nur-Eingangsmodul:	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members
	Nur-Ausgangsmodul:	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:O.Output Members
	Kombinations-E/A:	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members Modulename:O.Output Members

Tabelle 21 – Weitere Informationen

Quelle	Beschreibung
Kapitel 9, Zustandsüberwachung und Fehlerbehebung	Enthält Informationen zur Überwachung der Sicherheits-Tag-Daten
Steuerungen Logix5000 – E/A- und Tag-Daten – Programmierhandbuch, Publikation 1756-PM004	Enthält Informationen zur Adressierung von Standard-E/A-Modulen

Überwachen des Sicherheits-E/A-Modulstatus

Sie können den Status des Sicherheits-E/A-Moduls über die explizite Nachrichtenübertragung oder über die Statusanzeigen der E/A-Module überwachen.

Diese Publikationen bieten Informationen zur Behebung von E/A-Modulfehlern:

- Guard I/O DeviceNet Safety Modules User Manual, Publikation 1791DS-UM001
- Guard I/O EtherNet/IP-Sicherheitsmodule – Benutzerhandbuch, Publikation 1791ES-UM001
- POINT Guard I/O-Sicherheitsmodule – Installations- und Benutzerhandbuch, Publikation 1734-UM013

Tabelle 22 – Betriebsweise der Statusanzeigen

Anzeige	Status	Beschreibung		
		Guard I/O DeviceNet-Module	**Guard I/O EtherNet/IP-Module**	**POINT Guard I/O-Module**
Modulstatus (MS)	aus	Keine Stromversorgung.		
	grün, ein	Betrieb unter normalen Bedingungen.		
	grün, blinkend	Gerät im Leerlauf.		
	rot, blinkend	Ein behebbarer Fehler liegt vor.	Es liegt ein behebbarer Fehler vor oder es läuft ein Firmware-Update.	
	rot, ein	Ein nicht behebbarer Fehler liegt vor.		
	rot/grün, blinkend	Selbsttest wird durchgeführt.	Es laufen Selbsttests oder das Modul ist nicht richtig konfiguriert. Weitere Informationen erhalten Sie über die Statusanzeige des Netzwerks.	
Netzwerk-status (NS)	aus	Gerät ist nicht online oder wird evtl. nicht mit Strom versorgt.		
	grün, ein	Gerät ist online; Verbindungen sind aufgebaut.		
	grün, blinkend	Gerät ist online; keine Verbindungen aufgebaut.		
	rot, blinkend	Kommunikations-Timeout.	Kommunikations-Timeout oder es läuft ein Firmware-Update.	
	rot, ein	Kommunikationsverlust. Das Gerät hat einen Fehler erkannt, der die Netzwerkkommunikation verhindert.		
	rot/grün, blinkend	Ein Kommunikationsfehler liegt vor oder die Sicherheitsnetzwerknummer (SNN) wird gerade festgelegt.	Selbsttest wird durchgeführt.	Nicht zutreffend.
Eingangs-punkte (IN*x*)	aus	Sicherheitseingang ist aus.		
	gelb, ein	Sicherheitseingang ist an.		
	rot, ein	Ein Fehler ist in der Eingangsschaltung aufgetreten.		
	rot, blinkend	Bei ausgewähltem Doppelkanalbetrieb ist ein Fehler in der Partnereingangsschaltung aufgetreten.		
Ausgangs-punkte (O*x*)	aus	Sicherheitsausgang ist aus.		
	gelb, ein	Sicherheitsausgang ist an.		
	rot, ein	Ein Fehler ist in der Ausgangsschaltung aufgetreten.		
	rot, blinkend	Bei ausgewähltem Doppelkanalbetrieb ist ein Fehler in der Partnerausgangsschaltung aufgetreten.		
Ausgangs-punkte testen (T*x*)	aus	Nicht zutreffend.	Der Ausgang ist ausgeschaltet.	Nicht zutreffend.
	gelb, ein		Der Ausgang ist eingeschaltet.	
	rot, ein		Ein Fehler ist in der Ausgangsschaltung aufgetreten.	
LOCK	gelb, ein	Gerätekonfiguration ist verriegelt.	Die Software RSLogix 5000 unterstützt diese Funktion nicht.	
	gelb, blinkend	Gerätekonfiguration ist gültig, aber Gerät ist nicht verriegelt.		
	gelb, aus	Ungültig, keine Konfigurationsdaten oder das Gerät wurde über die Software RSLogix 5000 konfiguriert.		

Tabelle 22 – Betriebsweise der Statusanzeigen

Anzeige	Status	Beschreibung		
		Guard I/O DeviceNet-Module	**Guard I/O EtherNet/IP-Module**	**POINT Guard I/O-Module**
IN PWR	grün, aus	Keine Leistungsaufnahme.		Nicht zutreffend.
	grün, ein	Eingangsleistungsaufnahme erfüllt die Spezifikationen.		
	gelb, ein	Eingangsleistungsaufnahme liegt außerhalb der Spezifikationen.		
OUT PWR	grün, aus	Keine Ausgangsleistung.		
	grün, ein	Ausgangsleistungsaufnahme erfüllt die Spezifikationen.		
	gelb, ein	Ausgangsleistungsaufnahme liegt außerhalb der Spezifikationen.		
PWR	grün, aus	Nicht zutreffend.		Keine Stromversorgung.
	grün, ein			Leistungsaufnahme erfüllt die Spezifikationen.
	gelb, ein			Leistungsaufnahme liegt außerhalb der Spezifikationen.

Zurücksetzen eines Moduls auf die Werkseinstellungen

Wenn zuvor ein Guard I/O-Modul verwendet wurde, löschen Sie die vorherige Konfiguration durch Zurücksetzen des Moduls auf seine Werksteinstellung, bevor Sie es in einem Sicherheitsnetzwerk installieren.

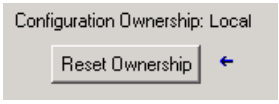
Wenn die Software RSLogix 5000 online geschaltet ist, zeigt die Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) die aktuellen Verwaltungsrechte an der Konfiguration an. Wenn das geöffnete Projekt die Verwaltungsrechte an der Konfiguration hat, wird „Local“ (Zentral) angezeigt. Wenn ein zweites Gerät die Konfiguration verwaltet, werden „Remote“ (Dezentral) sowie die Sicherheitsnetzwerknummer (SNN) und Netzknotenadresse oder Steckplatznummer des Konfigurationsverwalters angezeigt. „Communication error“ (Kommunikationsfehler) wird angezeigt, wenn das Auslesen des Moduls misslingt.

Wenn die Verbindung „Local“ (Zentral) ist, müssen Sie die Modulverbindung vor dem Zurücksetzen der Verwaltungsrechte sperren. Gehen Sie wie folgt vor, um das Modul zu sperren.

1. Klicken Sie mit der rechten Maustaste auf das Modul und wählen Sie „Properties“ (Eigenschaften) aus.
2. Klicken Sie auf die Registerkarte „Connection“ (Verbindung).
3. Wählen Sie „Inhibit Connection“ (Verbindung sperren) aus.
4. Klicken Sie auf „Apply“ (Anwenden) und anschließend auf „OK“.

Gehen Sie wie folgt vor, um das Modul auf seine werkseitige Konfiguration zurückzusetzen, wenn Sie online geschaltet sind.

1. Klicken Sie mit der rechten Maustaste auf das Modul und wählen Sie „Properties“ (Eigenschaften) aus.
2. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).
3. Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen).



TIPP Sie können die Verwaltungsrechte nicht zurücksetzen, wenn noch Änderungen an den Moduleigenschaften ausstehen oder eine Sicherheits-Task-Signatur bzw. eine Sicherheitsverriegelung vorliegt.

Austauschen eines Moduls mithilfe der Software RSLogix 5000

Sie können die Software RSLogix 5000 verwenden, um ein Guard I/O-Modul auf einem Ethernet-Netzwerk auszutauschen. Beim Austausch eines Guard I/O-Moduls auf einem DeviceNet-Netzwerk hängt die Auswahl der Software vom Modultyp ab.

Tabelle 23 – Software

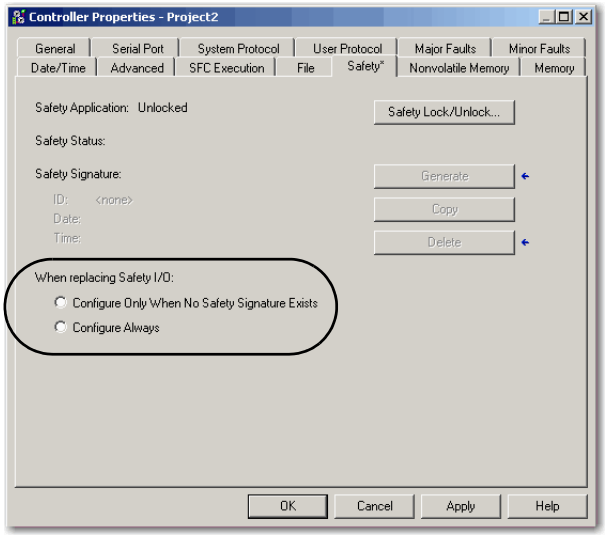
Verwendetes Modul	Zu verwendende Software	Siehe
Guard I/O-Modul der Serie 1791DS mit Adapter 1756-DNB	RSLogix 5000, Software	unten
POINT Guard I/O-Modul der Serie 1734 mit Adapter 1734-PDN	Software RSNetWorx for DeviceNet	Austauschen eines POINT Guard I/O-Moduls über die Software RSNetWorx for DeviceNet auf Seite 89

Wenn Sie auf einen Teil des CIP Safety-Systems angewiesen sind, um das SIL 3-Verhalten während des Austauschs und der Funktionsprüfung eines Moduls aufrecht zu erhalten, kann das Merkmal „Configure Always“ (Immer konfigurieren) nicht verwendet werden. Siehe Austausch bei aktivierter Option „Configure Only When No Safety (Task) Signature Exists“ (Nur konfigurieren, wenn keine Sicherheits- (Task-) Signatur vorliegt) auf Seite 83.

Falls Sie nicht auf das gesamte routingfähige CIP Safety-Steuerungssystem angewiesen sind, um das SIL 3/PLe-Verhalten während des Austauschs und der Funktionsprüfung eines Moduls aufrechtzuerhalten, kann das Merkmal „Configure Always“ (Immer konfigurieren) verwendet werden. Siehe Austausch bei aktivierter Option „Configure Always“ (Immer konfigurieren) auf Seite 87.

Der Modulaustausch wird auf der Registerkarte „Safety“ (Sicherheit) der GuardLogix-Steuerung konfiguriert.

Abbildung 22 – Austauschen eines Sicherheits-E/A-Moduls



Austausch bei aktivierter Option „Configure Only When No Safety (Task) Signature Exists“ (Nur konfigurieren, wenn keine Sicherheits- (Task-) Signatur vorliegt)

Beim Austausch eines Moduls wird die Konfiguration von der Sicherheitssteuerung heruntergeladen, wenn die Gerätekennung (DeviceID) des neuen Moduls mit der des ursprünglichen Moduls übereinstimmt. Die Gerätekennung setzt sich aus der Knoten-/IP-Adresse und der Sicherheitsnetzwerknummer (SNN) zusammen. Sie wird immer aktualisiert, wenn die SNN konfiguriert wird.

Wenn für das Projekt die Option „Configure Only When No Safety (Task) Signature Exists“ (Nur konfigurieren, wenn keine Sicherheits- (Task-) Signatur vorliegt) ausgewählt ist, wenden Sie die in Tabelle 24 beschriebene geeignete Vorgehensweise an, um das POINT Guard I/O-Modul auf Grundlage Ihres Szenarios auszutauschen. Wenn Sie die beschriebenen Schritte ordnungsgemäß durchgeführt haben, stimmt die Gerätekennung mit der ursprünglichen ID

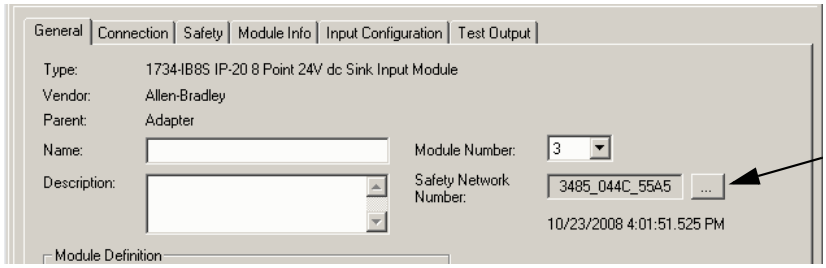
überein, wodurch die Sicherheitssteuerung in der Lage ist, die richtige Modulkonfiguration herunterzuladen. Anschließend wird die Sicherheitsverbindung erneut hergestellt.

Tabelle 24 – Austauschen eines Moduls

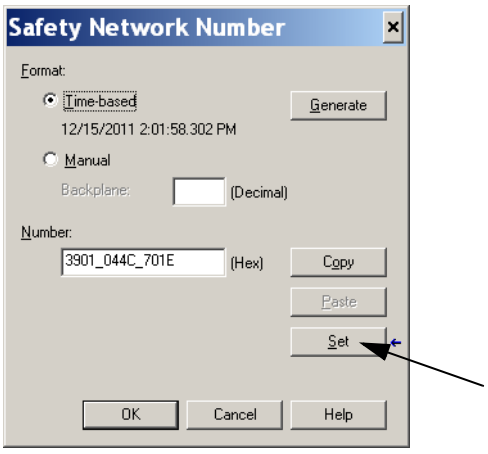
GuardLogix-Sicherheitssignatur vorhanden	Zustand Austauschmodule	Erforderliche Maßnahme
Nein	Keine SNN (Werkseinstellungen)	Keine. Das Modul ist einsatzbereit.
Ja oder Nein	Gleiche SNN wie ursprüngliche Sicherheits-Task-Konfiguration	Keine. Das Modul ist einsatzbereit.
Ja	Keine SNN (Werkseinstellungen)	Siehe Scenario 1 – Austauschmodul ist im Werkszustand und Sicherheits- (Task-) Signatur liegt vor auf Seite 84.
Ja	Andere SNN als ursprüngliche Sicherheits-Task-Konfiguration	Siehe Scenario 2 – Austauschmodul hat andere SNN als ursprüngliches Modul und Sicherheits- (Task-) Signatur liegt vor auf Seite 85.
Nein		Siehe Scenario 3 – Austauschmodul hat andere SNN als ursprüngliches Modul und Sicherheits- (Task-) Signatur liegt nicht vor auf Seite 87.

Scenario 1 – Austauschmodul ist im Werkszustand und Sicherheits- (Task-) Signatur liegt vor

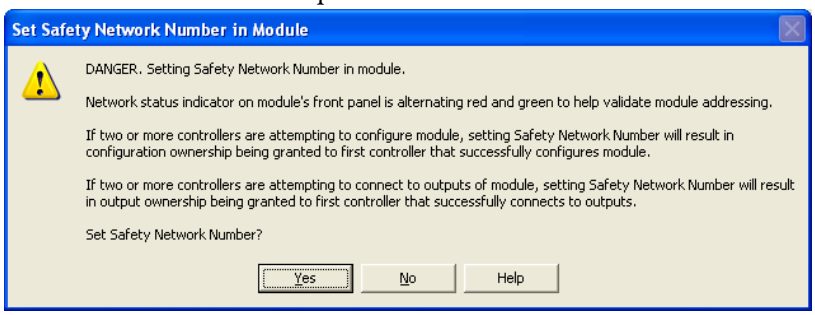
1. Entfernen Sie das alte E/A-Modul und installieren Sie das neue Modul.
2. Klicken Sie mit der rechten Maustaste auf das POINT Guard I/O-Austauschmodul und wählen Sie „Properties“ (Eigenschaften) aus.
3. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.



4. Klicken Sie auf „Set“ (Festlegen).



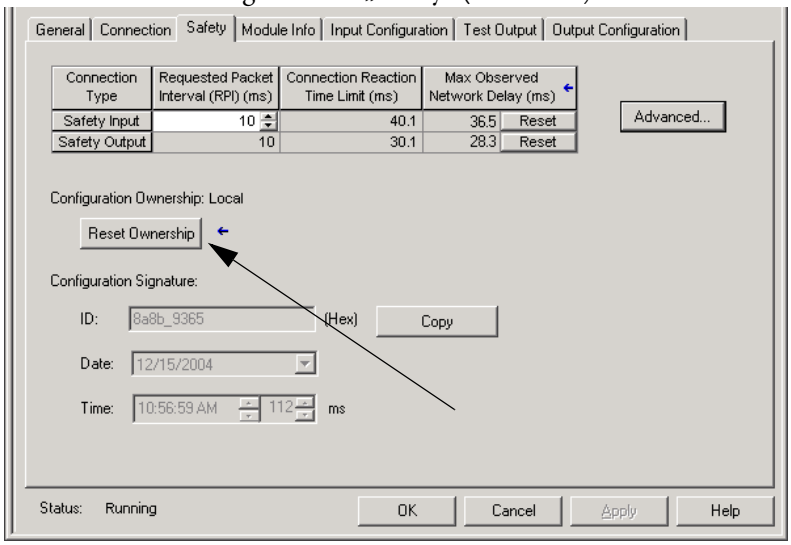
5. Vergewissern Sie sich, dass die Statusanzeige für den Netzwerkstatus (NS) am richtigen Modul abwechselnd rot und grün aufleuchtet, bevor Sie im Bestätigungsdialogfeld auf „Yes“ (Ja) klicken, um die SNN festzulegen und das Austauschmodul zu akzeptieren.



6. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Modul und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

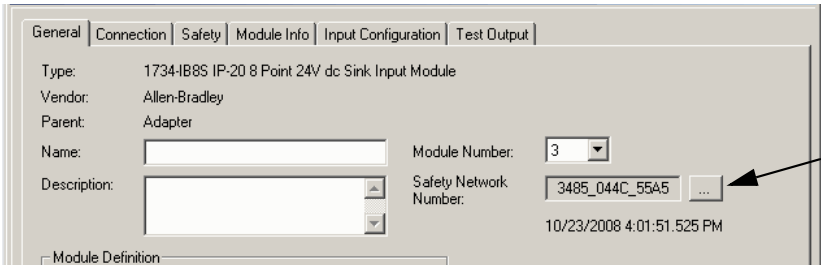
Scenario 2 – Austauschmodul hat andere SNN als ursprüngliches Modul und Sicherheits-(Task-) Signatur liegt vor

1. Entfernen Sie das alte E/A-Modul und installieren Sie das neue Modul.
2. Klicken Sie mit der rechten Maustaste auf Ihr POINT Guard I/O-Modul und wählen Sie „Properties“ (Eigenschaften) aus.
3. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).

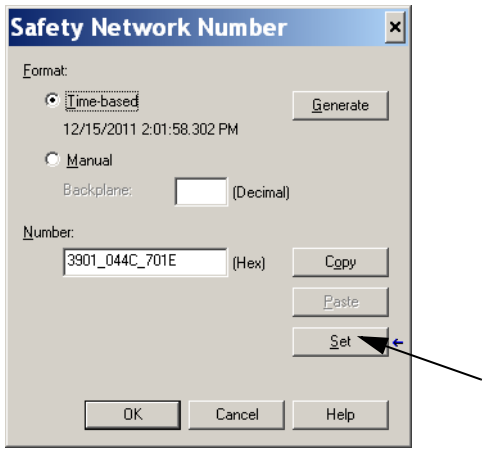


4. Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen).
5. Klicken Sie auf „OK“.
6. Klicken Sie mit der rechten Maustaste auf Ihre Steuerung und wählen Sie „Properties“ (Eigenschaften) aus.

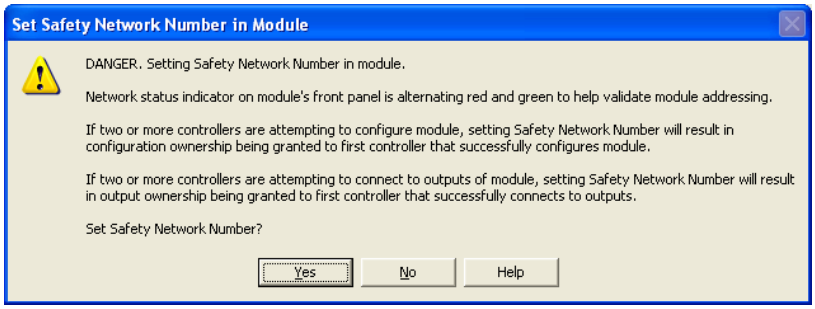
7. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.



8. Klicken Sie auf „Set“ (Festlegen).



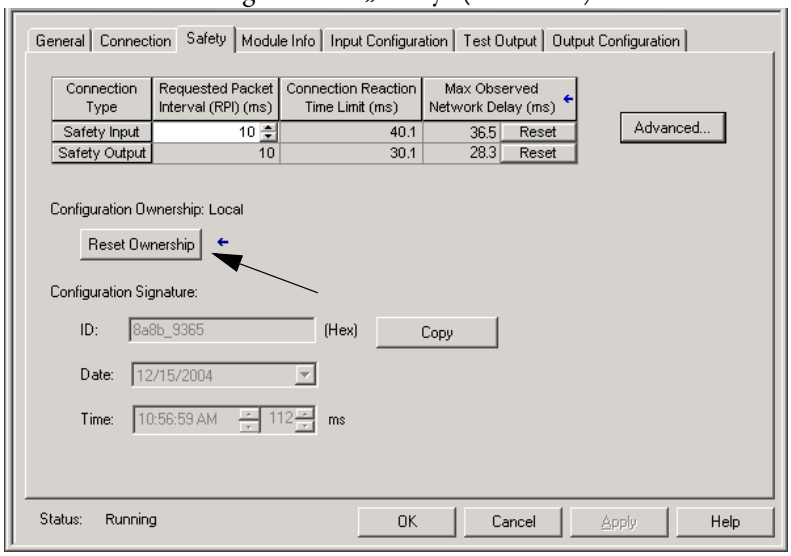
9. Vergewissern Sie sich, dass die Statusanzeige für den Netzwerkstatus (NS) am richtigen Modul abwechselnd rot und grün aufleuchtet, bevor Sie im Bestätigungsdialogfeld auf „Yes“ (Ja) klicken, um die SNN festzulegen und das Austauschmodul zu akzeptieren.



10. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Modul und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

Scenario 3 – Austauschmodul hat andere SNN als ursprüngliches Modul und Sicherheits-(Task-) Signatur liegt nicht vor

1. Entfernen Sie das alte E/A-Modul und installieren Sie das neue Modul.
2. Klicken Sie mit der rechten Maustaste auf Ihr POINT Guard I/O-Modul und wählen Sie „Properties“ (Eigenschaften) aus.
3. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).



4. Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen).
5. Klicken Sie auf „OK“.
6. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Modul und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

Austausch bei aktivierter Option „Configure Always“ (Immer konfigurieren)

ACHTUNG: Aktivieren Sie die Option „Configure Always“ (Immer konfigurieren) nur, wenn die Beibehaltung des SIL 3-Verhaltens während des Austauschs und der Funktionstests eines Moduls **nicht** vom gesamten CIP Safety-Steuerungssystem abhängt.

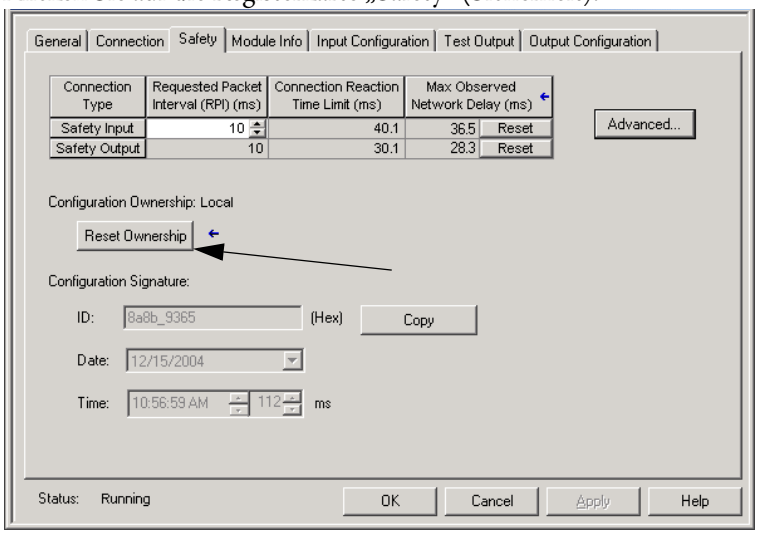
Installieren Sie Module im Werkszustand in einem CIP Safety-Netzwerk bei aktivierter Funktion „Configure Always“ (Immer konfigurieren) nur, wenn Sie dieses Austauschverfahren befolgen.

Wenn die Option „Configure Always“ (Immer konfigurieren) in der Software RSLogix 5000 aktiviert ist, sucht die Steuerung automatisch ein Austauschmodul, das den folgenden Anforderungen entspricht, und stellt eine Verbindung zu diesem Modul her:

- Die Steuerung hat an dieser Netzwerkadresse Konfigurationsdaten für ein kompatibles Modul.
- Das Modul befindet sich im Werkszustand oder verfügt über eine SNN, die mit der Konfiguration übereinstimmt.

Wenn für die Projektkonfiguration die Option „Configure Always“ (Immer konfigurieren) aktiviert ist, wenden Sie die entsprechende Vorgehensweise zum Austausch eines POINT Guard I/O-Moduls an.

1. Entfernen Sie das alte E/A-Modul und installieren Sie das neue Modul.
   a. Befindet sich das Modul im Werkszustand, fahren Sie mit Schritt 6 fort. Es muss keine Maßnahme ergriffen werden, damit die GuardLogix-Steuerung die Verwaltungsrechte für das Modul erhält.
   b. Tritt ein Fehler aufgrund nicht übereinstimmender SNN auf, fahren Sie mit dem nächsten Schritt fort, um das Modul in den Werkszustand zurückzusetzen.
2. Klicken Sie mit der rechten Maustaste auf Ihr POINT Guard I/O-Modul und wählen Sie „Properties“ (Eigenschaften) aus.
3. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).



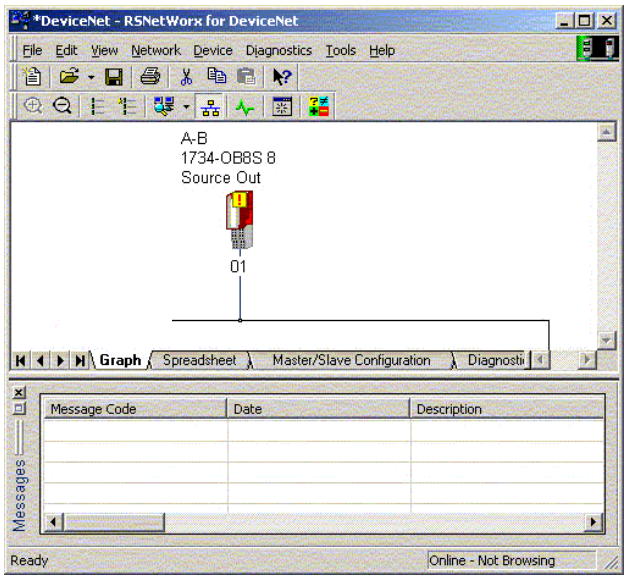
4. Klicken Sie auf „Reset Ownership“ (Verwaltungsrechte zurücksetzen).
5. Klicken Sie auf „OK“.
6. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Modul und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

Austauschen eines POINT Guard I/O-Moduls über die Software RSNetWorx for DeviceNet

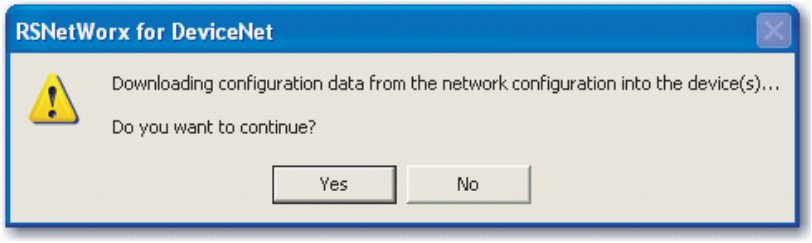
Gehen Sie wie im Folgenden beschrieben vor, um ein POINT Guard I/O-Modul auszutauschen, wenn das Modul und die Steuerung auf einem DeviceNet-Netzwerk betrieben werden.

1. Tauschen Sie das Modul aus und stimmen Sie die Knotennummer mit der des ursprünglichen Moduls ab.
2. Öffnen Sie Ihr Projekt in der Software RSNetWorx for DeviceNet.

   Befindet sich das Austauschmodul im Werkszustand oder verfügt es über eine SNN, die nicht mit der des ursprünglichen Moduls übereinstimmt, ist das Modul mit einem Ausrufzeichen versehen.

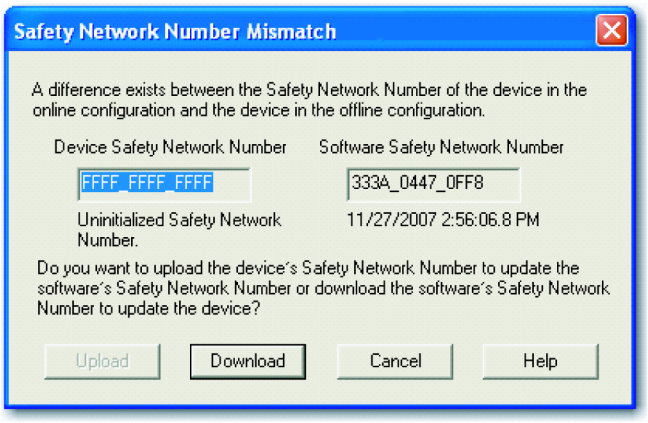


3. Klicken Sie mit der rechten Maustaste auf das Modul und wählen „Download to Device“ (Auf Gerät herunterladen).

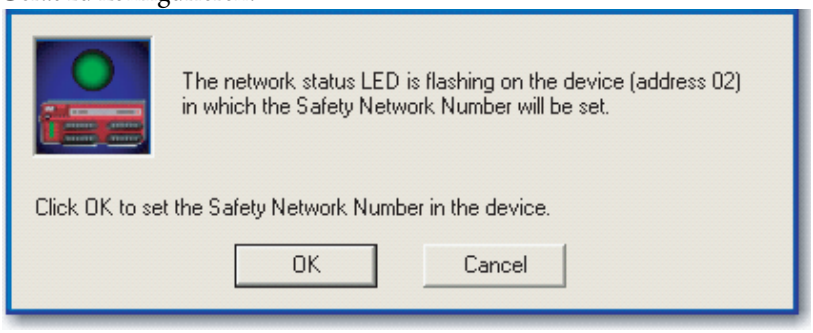


4. Klicken Sie auf „Yes“ (Ja), um den Vorgang zu bestätigen.

5. Klicken Sie auf „Download“ (Herunterladen) im Dialogfeld „Safety Network Number Mismatch“ (Nicht übereinstimmende Sicherheitsnetzwerknummer), um die SNN auf dem Austauschmodul zu konfigurieren.



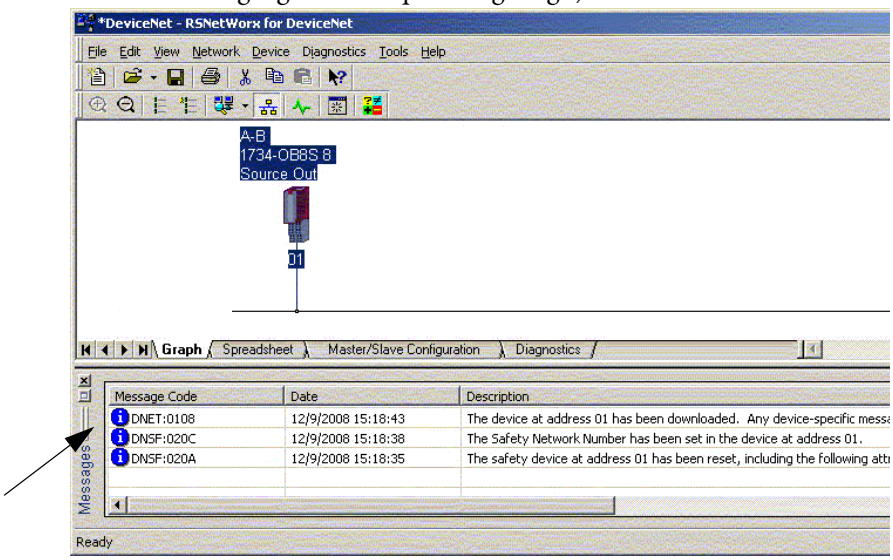
6. Vergewissern Sie sich, dass die Anzeige für den Netzwerkstatus (NS) am richtigen Modul blinkt und klicken Sie auf „OK“, um die SNN auf diesem Gerät zu konfigurieren.



Die Software RSNetWorx for DeviceNet bestätigt, dass die SNN konfiguriert wurde.

Nach dem erfolgreichen Herunterladen zeigt das Hauptprojekt die folgende Meldung an: „The device at address *xx* has been downloaded. Any device-specific messages related to the download operation are displayed separately.“ (Das Gerät an Adresse xx wurde heruntergeladen.

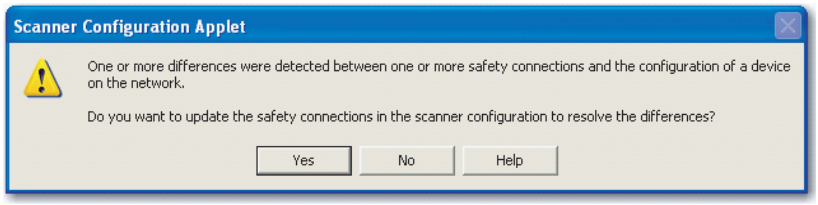
Alle gerätespezifischen Meldungen im Zusammenhang mit dem Download-Vorgang werden separat angezeigt.)



Angenommen, dass dies die richtige Konfiguration von der ursprünglichen DNT-Datei ist, stimmen die SNN und die Konfigurationssignatur nun mit der ursprünglichen SNN bzw. Signatur überein. Wenn bereits ein Anschluss an die Steuerung besteht, wird eine Verbindung hergestellt. Die Steuerung kann im Run-Modus verbleiben, während die Konfiguration auf das Austauschmodul heruntergeladen wird.

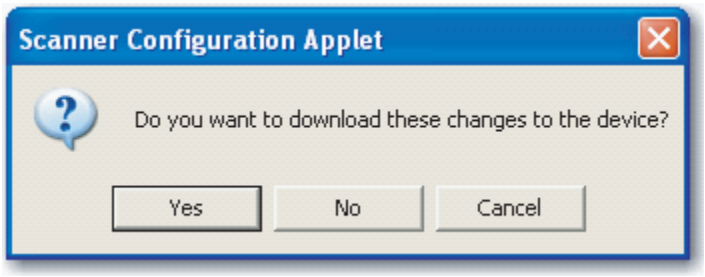
Wenn Sie diese Konfiguration auf eine temporäre Einrichtung herunterladen, platzieren Sie das Modul im Netzwerk, wo es automatisch eine Verbindung zur Steuerung herstellt.

Stammte die auf das Modul heruntergeladene Konfiguration nicht von der ursprünglichen DNT-Datei, stimmt die Konfigurationssignatur nicht mit der ursprünglichen Signatur überein. Auch wenn Sie dieselben Parameter in einer neuen DNT-Datei erzeugen, unterscheiden sich die Zeit- und Datumsanteile der Signatur, so dass die Verbindung zur Steuerung nicht hergestellt wird. Klicken Sie in diesem Fall auf die Registerkarte „Safety Connection“ (Sicherheitsverbindung) für die Steuerung, die meldete, dass eine andere Konfigurationssignatur vorliegt. Ihnen wird dann die Option angeboten, die neue Konfigurationssignatur abzustimmen. Sie sollten jedoch zuerst das Sicherheitssystem erneut validieren, da nicht die ursprüngliche DNT-Datei verwendet wird.



7. Klicken Sie auf „Yes“ (Ja).

   Dadurch wird der Run-Modus der Steuerung beendet und Sie werden aufgefordert, die Änderungen herunterzuladen.



8. Klicken Sie auf „Yes“ (Ja), um die neue Verbindungskonfiguration auf die SmartGuard-Steuerung herunterzuladen.

   Nach dem Download wechselt die Steuerung wieder zurück in den Run-Modus und die Verbindung zum Austauschmodul wird hergestellt.

9. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Modul und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

Entwicklung von Sicherheitsanwendungen

In diesem Kapitel werden die Komponenten erläutert, aus denen ein Sicherheitsprojekt besteht. Es bietet Informationen zur Verwendung der Funktionen, die die Integrität der Sicherheitsanwendung schützen, wie z. B. die Sicherheits-Task-Signatur und die Sicherheitsverriegelung.

Informationen zu Richtlinien und Anforderungen für die Entwicklung und Inbetriebnahme von SIL 3- und PLe-Sicherheitsanwendungen enthält die Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch.

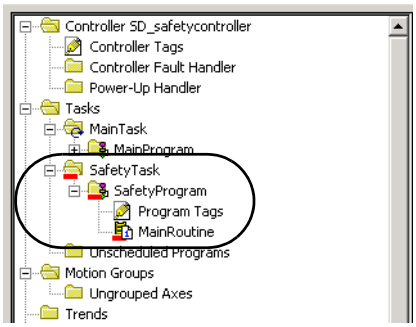
Das Sicherheitsreferenzhandbuch beinhaltet folgende Themen:

- Erstellen einer detaillierten Projektspezifikation
- Schreiben, Dokumentieren und Testen der Anwendung
- Generieren der Sicherheits-Task-Signatur, um das Projekt zu identifizieren und zu schützen
- Bestätigen des Projekts durch Ausdruck oder Anzeige des hochgeladenen Projekts und durch manuelles Vergleichen der Konfigurationen, Sicherheitsdaten und der Sicherheitsprogrammlogik
- Verifizieren des Projekts durch Prüffälle, Simulationen, Funktionsverifikationsprüfungen und eine unabhängige Sicherheitsüberprüfung, falls erforderlich
- Verriegeln der Sicherheitsanwendung
- Berechnen der Reaktionszeit des Systems

Die Sicherheits-Task

Wenn Sie ein Sicherheitssteuerungsprojekt erstellen, generiert die Software RSLogix 5000 automatisch eine Sicherheits-Task mit einem Sicherheitsprogramm und einer Haupt(sicherheits)routine.

Abbildung 23 – Sicherheits-Task im Controller Organizer (Steuerungsorganisator)



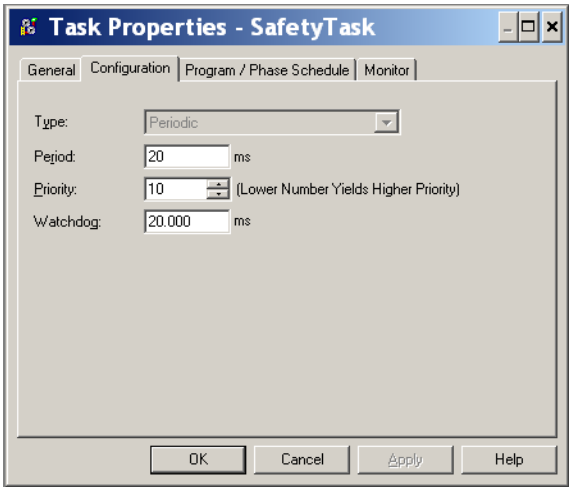
Innerhalb der Sicherheits-Task können Sie mehrere Sicherheitsprogramme verwenden, die aus mehreren Sicherheitsroutinen bestehen. Die GuardLogix-Steuerung unterstützt eine Sicherheits-Task. Die Sicherheits-Task kann nicht gelöscht werden.

Innerhalb der Sicherheits-Task können Sie keine Standardprogramme planen oder Standardroutinen ausführen.

Spezifizieren der Sicherheits-Task-Zeitspanne

Die Sicherheits-Task ist eine periodische/zeitgesteuerte Task. Sie wählen die Task-Priorität und den Überwachungszeitraum über das Dialogfeld „Task Properties – Safety Task“ (Task-Eigenschaften – Sicherheits-Task) aus. Öffnen Sie das Dialogfeld, indem Sie mit der rechten Maustaste auf die Sicherheits-Task klicken und dann „Properties“ (Eigenschaften) auswählen.

Abbildung 24 – Konfigurieren der Zeitspanne für die Sicherheits-Task



Die Sicherheits-Task muss über die Priorität „Hoch“ verfügen. Sie geben sowohl die Zeitspanne der Sicherheits-Task (in ms) als auch den Watchdog der Sicherheits-Task (in ms) an. Die Sicherheits-Task-Zeitspanne ist der Zeitraum, in dem die Sicherheits-Task ausgeführt wird. Der Sicherheits-Task-Watchdog ist die maximale, zugelassene Zeit vom Start der Ausführung der Sicherheits-Task bis zu deren Beendigung.

Die Zeitspanne der Sicherheits-Task ist begrenzt auf ein Maximum von 500 ms und kann online nicht geändert werden. Stellen Sie sicher, dass der Sicherheits-Task genügend Zeit zum Abschluss der Logikausführung bleibt, bevor sie erneut ausgelöst wird. Wenn während des Überwachungszeitraums für die Sicherheits-Task ein Timeout auftritt, wird ein nicht behebbarer Sicherheitsfehler in der Sicherheitssteuerung generiert.

Die Zeitspanne für die Sicherheits-Task wirkt sich direkt auf die Reaktionszeit des Systems aus.

Publikation 1756-RM093, „Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch“, enthält detaillierte Informationen über die Berechnung der Reaktionszeit des Systems.

Ausführen der Sicherheits-Task

Die Sicherheits-Task wird genau so ausgeführt wie eine periodische Standard-Task, allerdings mit folgenden Ausnahmen:

- Die Sicherheits-Task beginnt mit der Ausführung erst, wenn die Primärsteuerung und der Sicherheitspartner ihre Steuerungspartnerschaft festlegen. (Standard-Tasks beginnen mit der Ausführung, sobald die Steuerung in den Run-Modus wechselt.)

- Alle Sicherheitseingangs-Tags (Eingänge, konsumiert und zugeordnet) werden aktualisiert und zu Beginn der Ausführung der Sicherheits-Task eingefroren.

  Auf Seite 106 finden Sie weitere Informationen über die Zuordnung von Sicherheits-Tags.

- Die Werte der Sicherheitsausgangs-Tags (Ausgänge und produzierte Werte) werden nach Abschluss der Ausführung der Sicherheits-Task aktualisiert.

Sicherheitsprogramme

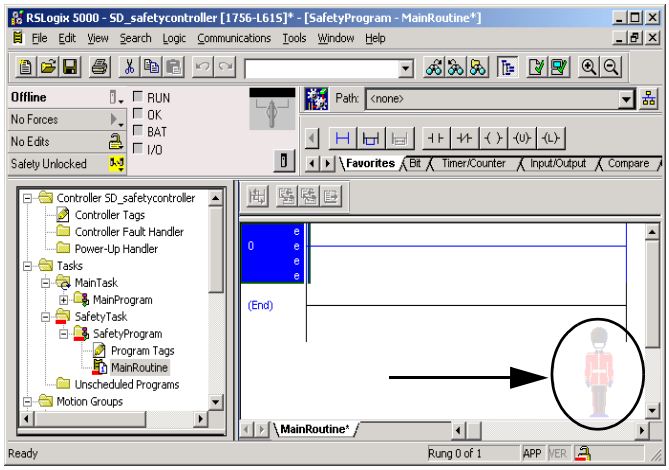
Sicherheitsprogramme besitzen sämtliche Attribute eines Standardprogramms, werden jedoch in der Sicherheits-Task geplant und können nur Sicherheitskomponenten enthalten. Sicherheitsprogramme können nur Sicherheitsroutinen enthalten, von denen eine als Hauptroutine bestimmt sein muss und eine als Fehlerroutine bestimmt sein kann.

Sicherheitsprogramme können keine Standardroutinen oder Standard-Tags enthalten.

Sicherheitsroutinen

Sicherheitsroutinen besitzen sämtliche Attribute einer Standardroutine, sind jedoch nur in einem Sicherheitsprogramm vorhanden. Momentan wird für Sicherheitsroutinen nur die Kontaktplanlogik unterstützt.

TIPP Die Software RSLogix 5000 verwendet ein Wasserzeichen, um visuell zwischen einer Sicherheitsroutine und einer Standardroutine zu unterscheiden.



Sicherheits-Tags

Ein Tag ist ein Bereich im Speicher der Steuerung, in dem Daten gespeichert werden. Tags sind der grundlegende Mechanismus zur Speicherzuweisung, zur Bezugnahme auf Daten aus der Logik sowie zur Datenüberwachung. Sicherheits-Tags besitzen alle Attribute von Standard-Tags sowie zusätzliche zertifizierte Mechanismen zur Sicherstellung der SIL 3-Datenintegrität.

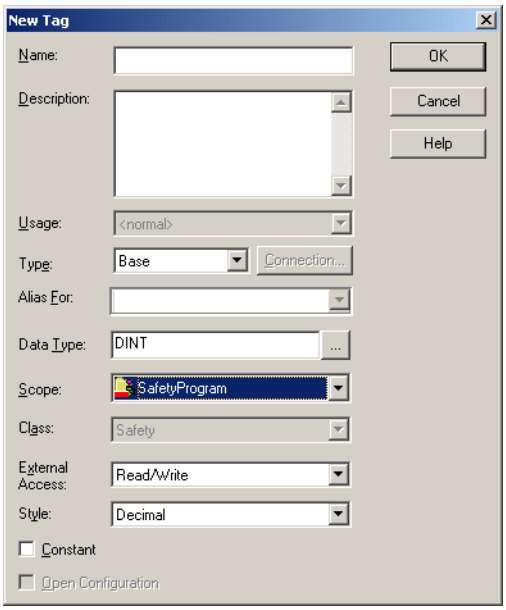
Folgende Eigenschaften sind einem Tag bei seiner Erstellung zuzuweisen:

- Name
- Beschreibung (optional)
- Tag-Typ
- Datentyp
- Bereich
- Klasse
- Stil
- Externer Zugriff

Sie können auch angeben, ob die Tag-Werte konstant sein sollen.

Öffnen Sie zum Erstellen eines Sicherheits-Tags das Dialogfeld „New Tag“ (Neues Tag), indem Sie mit der rechten Maustaste auf „Controller Tags“ (Steuerungs-Tags) oder „Program Tags“ (Programm-Tags) klicken und „New Tag“ (Neues Tag) auswählen.

Abbildung 25 – Erstellen eines neuen Tags



Tag-Typ

In Tabelle 25 werden die vier Tag-Typen definiert: Basis, Alias, Produziert und Konsumiert.

Tabelle 25 – Vier Tag-Typen

Tag-Typ	Beschreibung
Basis	Diese Tags speichern Werte, die von der Logik innerhalb des Projekts verwendet werden.
Alias	Ein Tag, das auf ein anderes Tag hinweist. Ein Alias-Tag kann auf ein anderes Alias-Tag oder ein Basis-Tag hinweisen. Ein Alias-Tag kann sich auch auf eine Komponente eines anderen Tags beziehen, indem es auf ein Glied einer Struktur verweist, ein Datenfeldelement oder ein Bit innerhalb eines Tags oder eines Glieds. **WICHTIG:** Das Aliasing zwischen Standard-Tags und Sicherheits-Tags ist in Sicherheitsanwendungen unzulässig. Stattdessen ermöglicht die entsprechende Sicherheits-Tag-Zuordnungsfunktion eine Zuordnung von Standard-Tags zu Sicherheits-Tags. Siehe Zuordnen von Sicherheits-Tags auf Seite 106.
Produziert	Ein Tag, das von einer Steuerung für die Verwendung durch andere Steuerungen zur Verfügung gestellt wird. Maximal 15 Steuerungen können gleichzeitig Daten konsumieren (empfangen). Ein produziertes Tag sendet seine Daten an ein oder mehrere konsumierende Tags ohne Verwendung von Logik. Die produzierten Tag-Daten werden mit dem RPI des konsumierenden Tags übermittelt.
Konsumiert	Ein Tag, das Daten eines produzierten Tags empfängt. Der Datentyp des konsumierten Tags muss mit dem Datentyp des produzierten Tags übereinstimmen. Das angeforderte Paketintervall (RPI) des konsumierten Tags bestimmt den Zeitraum, in dem die Daten aktualisiert werden.

Datentyp

Der Datentyp definiert den Datentyp, den das Tag speichert, wie z. B. Bit oder Ganzzahl.

Datentypen können zu Strukturen kombiniert werden. Eine Struktur stellt einen eindeutigen Datentyp zur Verfügung, der mit einer bestimmten Anforderung übereinstimmt. Innerhalb einer Struktur wird jeder individuelle Datentyp als Glied bezeichnet. Wie Tags haben auch Glieder einen Namen und einen Datentyp. Sie können Ihre eigenen Strukturen als benutzerdefinierte Datentypen erstellen.

Logix-Steuerungen enthalten vordefinierte Datentypen für die Verwendung mit spezifischen Befehlen.

Für Sicherheits-Tags sind nur die folgenden Datentypen zulässig:

Tabelle 26 – Gültige Datentypen für Sicherheits-Tags

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

Datentypen des Typs REAL sind in 1756-L7*x*S-Steuerungsprojekten gültig; in 1756-L6*x*S- oder 1768-L4*x*S-Steuerungsprojekten sind sie dagegen ungültig.

WICHTIG Diese Einschränkung beinhaltet benutzerdefinierte Datentypen, die einen der vordefinierten Datentypen enthalten.

Bereich

Der Bereich eines Tags legt fest, wo Sie Zugriff auf die Tag-Daten haben. Wenn Sie ein Tag erstellen, definieren Sie dieses als Steuerungs-Tag (globale Daten) oder als Programm-Tag für ein spezifisches Sicherheitsprogramm oder ein Standardprogramm (lokale Daten). Sicherheits-Tags können Steuerungsbereichs- oder Sicherheitsprogrammbereichs-Tags sein.

Steuerungsbereichs-Tags

Bei den Steuerungsbereichs-Sicherheits-Tags haben sämtliche Programme Zugriff auf die Sicherheitsdaten. Steuerungsbereichs-Tags sind notwendig, wenn sie:

- in mehr als einem Programm des Projekts verwendet werden.
- zum Produzieren oder Konsumieren von Daten verwendet werden.
- für die Kommunikation mit einem PanelView-/Bedienerschnittstellen-Terminal verwendet werden.
- zum Zuordnen von Sicherheits-Tags verwendet werden.
  Weitere Informationen finden Sie unter Zuordnen von Sicherheits-Tags auf Seite 106.

Steuerungsbereichs-Sicherheits-Tags können von Standardroutinen gelesen, aber nicht geschrieben werden.

WICHTIG	Steuerungsbereichs-Sicherheits-Tags können von jeder Standardroutine gelesen werden. Die Aktualisierungsgeschwindigkeit des Sicherheits-Tags basiert auf der Zeitspanne der Sicherheits-Task.

Die mit Sicherheits-E/A und produzierten oder konsumierten Sicherheitsdaten assoziierten Tags müssen Steuerungsbereichs-Sicherheits-Tags sein. Für produzierte/konsumierte Sicherheits-Tags müssen Sie einen benutzerdefinierten Datentyp erstellen, wobei das erste Glied der Tag-Struktur für den Status der Verbindung reserviert ist. Dieses Glied ist ein vordefinierter Datentyp mit dem Namen CONNECTION_STATUS.

Tabelle 27 – Weitere Informationen

Quelle	Beschreibung
Sicherheitsverbindungen auf Seite 131	Enthält weitere Informationen zum Glied CONNECTION_STATUS (VERBINDUNGS_STATUS)
Steuerungen Logix5000 – E/A- und Tag-Daten – Programmierhandbuch, Publikation 1756-PM004	Enthält Anweisungen zur Erstellung benutzerdefinierter Datentypen

Programmbereichs-Tags

Bei Programmbereichs-Tags werden die Daten von den anderen Programmen isoliert. Die Wiederverwendung von Programmbereichs-Tag-Namen ist zwischen Programmen erlaubt.

Programmbereichs-Sicherheits-Tags können nur über eine Sicherheitsroutine in demselben Sicherheitsprogramm gelesen oder geschrieben werden.

Klasse

Tags können als Standard- oder als Sicherheits-Tags klassifiziert werden. Tags, die als Sicherheits-Tags klassifiziert sind, müssen über einen Datentyp verfügen, der für Sicherheits-Tags zulässig ist.

Wenn Sie Programmbereichs-Tags erstellen, wird die Klasse automatisch spezifiziert, und zwar abhängig davon, ob das Tag in einem Standard- oder einem Sicherheitsprogramm erstellt wurde.

Wenn Sie Steuerungsbereichs-Tags erstellen, müssen Sie die Klasse des Tags manuell auswählen.

Konstanter Wert

Wenn Sie ein Tag als konstanten Wert festlegen, kann dieses nicht durch die Logik in der Steuerung oder durch eine externe Anwendung wie z. B. eine Bedienerschnittstelle geändert werden. Tags mit konstanten Werten können nicht geforct werden.

Über die Software RSLogix 5000 können konstante Standard-Tags und Sicherheits-Tags geändert werden, sofern keine Sicherheits-Task-Signatur vorliegt. Sicherheits-Tags können nicht geändert werden, wenn eine Sicherheits-Task-Signatur vorliegt.

Externer Zugriff

Der externe Zugriff definiert die Zugriffsebene, die für ein externes Gerät, wie z. B. eine Bedienerschnittstelle (HMI), zum Anzeigen oder Ändern von Tag-Werten zulässig ist. Der Zugriff über die Software RSLogix 5000 wird durch diese Einstellung nicht beeinflusst. Standardmäßig ist der Lese-/Schreibzugriff aktiviert.

Tabelle 28 – Stufen für externen Zugriff

Einstellung für externen Zugriff	Beschreibung
None (Ohne)	Von außerhalb der Steuerung kann nicht auf Tags zugegriffen werden.
Read Only (Schreibgeschützt)	Die Tags können durchsucht und angezeigt werden. Von außerhalb der Steuerung sind jedoch keine Änderungen an diesen Tags möglich.
Read/Write (Lese-/Schreibzugriff)	Die Standard-Tags können von außerhalb der Steuerung durchsucht, angezeigt und geändert werden.

Für Alias-Tags entspricht der Typ des externen Zugriffs dem Typ, der für das Basis-Ziel-Tag konfiguriert wurde.

Produzierte/konsumierte Sicherheits-Tags

Um Sicherheitsdaten zwischen GuardLogix-Steuerungen zu übertragen, müssen Sie produzierte und konsumierte Sicherheits-Tags verwenden. Alle produzierten und konsumierten Tags erfordern eine Verbindung. Der Standardverbindungstyp für produzierte und konsumierte Tags ist ab Version 19 der Software RSLogix 5000 Unicast.

Tabelle 29 – Produzierte und konsumierte Verbindungen

Tag	Beschreibung der Verbindung
Produziert	Eine GuardLogix-Steuerung kann Sicherheits-Tags für andere 1756- oder 1768-GuardLogix-Steuerungen produzieren (an diese senden). Die produzierende Steuerung verwendet für jeden Consumer eine einzelne Verbindung.
Konsumiert	GuardLogix-Steuerungen können Sicherheits-Tags von anderen 1756- oder 1768-GuardLogix-Steuerungen konsumieren (empfangen). Jedes konsumierte Tag konsumiert eine Verbindung.

Produzierte und konsumierte Sicherheits-Tags unterliegen den folgenden Einschränkungen:

- Nur auf Steuerungsbereichs-Sicherheits-Tags kann gemeinsam zugegriffen werden.
- Produzierte und konsumierte Sicherheits-Tags sind auf 128 Byte begrenzt.
- Produzierte/konsumierte Tag-Paare müssen den gleichen benutzerdefinierten Datentyp haben.
- Das erste Glied dieses benutzerdefinierten Datentyps muss vom vordefinierten Datentyp CONNECTION_STATUS sein.
- Das angeforderte Paketintervall (RPI) des konsumierten Sicherheits-Tags muss der Zeitspanne der Sicherheits-Task der produzierenden GuardLogix-Steuerung entsprechen.

Die richtige Konfiguration produzierter und konsumierter Sicherheits-Tags für die gemeinsame Datennutzung zwischen Peer-Sicherheitssteuerungen erfordert das richtige Konfigurieren der Peer-Sicherheitssteuerungen, das Produzieren eines Sicherheits-Tags und das Konsumieren eines Sicherheits-Tags, wie nachfolgend beschrieben.

Konfigurieren der Sicherheitsnetzwerknummern von Peer-Sicherheitssteuerungen

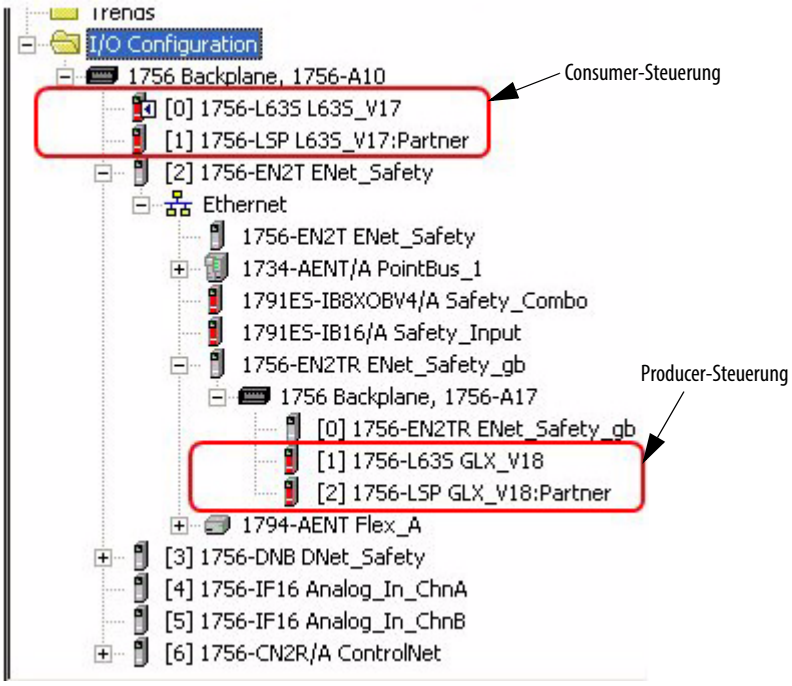
Die Peer-Sicherheitssteuerung unterliegt den gleichen Konfigurationsanforderungen wie die lokale Sicherheitssteuerung. Die Peer-Sicherheitssteuerung muss ebenfalls über eine Sicherheitsnetzwerknummer (SNN) verfügen. Die SNN der Peer-Sicherheitssteuerung hängt von deren Platzierung im System ab.

Tabelle 30 – SNN und Steuerungsplatzierung

Position der Peer-Sicherheitssteuerung	SNN
Im lokalen Chassis	GuardLogix-Steuerungen, die sich im selben Chassis befinden, müssen auch dieselbe SNN aufweisen.
In einem anderen Chassis	Die Steuerung muss über eine eindeutige SNN verfügen.

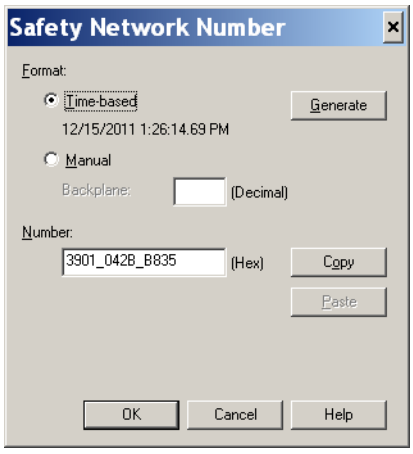
Gehen Sie wie folgt vor, um die SNN zu kopieren und einzufügen.

1. Fügen Sie die Producer-Steuerung dem E/A-Konfigurationsverzeichnis der Consumer-Steuerung hinzu.



2. Klicken Sie im Steuerungsprojekt des Producers mit der rechten Maustaste auf die produzierende Steuerung und wählen Sie „Controller Properties“ (Steuerungseigenschaften) aus.
3. Kopieren Sie die SNN der Producer-Steuerung.

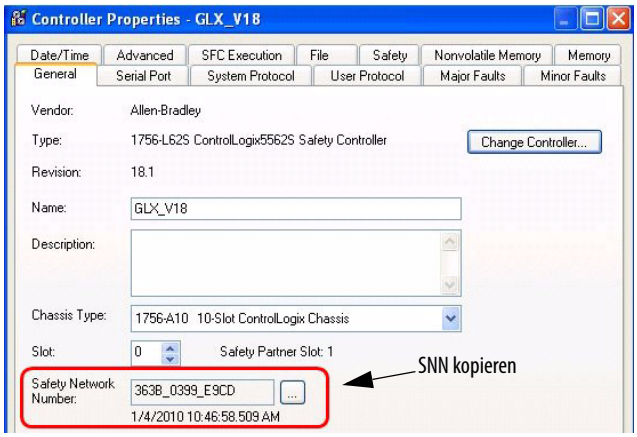
TIPP Eine SNN kann mithilfe einer Schaltfläche im Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) kopiert und eingefügt werden. Öffnen Sie das entsprechende Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer), indem Sie jeweils rechts neben dem SNN-Feld im Eigenschaftendialogfeld auf die Schaltfläche ... klicken.



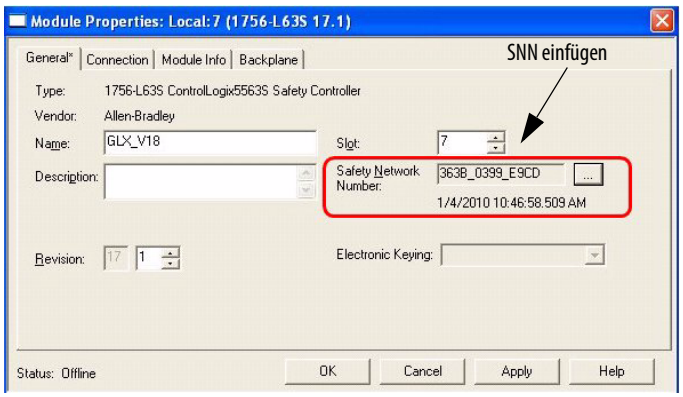
4. Klicken Sie im Steuerungsprojekt des Consumers mit der rechten Maustaste auf die produzierende Steuerung und wählen Sie „Module Properties“ (Moduleigenschaften) aus.

5. Fügen Sie die SNN der produzierenden Steuerung in das SNN-Feld ein.

Dialogfeld „Controller Properties“ (Steuerungseigenschaften) des Producers im Producer-Projekt



Dialogfeld „Module Properties“ (Moduleigenschaften) im Consumer-Projekt



Erstellen eines Sicherheits-Tags

Gehen Sie zum Erstellen eines Sicherheits-Tags wie folgt vor.

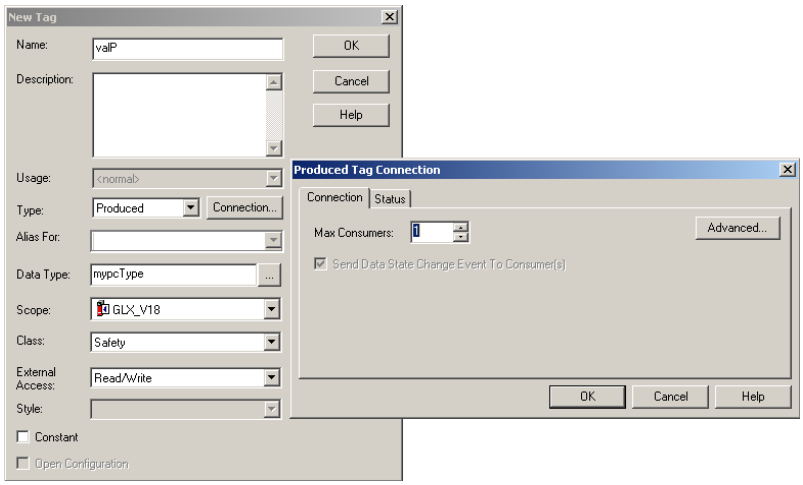
1. Erstellen Sie im Projekt der produzierenden Steuerung einen benutzerdefinierten Datentyp, der die Struktur der zu produzierenden Daten definiert.

   Vergewissern Sie sich, dass das erste Datenglied den Datentyp CONNECTION_STATUS aufweist.

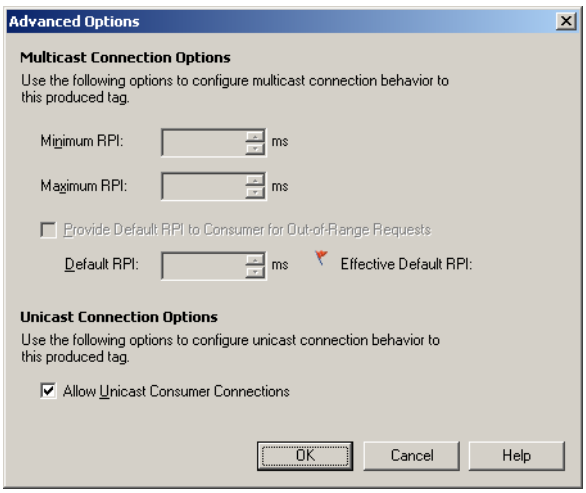
2. Klicken Sie mit der rechten Maustaste auf „Controller Tags“ (Steuerungs-Tags) und wählen Sie „New Tag“ (Neues Tag) aus.

3. Legen Sie als Typ „Produced“ (Produziert), für die Klasse „Safety“ (Sicherheit) und als Datentyp den in Schritt 1 erstellten benutzerdefinierten Datentyp fest.

4. Klicken Sie auf „Connection“ (Verbindung) und geben Sie die Anzahl der Steuerungen ein, die Daten konsumieren werden.



5. Klicken Sie auf „Advanced“ (Erweitert), wenn Sie den Verbindungstyp durch Deaktivierung von „Allow Unicast Consumer Connections“ (Unicast-Consumer-Verbindungen zulassen) ändern möchten.



6. Klicken Sie auf „OK“.

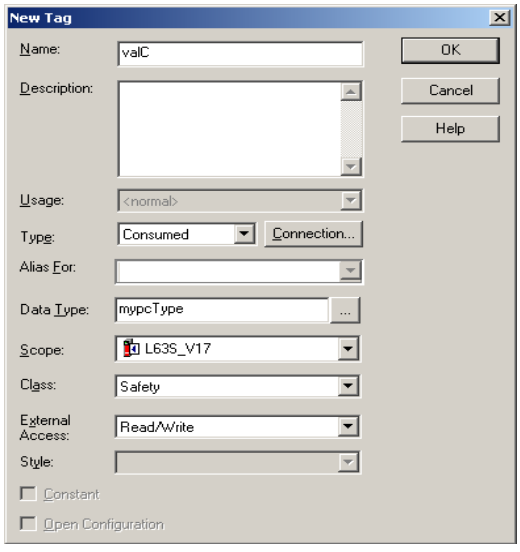
Konsumieren von Sicherheits-Tag-Daten

Gehen Sie wie folgt vor, um Daten zu konsumieren, die von einer anderen Steuerung produziert wurden.

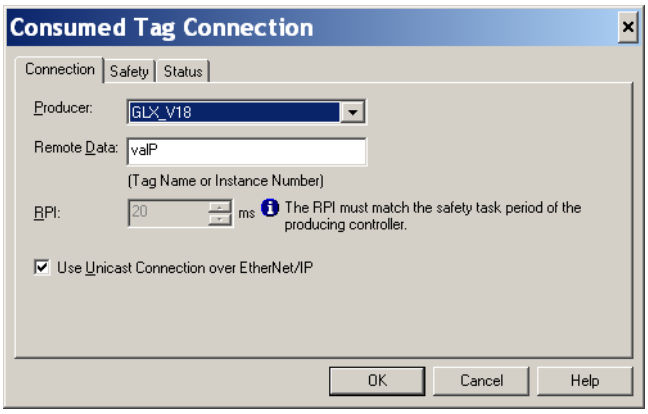
1. Erstellen Sie im Projekt der konsumierenden Steuerung einen benutzerdefinierten Datentyp, der mit dem im Producer-Projekt erstellten Datentyp identisch ist.

   TIPP Der benutzerdefinierte Datentyp kann aus dem Producer-Projekt kopiert und in das Consumer-Projekt eingefügt werden.

2. Klicken Sie mit der rechten Maustaste auf „Controller Tags“ (Steuerungs-Tags) und wählen Sie „New Tag“ (Neues Tag) aus.
3. Legen Sie als Typ „Consumed“ (Konsumiert), für die Klasse „Safety“ (Sicherheit) und als Datentyp den in Schritt 1 erstellten benutzerdefinierten Datentyp fest.



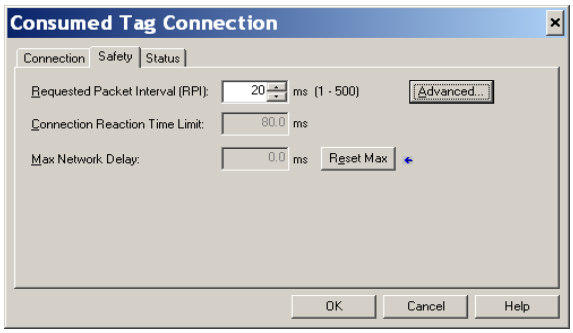
4. Klicken Sie auf „Connection“ (Verbindung), um das Dialogfeld „Consumed Tag Connection“ (Verbindung konsumiertes Tag) zu öffnen.



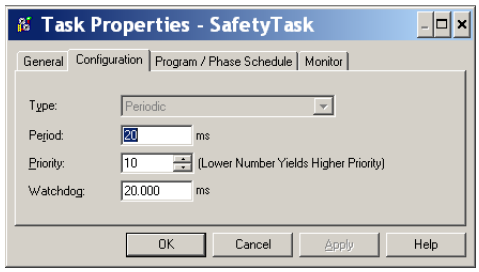
5. Wählen Sie die Steuerung, die Daten produziert.
6. Geben Sie den Namen des produzierten Tags ein.
7. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).
8. Geben Sie das angeforderte Paketintervall (RPI) für die Verbindung in Einheiten von 1 ms ein.

   Der Standardwert ist 20 ms.

Consumer-Projekt



Producer-Projekt

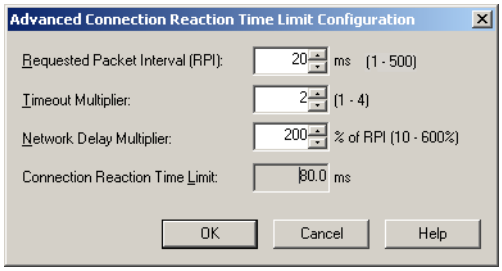


Das angeforderte Paketintervall (RPI) spezifiziert den Zeitraum, in dem die Daten über eine Verbindung aktualisiert werden. Das RPI des konsumierten Sicherheits-Tags muss der Sicherheits-Task-Zeitspanne des produzierenden Sicherheitsprojekts entsprechen.

Die Reaktionszeitgrenze der Verbindung ist das maximale Alter der Sicherheitspakete auf der zugehörigen Verbindung. Für einfache Zeitmessungsbedingungen kann eine zweckmäßige Reaktionszeitgrenze der Verbindung durch Einstellen des RPI erreicht werden.

Die maximale Netzwerkverzögerung ist die beobachtete maximale Transportverzögerung vom Zeitpunkt der Datenerzeugung bis zum Zeitpunkt des Datenempfangs. Im Online-Modus können Sie die maximale Netzwerkverzögerung durch Klicken auf die Schaltfläche „Reset Max“ (Zurücksetzen Max) zurücksetzen.

9. Wenn die Reaktionszeitgrenze der Verbindung übernommen werden soll, klicken Sie auf „OK“. Wenn Sie weitere Anforderungen haben, klicken Sie auf „Advanced“ (Erweitert), um die erweiterten Parameter für die Reaktionszeitgrenze der Verbindung aufzurufen.



Der Timeout-Multiplikator bestimmt die Anzahl der RPIs, die auf ein Paket gewartet wird, bevor ein Verbindungs-Timeout erfolgt.

Der Netzwerkverzögerungs-Multiplikator definiert die Nachrichtentransportzeit, die durch das CIP Safety-Protokoll erzwungen wird. Er spezifiziert die Verzögerung durch die Übertragung vom Producer zum Consumer und zurück und die Rückbestätigung zum Producer. Sie können den Netzwerkverzögerungs-Multiplikator verwenden, um die Reaktionszeitgrenze der Verbindung zu erhöhen oder zu verringern.

Tabelle 31 – Weitere Informationen

Quelle	Beschreibung
Seite 73 bis 77	Enthält weitere Informationen zur Einstellung des angeforderten Paketintervalls (RPI) und dazu, wie sich maximale Netzwerkverzögerung, Timeout-Multiplikator und Netzwerkverzögerungs-Multiplikatoren auf die Reaktionszeitgrenze der Verbindung auswirken
Kapitel 9	Enthält Informationen zum vordefinierten Datentyp CONNECTION_STATUS (VERBINDUNGSSTATUS)
Logix5000-Steuerungen – Produzierte und konsumierte Tags – Programmierhandbuch, Publikation 1756-PM011	Stellt ausführliche Informationen zum Verwenden produzierter und konsumierter Tags zur Verfügung

Zuordnen von Sicherheits-Tags

Auf Steuerungsbereichs-Standard-Tags kann nicht direkt durch eine Sicherheitsroutine zugegriffen werden. Damit in Sicherheits-Task-Routinen Standard-Tag-Daten verwendet werden können, stellen die GuardLogix-Steuerungen eine Zuordnungsfunktion (Mapping) für Sicherheits-Tags zur Verfügung, mit der Standard-Tag-Werte in den Sicherheits-Task-Speicher kopiert werden können.

Einschränkungen

Das Zuordnen von Sicherheits-Tags unterliegt folgenden Einschränkungen:

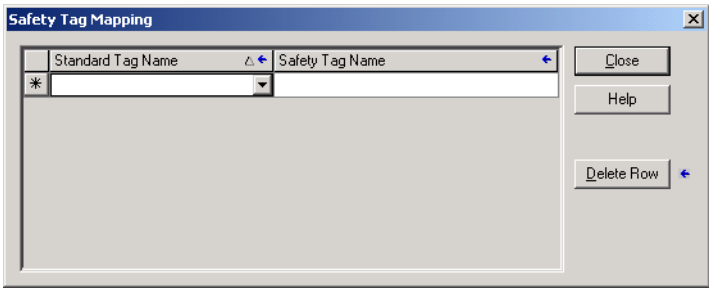
- Beim Sicherheits-Tag- und Standard-Tag-Paar muss es sich um Steuerungsbereichs-Tags handeln.
- Die Datentypen des Sicherheits- und Standard-Tag-Paars müssen übereinstimmen.
- Alias-Tags sind nicht zulässig.
- Die Zuordnung muss für die gesamte Tag-Ebene erfolgen. Zum Beispiel, myTimer.pre ist nicht zulässig, wenn myTimer ein TIMER-Tag ist.
- Ein Zuordnungspaar entspricht einem Standard-Tag, das einem Sicherheits-Tag zugeordnet ist.
- Sie können ein Standard-Tag keinem Sicherheits-Tag zuordnen, das als Konstante gekennzeichnet wurde.
- Die Tag-Zuordnung kann nicht geändert werden, wenn:
  - das Projekt sicherheitsverriegelt ist.
  - eine Sicherheits-Task-Signatur vorliegt.
  - der Schlüsselschalter sich in der RUN-Position befindet.
  - ein nicht behebbarer Sicherheitsfehler vorliegt.
  - eine ungültige Partnerschaft zwischen der Primärsteuerung und dem Sicherheitspartner besteht.

ACHTUNG: Beim Verwenden von Standarddaten in einer Sicherheitsroutine sind Sie dafür verantwortlich, eine zuverlässige Methode zur angemessenen Nutzung der Daten bereitzustellen. Wenn Sie Standarddaten in einem Sicherheits-Tag verwenden, werden diese nicht zu Sicherheitsdaten. Sie dürfen einen SIL 3/PLe-Sicherheitsausgang nicht direkt mit Standard-Tag-Daten steuern.

Weitere Informationen enthält die Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch.

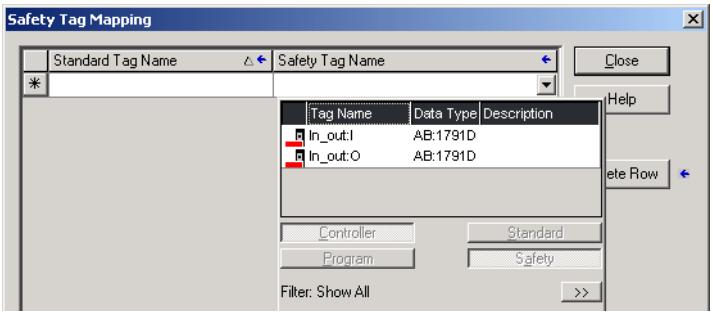
Erstellen von Tag-Zuordnungspaaren

1. Wählen Sie im Menü „Logic“ (Logik) die Option „Map Safety Tags“ (Sicherheits-Tags zuordnen) aus, um das Dialogfeld „Safety Tag Mapping“ (Zuordnung von Sicherheits-Tags) zu öffnen.



2. Fügen Sie ein bestehendes Tag in die Spalte „Standard Tag Name“ (Standard-Tag-Name) oder die Spalte „Safety Tag Name“ (Sicherheits-Tag-Name) ein, indem Sie den Tag-Namen in die Zelle eingeben oder ein Tag aus dem Pulldown-Menü auswählen.

   Klicken Sie auf den Pfeil, um ein Dialogfeld mit einer gefilterten Tag-Suche aufzurufen. Wenn Sie sich in der Spalte „Standard Tag Name“ (Standard-Tag-Name) befinden, zeigt der Browser nur die Steuerungsbereichs-Standard-Tags an. Wenn Sie sich in der „Spalte Safety Tag Name“ (Sicherheits-Tag-Name) befinden, zeigt der Browser die Steuerungsbereichs-Sicherheits-Tags an.



3. Fügen Sie ein neues Tag in die Spalte „Standard Tag Name“ (Standard-Tag-Name) oder die Spalte „Safety Tag Name“ (Sicherheits-Tag-Name) ein, indem Sie mit der rechten Maustaste in die leere Zelle klicken, „New Tag“ (Neues Tag) auswählen und den Tag-Namen in die Zelle eingeben.
4. Klicken Sie mit der rechten Maustaste in die Zelle und wählen Sie „New ‚tagname‘“, wobei ‚tagname‘ der Text ist, den Sie in die Zelle eingegeben haben.

Überwachen des Tag-Zuordnungsstatus

Die äußerste linke Spalte des Dialogfelds „Safety Tag Mapping“ (Zuordnung von Sicherheits-Tags) zeigt den Status des zugeordneten Paars an.

Tabelle 32 – Symbole zum Tag-Zuordnungsstatus

Zelleninhalte	Beschreibung
leer	Die Tag-Zuordnung ist gültig.
	Im Offline-Modus zeigt das Symbol X an, dass die Tag-Zuordnung ungültig ist. Sie können in eine andere Zeile wechseln oder das Dialogfeld „Safety Tag Mapping“ (Zuordnung von Sicherheits-Tags) schließen.(1) Im Online-Modus hat eine ungültige Tag-Zuordnung eine Fehlermeldung zur Folge, die erläutert, warum die Zuordnung ungültig ist. Sie können nicht in eine andere Zeile wechseln oder das Dialogfeld „Safety Tag Mapping“ (Zuordnung von Sicherheits-Tags) schließen, wenn ein Tag-Zurordnungsfehler vorliegt.
	Zeigt die Zeile an, die momentan aktiv ist.
	Steht für die Zeile „Create New Mapped Tag“ (Neues zugeordnetes Tag erstellen).
	Steht für eine ausstehende Änderung.

(1) Die Tag-Zuordnung wird auch während der Projektverifizierung überprüft. Eine ungültige Tag-Zuordnung resultiert in einem Projektverifizierungsfehler.

Weitere Informationen enthält der Abschnitt zu den Einschränkungen bei der Zuordnung von Tags auf Seite 107.

Schutz von Sicherheitsanwendungen

Sie können Ihr Anwendungsprogramm vor unbefugten Änderungen schützen, wenn Sie für die Steuerung eine Sicherheitsverriegelung aktivieren und die Sicherheits-Task-Signatur erstellen und speichern.

Sicherheitsverriegelung der Steuerung

Die GuardLogix-Steuerung kann sicherheitsverriegelt werden, um sicherheitsbezogene Steuerungskomponenten vor Änderungen zu schützen. Die Funktion für die Sicherheitsverriegelung gilt nur für Sicherheitskomponenten wie z. B. die Sicherheits-Task, Sicherheitsprogramme, Sicherheitsroutinen, Sicherheits-Add-On-Befehle, Sicherheits-Tags, Sicherheits-E/A und die Sicherheits-Task-Signatur.

Die nachfolgenden Aktionen sind im Sicherheitsteil der Anwendung erlaubt, wenn die Steuerung sicherheitsverriegelt ist:

- Online-/Offline-Programmierung oder -Bearbeitung (einschließlich der Sicherheits-Add-On-Befehle)
- Forcen der Sicherheits-E/A
- Ändern des gesperrten Zustands von Sicherheits-E/A oder produzierten Verbindungen
- Manipulation von Sicherheitsdaten (außer durch Sicherheitsroutinenlogik)
- Erstellen oder Löschen der Sicherheits-Task-Signatur

TIPP Der Text der Sicherheitsstatus-Schaltfläche der Online-Leiste zeigt den Status der Sicherheitsverriegelung an.

Auf der Anwendungsleiste sind auch die folgenden Symbole abgebildet, die den Status der Sicherheitsverriegelung der Sicherheitssteuerung anzeigen.

- = Steuerung sicherheitsverriegelt
- = Steuerung sicherheitsentriegelt

Sie können das Steuerungsprojekt sicherheitsverriegeln, und zwar unabhängig davon, ob Sie online oder offline sind, und unabhängig davon, ob Sie die Originalquelle des Programms haben oder nicht. Es dürfen allerdings keine Sicherheits-Force-Zustände oder ausstehenden Online-Sicherheitsbearbeitungen vorhanden sein.

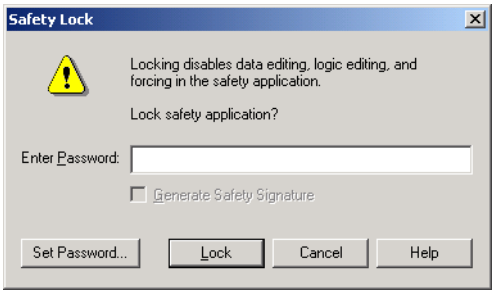
Der sicherheitsverriegelte bzw. sicherheitsentriegelte Zustand kann nicht geändert werden, wenn sich der Schlüsselschalter in der RUN-Position befindet.

TIPP Das Aktivieren oder Deaktivieren der Sicherheitsverriegelung wird im Steuerungsprotokoll aufgezeichnet.

Weitere Informationen zum Zugriff auf das Steuerungsprotokoll finden Sie in der Publikation 1756-PM015, Logix5000-Steuerungen – Informationen und Status – Programmierhandbuch.

Sie können über die Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) oder durch Auswählen von „Tools>Safety>Safety Lock/Unlock“ (Tools>Sicherheit>Sicherheitsverriegelung/-entriegelung) die Sicherheitsverriegelung für die Steuerung aktivieren und deaktivieren.

Abbildung 26 – Aktivieren der Sicherheitsverriegelung der Steuerung



Wenn Sie die Funktion der Sicherheitsverriegelung mit einem Kennwort schützen wollen, müssen Sie dieses in das Feld „Enter Password“ (Kennwort eingeben) eingeben. Andernfalls klicken Sie auf „Lock“ (Verriegeln).

Sie können das Kennwort auch über das Dialogfeld „Safety Lock“ (Sicherheitsverriegelung) einstellen oder ändern. Siehe Seite 51.

Die in diesem Abschnitt beschriebene Funktion für die Sicherheitsverriegelung und die RSLogix-Standardsicherheitsmaßnahmen gelten für GuardLogix-Steuerungsanwendungen.

Weitere Informationen zu den RSLogix 5000-Sicherheitsfunktionen finden Sie in der Publikation 1756-PM016, Logix5000 Controllers Security Programming Manual.

Erstellen einer Sicherheits-Task-Signatur

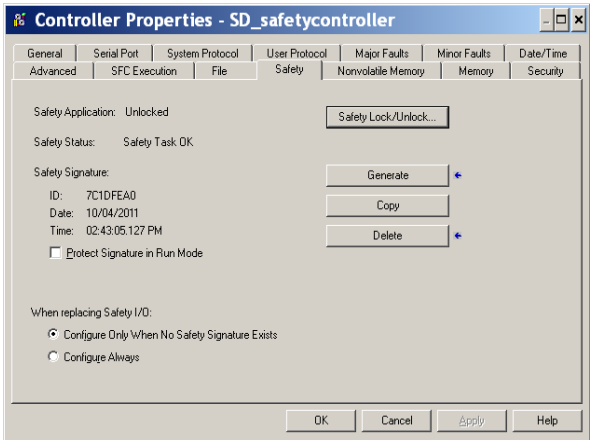
Vor der Verifizierungsprüfung müssen Sie die Sicherheits-Task-Signatur erstellen. Sie können diese Sicherheits-Task-Signatur nur erstellen, wenn die sicherheitsentriegelte GuardLogix-Steuerung im Programm-Modus online ist und keine Sicherheits-Force-Zustände, ausstehenden Online-Sicherheitsbearbeitungen oder Sicherheitsfehler vorliegen. Der Sicherheitsstatus muss „Safety Task OK“ (Sicherheits-Task OK) lauten.

Darüber hinaus können Sie keine Sicherheits-Task-Signatur erstellen, wenn sich die Steuerung im Run-Modus bei aktiviertem Run-Modus-Schutz befindet.

TIPP Sie können den Sicherheitsstatus über die Sicherheitsstatus-Schaltfläche auf der Online-Leiste (siehe Seite 130) oder auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Controller Properties“ (Steuerungseigenschaften), wie auf Seite 111 dargestellt, einsehen.

Sie können die Sicherheits-Task-Signatur auf der Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) durch Klicken auf die Schaltfläche „Generate“ (Generieren) erstellen. Alternativ dazu können Sie „Tools>Safety>Generate Signature“ (Tools>Sicherheit>Signatur generieren) auswählen.

Abbildung 27 – Registerkarte „Sicherheit“



Gegebenenfalls werden Sie aufgefordert, eine bereits bestehende Signatur zu überschreiben.

TIPP Das Erstellen und Löschen der Sicherheits-Task-Signatur wird im Steuerungsprotokoll aufgezeichnet.

Weitere Informationen zum Zugriff auf das Steuerungsprotokoll finden Sie in der Publikation 1756-PM015, Logix5000-Steuerungen – Informationen und Status – Programmierhandbuch.

Wenn eine Sicherheits-Task-Signatur vorhanden ist, sind die nachfolgenden Aktionen im Sicherheitsteil der Anwendung nicht zulässig.

- Online-/Offline-Programmierung oder -Bearbeitung (einschließlich der Sicherheits-Add-On-Befehle)
- Forcen der Sicherheits-E/A
- Ändern des gesperrten Zustands von Sicherheits-E/A oder Producer-Steuerungen
- Manipulation von Sicherheitsdaten (außer durch Sicherheitsroutinenlogik)

Kopieren der Sicherheits-Task-Signatur

Über die Schaltfläche „Copy“ (Kopieren) können Sie ein Protokoll der Sicherheits-Task-Signatur zur Verwendung bei Dokumentation, Vergleich und Validierung des Sicherheitsprojekts erstellen. Klicken Sie auf „Copy“ (Kopieren), um die ID-, Datum- und Zeitkomponenten in die Windows-Zwischenablage zu kopieren.

Löschen der Sicherheits-Task-Signatur

Klicken Sie auf „Delete“ (Löschen), um die Sicherheits-Task-Signatur zu löschen. Die Sicherheits-Task-Signatur kann in folgenden Fällen nicht gelöscht werden:

- wenn die Steuerung sicherheitsverriegelt ist.
- wenn sich die Steuerung im Run-Modus befindet und der Schlüsselschalter auf RUN steht.
- wenn sich die Steuerung im Run-Modus oder Remote Run-Modus befindet und der Run-Modus-Schutz aktiviert ist.

ACHTUNG: Wenn Sie die Sicherheits-Task-Signatur löschen, müssen Sie Ihr System erneut testen und überprüfen, ob die Anforderungen von SIL 3/PLe weiterhin erfüllt werden.

Weitere Informationen zu den Anforderungen für SIL 3/PLe finden Sie in der Publikation 1756-RM093, Steuerungssysteme GuardLogix – Sicherheitsreferenzhandbuch.

Softwareeinschränkungen

Die Verfügbarkeit einiger Menüpunkte und Funktionsmerkmale (z. B. Ausschneiden, Einfügen, Löschen, Suchen und Ersetzen) wird zum Schutz der Sicherheitskomponenten vor Änderung durch die Programmiersoftware eingeschränkt, wenn:

- wenn die Steuerung sicherheitsverriegelt ist.
- eine Sicherheits-Task-Signatur vorliegt.
- Sicherheitsfehler vorhanden sind.
- der Sicherheitsstatus wie folgt lautet:
  - Partner fehlt.
  - Partner nicht verfügbar.
  - Hardware inkompatibel.
  - Firmware inkompatibel.

Trifft auch nur eine dieser Bedingungen zu, ist Folgendes nicht möglich:

- Erstellen oder Ändern von Sicherheitsobjekten, wie z. B. Sicherheitsprogrammen, Sicherheitsroutinen, Sicherheits-Tags, Sicherheits-Add-On-Befehlen und Sicherheits-E/A-Modulen.

  WICHTIG Die Abtastzeiten der Sicherheits-Task und Sicherheitsprogramme können im Online-Modus zurückgesetzt werden.

- Anwendung von Force-Zuständen auf Sicherheits-Tags.
- Erstellung neuer Sicherheits-Tag-Zuordnungen.
- Änderung oder Löschung von Tag-Zuordnungen.
- Änderung oder Löschung benutzerdefinierter Datentypen, die von Sicherheits-Tags verwendet werden.
- Änderung des Steuerungsnamens, der Beschreibung, des Chassistyps, des Steckplatzes und der Sicherheitsnetzwerknummer.
- Änderung oder Löschung der Sicherheits-Task-Signatur im sicherheitsverriegelten Zustand.

Schalten der Steuerung in den Online-Modus

Verbinden der Steuerung mit dem Netzwerk

Wenn noch nicht geschehen, verbinden Sie die Steuerung mit dem Netzwerk.

Tabelle 33 – Kommunikationsanschlüsse

Für diesen Anschlusstyp	Verwenden Sie	Siehe
Seriell	Kabel 1756-CP3 oder 1747-CP3	Anschließen der Workstation an die serielle Schnittstelle der 1756-L6xS-Steuerung auf Seite 38
USB	USB 2.0-Kabel	Anschließen der Workstation an den USB-Anschluss der 1756-L7xS-Steuerung auf Seite 36
EtherNet/IP	EtherNet/IP-Modul in einem unbelegten Steckplatz im selben Chassis wie die Steuerung	Anschluss Ihrer EtherNet/IP-Geräte an den Computer auf Seite 114
DeviceNet	Modul 1756-DNB in einem unbelegten Steckplatz im selben Chassis wie die Steuerung	Verbinden Ihres ControlNet-Kommunikationsmoduls oder Ihres DeviceNet-Scanners mit Ihrem Computer auf Seite 114
ControlNet	Modul 1756-CN2 in einem unbelegten Steckplatz im selben Chassis wie die Steuerung	

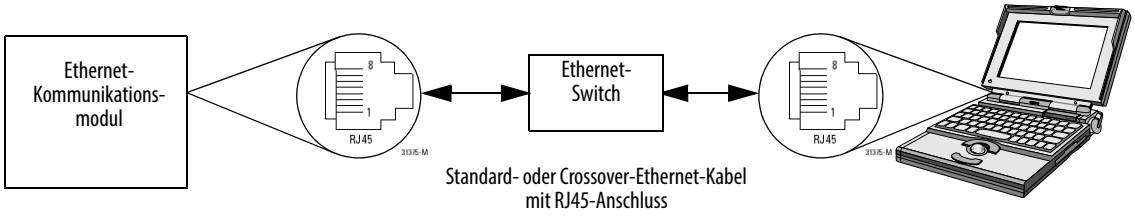
Anschluss Ihrer EtherNet/IP-Geräte an den Computer

WARNUNG: Wenn Sie das Verbindungskabel anschließen oder abziehen, solange die Stromversorgung dieses Moduls oder eines anderen Geräts im Netzwerk eingeschaltet ist, kann ein elektrischer Lichtbogen erzeugt werden. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden.

Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

Verbinden Sie Ihr EtherNet/IP-Gerät und den Computer mit einem Ethernet-Kabel.

Abbildung 28 – Ethernet-Anschlüsse



Verbinden Ihres ControlNet-Kommunikationsmoduls oder Ihres DeviceNet-Scanners mit Ihrem Computer

Zugriff auf das ControlNet- oder DeviceNet-Netzwerk erhalten Sie, indem Sie entweder:

- eine direkte Verbindung zum Netzwerk herstellen oder
- eine Verbindung zu einem seriellen oder einem EtherNet/IP-Netzwerk herstellen und zum gewünschten Netzwerk navigieren (Bridge). Dies verlangt keine zusätzliche Programmierung.

Konfigurieren eines EtherNet/IP-, ControlNet- oder DeviceNet-Treibers

Informationen zum Konfigurieren eines Treibers finden Sie in der entsprechenden Publikation.

- EtherNet/IP Modules in Logix5000 Control Systems, Publikation ENET-UM001
- ControlNet Modules in Logix5000 Control Systems User Manual, Publikation CNET-UM001
- DeviceNet Modules in Logix5000 Control Systems, Publikation DNET-UM004

Faktoren, die das Schalten in den Online-Modus beeinflussen

Die Software RSLogix 5000 legt fest, ob Sie mit einer Zielsteuerung abhängig davon online gehen können, ob das Offline-Projekt neu ist oder ob Änderungen im Offline-Projekt vorgenommen wurden. Wenn das Projekt neu ist, müssen Sie zuerst das Projekt auf die Steuerung herunterladen. Wenn am Projekt Änderungen vorgenommen wurden, werden Sie zum Hoch- oder Herunterladen aufgefordert. Falls keine Änderungen vorgenommen wurden, können Sie in den Online-Modus schalten, um die Ausführung des Projekts zu überwachen.

Diese Prozesse werden von verschiedenen Faktoren beeinflusst, so z. B. von der Funktion „Project to Controller Match“ (Übereinstimmung zwischen Projekt und Steuerung), vom Sicherheitsstatus und von den Sicherheitsfehlern, ob eine Sicherheits-Task-Signatur vorliegt oder nicht sowie vom Status der Sicherheitsverriegelung/-entriegelung des Projekts und der Steuerung.

Übereinstimmung zwischen Projekt und Steuerung

Die Funktion „Project to Controller Match“ (Übereinstimmung zwischen Projekt und Steuerung) hat Auswirkungen auf das Herunterladen, das Hochladen und auf die Verfahren zum Online-Schalten von Standard- und Sicherheitsprojekten.

Wenn die Option „Project to Controller Match“ (Übereinstimmung zwischen Projekt und Steuerung) im Offline-Projekt aktiviert ist, vergleicht die Software RSLogix 5000 die Seriennummer der Steuerung im Offline-Projekt mit der Seriennummer der angeschlossenen Steuerung. Falls diese nicht übereinstimmen, müssen Sie entweder das Hoch- bzw. Herunterladen abbrechen, eine Verbindung zur richtigen Steuerung herstellen oder bestätigen, dass Sie eine Verbindung zur richtigen Steuerung hergestellt haben. In diesem Fall wird die Seriennummer im Projekt aktualisiert, damit sie mit der Zielsteuerung übereinstimmt.

Firmware-Versionsübereinstimmung

Die Firmware-Versionsübereinstimmung hat Auswirkungen auf den Download-Prozess. Falls die Version der Steuerung nicht mit der Version des Projekts übereinstimmt, werden Sie aufgefordert, die Firmware der Steuerung zu aktualisieren. Mit Hilfe der Software RSLogix 5000 können Sie die Firmware als Teil der Download-Sequenz aktualisieren.

WICHTIG	Um die Firmware der Steuerung zu aktualisieren, müssen Sie zuerst ein Firmware-Upgrade-Kit installieren. Ein Upgrade-Kit wird auf einer Ergänzungs-CD zusammen mit der Software RSLogix 5000 geliefert.

TIPP Für ein Firmware-Upgrade können Sie auch in der Software RSLogix 5000 im Menü „Tools“ (Extras) die Option „ControlFLASH™“ (Flash-Speicher der Steuerung) auswählen.

Sicherheitsstatus/-fehler

Das Hochladen der Programmlogik und das Online-Schalten sind, unabhängig vom Sicherheitsstatus, immer zulässig. Sicherheitsstatus und -fehler wirken sich nur auf das Herunterladen aus.

Sie können den Sicherheitsstatus über die Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) einsehen.

Sicherheits-Task-Signatur sowie sicherheitsverriegelter und -entriegelter Zustand

Das Vorliegen einer Sicherheits-Task-Signatur und des sicherheitsverriegelten oder -entriegelten Zustands der Steuerung wirken sich auf das Hoch- und Herunterladen aus.

Beim Upload

Wenn die Steuerung über eine Sicherheits-Task-Signatur verfügt, werden die Sicherheits-Task-Signatur und der Verriegelungszustand der Sicherheits-Task mit dem Projekt hochgeladen. Wenn das Projekt in der Steuerung zum Beispiel sicherheitsentriegelt war, bleibt das Offline-Projekt nach dem Hochladen sicherheitsentriegelt, selbst wenn es vor dem Hochladen verriegelt war.

Nach dem Hochladen stimmt die Sicherheits-Task-Signatur im Offline-Projekt mit der Sicherheits-Task-Signatur der Steuerung überein.

Beim Herunterladen

Das Vorhandensein einer Sicherheits-Task-Signatur und des sicherheitsverriegelten Zustands der Steuerung bestimmt, ob das Herunterladen fortgesetzt werden kann.

Tabelle 34 – Auswirkung von Sicherheitsverriegelung und Sicherheits-Task-Signatur auf das Herunterladen

Sicherheitsverriegelungs-zustand	Status der Sicherheits-Task-Signatur	Download-Funktionalität
Steuerung sicherheitsentriegelt	Die Sicherheits-Task-Signatur im Offline-Projekt stimmt mit der Sicherheits-Task-Signatur der Steuerung überein.	Alle Standardprojektkomponenten werden heruntergeladen. Sicherheits-Tags werden auf die zum Zeitpunkt der Signaturerstellung für die Sicherheits-Task eingestellten Werte zurückgesetzt. Die Sicherheits-Task wird nicht heruntergeladen. Der Status der Sicherheitsverriegelung stimmt mit dem Status im Offline-Projekt überein.
	Die Signaturen der Sicherheits-Tasks stimmen nicht überein.	Wenn in der Steuerung eine Sicherheits-Task-Signatur vorlag, wird diese automatisch gelöscht und das gesamte Projekt wird heruntergeladen. Der Status der Sicherheitsverriegelung stimmt mit dem Status im Offline-Projekt überein.
Steuerung sicherheitsverriegelt	Die Signaturen der Sicherheits-Tasks stimmen überein.	Wenn das Offline-Projekt und die Steuerung sicherheitsverriegelt sind, werden alle Standardprojektkomponenten heruntergeladen und die Sicherheits-Task wird erneut mit den Werten initialisiert, die beim Erstellen der Sicherheits-Task-Signatur vorlagen. Ist das Offline-Projekt nicht sicherheitsverriegelt, die Steuerung jedoch schon, wird das Herunterladen blockiert und erst wieder nach Entriegelung der Steuerung fortgesetzt.
	Die Signaturen der Sicherheits-Tasks stimmen nicht überein.	Sie müssen zur Fortsetzung des Download-Vorgangs die Steuerung sicherheitsentriegeln. Wenn in der Steuerung eine Sicherheits-Task-Signatur vorlag, wird diese automatisch gelöscht und das gesamte Projekt wird heruntergeladen. Der Status der Sicherheitsverriegelung stimmt mit dem Status im Offline-Projekt überein.

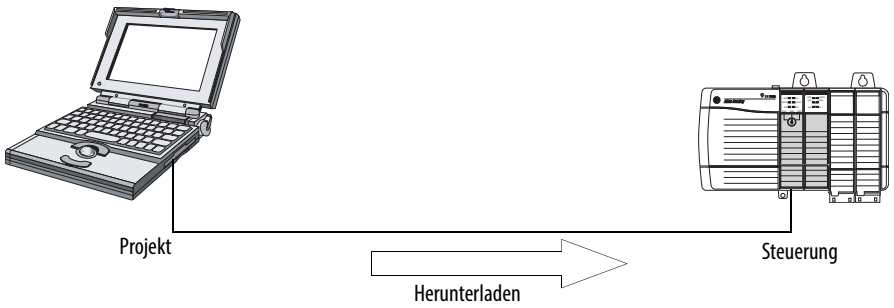
WICHTIG Unterscheidet sich während des Herunterladens auf eine sicherheitsentriegelte Steuerung die Firmware in der Steuerung von der im Offline-Projekt, gehen Sie auf eine der folgenden Weisen vor:

- Aktualisieren Sie die Steuerung, so dass diese mit dem Offline-Projekt übereinstimmt. Nach Abschluss der Aktualisierung wird das gesamte Projekt heruntergeladen.
- Aktualisieren Sie das Projekt entsprechend der Steuerungsversion.

Wenn Sie das Projekt aktualisieren, wird die Sicherheits-Task gelöscht und das System muss erneut validiert werden.

Herunterladen

Gehen Sie wie folgt vor, um Ihr Projekt von Ihrem Computer auf Ihre Steuerung zu übertragen.



1. Stellen Sie den Schlüsselschalter der Steuerung auf REM.
2. Öffnen Sie das RSLogix 5000-Projekt, das Sie herunterladen möchten.
3. Legen Sie den Pfad zur Steuerung fest.
   a. Klicken Sie auf „Who Active“ (Aktive Geräte)  .
   b. Wählen Sie die Steuerung aus.
   Klicken Sie zum Öffnen einer Ebene auf das Pluszeichen (+). Ist bereits eine Steuerung ausgewählt, stellen Sie sicher, dass es sich um die richtige Steuerung handelt.
4. Klicken Sie auf „Download“ (Herunterladen).

   Die Software vergleicht die folgenden Informationen im Offline-Projekt und in der Steuerung.
   - Seriennummer der Steuerung (wenn die Option „Übereinstimmung zwischen Projekt und Steuerung“ ausgewählt ist)
   - Haupt- und Nebenversionen der Firmware
   - Sicherheitsstatus
   - Sicherheits-Task-Signatur (falls vorhanden)
   - Sicherheitsverriegelungszustand

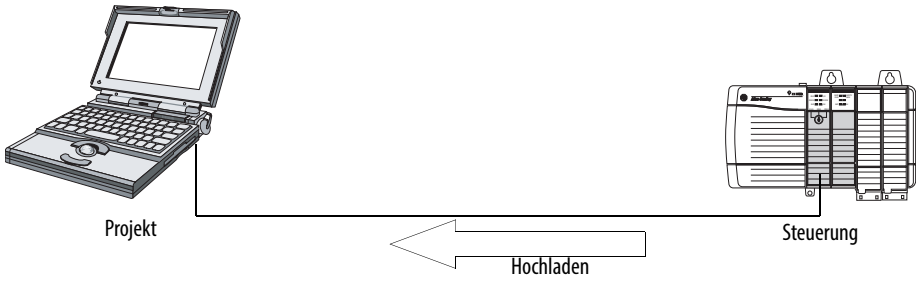
5. Befolgen Sie die Anweisungen in dieser Tabelle, um den Download-Vorgang basierend auf der Antwort der Software abzuschließen.

Zeigt die Software Folgendes an	Dann
Download auf die Steuerung.	Wählen Sie „Download“ (Herunterladen) aus. Das Projekt wird auf die Steuerung heruntergeladen und die Software RSLogix 5000 wechselt in den Online-Modus.
Download auf die Steuerung nicht möglich. Keine Übereinstimmung zwischen der Seriennummer des Offline-Projekts und der Seriennummer der Steuerung. Die ausgewählte Steuerung könnte die falsche Steuerung sein.	Schließen Sie die korrekte Steuerung an oder überprüfen Sie, dass es sich um die korrekte Steuerung handelt. Aktivieren Sie sodann das Optionsfeld „Update project serial number“ (Seriennummer des Projekts aktualisieren) und setzen Sie den Download-Vorgang fort. Die Seriennummer des Projekts wird entsprechend der Seriennummer der Steuerung geändert.
Download auf die Steuerung nicht möglich. Die Hauptversion des Offline-Projekts und die Firmware der Steuerung sind nicht kompatibel.	Wählen Sie „Update Firmware“ (Firmware aktualisieren). Klicken Sie nach Auswahl der erforderlichen Version auf „Update“ (Aktualisieren). Bestätigen Sie Ihre Wahl, indem Sie auf „Yes“ (Ja) klicken.
Download auf die Steuerung nicht möglich. Sicherheitspartner fehlt oder ist nicht verfügbar.	Download-Vorgang abbrechen. Installieren Sie einen kompatiblen Sicherheitspartner, bevor Sie einen erneuten Download-Versuch starten.
Download auf die Steuerung nicht möglich. Die Firmware-Version des Sicherheitspartners ist mit der Primärsteuerung nicht kompatibel.	Aktualisieren Sie die Firmware-Version des Sicherheitspartners. Wählen Sie „Update Firmware“ (Firmware aktualisieren). Klicken Sie nach Auswahl der erforderlichen Version auf „Update“ (Aktualisieren). Bestätigen Sie Ihre Wahl, indem Sie auf „Yes“ (Ja) klicken.
Download auf die Steuerung nicht möglich. Die Sicherheitspartnerschaft wurde nicht hergestellt.	Brechen Sie den Download-Vorgang ab und starten Sie einen erneuten Versuch.
Download auf die Steuerung nicht möglich. Die inkompatible Sicherheits-Task-Signatur kann nicht gelöscht werden, solange das Projekt sicherheitsverriegelt ist.	Brechen Sie den Download-Vorgang ab. Zum Herunterladen des Projekts müssen Sie die Sicherheitsverriegelung des Offline-Projekts deaktivieren, die Sicherheits-Task-Signatur löschen und das Projekt herunterladen. **WICHTIG:** Das Sicherheitssystem erfordert eine erneute Validierung.
Herunterladen unter Beibehaltung der Sicherheits-Task-Signatur nicht möglich. Die Nebenversion der Steuerungs-Firmware ist mit der Sicherheits-Task-Signatur im Offline-Projekt nicht kompatibel.	• Ist die Nebenversion der Steuerungs-Firmware nicht kompatibel, aktualisieren Sie zur Beibehaltung der Sicherheits-Task-Signatur die Firmware-Version in der Steuerung, sodass sie exakt mit dem Offline-Projekt übereinstimmt. Laden Sie dann das Offline-Projekt herunter. • Um trotz der Inkompatibilität der Sicherheits-Task-Signatur mit dem Herunterladen fortzufahren, klicken Sie auf „Download“ (Herunterladen). Die Sicherheits-Task-Signatur wird gelöscht. **WICHTIG:** Das Sicherheitssystem erfordert eine erneute Validierung.
Download auf die Steuerung nicht möglich. Die Steuerung ist verriegelt. Die Signaturen der Sicherheits-Tasks von Steuerung und Offline-Projekt stimmen nicht überein.	Wählen Sie „Unlock“ (Entriegeln). Das Dialogfeld „Safety Unlock for Download“ (Sicherheitsentriegelung für Herunterladen) wird angezeigt. Bestätigen Sie nach Auswahl des Optionsfelds „Delete Signature“ (Signatur löschen) und „Unlock“ (Entriegeln) Ihre Eingabe mit „Yes“ (Ja).
In der Sicherheitssteuerung tritt ein nicht behebbarer Sicherheitsfehler auf. Es wurde kein CST-Master (Master für koordinierte Systemzeit) festgelegt.	Wählen Sie „Enable Time Synchronization“ (Zeitsynchronisierung aktivieren) aus und klicken Sie zum Fortsetzen des Vorgangs auf „Download“ (Herunterladen).

Im Anschluss an das erfolgreiche Herunterladen stimmen der Sicherheitsverriegelungszustand und die Sicherheits-Task-Signatur der Steuerung mit dem heruntergeladenen Projekt überein. Sicherheitsdaten werden mit den Werten initialisiert, die während der Erstellung der Sicherheits-Task-Signatur vorlagen.

Hochladen

Gehen Sie wie folgt vor, um ein Projekt aus der Steuerung auf Ihren Computer zu übertragen.



1. Legen Sie den Pfad zur Steuerung fest.
   a. Klicken Sie auf „Who Active“ (Aktive Geräte)  .
   b. Wählen Sie die Steuerung aus.
   Klicken Sie zum Erweitern einer Ebene auf das Pluszeichen (+). Ist bereits eine Steuerung ausgewählt, stellen Sie sicher, dass es sich um die richtige Steuerung handelt.
2. Klicken Sie auf „Upload“ (Hochladen).
3. Falls die Projektdatei nicht vorhanden ist, wählen Sie „File>Select>Yes“ (Datei>Auswählen>Ja) aus.
4. Falls das Projekt bereits besteht, wählen Sie es aus.

   Ist die Überprüfung der Übereinstimmung zwischen Projekt und Steuerung aktiviert, überprüft die Software RSLogix 5000, ob die Seriennummer des geöffneten Projekts und die Seriennummer der Steuerung übereinstimmen.

   Stimmen die Seriennummern nicht überein, können Sie:
   - den Upload-Vorgang abbrechen und eine Verbindung zu einer übereinstimmenden Steuerung herstellen. Starten Sie den Upload-Vorgang dann erneut.
   - ein neues Projekt zum Hochladen auswählen oder ein anderes Projekt auswählen, indem Sie auf „Select File“ (Datei auswählen) klicken.
   - die Seriennummer des Projekts aktualisieren, so dass sie mit der Steuerung übereinstimmt, indem Sie das Optionsfeld „Update Project Serial Number“ (Seriennummer des Projekts aktualisieren) auswählen und dann auf „Upload“ (Hochladen) klicken.
5. Die Software prüft, ob das geöffnete Projekt mit dem Steuerungsprojekt übereinstimmt.
   a. Stimmen die Projekte nicht überein, müssen Sie eine übereinstimmende Datei auswählen oder den Upload-Vorgang abbrechen.
   b. Stimmen die Projekte überein, führt die Software eine Prüfung auf Änderungen im (geöffneten) Offline-Projekt durch.

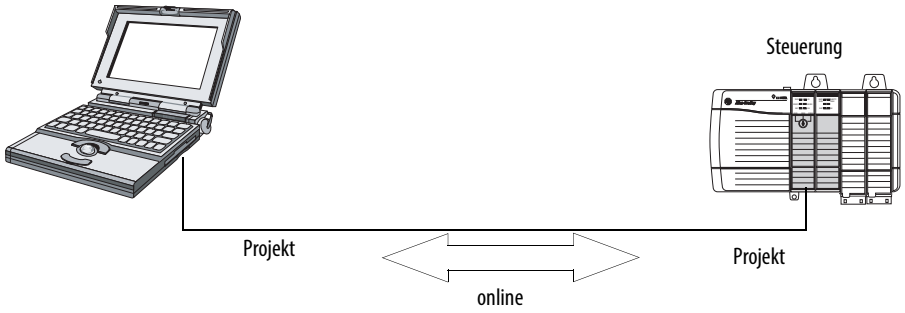
6. Die Software sucht nach Änderungen im Offline-Projekt.
   a. Wurden im Offline-Projekt keine Änderungen vorgenommen, können Sie ohne Hochladen in den Online-Modus schalten. Klicken Sie auf „Go Online“ (Online schalten).
   b. Wurden Änderungen im geöffneten Projekt vorgenommen, die in der Steuerung nicht vorhanden sind, können Sie sich für das Hochladen des Projekts oder das Abbrechen des Hochladens entscheiden oder eine andere Datei auswählen.

   Bei Auswahl von „Upload“ (Hochladen) werden die Standard- und Sicherheitsanwendungen hochgeladen. Ist eine Sicherheits-Task-Signatur vorhanden, wird sie ebenfalls hochgeladen. Der Sicherheitsverriegelungszustand des Projekts zeigt den ursprünglichen Zustand des Online-(Steuerungs-)Projekts an.

   TIPP Ist vor dem Hochladen eine Offline-Sicherheits-Task-Signatur vorhanden oder ist das Offline-Projekt sicherheitsverriegelt, die Steuerung aber sicherheitsentriegelt oder keine Sicherheits-Task-Signatur vorhanden, werden die Offline-Sicherheits-Task-Signatur und der Sicherheitsverriegelungszustand durch die Online-Werte (sicherheitsentriegelt und ohne Sicherheits-Task-Signatur) ersetzt. Wenn diese Änderungen nicht dauerhaft sein sollen, speichern Sie das Offline-Projekt nach dem Upload-Vorgang nicht ab.

Schalten in den Online-Modus

Gehen Sie wie folgt vor, um in den Online-Modus zu schalten und ein von der Steuerung ausgeführtes Projekt zu überwachen.



1. Legen Sie den Pfad zur Steuerung fest.
   a. Klicken Sie auf „Who Active“ (Aktive Geräte)  .
   b. Wählen Sie die Steuerung aus.
   Klicken Sie zum Erweitern einer Ebene auf das Pluszeichen (+). Ist bereits eine Steuerung ausgewählt, stellen Sie sicher, dass es sich um die richtige Steuerung handelt.
2. Klicken Sie auf „Go Online“ (Online schalten).

   Die Software überprüft Folgendes:
   - Stimmen Seriennummern von Offline-Projekt und Steuerung überein, falls die Option „Project to Controller Match “ (Übereinstimmung zwischen Projekt und Steuerung) ausgewählt ist?
   - Enthält das Offline-Projekt Änderungen, die nicht im Steuerungsprojekt enthalten sind?

- Stimmen die Versionen von Offline-Projekt und Steuerungs-Firmware überein?
- Sind Offline-Projekt oder Steuerung sicherheitsverriegelt?
- Besitzen Offline-Projekt oder Steuerung kompatible Sicherheits-Task-Signaturen?

3. Befolgen Sie die Anweisungen in der nachfolgenden Tabelle, um eine Verbindung zur Steuerung herzustellen.

Tabelle 35 – Anschließen an die Steuerung

Zeigt die Software Folgendes an	Dann
Verbindung zur Steuerung nicht möglich. Keine Übereinstimmung zwischen der Seriennummer des Offline-Projekts und der Seriennummer der Steuerung. Die ausgewählte Steuerung könnte die falsche Steuerung sein.	Stellen Sie eine Verbindung zur richtigen Steuerung her, wählen Sie eine andere Projektdatei oder das Optionsfeld „Update project serial number" (Seriennummer des Projekts aktualisieren) und dann „Go Online" (Online schalten) aus, um eine Verbindung zur Steuerung herzustellen und die Seriennummer des Offline-Projekts entsprechend der Steuerung zu aktualisieren.
Verbindung zur Steuerung nicht möglich. Die Version des Offline-Projekts und die Firmware der Steuerung sind nicht kompatibel.	Wählen Sie eine der folgenden Optionen: • Wählen Sie „Update Firmware" (Firmware aktualisieren). Klicken Sie nach Auswahl der erforderlichen Version auf „Update" (Aktualisieren). Bestätigen Sie Ihre Wahl, indem Sie auf „Yes" (Ja) klicken. **WICHTIG:** Das Online-Projekt wird gelöscht. • Damit das Online-Projekt erhalten bleibt, brechen Sie den Online-Prozess ab und installieren Sie eine Version der Software RSLogix 5000, die mit der Firmware-Version Ihrer Steuerung kompatibel ist.
Sie müssen einen Upload oder Download durchführen, um mit dem geöffneten Projekt in den Online-Modus zu wechseln.	Wählen Sie eine der folgenden Optionen: • „Upload" (Hochladen), um das Offline-Projekt zu aktualisieren. • „Download" (Herunterladen), um das Steuerungsprojekt zu aktualisieren. • Wählen Sie „File" (Datei) aus, um ein anderes Offline-Projekt auszuwählen.
Verbindung unter Erhalt der Sicherheits-Task-Signatur nicht möglich. Die Nebenversion der Steuerungs-Firmware ist mit der Sicherheits-Task-Signatur im Offline-Projekt nicht kompatibel.	• Ist die Nebenversion der Steuerungs-Firmware nicht kompatibel, aktualisieren Sie zur Beibehaltung der Sicherheits-Task-Signatur die Firmware-Version in der Steuerung, sodass sie exakt mit dem Offline-Projekt übereinstimmt. Schalten Sie dann zur Steuerung in den Online-Modus. • Um trotz der Inkompatibilität der Sicherheits-Task-Signatur mit dem Herunterladen fortzufahren, klicken Sie auf „Download" (Herunterladen). Die Sicherheits-Task-Signatur wird gelöscht. **WICHTIG:** Das Sicherheitssystem erfordert eine erneute Validierung.
Verbindung zur Steuerung nicht möglich. Die inkompatible Sicherheits-Task-Signatur kann nicht gelöscht werden, solange das Projekt sicherheitsverriegelt ist.	Brechen Sie den Online-Prozess ab. Sie müssen das Offline-Projekt zuerst sicherheitsentriegeln, bevor Sie versuchen, in den Online-Modus zu schalten.

Wenn die Steuerung und die Software RSLogix 5000 online geschaltet sind, stimmen der Sicherheitsverriegelungszustand und die Sicherheits-Task-Signatur der Steuerung mit dem Projekt der Steuerung überein. Der Sicherheitsverriegelungszustand und die Sicherheits-Task-Signatur des Offline-Projekts werden durch die Steuerung überschrieben. Wenn die Änderungen am Offline-Projekt nicht dauerhaft sein sollen, speichern Sie die Projektdatei nach dem Schalten in den Online-Modus nicht ab.

Notizen:

Speichern und Laden von Projekten mithilfe des nichtflüchtigen Speichers

Verwenden von Speicherkarten für nichtflüchtigen Speicher

GuardLogix-Steuerungen ab Version 18 unterstützen eine Speicherkarte für den nichtflüchtigen Speicher. Der nichtflüchtige Speicher ermöglicht das Speichern einer Kopie Ihres Projekts in der Steuerung. Die Steuerung benötigt zum Speichern dieser Kopie keine Stromversorgung oder Batterie.

Sie können das gespeicherte Projekt in folgenden Situationen aus dem nichtflüchtigen Speicher in den Anwenderspeicher der Steuerung laden:

- bei jedem Einschalten
- immer wenn sich kein Projekt in der Steuerung befindet und diese eingeschaltet wird
- jederzeit über die Software RSLogix 5000.

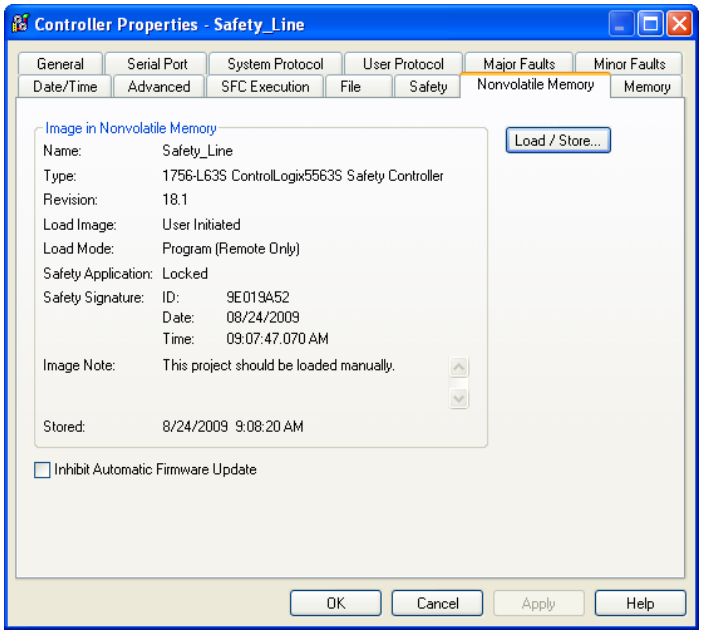
WICHTIG Im nichtflüchtigen Speicher wird der Inhalt des Anwenderspeichers zum Zeitpunkt der Speicherung des Projekts gespeichert:

- Änderungen, die Sie nach dem Speichern des Projekts vornehmen, werden im nichtflüchtigen Speicher nicht widergespiegelt.
- Wenn Sie am Projekt vorgenommene Änderungen nicht speichern, werden diese beim Laden des Projekts aus dem nichtflüchtigen Speicher überschrieben. In diesem Fall müssen Sie das Projekt hoch- bzw. herunterladen, um in den Online-Modus schalten zu können.
- Wenn Sie online durchgeführte Änderungen, geänderte Tag-Werte oder einen geänderten ControlNet-Netzwerkplan speichern möchten, müssen Sie das Projekt nach dem Ausführen dieser Änderungen erneut speichern.

ACHTUNG: Entfernen Sie die Speicherkarte nicht, während die Steuerung Daten von der Karte liest oder auf diese schreibt. Dies wird durch ein grünes Blinklicht der Statusanzeige OK signalisiert. Dadurch könnten die Daten auf der Karte oder in der Steuerung beschädigt werden. Auch die zuletzt geladene Firmware in der Steuerung könnte dadurch Schaden nehmen. Lassen Sie die Karte in der Steuerung, bis die Statusanzeige OK kontinuierlich grün leuchtet.

Wenn eine Speicherkarte installiert ist, können Sie den Inhalt der Karte auf der Registerkarte „Nonvolatile Memory“ (Nichtflüchtiger Speicher) im Dialogfenster „Controller Properties“ (Steuerungseigenschaften) anzeigen. Wenn eine Sicherheitsanwendung auf der Karte gespeichert ist, werden der Sicherheitsverriegelungsstatus und die Sicherheits-Task-Signatur angezeigt.

Abbildung 29 – Registerkarte „Nonvolatile Memory“ (Nichtflüchtiger Speicher)



Ausführliche Informationen zur Verwendung des nichtflüchtigen Speichers finden Sie in der Publikation 1756-PM017, Logix5000 Controllers Nonvolatile Memory Programming Manual.

Speichern eines Sicherheitsprojekts

Sie können ein Sicherheitsprojekt nicht speichern, wenn der Status der Sicherheits-Task „Safety Task Inoperable“ (Sicherheits-Task nicht funktionsbereit) lautet. Wenn Sie ein Sicherheitsprojekt speichern, wird die Firmware der Primärsteuerung und des Sicherheitspartners auf der Speicherkarte gespeichert.

Wenn die Steuerung keine Anwendung enthält, können Sie die Firmware der Sicherheitssteuerung nur speichern, wenn eine gültige Partnerschaft vorhanden ist. Durch das alleinige Laden der Firmware wird die Bedingung „Safety Task Inoperable“ (Sicherheits-Task nicht funktionsbereit) nicht gelöscht.

Wenn beim Speichern eines Projekts eine Sicherheits-Task-Signatur vorhanden ist:

- werden Sicherheits-Tags mit dem Wert gespeichert, den sie beim ersten Erstellen der Signatur aufwiesen.
- werden Standard-Tags aktualisiert.
- wird die aktuelle Sicherheits-Task-Signatur gespeichert.

Wenn Sie ein Sicherheitsanwendungsprojekt auf eine Speicherkarte speichern, sollten Sie als Lademodus die Option „Program (Remote Only)“ (Programm (nur dezentral)) auswählen, also den Modus, in den die Steuerung nach dem Laden wechseln soll.

Laden eines Sicherheitsprojekts

Sie können einen Ladevorgang vom nichtflüchtigen Speicher nur unter folgenden Bedingungen einleiten:

- Der Steuerungstyp, der von dem im nichtflüchtigen Speicher abgelegten Projekt angegeben wird, stimmt mit dem Steuerungstyp überein.
- Die Haupt- und Nebenversionen des Projekts im nichtflüchtigen Speicher stimmen mit den Haupt- und Nebenversionen auf der Steuerung überein.
- Ihre Steuerung befindet sich nicht im Run-Modus.

Es gibt mehrere Möglichkeiten, wann (unter welchen Bedingungen) ein Projekt in den Anwenderspeicher der Steuerung geladen werden kann.

Tabelle 36 – Optionen zum Laden eines Projekts

Laden des Projekts	Auswahl dieser „Load Image"-Option (Abbilddatei laden)	Hinweise
Bei jedem Einschalten oder Aus- und Wiedereinschalten	On Power Up (Beim Einschalten)	• Beim Aus- und Einschalten der Versorgungsspannung gehen alle online durchgeführten Änderungen, geänderten Tag-Werte und Netzwerkpläne verloren, sofern Sie diese nicht in den nichtflüchtigen Speicher geschrieben haben. • Die Steuerung lädt das gespeicherte Projekt und die Firmware bei jedem Einschalten (unabhängig von der Firmware oder der Anwendung in der Steuerung). Der Ladevorgang findet statt, ganz gleich, ob die Steuerung sicherheitsverriegelt ist oder über eine Sicherheits-Task-Signatur verfügt. • Sie können die Software RSLogix 5000 stets zum Laden des Projekts verwenden.
Wenn sich kein Projekt in der Steuerung befindet und Sie die Spannungsversorgung des Chassis einschalten oder aus- und wieder einschalten	On Corrupt Memory (Bei beschädigtem Speicher)	• Wenn beispielsweise die Batterie entladen ist und die Spannungsversorgung der Steuerung unterbrochen ist, wird das Projekt aus dem Speicher gelöscht. Beim Wiederherstellen der Spannungsversorgung wird bei dieser Ladeoption das Projekt wieder in die Steuerung geladen. • Die Steuerung aktualisiert die Firmware in der Primärsteuerung oder im Sicherheitspartner, sofern erforderlich. Die im nichtflüchtigen Speicher abgelegte Anwendung wird ebenfalls geladen, während die Steuerung in den ausgewählten Modus (Program oder Run) wechselt. • Sie können die Software RSLogix 5000 stets zum Laden des Projekts verwenden.
Nur über die Software RSLogix 5000	User Initiated (Vom Anwender initiiert)	• Wenn der Steuerungstyp und die Haupt- und Nebenversionen des Projekts im nichtflüchtigen Speicher mit dem Steuerungstyp und den Haupt- sowie Nebenversionen der Steuerung übereinstimmen, können Sie einen Ladevorgang einleiten (unabhängig vom Status der Sicherheits-Task). • Ein Projekt kann nur auf eine sicherheitsverriegelte Steuerung geladen werden, wenn die im nichtflüchtigen Speicher des Projekts abgelegte Sicherheits-Task-Signatur mit der Signatur des Projekts in der Steuerung übereinstimmt. • Stimmen die Signaturen nicht überein bzw. ist die Steuerung ohne Sicherheits-Task-Signatur sicherheitsverriegelt, werden Sie aufgefordert, zunächst die Steuerung zu entriegeln. **WICHTIG:** Wenn Sie die Steuerung entriegeln und einen Ladevorgang aus dem nichtflüchtigen Speicher einleiten, werden nach Abschluss des Ladevorgangs Sicherheitsverriegelungsstatus, Kennwörter und Sicherheits-Task-Signatur auf die Werte im nichtflüchtigen Speicher gesetzt. • Stimmt die Firmware der Primärsteuerung mit der Version im nichtflüchtigen Speicher überein, wird die Firmware des Sicherheitspartners aktualisiert, sofern erforderlich; die im nichtflüchtigen Speicher abgelegte Anwendung wird geladen, sodass der Sicherheits-Task-Status „Safety Task Operable" (Sicherheits-Task funktionsbereit) lautet, und die Steuerung wechselt in den ausgewählten Modus (Program oder Run).

WICHTIG Vergewissern Sie sich vor der Verwendung der Software ControlFLASH, dass die SD-Karte entriegelt ist, wenn „On Power Up" (Beim Einschalten) ausgewählt ist. Andernfalls werden die aktualisierten Daten möglicherweise von der Firmware auf der Speicherkarte überschrieben.

Verwenden der Energiespeichermodule (nur 1756-L7*x*S-Steuerungen)

Sie können die GuardLogix-Energiespeichermodule (ESMs) zur Ausführung der folgenden Aufgaben verwenden:

- Versorgen der 1756-L7*x*S-Steuerung mit Spannung, um das Programm im integrierten, nichtflüchtigen Speicher der Steuerung speichern zu können, nachdem die Spannungsversorgung zum Chassis unterbrochen wurde oder nachdem die Steuerung aus einem eingeschalteten Chassis ausgebaut wurde.

  WICHTIG Wenn Sie ein ESM zum Speichern des Programms im integrierten, nichtflüchtigen Speicher verwenden, speichern Sie das Programm **nicht** auf der in der Steuerung installierten SD-Karte.

- Löschen des Programms aus dem integrierten, nichtflüchtigen Speicher der 1756-L7*x*S-Steuerung. Weitere Informationen finden Sie unter Löschen des Programms aus dem integrierten nichtflüchtigen Speicher.

In der folgenden Tabelle sind die ESMs beschrieben.

Tabelle 37 – Energiespeichermodule

Bestellnummer	Beschreibung
1756-ESMCAP(XT)	Kondensator-basiertes ESM In den 1756-L7*x*S-Steuerungen ist dieses ESM bereits vorinstalliert.
1756-ESMNSE(XT)	Kondensator-basiertes ESM ohne Backupleistung für die Uhrzeit Verwenden Sie dieses ESM, wenn für Ihre Anwendung das installierte ESM seine gespeicherte Restenergie auf 200 µJ oder weniger abbauen muss, bevor es in Ihre Anwendung integriert oder aus ihr ausgebaut werden kann. Außerdem können Sie dieses ESM nur mit der Steuerung 1756-L73S (8 MB) oder einer Steuerung mit kleinerem Speicher verwenden.
1756-ESMNRM(XT)	Sicheres, Kondensator-basiertes ESM (kann nicht ausgebaut werden) Dieses ESM bietet Ihrer Anwendung verbesserte Sicherheit, da es den physischen Zugriff auf den USB-Anschluss und die SD-Karte verhindert.
1756-SPESMNSE(XT)	Kondensator-basiertes ESM ohne Uhrzeit-Backupleistung für den Sicherheitspartner Verwenden Sie dieses ESM, wenn für Ihre Anwendung das installierte ESM seine gespeicherte Restenergie auf 200 µJ oder weniger abbauen muss, bevor es in Ihre Anwendung integriert oder aus ihr ausgebaut werden kann. Im Sicherheitspartner für den Einsatz unter extremen Umgebungsbedingungen 1756-L7SPXT ist das 1756-SPESMNSEXT vorinstalliert.
1756-SPESMNRM(XT)	Sicheres, Kondensator-basiertes ESM (kann nicht ausgebaut werden) für den Sicherheitspartner

Speichern des Programms im integrierten, nichtflüchtigen Speicher

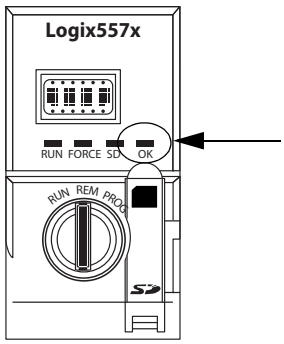
Gehen Sie wie folgt vor, um das Programm im nichtflüchtigen Speicher zu sichern, wenn die Spannungsversorgung der Steuerung unterbrochen wird.

1. Unterbrechen Sie die Spannungsversorgung der Steuerung.

   Dazu haben Sie zwei Möglichkeiten:
   - Ausschalten der Chassisspannung, während die Steuerung im Chassis installiert ist.
   - Ausbauen der Steuerung aus einem eingeschalteten Chassis.

Sobald die Steuerung nicht mehr mit Spannung versorgt wird, leuchtet die Statusleuchte „OK“ bis nach Abschluss der Programmspeicherung rot.

Abbildung 30 – Statusleuchte „OK“.



2. Lassen Sie das ESM in der Steuerung, bis die Statusleuchte „OK“ erlischt.

3. Bauen Sie, wenn erforderlich, das ESM aus der Steuerung aus, wenn die rote Statusleuchte „OK“ erloschen ist.

Löschen des Programms aus dem integrierten nichtflüchtigen Speicher

Gehen Sie, wenn Ihre Anwendung es zulässt, wie folgt vor, um das Programm aus dem integrierten, nichtflüchtigen Speicher der 1756-L7*x*S-Steuerung zu löschen.

1. Bauen Sie das ESM aus der Steuerung aus.

2. Unterbrechen Sie die Spannungsversorgung der Steuerung, indem Sie die Chassisspannung, während die Steuerung im Chassis installiert ist, ausschalten oder die Steuerung aus einem eingeschalteten Chassis ausbauen.

3. Bauen Sie das ESM wieder in die Steuerung ein.

4. Stellen Sie die Spannungsversorgung der Steuerung wieder her.
   a. Wenn die Steuerung bereits im Chassis installiert ist, schalten Sie die Spannungsversorgung des Chassis wieder ein.
   b. Wenn die Steuerung nicht im Chassis installiert ist, installieren Sie zunächst die Steuerung wieder im Chassis und schalten Sie dann das Chassis wieder ein.

Abschätzen der ESM-Unterstützung für die Uhrzeit

Das ESM unterstützt die Aufrechterhaltung der Uhrzeit der Steuerung (Attribut „WallClockTime“), wenn die Spannungsversorgung unterbrochen wurde. Verwenden Sie die folgende Tabelle, um die die Haltezeit des ESM auf der Grundlage der Temperatur der Steuerung und des installierten ESM abzuschätzen.

Tabelle 38 – Temperatur gg. Haltezeit

	Haltezeit (in Tagen)		
Temperatur	**1756-ESMCAP(XT)**	**1756-ESMNRM(XT) 1756-SPESMNRM(XT)**	**1756-ESMNSE(XT) 1756-SPESMNSE(XT)**
20 °C	12	12	0
40 °C	10	10	0
60 °C	7	7	0

Verwalten der Firmware mit Firmware Supervisor

Ab Version 18 der Software RSLogix 5000 können Sie die Funktion Firmware Supervisor zum Verwalten der Firmware auf Steuerungen verwenden. Firmware Supervisor ermöglicht Steuerungen die automatische Aktualisierung von Geräten:

- Lokale und dezentrale Module können aktualisiert werden, wenn sie sich im Programm- oder Run-Modus befinden.
- Für eine exakte Übereinstimmung muss die elektronische Codierung konfiguriert werden.
- Das Firmware-Kit für das Zielgerät muss sich auf der Speicherkarte der Steuerung befinden.
- Das Gerät muss Firmware-Upgrades über das Dienstprogramm ControlFLASH unterstützen.

Nicht modulare, dezentrale E/A-Produkte, die sich direkt auf dem Netzwerk befinden, werden auch ohne Adapter von der Funktion Firmware Supervisor unterstützt. Hierzu zählen CIP Safety-E/A-Module in EtherNet/IP-Netzwerken. CIP Safety-E/A-Module in DeviceNet-Netzwerken und POINT Guard-E/A-Module werden noch nicht unterstützt.

Gehen Sie wie folgt vor, um Firmware Supervisor zu aktivieren.

1. Klicken Sie im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) auf die Registerkarte „Nonvolatile Memory“ (Nichtflüchtiger Speicher).
2. Klicken Sie auf „Load/Store“ (Laden/Speichern).
3. Wählen Sie im Pulldown-Menü „Automatic Firmware Updates“ (Automatische Firmware-Updates) die Optionen „Enable“(Aktivieren) und „Store Files to Image“ (Dateien in Abbilddatei speichern) aus.

Die Software RSLogix 5000 verschiebt die Firmware-Kits von Ihrem Computer auf die Speicherkarte der Steuerung, damit sie von Firmware Supervisor verwendet werden können.

TIPP Wenn Sie die Funktion Firmware Supervisor deaktivieren, deaktivieren Sie nur die über Firmware Supervisor vorgenommenen Updates. Hierzu zählen jedoch nicht die Firmware-Updates der Steuerung, die vorgenommen werden, wenn das Steuerungs-Abbild erneut von der Speicherkarte geladen wird.

Zustandsüberwachung und Fehlerbehebung

In Anhang A, Statusanzeigen, finden Sie Informationen zur Interpretation der Statusleuchten und Fehlermeldungen.

Anzeige des Status über die Online-Leiste

Die Online-Leiste zeigt Projekt- und Steuerungsinformationen an, einschließlich Steuerungsstatus, Force-Zustand, Online-Bearbeitungsstatus und Sicherheitsstatus.

Abbildung 31 – Statusschaltflächen

Wenn die Schaltfläche „Controller Status“ (Steuerungsstatus), wie vorstehend abgebildet, ausgewählt ist, zeigt die Online-Leiste den Steuerungsmodus (RUN) und den Status (OK) an. Die Anzeige BAT kombiniert den Status von Primärsteuerung und Sicherheitspartner. Falls einer oder beide einen Batteriefehler aufweisen, leuchtet die Statusanzeige auf. Die Anzeige I/O kombiniert den Status von Standard- und Sicherheits-E/A und verhält sich genau wie die Statusanzeige auf der Steuerung. Das E/A-Modul mit dem schwerwiegendsten Fehlerzustand wird neben der Statusanzeige eingeblendet.

Wenn die Schaltfläche „Safety Status“ (Sicherheitsstatus) ausgewählt ist, wie nachfolgend dargestellt, zeigt die Online-Leiste die Sicherheits-Task-Signatur an.

Abbildung 32 – Online-Anzeige der Sicherheitssignatur

Die Schaltfläche „Safety Status“ (Sicherheitsstatus) selbst zeigt an, ob die Steuerung sicherheitsverriegelt bzw. -entriegelt oder fehlerhaft ist. Sie zeigt auch ein Symbol an, das den Sicherheitsstatus beschreibt.

Tabelle 39 – Sicherheitsstatussymbol

Sicherheitsstatus:	Angezeigtes Symbol:
Sicherheits-Task OK	
Sicherheits-Task nicht funktionsbereit	
Partner fehlt Partner nicht verfügbar Hardware inkompatibel Firmware inkompatibel	
Offline	

Die Symbole sind grün, wenn die Steuerung sicherheitsverriegelt ist, gelb, wenn die Steuerung sicherheitsentriegelt ist und rot, wenn bei der Steuerung ein Sicherheitsfehler vorliegt. Wenn eine Sicherheits-Task-Signatur vorliegt, ist das Symbol mit einem kleinen Kontrollhäkchen versehen. 

Überwachen von Verbindungen

Sie können den Status von Standard- und Sicherheitsverbindungen überwachen.

Alle Verbindungen

Falls 100 ms lang keine Kommunikation mit einem Gerät in der E/A-Konfiguration der Steuerung stattfindet, erfolgt ein Kommunikations-Timeout und die Steuerung gibt folgende Warnmeldungen aus:

- Die Anzeige „ I/O“ (E/A) auf der Vorderseite der Steuerung blinkt grün.
- Ein Warnsymbol  wird über dem E/A-Konfigurationsordner und über dem Gerät mit dem Timeout angezeigt.
- Ein Modulfehler wird erzeugt, auf den Sie über die Registerkarte „Connection“ (Verbindung) im Dialogfeld „Module Properties“ (Moduleigenschaften) für das Modul oder über den GSV-Befehl zugreifen können.

ACHTUNG: Sicherheits-E/A und Producer-/Consumer-Verbindungen können nicht so konfiguriert werden, dass die Steuerung bei einem Verbindungsausfall automatisch in den Fehlerzustand übergeht. Daher müssen Sie die Verbindungsfehler überwachen, um sicherzustellen, dass das Sicherheitssystem die SIL 3/PLe-Integrität beibehält.

Siehe Sicherheitsverbindungen.

Sicherheitsverbindungen

Für Tags, die zu produzierten oder konsumierten Sicherheitsdaten gehören, können Sie den Status der Sicherheitsverbindungen mithilfe des Glieds CONNECTION_STATUS überwachen. Für die Überwachung von Eingangs- und Ausgangsverbindungen haben Sicherheits-E/A-Tags ein Verbindungsstatus-Glied mit dem Namen SafetyStatus. Beide Datentypen enthalten zwei Bits: RunMode und ConnectionFaulted.

Der RunMode-Wert zeigt an, ob konsumierte Daten gerade aktiv durch ein Gerät aktualisiert werden, das sich im Run-Modus (1) oder im Leerlaufstatus (0) befindet. Der Leerlaufstatus wird angezeigt, wenn die Verbindung geschlossen ist, die Sicherheits-Task fehlerhaft ist oder sich die dezentrale Steuerung oder das dezentrale Gerät im Programm- oder Testmodus befindet.

Der ConnectionFaulted-Wert zeigt an, ob die Sicherheitsverbindung zwischen dem Sicherheits-Producer und dem Sicherheits-Consumer gültig (Valid) (0) oder fehlerhaft (Faulted) (1) ist. Falls ConnectionFaulted infolge eines Verlusts der physischen Verbindung auf fehlerhaft (1) gesetzt wird, werden die Sicherheitsdaten auf null zurückgesetzt.

Die nachfolgende Tabelle beschreibt die Kombinationen der RunMode- und ConnectionFaulted-Zustände.

Tabelle 40 – Sicherheitsverbindungsstatus

RunMode-Status	ConnectionFaulted-Status	Betrieb der Sicherheitsverbindung
1 = Run	0 = gültig	Die Daten werden aktiv vom produzierenden Gerät gesteuert. Das produzierende Gerät befindet sich im Run-Modus.
0 = Leerlauf	0 = gültig	Die Verbindung ist aktiv und das produzierende Gerät befindet sich im Leerlauf. Die Sicherheitsdaten werden auf null zurückgesetzt.
0 = Leerlauf	1 = fehlerhaft	Die Sicherheitsverbindung ist fehlerhaft. Der Status des produzierenden Geräts ist unbekannt. Die Sicherheitsdaten werden auf null zurückgesetzt.
1 = Run	1 = fehlerhaft	Ungültiger Status.

Falls ein Modul gesperrt ist, wird das ConnectionFaulted-Bit auf fehlerhaft (1) und das RunMode-Bit auf Leerlauf (0) gesetzt, und zwar für jede Verbindung, die mit dem Modul besteht. Als Folge werden die konsumierten Sicherheitsdaten auf null zurückgesetzt.

Überwachen von Status-Flags

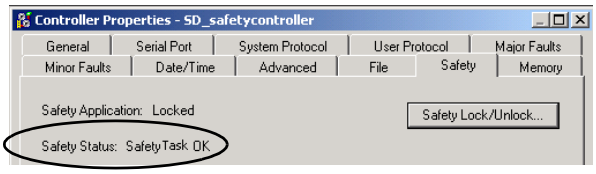
Logix-Steuerungen, einschließlich GuardLogix-Steuerungen, unterstützen Statuskennwörter, die Sie in Ihrer Logik zur Überwachung bestimmter Ereignisse verwenden können.

Weitere Informationen zur Verwendung dieser Kennwörter finden Sie in der Publikation 1756-PM015, Logix5000-Steuerungen – Informationen und Status – Programmierhandbuch.

Überwachen des Sicherheitsstatus

Sie können Informationen zum Sicherheitsstatus der Steuerung in der Online-Leiste über die Schaltfläche zum Sicherheitsstatus und auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Controller Properties“ (Steuerungseigenschaften) aufrufen.

Abbildung 33 – Status der Sicherheits-Task



Die möglichen Werte für den Sicherheitsstatus sind:

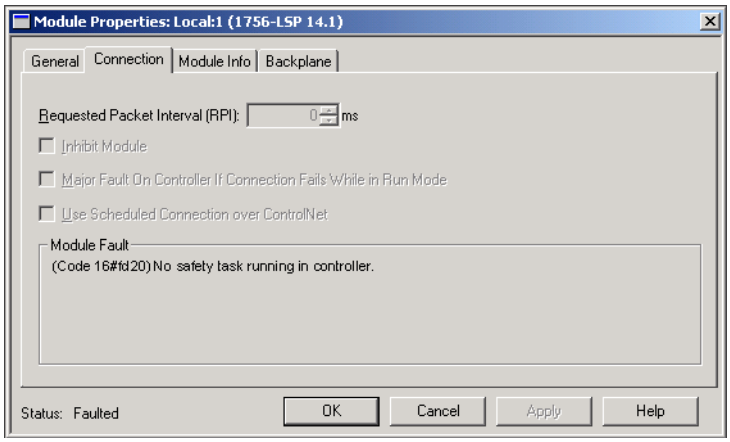
- Sicherheitspartner fehlt oder ist nicht verfügbar.
- Sicherheitspartner-Hardware ist nicht kompatibel mit der Primärsteuerung.
- Sicherheitspartner-Firmware ist inkompatibel mit der Primärsteuerung.
- Sicherheits-Task nicht funktionsbereit.
- Sicherheits-Task OK.

Mit Ausnahme von „Sicherheits-Task OK“ zeigen die oben genannten Beschreibungen, dass ein nicht behebbarer Sicherheitsfehler vorliegt.

Die Fehlercodes und erforderlichen Maßnahmen finden Sie im Abschnitt Schwerwiegende Sicherheitsfehler (Typ 14) auf Seite 134.

Der Status des Sicherheitspartners kann auf der Registerkarte „Connection“ (Verbindung) des Dialogfelds „Module Properties“ (Moduleigenschaften) eingesehen werden.

Abbildung 34 – Status des Sicherheitspartners



Steuerungsfehler

Bei Fehlern im GuardLogix-System kann es sich um nicht behebbare Steuerungsfehler, nicht behebbare Sicherheitsfehler in der Sicherheitsanwendung oder behebbare Sicherheitsfehler in der Sicherheitsanwendung handeln.

Nicht behebbare Steuerungsfehler

Diese treten auf, wenn die interne Diagnose der Steuerung fehlschlägt. Wenn ein nicht behebbarer Steuerungsfehler auftritt, stoppt die Ausführung der Sicherheits-Task und die CIP Safety-E/A-Module werden in den sicheren Zustand versetzt. Die Wiederherstellung des korrekten Betriebs erfordert ein erneutes Herunterladen des Anwendungsprogramms.

Nicht behebbare Sicherheitsfehler in der Sicherheitsanwendung

Wenn ein nicht behebbarer Sicherheitsfehler in der Sicherheitsanwendung auftritt, werden die Sicherheitslogik und das Sicherheitsprotokoll beendet. Fehler beim Sicherheits-Task-Watchdog und bei der Steuerungspartnerschaft fallen in diese Kategorie.

Falls die Sicherheits-Task einen nicht behebbaren Sicherheitsfehler erkennt, der im Fehlerbehebungsprogramm der Steuerung gelöscht wird, wird die Standardanwendung weiter ausgeführt.

ACHTUNG: Ein Sicherheitsfehler wird durch Überschreiben nicht gelöscht! Wenn Sie den Sicherheitsfehler überschreiben, obliegt es Ihnen, zu beweisen, dass durch diese Maßnahme der sichere Betrieb nicht beeinträchtigt wird.

Sie müssen Ihrer Zertifizierungsbehörde den Beweis erbringen, dass durch den Umstand, dass ein Teil des Systems weiterarbeitet, der sichere Betrieb aufrecht erhalten bleibt.

Falls eine Sicherheits-Task-Signatur vorliegt, müssen Sie nur den Fehler löschen, damit die Sicherheits-Task arbeiten kann. Falls keine Sicherheits-Task-Signatur vorliegt, funktioniert die Sicherheits-Task erst wieder, nachdem die gesamte Anwendung erneut heruntergeladen wurde.

Korrigierbare Sicherheitsfehler in der Sicherheitsanwendung

Wenn ein korrigierbarer Fehler in der Sicherheitsanwendung auftritt, kann das System die Ausführung der Sicherheits-Task abhängig davon anhalten, ob der Fehler durch das Fehlerbehebungsprogramm in der Sicherheitsanwendung bearbeitet wird oder nicht.

Falls ein korrigierbarer Fehler durch das Programm gelöscht wird, kann die Sicherheits-Task ohne Unterbrechung mit der Ausführung fortfahren.

Falls ein korrigierbarer Fehler in der Sicherheitsanwendung nicht durch das Programm gelöscht wird, tritt ein korrigierbarer Sicherheitsfehler vom Typ 14, Code 2, auf. Die Ausführung des Sicherheitsprogramms wird gestoppt und die Sicherheitsprotokollverbindungen werden geschlossen und zur Reinitialisierung neu geöffnet. Sicherheitsausgänge werden in den sicheren Zustand geschaltet und der Producer der konsumierten Sicherheits-Tags erteilt den Consumern den Befehl, sie ebenfalls in einen sicheren Zustand zu schalten.

Behebbare Fehler ermöglichen es Ihnen, die Standard- und/oder Sicherheitsanwendung sowie die Ursache des Fehlers entsprechend zu korrigieren. Falls jedoch eine Sicherheits-Task-Signatur vorliegt oder die Steuerung sicherheitsverriegelt ist, müssen Sie zuerst die Steuerung entriegeln und die Sicherheits-Task-Signatur löschen, bevor Sie die Sicherheitsanwendung bearbeiten können.

Anzeigen von Fehlern

Das Dialogfeld „Recent Faults“ (Letzte Fehler) auf der Registerkarte „Major Faults“ (Schwerwiegende Fehler) des Dialogfelds „Controller Properties“ (Steuerungseigenschaften) enthält zwei Unter-Registerkarten: eine für Standardfehler und eine für Sicherheitsfehler.

Die Statusanzeige auf der 1756-L7*x*S-Steuerung gibt auch Fehlercodes zusammen mit einer kurzen Statusmeldung an (siehe ab Seite 141).

Fehlercodes

Tabelle 41 enthält die Fehlercodes, die sich speziell auf GuardLogix-Steuerungen beziehen. Typ und Code entsprechen dem Typ und dem Code auf der Registerkarte „Major Faults“ (Schwerwiegende Fehler) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) und im Objekt PROGRAM, Attribut MAJORFAULTRECORD bzw. MINORFAULTRECORD.

Tabelle 41 – Schwerwiegende Sicherheitsfehler (Typ 14)

Code	Ursache	Status	Erforderliche Maßnahmen
01	Task-Watchdog abgelaufen. Anwender-Task konnte nicht in einem spezifizierten Zeitraum abgeschlossen werden. Ein Programmfehler hat eine Endlosschleife verursacht, das Programm ist zu komplex, um so schnell wie angegeben zu arbeiten, eine Task höherer Priorität verhindert die Beendigung dieser Task oder der Sicherheitspartner wurde entfernt.	Nicht behebbar	Den Fehler löschen. Falls eine Sicherheits-Task-Signatur vorliegt, wird der Sicherheitsspeicher neu initialisiert und die Sicherheits-Task beginnt mit der Ausführung. Falls keine Sicherheits-Task-Signatur vorliegt, müssen Sie das Programm erneut herunterladen, damit die Sicherheits-Task ausgeführt werden kann. Setzen Sie den Sicherheitspartner wieder ein, falls er entfernt wurde.
02	Ein Fehler liegt in einer Routine der Sicherheits-Task vor.	Behebbar	Korrigieren Sie den Fehler in der Anwenderprogrammlogik.
03	Sicherheitspartner fehlt.	Nicht behebbar	Installieren Sie einen kompatiblen Sicherheitspartner.
04	Sicherheitspartner ist nicht verfügbar.	Nicht behebbar	Installieren Sie einen kompatiblen Sicherheitspartner.
05	Sicherheitspartner-Hardware ist nicht kompatibel.	Nicht behebbar	Installieren Sie einen kompatiblen Sicherheitspartner.
06	Sicherheitspartner-Firmware ist nicht kompatibel.	Nicht behebbar	Aktualisieren Sie den Sicherheitspartner, sodass die Haupt- und Nebenversion der Firmware mit der Primärsteuerung übereinstimmen.
07	Sicherheits-Task ist nicht funktionsbereit. Dieser Fehler tritt auf, wenn die Sicherheitslogik ungültig ist, also wenn z. B. eine nicht übereinstimmende Logik zwischen der Primärsteuerung und dem Sicherheitspartner vorliegt, ein Timeout des Überwachungszeitraums aktiviert wurde oder wenn der Speicher fehlerhaft ist.	Nicht behebbar	Den Fehler löschen. Falls eine Sicherheits-Task-Signatur vorhanden ist, wird der Sicherheitsspeicher über die Sicherheits-Task-Signatur erneut initialisiert und die Sicherheits-Task beginnt mit der Ausführung. Falls keine Sicherheits-Task-Signatur vorliegt, müssen Sie das Programm erneut herunterladen, damit die Sicherheits-Task ausgeführt werden kann.
08	Koordinierte Systemzeit (CST) nicht gefunden.	Nicht behebbar	Den Fehler löschen. Konfigurieren Sie ein Gerät als CST-Master.
09	Nicht behebbarer Steuerungsfehler des Sicherheitspartners.	Nicht behebbar	Löschen Sie den Fehler und laden Sie das Programm erneut herunter. Falls das Problem weiterhin besteht, ersetzen Sie den Sicherheitspartner.

Ein behebbarer, geringfügiger Fehlertyp (10), Code 11, tritt auf, wenn die Batterie des 1756-LSP-Sicherheitspartners fehlt oder ausgetauscht werden muss.

Informationen zum Austausch der Batterie finden Sie in Anhang B.

Publikation 1756-PM014, „Logix5000-Steuerungen – Schwerwiegende, geringfügige und E/A-Fehler – Programmierhandbuch“, enthält Beschreibungen der Fehlercodes, die häufig für Logix-Steuerungen angezeigt werden.

Entwickeln einer Fehlerroutine

Wenn ein Fehlerzustand auftritt, der so schwerwiegend ist, dass die Steuerung abschaltet, generiert die Steuerung einen schwerwiegenden Fehler und stoppt die Ausführung der Logik.

Abhängig von der jeweiligen Anwendung kann es unter Umständen nicht erwünscht sein, dass alle Sicherheitsfehler das gesamte System abschalten. In solchen Situationen kann eine Fehlerroutine eingesetzt werden, durch die ein spezifischer Fehler gelöscht und damit die Fortsetzung des Betriebs des Standardsteuerungsteils des Systems ermöglicht wird, oder einige Ausgänge können so konfiguriert werden, dass sie eingeschaltet bleiben.

ACHTUNG: Sie müssen Ihrer Zertifizierungsbehörde den Beweis erbringen, dass durch den Umstand, dass ein Teil des Systems weiterarbeitet, der sichere Betrieb aufrecht erhalten bleibt.

Die Steuerung unterstützt zwei Ebenen zur Handhabung schwerwiegender Fehler:

- Programmfehlerroutine
- Steuerungsfehlerbehebungsprogramm

Beide Routinen können die GSV- und SSV-Befehle, wie auf Seite 136 beschrieben, verwenden.

Programmfehlerroutine

Für jedes Programm kann eine eigene Fehlerroutine verwendet werden. Die Steuerung führt die Programmfehlerroutine aus, wenn ein Befehl fehlerhaft ausgeführt wird. Löscht die Programmfehlerroutine den Fehler nicht oder ist keine Programmfehlerroutine vorhanden, beginnt die Steuerung mit der Ausführung des Steuerungsfehlerbehebungsprogramms, sofern vorhanden.

Steuerungsfehlerbehebungsprogramm

Das Steuerungsfehlerbehebungsprogramm ist eine optionale Komponente, die ausgeführt wird, wenn die Programmfehlerroutine den Fehler nicht löschen konnte oder eine solche nicht existiert.

Sie können nur ein (1) Programm zur Behebung von Steuerungsfehlern erstellen. Nachdem Sie das Programm erstellt haben, müssen Sie eine Routine als Hauptroutine konfigurieren.

Publikation 1756-PM014, „Logix5000-Steuerungen – Schwerwiegende, geringfügige und E/A-Fehler – Programmierhandbuch“, enthält Informationen zum Erstellen und Testen einer Fehlerroutine.

Verwendung der GSV/SSV-Befehle

Logix-Steuerungen speichern Systemdaten in Objekten und nicht in Statusdateien. Sie können die Befehle „Systemwert abrufen“ (GSV) und „Systemwert einstellen“ (SSV) verwenden, um die Steuerungsdaten zu erhalten und einzustellen.

Der GSV-Befehl ruft die spezifizierten Informationen ab und platziert sie am spezifizierten Ziel. Der SSV-Befehl ändert das spezifizierte Attribut mit Daten von der Quelle des Befehls. Wenn Sie einen GSV- oder SSV-Befehl eingeben, zeigt die Programmiersoftware die Objektklassen, Objektnamen und Attributnamen für jeden Befehl an.

Für Standard-Tasks können Sie den GSV-Befehl verwenden, um die Werte für die verfügbaren Attribute zu erhalten. Bei Verwendung des SSV-Befehls zeigt die Software nur die Attribute an, die Sie einstellen dürfen.

Für die Sicherheits-Task sind die GSV- und SSV-Befehle restriktiver. Die SSV-Befehle in Sicherheits- und Standard-Tasks können das Bit 0 (schwerwiegender Fehler) im Modusattribut eines E/A-Sicherheitsmoduls nicht setzen.

Für Sicherheitsobjekte zeigt Tabelle 42, für welche Attribute Sie mit dem GSV-Befehl Werte abrufen können und welche Attribute Sie mit dem SSV-Befehl in Sicherheits- und Standard-Tasks festlegen können.

ACHTUNG: Gehen Sie vorsichtig bei der Verwendung der GSV-/SSV-Befehle vor. Änderungen an Objekten können zu unvorhergesehenem Steuerungsbetrieb oder Verletzungen des Bedienpersonals führen.

Tabelle 42 – GSV/SSV-Zugänglichkeit

Sicherheitsobjekt	Attributname	Datentyp	Attributbeschreibung	Zugänglich über Sicherheits-Task		Zugänglich über Standard-Task	
				GSV	SSV	GSV[4]	SSV
Sicherheits-Task	Instance	DINT	Liefert die Instanznummer dieses Task-Objekts. Gültige Werte sind 0 bis 31.	✓		✓	
	MaximumInterval	DINT[2]	Das maximale Zeitintervall zwischen aufeinander folgenden Ausführungen dieser Task.			✓	✓
	MaximumScanTime	DINT	Aufgezeichnete maximale Ausführungszeit (ms) für diese Task.			✓	✓
	MinimumInterval	DINT[2]	Das minimale Zeitintervall zwischen aufeinander folgenden Ausführungen dieser Task.			✓	✓
	Priority	INT	Relative Priorität dieser Task im Vergleich zu anderen Tasks. Gültige Werte sind 0 bis 15.	✓		✓	
	Rate	DINT	Zeitspanne für die Task (in ms), oder Timeout-Wert für die Task (in ms).	✓		✓	
	Watchdog	DINT	Zeitlimit (in ms) für die Ausführung aller Programme, die mit dieser Task assoziiert sind.	✓		✓	
Sicherheitsprogramm	Instance	DINT	Liefert die Instanznummer dieses Programmobjekts.	✓		✓	
	MajorFaultRecord[1]	DINT[11]	Zeichnet schwerwiegende Fehler für dieses Programm auf.	✓	✓	✓	
	MaximumScanTime	DINT	Aufgezeichnete maximale Ausführungszeit (ms) für dieses Programm.			✓	✓

Tabelle 42 – GSV/SSV-Zugänglichkeit

Sicherheits-objekt	Attributname	Datentyp	Attributbeschreibung	Zugänglich über Sicherheits-Task		Zugänglich über Standard-Task	
				GSV	SSV	GSV[4]	SSV
Sicherheits-routine	Instance	DINT	Liefert die Instanznummer dieses Routineobjekts. Gültige Werte sind 0 bis 65 535.	✓			
Sicherheits-steuerung	SafetyLocked	SINT	Zeigt, ob die Steuerung sicherheitsverriegelt oder sicherheitsentriegelt ist.	✓		✓	
	SafetyStatus[2]	INT	Legt den Sicherheitsstatus wie folgt fest als: • Sicherheits-Task OK. (1000000000000000) • Sicherheits-Task nicht funktionsbereit. (1000000000000001) • Partner fehlt. (0000000000000000) • Partner nicht verfügbar. (0000000000000001) • Hardware inkompatibel. (0000000000000010) • Firmware inkompatibel. (0000000000000011)			✓	
	SafetySignatureExists	SINT	Zeigt an, ob eine Sicherheits-Task-Signatur vorliegt.	✓		✓	
	SafetySignatureID	DINT	32-Bit-Identifikationsnummer.			✓	
	SafetySignature	String[3]	32-Bit-Identifikationsnummer.			✓	
	SafetyTaskFaultRecord[1][2]	DINT[11]	Zeichnet Sicherheits-Task-Fehler auf.			✓	
AOI (Sicherheit)	LastEditDate	LINT	Datum- und Uhrzeitstempel der letzten Änderung an der Definition eines Add-On-Befehls.			✓	
	SignatureID	DINT	ID-Nummer.			✓	
	SafetySignatureID	DINT	32-Bit-Identifikationsnummer.			✓	

(1) Weitere Informationen dazu, wie Sie auf dieses Attribut zugreifen können, finden Sie im Abschnitt Zugreifen auf die „FaultRecord"-Attribute auf Seite 137.
(2) Weitere Informationen dazu, wie Sie auf dieses Attribut zugreifen können, finden Sie im Abschnitt Erfassen von Fehlerinformationen auf Seite 138.
(3) Länge = 37.
(4) Von der Standard-Task ist die GSV-Zugänglichkeit der Sicherheitsobjektattribute die gleiche wie für Standardobjektattribute.

Zugreifen auf die „FaultRecord"-Attribute

Erstellen Sie eine benutzerdefinierte Struktur, um den Zugriff auf die Attribute „MajorFaultRecord" und „SafetyTaskFaultRecord" zu vereinfachen.

Tabelle 43 – Parameter für den Zugriff auf „FaultRecord"-Attribute

Name	Datentyp	Stil	Beschreibung
TimeLow	DINT	Dezimal	Die unteren 32 Bit des Werts für den Fehlerzeitstempel
TimeHigh	DINT	Dezimal	Die oberen 32 Bit des Werts für den Fehlerzeitstempel
Typ	INT	Dezimal	Fehlertyp (Programm, E/A oder Sonstiges)
Code	INT	Dezimal	Eindeutiger Code für diesen Fehler (abhängig vom Fehlertyp)
Info	DINT[8]	Hexadezimal	Fehlerspezifische Informationen (abhängig vom Fehlertyp und -code)

Weitere Informationen zur Verwendung der GSV- und SSV-Befehle finden Sie im Kapitel zu den Eingangs-/Ausgangsbefehlen in der Publikation 1756-RM003, Logix5000-Steuerungen – Allgemeine Befehle – Referenzhandbuch.

Erfassen von Fehlerinformationen

Die Attribute „SafetyStatus“ und „SafetyTaskFaultRecord“ können Informationen zu nicht behebbaren Fehlern erfassen. Verwenden Sie im Fehlerbearbeitungsprogramm der Steuerung einen GSV-Befehl, um die Fehlerinformationen zu erfassen und zu speichern. Der GSV-Befehl kann in einer Standard-Task in Verbindung mit einer Routine des Fehlerbearbeitungsprogramms der Steuerung verwendet werden, die den Fehler löscht und die weitere Ausführung der Standard-Tasks ermöglicht.

Statusanzeigen

Statusanzeigen der 1756-L6*x*S-Steuerung

Der Status der Primärsteuerung und des Sicherheitspartners kann über die LED-Statusanzeigen abgelesen werden.

Tabelle 44 – Erläuterung der Statusanzeigen auf der 1756-L6*x*S-Steuerung

Anzeige	Status	Beschreibung der Primärsteuerung	Beschreibung des Sicherheitspartners
RUN	Aus	Es werden keine Anwender-Tasks ausgeführt. Steuerung ist im PROGram-Modus.	Nicht zutreffend
	Grün	Steuerung ist im RUN-Modus.	Nicht zutreffend
SAFE RUN	Aus	Nicht zutreffend	Die Anwender-Sicherheits-Task oder die Sicherheitsausgänge sind deaktiviert. Die Steuerung befindet sich im PROGram- oder im Testmodus oder die Sicherheits-Task ist fehlerhaft.
	Grün	Nicht zutreffend	Die Anwender-Sicherheits-Task und die Sicherheitsausgänge sind aktiviert. Die Sicherheitsanwendung wird ausgeführt. Die Sicherheits-Task-Signatur liegt vor.
	Grün, blinkend	Nicht zutreffend	Die Anwender-Sicherheits-Task und die Sicherheitsausgänge sind aktiviert. Die Sicherheitsanwendung wird ausgeführt. Die Sicherheits-Task-Signatur liegt nicht vor.
FORCE	Aus	Keine Force-Zustände, Standard oder Sicherheit, sind auf der Steuerung aktiviert.	Nicht zutreffend
	Bernstein	Standard- und/oder Sicherheits-Force-Zustände wurden aktiviert.	Nicht zutreffend
	Bernstein, blinkend	Eine oder mehrere E/A-Adressen, Standard und/oder Sicherheit, wurden in einen Ein- oder Aus-Zustand geforct, aber Force-Zustände sind nicht aktiviert.	Nicht zutreffend
BAT	Aus	Batterie kann Speicher unterstützen.	Batterie kann Speicher unterstützen.
	Rot	Batterie kann Speicher nicht unterstützen.	Batterie kann Speicher nicht unterstützen.
OK	Aus	Keine Stromversorgung.	Keine Stromversorgung.
	Grün	Die Steuerung arbeitet ohne Fehler.	Der Sicherheitspartner arbeitet ohne Fehler.
	Rot, blinkend	Nicht behebbarer Fehler oder behebbarer Fehler wird vom Fehlerbearbeitungsprogramm nicht bearbeitet. Alle Anwender-Tasks, sowohl Standard als auch Sicherheit, werden gestoppt.	Nicht zutreffend
	Rot	Einschaltvorgang oder nicht behebbarer Steuerungsfehler.	Einschaltvorgang oder nicht behebbarer Steuerungsfehler.

Tabelle 44 – Erläuterung der Statusanzeigen auf der 1756-L6*x*S-Steuerung

Anzeige	Status	Beschreibung der Primärsteuerung	Beschreibung des Sicherheitspartners
I/O[1]	Aus	Keine Aktivität. Keine E/A konfiguriert.	Nicht zutreffend
	Grün	Steuerung kommuniziert mit allen konfigurierten E/A-Geräten, sowohl Standard als auch Sicherheit).	Nicht zutreffend
	Grün, blinkend	Mindestens ein E/A-Gerät antwortet nicht.	Nicht zutreffend
	Rot, blinkend	Steuerung kommuniziert mit keinem der konfigurierten E/A-Module.	Nicht zutreffend
RS232	Aus	Keine Aktivität.	Nicht zutreffend
	Grün	Daten werden empfangen oder übertragen.	Nicht zutreffend
SAFETY TASK	Aus	Nicht zutreffend	Keine Partnerschaft aufgebaut. Primärsteuerung fehlt, arbeitet nicht korrekt oder ihre Firmware-Version ist nicht kompatibel mit der des Sicherheitspartners.
	Grün	Nicht zutreffend	Steuerungsstatus ist „OK“. Die koordinierte Systemzeit (CST) ist synchronisiert und Sicherheits-E/A-Verbindungen sind hergestellt.
	Grün, blinkend	Nicht zutreffend	Steuerungsstatus ist „OK“. Die koordinierte Systemzeit (CST) ist nicht synchronisiert, weder in der Primärsteuerung noch im Sicherheitspartner.
	Rot	Nicht zutreffend	Partnerschaft ist verloren gegangen und es konnte keine neue Partnerschaft festgelegt werden. Primärsteuerung fehlt, arbeitet nicht korrekt oder ihre Firmware-Version ist nicht kompatibel mit der des Sicherheitspartners.
	Rot, blinkend	Nicht zutreffend	Sicherheits-Task ist nicht funktionsbereit.

(1) E/A beinhalten produzierte/konsumierte Tags von anderen Steuerungen.

Statusanzeigen der 1756-L7*x*S-Steuerungen

Der Status der Primärsteuerung kann über vier Statusanzeigen abgelesen werden.

Tabelle 45 – Erläuterung der Statusanzeigen an der 1756-L7*x*S-Primärsteuerung

Anzeige	Status	Beschreibung
RUN	Aus	Es werden keine Anwender-Tasks ausgeführt. Steuerung ist im PROGram-Modus.
	Grün	Steuerung ist im RUN-Modus.
FORCE	Aus	Keine Force-Zustände, Standard oder Sicherheit, sind auf der Steuerung aktiviert.
	Bernstein	Standard- und/oder Sicherheits-Force-Zustände wurden aktiviert. **Gehen Sie beim Installieren (Hinzufügen) eines Force-Zustands vorsichtig vor. Nach dem Installieren eines Force-Zustands wird dieser sofort wirksam.**
	Bernstein, blinkend	Eine oder mehrere E/A-Adressen, Standard und/oder Sicherheit, wurden in einen Ein- oder Aus-Zustand geforct, aber Force-Zustände sind nicht aktiviert. **Gehen Sie beim Aktivieren von E/A-Force-Zuständen vorsichtig vor. Bei Aktivierung von E/A-Force-Zuständen werden auch alle bestehenden E/A-Force-Zustände wirksam.**
SD	Aus	Auf der Speicherkarte findet keine Aktivität statt.
	Grün, blinkend	Die Steuerung liest Daten von der Speicherkarte oder schreibt Daten auf diese. Nehmen Sie die Speicherkarte nicht heraus, während die Steuerung Daten liest oder schreibt.
	Grün	
	Rot, blinkend	Die Speicherkarte verfügt über kein gültiges Dateisystem.
	Rot	Die Speicherkarte wird von der Steuerung nicht erkannt.

Tabelle 45 – Erläuterung der Statusanzeigen an der 1756-L7*x*S-Primärsteuerung

Anzeige	Status	Beschreibung
OK	Aus	Keine Stromversorgung.
	Grün	Die Steuerung arbeitet ohne Fehler.
	Rot, blinkend	• Nicht behebbarer Fehler oder behebbarer Fehler wird vom Fehlerbearbeitungsprogramm nicht bearbeitet. Alle Anwender-Tasks, sowohl Standard als auch Sicherheit, werden gestoppt. • Handelt es sich um eine neue Steuerung im Anlieferungszustand, muss ein Firmware-Upgrade ausgeführt werden. Die Statusanzeige zeigt an, dass eine Firmware-Installation erforderlich ist.
	Rot	• Die Steuerung führt eine Einschaltdiagnose aus. • Ein nicht behebbarer schwerwiegender Fehler ist aufgetreten und das Programm wurde aus dem Speicher gelöscht. • Der Kondensator im Energiespeichermodul (ESM) wird beim Abschalten entladen. • Die Steuerung ist eingeschaltet, jedoch nicht betriebsbereit. • Die Steuerung lädt ein Projekt in den nichtflüchtigen Speicher.

Der 1756-L7SP-Sicherheitspartner verfügt über die Statusanzeige „OK“.

Tabelle 46 – 1756-L7SP Statusanzeige

Anzeige	Status	Beschreibung
OK	Aus	Keine Stromversorgung.
	Grün	Der Sicherheitspartner arbeitet ohne Fehler.
	Rot	Einschaltvorgang oder nicht behebbarer Steuerungsfehler.

Statusanzeige an der 1756-L7*x*S-Steuerung

In der Statusanzeige der 1756-L7*x*S-Steuerung werden im Bildlaufverfahren Meldungen angezeigt, die Informationen zur Firmwareversion, zum Status des Energiespeichermoduls (Energy Storage Module, ESM), zum Projektstatus und zu schwerwiegenden Fehlern der Steuerung bereitstellen.

Sicherheitsbezogene Statusmeldungen

Die Anzeige der Primärsteuerung kann die folgenden Meldungen anzeigen. Der Sicherheitspartner zeigt „L7SP“ an.

Tabelle 47 – Sicherheitsbezogene Statusanzeige

Meldung	Bedeutung
No Safety Signature	Sicherheits-Task wird im Run-Modus ohne Sicherheits-Task-Signatur ausgeführt.
Safety Partner Missing	Sicherheitspartner fehlt oder ist nicht verfügbar.
Hardware Incompatible	Sicherheitspartner-Hardware nicht kompatibel mit Hardware der Primärsteuerung.
Firmware Incompatible	Versionsstände der Hardware von Sicherheitspartner und Primärsteuerung nicht kompatibel.
No CST Master	Master für koordinierte Systemzeit (CST) nicht gefunden.
Safety Task Inoperable	Sicherheitslogik ungültig. Dieser Fehler tritt auf, wenn z. B. keine Übereinstimmung zwischen der Primärsteuerung und dem Sicherheitspartner vorliegt, ein Timeout des Überwachungszeitraums erfolgt ist oder der Speicher fehlerhaft ist.
Safety Unlocked	Steuerung befindet sich im Run-Modus und verfügt über eine Sicherheitssignatur, ist jedoch nicht sicherheitsverriegelt.

Allgemeine Statusmeldungen

Die in Tabelle 48 beschriebenen Meldungen werden üblicherweise beim Ein- und Ausschalten und während des Betriebs der Steuerung angezeigt. Diese Meldungen informieren über den Status der Steuerung und des ESM.

Tabelle 48 – Allgemeine Statusmeldungen

Meldung	Bedeutung
Keine Meldung	Die Steuerung ist ausgeschaltet oder ein nicht behebbarer schwerwiegender Fehler (MNRF) ist aufgetreten. Prüfen Sie die Statusleuchte „OK“, um zu ermitteln, ob die Steuerung eingeschaltet ist, und um den Zustand der Steuerung zu bestimmen.
TEST	Die Steuerung führt Einschalttests durch.
PASS	Die Einschalttests wurden erfolgreich abgeschlossen.
SAVE	Ein Projekt wird beim Abschalten auf die SD-Karte gespeichert. Weitere Statusinformationen können Sie an der Statusleuchte „SD“ ablesen (siehe Seite 140). Warten Sie, bis der Speichervorgang abgeschlossen ist, bevor Sie die SD-Karte ausbauen oder die Spannungsversorgung unterbrechen.
LOAD	Ein Projekt wird beim Einschalten von der SD-Karte auf die Steuerung geladen. Weitere Statusinformationen können Sie an der Statusleuchte „SD“ ablesen (siehe Seite 140). Warten Sie, bis der Ladevorgang abgeschlossen ist, bevor Sie die SD-Karte ausbauen, das ESM-Modul entfernen oder die Spannungsversorgung unterbrechen.
UPDT	Beim Einschalten wird ein Firmware-Upgrade von der SD-Karte ausgeführt. Weitere Statusinformationen können Sie an der Statusleuchte „SD“ ablesen (siehe Seite 140). Soll die Firmware beim Einschalten nicht aktualisiert werden, ändern Sie die Einstellung für die Eigenschaft „Load Image“ (Abbilddatei laden) der Steuerung.
CHRG	Das Kondensator-basierte ESM wird geladen.
1756-L7*x*/*X*	Die Bestellnummer und Serie der Steuerung.
Rev *XX.xxx*	Die Haupt- und Nebenversion der Steuerungsfirmware.
No Project	In der Steuerung ist kein Projekt geladen. Verwenden Sie zum Laden eines Projekts in die Steuerung die Software RS Logix 5000 oder eine SD-Karte.
Projektname	Der Name des Projekts, das aktuell in der Steuerung geladen ist. Der angezeigte Name basiert auf dem Projektnamen, der in der Software RSLogix 5000 festgelegt wurde.
BUSY	Die E/A-Module, die der Steuerung zugewiesen sind, werden noch nicht vollständig mit Spannung versorgt. Warten Sie, bis der Einschaltvorgang und der Selbsttest der E/A-Module abgeschlossen sind.
Corrupt Certificate Received	Das der Firmware zugeordnete Sicherheitszertifikat ist fehlerhaft. Laden Sie unter http://www.rockwellautomation.com/support/ die Firmwareversion herunter, auf die Sie ein Upgrade durchführen möchten. Ersetzen Sie die zuvor installierte Firmwareversion durch die Version, die auf der Website des technischen Supports zur Verfügung gestellt wurde.
Corrupt Image Received	Die Firmwaredatei ist fehlerhaft. Laden Sie unter http://www.rockwellautomation.com/support/ die Firmwareversion herunter, auf die Sie ein Upgrade durchführen möchten. Ersetzen Sie die zuvor installierte Firmwareversion durch die Version, die auf der Website des technischen Supports zur Verfügung gestellt wurde.
ESM Not Present	Es ist kein ESM vorhanden und die Steuerung kann die Anwendung beim Ausschalten nicht speichern. Setzen Sie ein kompatibles ESM ein und unterbrechen Sie, sofern Sie ein Kondensator-basiertes ESM verwenden, die Spannungsversorgung erst, wenn das ESM geladen ist.
ESM Incompatible	Das ESM ist hinsichtlich der Speichergröße nicht mit der Steuerung kompatibel. Ersetzen Sie das inkompatible ESM durch ein kompatibles ESM.
ESM Hardware Failure	Es ist ein ESM-Fehler aufgetreten und die Steuerung kann das Programm im Falle einer Abschaltung nicht speichern. Ersetzen Sie das ESM, bevor Sie die Spannungsversorgung der Steuerung unterbrechen, damit das Steuerungsprogramm gespeichert werden kann.
ESM Energy Low	Das Kondensator-basierte ESM verfügt nicht über ausreichend Energie, um der Steuerung im Falle einer Abschaltung die Speicherung des Programms zu ermöglichen. Ersetzen Sie das ESM.
ESM Charging	Das Kondensator-basierte ESM wird geladen. Unterbrechen Sie die Spannungsversorgung erst, wenn der Ladevorgang abgeschlossen ist.
Flash in Progress	Ein von den Dienstprogrammen ControlFLASH oder AutoFlash eingeleitetes Firmware-Upgrade wird ausgeführt. Warten Sie, bis das Firmware-Upgrade abgeschlossen wurde, ohne den Vorgang zu unterbrechen.
Firmware Installation Required	Die Steuerung verwendet die Boot-Firmware (also Version 1.*xxx*) und benötigt ein Firmware-Upgrade. Aktualisieren Sie die Steuerungsfirmware.
SD Card Locked	Es ist eine gesperrte SD-Karte installiert.

Fehlermeldungen

Wenn in der Steuerung ein Fehler auftritt, können in der Statusanzeige die folgenden Meldungen angezeigt werden.

Tabelle 49 – Fehlermeldungen(1)

Meldung	Bedeutung
Major Fault T*XX*:C*XX message*	Es wurde ein schwerwiegender Fehler des Typs *XX* und mit dem Code *XX* erkannt. Wenn beispielsweise die Statusanzeige den schwerwiegenden Fehler „T04:C42 Invalid JMP Target“ anzeigt, ist ein JMP-Befehl so programmiert, dass zu einem ungültigen LBL-Befehl gewechselt wird.
I/O Fault Local:*X #XXXX message*	An einem Modul im zentralen Chassis ist ein E/A-Fehler aufgetreten. Steckplatznummer und Fehlercode werden zusammen mit einer kurzen Beschreibung angegeben. So weist z. B. „I/O Fault Local:3 #0107 Connection Not Found“ darauf hin, dass eine Verbindung zum zentralen E/A-Modul in Steckplatz 3 nicht offen ist. Ergreifen Sie die erforderlichen Maßnahmen für den angegebenen Fehlertyp.
I/O Fault *ModuleName #XXXX message*	An einem Modul in einem dezentralen Chassis ist ein E/A-Fehler aufgetreten. Der Name des fehlerhaften Moduls, wie er im E/A-Konfigurationsverzeichnis der Software RS Logix 5000 konfiguriert ist, wird mit dem Fehlercode und einer kurzen Beschreibung des Fehlers angezeigt. So weist z. B. „ I/O Fault My_Module #0107 Connection Not Found“ darauf hin, dass eine Verbindung zum Modul mit dem Namen „My_Module“ nicht offen ist. Ergreifen Sie die erforderlichen Maßnahmen für den angegebenen Fehlertyp.
I/O Fault *ModuleParent:X #XXXX message*	An einem Modul in einem dezentralen Chassis ist ein E/A-Fehler aufgetreten. Es ist der Name des übergeordneten Moduls angegeben, da im E/A-Konfigurationsverzeichnis der Software RS Logix 5000 kein Modulname konfiguriert ist. Zusätzlich ist der Fehlercode mit einer kurzen Beschreibung des Fehlers angegeben. So weist z. B. „I/O Fault My_CNet:3 #0107 Connection Not Found“ darauf hin, dass eine Verbindung zu einem Modul in Steckplatz 3 des Chassis mit dem Kommunikationsmodul namens „My_CNet“ nicht offen ist. Ergreifen Sie die erforderlichen Maßnahmen für den angegebenen Fehlertyp.
X I/O Faults	Es liegen E/A-Fehler vor, wobei *X* die Anzahl der vorliegenden E/A-Fehler ist. Wenn mehrere E/A-Fehler vorliegen, gibt die Steuerung den zuerst gemeldeten Fehler an. Beim Beheben der einzelnen E/A-Fehler wird die angegebene Zahl der Fehler kleiner und der nächste gemeldete Fehler wird von der E/A-Fehlermeldung angezeigt. Ergreifen Sie die erforderlichen Maßnahmen für den angegebenen Fehlertyp.

(1) Einzelheiten zu den einzelnen E/A-Fehlercodes finden Sie in der Publikation 1756-PM014, Logix5000-Steuerungen – Schwerwiegende, geringfügige und E/A-Fehler – Programmierhandbuch.

Meldungen zu schwerwiegenden, behebbaren Fehlern

Auf schwerwiegende, behebbare Fehler wird durch „Major Fault T*XX*:C*XX message*“ in der Statusanzeige der Steuerung hingewiesen. In Tabelle 50 auf Seite 144 sind die speziellen Fehlertypen, Codes und die zugehörigen Meldungen aufgeführt, wie sie in der Statusanzeige erscheinen.

Ausführliche Beschreibungen und Vorschläge zur Behebung schwerwiegender, behebbarer Fehler finden Sie in der Publikation 1756-PM014, Logix5000-Steuerungen – Schwerwiegende, geringfügige und E/A-Fehler – Programmierhandbuch.

Tabelle 50 – Statusmeldungen zu schwerwiegenden, behebbaren Fehlern

Typ	Code	Meldung
1	1	Run Mode Powerup
1	60	Non-recoverable
1	61	Non-recoverable – Diagnostics Saved
1	62	Non-recoverable – Program Saved
3	16	I/O Connection Failure
3	20	Chassis Failure
3	21	
3	23	Connection Failure
4	16	Unknown Instruction
4	20	Invalid Array Subscript
4	21	Control Structure LEN or POS < 0
4	31	Invalid JSR Parameter
4	34	Timer Failure
4	42	Invalid JMP Target
4	82	SFC Jump Back Failure
4	83	Value Out of Range
4	84	Stack Overflow
4	89	Invalid Target Step
4	90	Invalid Instruction
4	91	Invalid Context
4	92	Invalid Action
4	990	User-defined
4	991	
4	992	
4	993	
4	994	
4	995	
4	996	
4	997	
4	998	
4	999	
6	1	Task Watchdog Expired
7	40	Save Failure

Typ	Code	Meldung
7	41	Bad Restore Type
7	42	Bad Restore Revision
7	43	Bad Restore Checksum
8	1	Keyswitch Change Ignored
11	1	Positive Overtravel Limit Exceeded
11	2	Negative Overtravel Limit Exceeded
11	3	Position Error Tolerance Exceeded
11	4	Encoder Channel Connection Fault
11	5	Encoder Noise Event Detected
11	6	SERCOS Drive Fault
11	7	Synchronous Connection Fault
11	8	Servo Module Fault
11	9	Asynchronous Connection Fault
11	10	Motor Fault
11	11	Motor Thermal Fault
11	12	Drive Thermal Fault
11	13	SERCOS Communications Fault
11	14	Inactive Drive Enable Input Detected
11	15	Drive Phase Loss Detected
11	16	Drive Guard Fault
11	32	Motion Task Overlap Fault
11	33	CST Reference Loss Detected
18	1	CIP Motion Initialization Fault
18	2	CIP Motion Initialization Fault Mfg
18	3	CIP Motion Axis Fault
18	4	CIP Motion Axis Fault Mfg
18	5	CIP Motion Fault
18	6	CIP Module Fault
18	7	Motion Group Fault
18	8	CIP Motion Configuration Fault
18	9	CIP Motion APR Fault
18	10	CIP Motion APR Fault Mfg
18	128	CIP Motion Guard Fault

E/A-Fehlercodes

E/A-Fehler, die von der Steuerung angezeigt werden, erscheinen in der Statusanzeige in einem dieser Formate:

- I/O Fault Local:*X #XXXX message*
- I/O Fault *ModuleName #XXXX message*
- I/O Fault *ModuleParent*:*X #XXXX message*

Der erste Teil des Formats gibt die Position des fehlerhaften Moduls an. Wie die Position angegeben wird, hängt von Ihrer E/A-Konfiguration und den in der Software RS Logix 5000 angegebenen Moduleigenschaften ab.

Der letzte Teil des Formats, „#XXXX message“, kann für die Diagnose des E/A-Fehlertyps und der möglichen Gegenmaßnahmen verwendet werden.

Einzelheiten zu den einzelnen E/A-Fehlercodes finden Sie in der Publikation 1756-PM014, Logix5000-Steuerungen – Schwerwiegende, geringfügige und E/A-Fehler – Programmierhandbuch.

Tabelle 51 – E/A-Fehlermeldungen

Code	Meldung
#0001	Connection Failure
#0002	Insufficient Resource
#0003	Invalid Value
#0004	IOI Syntax
#0005	Destination Unknown
#0006	Partial Data Transferred
#0007	Connection Lost
#0008	Service Unsupported
#0009	Invalid Attribute Value
#000A	Attribute List Error
#000B	State Already Exists
#000C	Object Mode Conflict
#000D	Object Already Exists
#000E	Attribute Not Settable
#000F	Permission Denied
#0010	Device State Conflict
#0011	Reply Too Large
#0012	Fragment Primitive
#0013	Insufficient Command Data
#0014	Attribute Not Supported
#0015	Data Too Large
#0100	Connection In Use
#0103	Transport Not Supported
#0106	Ownership Conflict
#0107	Connection Not Found
#0108	Invalid Connection Type
#0109	Invalid Connection Size
#0110	Module Not Configured
#0111	RPI Out of Range
#0113	Out of Connections
#0114	Wrong Module

Code	Meldung
#0115	Wrong Device Type
#0116	Wrong Revision
#0117	Invalid Connection Point
#0118	Invalid Configuration Format
#0119	Module Not Owned
#011A	Out of Connection Resources
#0203	Connection Timeout
#0204	Unconnected Message Timeout
#0205	Invalid Parameter
#0206	Message Too Large
#0301	No Buffer Memory
#0302	Bandwidth Not Available
#0303	No Bridge Available
#0304	ControlNet Schedule Error
#0305	Signature Mismatch
#0306	CCM Not Available
#0311	Invalid Port
#0312	Invalid Link Address
#0315	Invalid Segment Type
#0317	Connection Not Scheduled
#0318	Invalid Link Address
#0319	No Secondary Resources Available
#031E	No Available Resources
#031F	No Available Resources
#0800	Network Link Offline
#0801	Incompatible Multicast RPI
#0802	Invld Safety Conn Size
#0803	Invld Safety Conn Format
#0804	Invld Time Correct Conn Format
#0805	Invld Ping Intrvl EPI Multiplier
#0806	Time Coord Msg Min Multiplier

E/A-Fehlermeldungen (Fortsetzung)

Code	Meldung
#0807	Time Expectation Multiplier
#0808	Timeout Multiplier
#0809	Invld Max Consumer Number
#080A	Invld CPCRC
#080B	Time Correction Conn ID Invld
#080C	Safety Cfg Signature Mismatch
#080D	Safety Netwk Num Not Set OutOfBx
#080E	Safety Netwk Number Mismatch
#080F	Cfg Operation Not Allowed
#0814	Data Type Mismatch
#FD01	Bad Backplane EEPROM
#FD02	No Error Code
#FD03	Missing Required Connection
#FD04	No CST Master
#FD05	Axis or GRP Not Assigned
#FD06	SERCOS Transition Fault
#FD07	SERCOS Init Ring Fault
#FD08	SERCOS Comm Fault
#FD09	SERCOS Init Node Fault
#FD0A	Axis Attribute Reject
#FD1F	Safety Data Fault
#FD20	No Safety Task Running
#FD21	Invld Safety Conn Parameter
#FE01	Invalid Connection Type
#FE02	Invalid Update Rate
#FE03	Invalid Input Connection
#FE04	Invalid Input Data Pointer
#FE05	Invalid Input Data Size
#FE06	Invalid Input Force Pointer
#FE07	Invalid Output Connection

Code	Meldung
#FE08	Invalid Output Data Pointer
#FE09	Invalid Output Data Size
#FE0A	Invalid Output Force Pointer
#FE0B	Invalid Symbol String
#FE0C	Invalid Scheduled P/C Instance
#FE0D	Invalid Symbol Instance
#FE0E	Module Firmware Updating
#FE0F	Invalid Firmware File Revision
#FE10	Firmware File Not Found
#FE11	Firmware File Invalid
#FE12	Automatic Firmware Update Failed
#FE13	Update Failed – Active Connection
#FE14	Searching Firmware File
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
–	

Warten der Batterie

Die GuardLogix 1756-L6*x*S-Primärsteuerungen und die 1756-LSP-Sicherheitspartner sind mit einer Lithiumbatterie ausgestattet, die nach einer gewissen Zeit ausgetauscht werden muss. Die GuardLogix 1756-L7*x*S-Steuerungen und die 1756-L7SP-Sicherheitspartner haben keine Batterie.

Abschätzen der Batterielebensdauer

Die Batterielebensdauer ist abhängig von der Chassistemperatur, von der Projektgröße und davon, wie oft die Steuerung aus- und wieder eingeschaltet wird. Die Batterielebensdauer hängt nicht davon ab, ob die Steuerung mit Strom versorgt wird oder nicht.

Vor dem Aufleuchten der Anzeige BAT

Verwenden Sie diese Tabelle, um den Zeitraum, bevor die Anzeige BAT rot aufleuchtet, im ungünstigsten Fall einzuschätzen.

Tabelle 52 – Batterielebensdauer vor dem Aufleuchten der Anzeige BAT (im ungünstigsten Fall)

Temperatur 2,54 cm (1 in.) Unter Chassis	Ein-/ Ausschaltzyklen pro Tag	Projektgröße			
		1 MB	2 MB	4 MB	8 MB
0–40 °C	3	3 Jahre	3 Jahre	26 Monate	20 Monate
	bis 2	3 Jahre	3 Jahre	3 Jahre	31 Monate
41–45 °C	3	2 Jahre	2 Jahre	2 Jahre	20 Monate
	bis 2	2 Jahre	2 Jahre	2 Jahre	2 Jahre
46–50 °C	bis 3	16 Monate	16 Monate	16 Monate	16 Monate
51–55 °C	bis 3	11 Monate	11 Monate	11 Monate	11 Monate
56–60 °C	bis 3	8 Monate	8 Monate	8 Monate	8 Monate

BEISPIEL

Unter den folgenden Bedingungen hält die Batterie mindestens 20 Monate, bevor die Anzeige BAT rot aufleuchtet.

- Die maximale Temperatur 2,54 cm unter dem Chassis beträgt 45 °C.
- Der Strom wird drei Mal pro Tag ein- und ausgeschaltet.
- Die Steuerung umfasst ein 8 MB großes Projekt.

Nach dem Aufleuchten der Anzeige BAT

WICHTIG Wenn die Anzeige BAT zum ersten Mal aufleuchtet, sobald Sie die Steuerung einschalten, ist die Batterielebensdauer kürzer als in Tabelle 53 angegeben. Es findet stets eine geringe Entladung der Batterie statt. Ein Teil der Batterielebensdauer kann möglicherweise bereits verbraucht worden sein, während die Steuerung abgeschaltet war und die Anzeige BAT daher nicht aufleuchten konnte.

Tabelle 53 – Batterielebensdauer nach dem Aufleuchten der Anzeige BAT (im ungünstigsten Fall)

Temperatur, max. 25,4 mm (1 in.) Unter dem Chassis	Ein-/ Ausschaltzyklen	Projektgröße			
		1 MB	2 MB	4 MB	8 MB
0–20 °C	3 Mal pro Tag	26 Wochen	18 Wochen	12 Wochen	9 Wochen
	1 Mal pro Tag	26 Wochen	26 Wochen	26 Wochen	22 Wochen
	1 Mal pro Monat	26 Wochen	26 Wochen	26 Wochen	26 Wochen
21–40 °C	3 Mal pro Tag	18 Wochen	14 Wochen	10 Wochen	8 Wochen
	1 Mal pro Tag	24 Wochen	21 Wochen	18 Wochen	16 Wochen
	1 Mal pro Monat	26 Wochen	26 Wochen	26 Wochen	26 Wochen
41–45 °C	3 Mal pro Tag	12 Wochen	10 Wochen	7 Wochen	6 Wochen
	1 Mal pro Tag	15 Wochen	14 Wochen	12 Wochen	11 Wochen
	1 Mal pro Monat	17 Wochen	17 Wochen	17 Wochen	17 Wochen
46–50 °C	3 Mal pro Tag	10 Wochen	8 Wochen	6 Wochen	6 Wochen
	1 Mal pro Tag	12 Wochen	11 Wochen	10 Wochen	9 Wochen
	1 Mal pro Monat	12 Wochen	12 Wochen	12 Wochen	12 Wochen
51–55 °C	3 Mal pro Tag	7 Wochen	6 Wochen	5 Wochen	4 Wochen
	1 Mal pro Tag	8 Wochen	8 Wochen	7 Wochen	7 Wochen
	1 Mal pro Monat	8 Wochen	8 Wochen	8 Wochen	8 Wochen
56–60 °C	3 Mal pro Tag	5 Wochen	5 Wochen	4 Wochen	4 Wochen
	1 Mal pro Tag	6 Wochen	6 Wochen	5 Wochen	5 Wochen
	1 Mal pro Monat	6 Wochen	6 Wochen	6 Wochen	6 Wochen

Wann ist die Batterie auszuwechseln?

Wenn die Batterie etwa zu 95 % entladen ist, warnt Sie die Steuerung wie folgt:

- Die Anzeige an der Vorderseite der Steuerung leuchtet rot (stetig rot).
- Es tritt ein geringfügiger Fehler auf (Typ 10, Code 10 für die Steuerung).

ACHTUNG: Um zu verhindern, dass aus Ihrer Batterie möglicherweise giftige Chemikalien austreten, ersetzen Sie Ihre Batterie gemäß dem folgenden Plan, auch wenn die Anzeige BAT nicht aufleuchtet.

Tabelle 54 – Austauschzeitplan für die Batterie

Temperatur 2,54 cm unter dem Chassis	Batterie auswechseln alle
–25 bis 35 °C (–13 bis 95 °F)	Kein Austausch erforderlich
36 bis 40 °C (96,8 bis 104 °F)	3 Jahre
41 bis 45 °C (105,8 bis 113 °F)	2 Jahre
46 bis 50 °C (114,8 bis 122 °F)	16 Monate
51 bis 55 °C (123,8 bis 131 °F)	11 Monate
56 bis 70 °C (132,8 bis 158 °F)	8 Monate

WICHTIG Da es sich bei der GuardLogix-Steuerung um eine 1oo2-Steuerung (zwei Prozessoren) handelt, wird dringend empfohlen, beide Steuerungsbatterien gleichzeitig auszuwechseln.

Auswechseln der Batterie

Diese Steuerung ist mit einer Lithiumbatterie versehen, die während der Lebensdauer des Produkts ersetzt werden muss. Bei der Handhabung und Entsorgung der Batterie müssen besondere Vorsichtsmaßnahmen getroffen werden.

ACHTUNG: Die Steuerung verwendet eine Lithiumbatterie, die potenziell gefährliche Chemikalien enthält.

Konsultieren Sie vor dem Umgang mit der Batterie die Publikation AG-5.4, „Guidelines for Handling Lithium Batteries“.

WARNUNG: Beim Anschließen oder Trennen der Batterie kann es zur Bildung eines elektrischen Lichtbogens kommen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden. Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

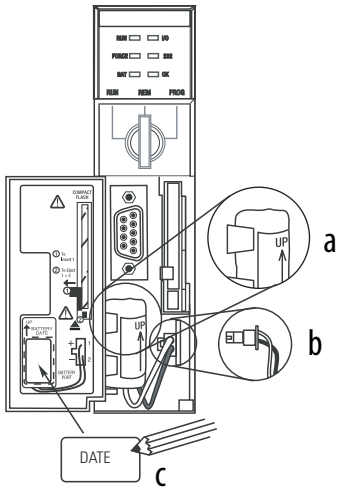
WICHTIG Falls die Batterie entfernt wird und es danach zu einem Verlust der Betriebsspannung kommt, geht das Projekt in der Steuerung verloren.

Gehen Sie zum Auswechseln der Batterie wie folgt vor.

1. Schalten Sie die Stromversorgung zum Chassis ein.
2. Weist die vorhandene Batterie Anzeichen von Undichtigkeit oder Beschädigung auf?

Wenn	Dann
Ja	Konsultieren Sie vor dem Umgang mit der Batterie die Publikation AG-5.4, „Guidelines for Handling Lithium Batteries“.
Nein	Fahren Sie mit dem nächsten Schritt fort.

3. Entfernen Sie die alte Batterie.
4. Installieren Sie eine neue Batterie des Typs 1756-BA2.
   a. Installieren Sie die Batterie wie dargestellt.
   b. Schließen Sie die Batterie an:
      + Rot
      – Schwarz
   c. Schreiben Sie das Installationsdatum der Batterie auf das Etikett der Batterie und befestigen Sie dieses auf der Innenseite der Steuerungsabdeckung.



ACHTUNG: Installieren Sie nur eine Batterie des Typs 1756-BA2. Bei Verwendung anderer Batterien kann die Steuerung beschädigt werden.

5. Überprüfen Sie, ob die Anzeige BAT auf der Vorderseite der Steuerung ausgeschaltet ist.

Wenn	Dann
Ja	Fahren Sie mit dem nächsten Schritt fort.
Nein	1. Stellen Sie sicher, dass die Batterie korrekt mit der Steuerung verbunden ist. 2. Falls die Anzeige BAT weiterhin leuchtet, installieren Sie eine andere Batterie des Typs 1756-BA2. 3. Wenn die Anzeige BAT nach dem Einbau einer anderen Batterie in Schritt 2 noch immer leuchtet, kontaktieren Sie Ihren Rockwell Automation-Vertreter oder Ihren Distributor vor Ort.

6. Entsorgen Sie die alte Batterie gemäß den örtlichen Bestimmungen.

WARNUNG: Verbrennen oder entsorgen Sie Lithiumbatterien nicht mit dem allgemeinen Hausmüll. Sie könnten bersten oder explodieren. Befolgen Sie die örtlichen Bestimmungen für die Entsorgung dieser Materialien. Sie sind rechtlich gesehen verantwortlich für jede Gefahr, die während der Entsorgung Ihrer Batterie entsteht.

ACHTUNG: Dieses Produkt ist mit einer versiegelten Lithiumbatterie versehen, die während der Lebensdauer des Produkts ersetzt werden muss.

Am Ende der Lebensdauer des Produkts darf die darin enthaltene Batterie nicht mit dem Hausmüll entsorgt werden.

Das Recycling von Batterien trägt zum Umweltschutz bei und sorgt für eine Bewahrung der natürlichen Ressourcen, da wertvolle Materialien wiedergewonnen werden.

Aufbewahrung von Ersatzbatterien

ACHTUNG: Da aus falsch gelagerten Batterien potenziell gefährliche Chemikalien auslaufen können, lagern Sie die Batterien wie folgt: Bewahren Sie Batterien immer kühl und trocken auf. Wir empfehlen für die Lagerung eine Temperatur von 25 °C bei einer relativen Luftfeuchtigkeit von 40–60 %. Sie können Batterien bis zu 30 Tage lang bei Temperaturen zwischen –45 und +85 °C lagern, z. B. während des Transports. Um ein mögliches Auslaufen zu vermeiden, lagern Sie Batterien nicht länger als 30 Tage bei Temperaturen über 60 °C.

Weitere Informationen

Informationen zur Handhabung, Lagerung und Entsorgung von Lithiumbatterien finden Sie in den Richtlinien zur Handhabung von Lithiumbatterien, Publikation AG-5.4.

Notizen:

Wechsel des Steuerungstyps in RSLogix 5000-Projekten

Da Sicherheitssteuerungen besonderen Anforderungen unterliegen und bestimmte Standardfunktionen nicht unterstützen, müssen Sie das Verhalten des Systems verstehen, wenn Sie in Ihrem RSLogix 5000-Projekt von einer Standard- zu einer Sicherheitssteuerung oder von einer Sicherheits- zu einer Standardsteuerung wechseln. Der Wechsel des Steuerungstyps wirkt sich auf Folgendes aus:

- Unterstützte Leistungsmerkmale
- Physische Konfiguration des Projekts (d. h. Sicherheitspartner und Sicherheits-E/A)
- Steuerungseigenschaften
- Projektkomponenten (z. B. Tasks, Programme, Routinen und Tags)
- Sicherheitsrelevante Add-On-Befehle.

Wechsel von einer Standard- zu einer Sicherheitssteuerung

Um erfolgreich von einer Standardsteuerung zu einer Sicherheitssteuerung zu wechseln, muss für den Sicherheitspartner der Chassissteckplatz rechts neben der Sicherheitsprimärsteuerung frei sein.

Nach der Bestätigung des Wechsels von einem Projekt mit Standardsteuerung zu einem Projekt mit Sicherheitssteuerung werden Sicherheitskomponenten erstellt, damit die Mindestanforderungen an eine Sicherheitssteuerung erfüllt werden:

- Die Sicherheits-Task wird nur erstellt, wenn die maximal herunterladbare Anzahl von Tasks noch nicht erreicht ist. Die Sicherheits-Task wird mit ihren Standardwerten initialisiert.
- Sicherheitskomponenten werden erstellt (d. h. Sicherheits-Task, Sicherheitsprogramm usw.).
- Eine zeitbasierte Sicherheitsnetzwerknummer (SNN) wird für das lokale Chassis generiert.

- Alle nicht von der Sicherheitssteuerung unterstützten Standardsteuerungsfunktionen, wie z. B. Redundanz, stehen im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) nicht mehr zur Verfügung (sofern dies zuvor der Fall war).

Wechsel von einer Sicherheits- zu einer Standardsteuerung

Nach der Bestätigung eines Wechsels von einem Projekt mit Sicherheitssteuerung zu einem Projekt mit Standardsteuerung werden einige Komponenten geändert und andere gelöscht, wie nachfolgend beschrieben:

- Der Sicherheitspartner 1756-LSP wird aus dem E/A-Chassis entfernt.
- Sicherheits-E/A-Module und ihre Tags werden gelöscht.
- Sicherheits-Task, Sicherheitsprogramme und Sicherheitsroutinen werden in Standard-Tasks, Standardprogramme und Standardroutinen geändert.
- Alle Sicherheits-Tags, ausgenommen konsumierte Sicherheits-Tags, werden in Standard-Tags geändert. Konsumierte Sicherheits-Tags werden gelöscht.
- Sicherheits-Tag-Zuordnungen werden gelöscht.
- Die Sicherheitsnetzwerknummer (SNN) wird gelöscht.
- Sicherheitsverriegelungs- und Sicherheitsentriegelungs-Kennwörter werden gelöscht.
- Wenn die Standardsteuerung Funktionen unterstützt, die für die Sicherheitssteuerung nicht zur Verfügung standen, werden diese neuen Merkmale im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) angezeigt.

  TIPP Peer-Sicherheitssteuerungen werden nicht gelöscht, selbst wenn sie keine Verbindungen mehr haben.

- Befehle können weiterhin auf Module verweisen, die bereits gelöscht wurden. In diesem Fall werden Verifizierungsfehler generiert.
- Konsumierte Tags werden beim Löschen des produzierenden Moduls ebenfalls gelöscht.
- Aufgrund der oben durchgeführten Systemänderungen werden sicherheitsspezifische Befehle und Sicherheits-E/A-Tags nicht verifiziert.

Enthält das Sicherheitssteuerungsprojekt Sicherheits-Add-On-Befehle, müssen Sie diese vor dem Wechsel des Steuerungstyps aus dem Projekt entfernen oder deren Klasse wieder in „Standard“ ändern.

Wechsel von einer 1756 GuardLogix- zu einer 1768 Compact GuardLogix-Steuerung oder umgekehrt

Wenn Sie von einem Sicherheitssteuerungstyp zu einem anderen wechseln, bleibt die Klasse der Tags, Routinen und Programme unverändert. Alle E/A-Module, die nicht mehr mit der Zielsteuerung kompatibel sind, werden gelöscht.

Die Darstellung des Sicherheitspartners wird so aktualisiert, dass sie für die Zielsteuerung geeignet ist:

- Der Sicherheitspartner wird in Steckplatz *x* (primärer Steckplatz + 1) erstellt, wenn Sie zu einer 1756 GuardLogix-Steuerung wechseln.
- Beim Wechsel zu einer 1768 Compact GuardLogix-Steuerung wird der Sicherheitspartner entfernt, da dieser sich innerhalb der Compact GuardLogix-Steuerung befindet.

TIPP Eine 1756 GuardLogix-Steuerung unterstützt 100 Sicherheitsprogramme in der Sicherheits-Task, während eine 1768 Compact GuardLogix-Steuerung 32 Sicherheitsprogramme unterstützt.

Wechsel von einer 1756-L7*x*S-Steuerung zu einer 1756-L6*x*S- oder 1768-L4*x*S-Steuerung

Fließkommabefehle, wie z. B. FAL, FLL, FSC, SIZE, CMP, SWPB und CPT werden in 1756-L7*x*S-Steuerungen unterstützt, nicht jedoch in 1756-L6*x*S- und 1768-L4*x*S-Steuerungen. Wenn Ihre Sicherheitsprogramme diese Anweisungen enthalten, kommt es beim Wechsel von einer 1756-L7*x*S-Steuerung zu einer 1756-L6*x*S- oder 1768-L4*x*S-Steuerung zu Verifizierungsfehlern.

Weitere Informationen

Weitere Informationen zu Add-On-Befehlen finden Sie in der Publikation 1756-PM010, Logix5000 Controllers Add-On Instructions Programming Manual.

Notizen:

Änderungshistorie

Da sowohl neue Steuerungen, Module und Anwendungen als auch neue Funktionen in der Software RSLogix 5000 verfügbar sind, wurde dieses Handbuch überarbeitet, um aktualisierte Informationen darin aufzunehmen. Dieser Anhang fasst kurz alle Änderungen zusammen, zu denen es in den früheren Versionen dieses Handbuchs gekommen ist.

Schlagen Sie in diesem Anhang nach, wenn Sie feststellen müssen, welche Änderungen im Verlauf der verschiedenen Versionen vorgenommen wurden. Dies kann insbesondere dann hilfreich sein, wenn Sie Ihre Hardware oder Software auf der Basis von Informationen aktualisieren möchten, die in früheren Versionen dieses Handbuchs ergänzt wurden.

1756-UM020H-EN-P April 2012

Korrigierte Liste der unterstützten Netzteile.

1756-UM020G-EN-P, Februar 2012

- Ergänzte Informationen zu 1756-L7*x*S- und 1756-L73SXT-Steuerungen
- Aktualisierte Liste der zusätzlich erhältlichen Ressourcen
- Ergänztes Kapitel zur Installation der Steuerung
- Hinzugefügte Informationen zu Unicast-Verbindungen für E/A-Module auf EtherNet/IP-Netzwerken
- Hinzugefügte Informationen zur Installation
- Hinzugefügte Informationen zum Run-Modus-Schutz für die Sicherheits-Task-Signatur
- Aktualisierte Verfahrensvorschriften für den Austausch von E/A, um verschiedene Austauschszenarien darzulegen
- Aktualisierter Höchstwert für angeforderte Paketintervalle (RPI)
- Zur Liste der für Sicherheits-Tags gültigen Typen hinzugefügte Datentypen DCA_INPUT und DCAF_INPUT
- Umstrukturierte Informationen zu produzierten und konsumierten Sicherheits-Tags und zur Konfiguration von Peer-Sicherheitssteuerungen, sodass alle Informationen jetzt in Kapitel 6 enthalten sind
- Hinzugefügte Informationen zu den Auswirkungen einer gesperrten SD-Karte auf ein Firmware-Update
- Hinzugefügte Informationen zur Verwendung des Energiespeichermoduls (Energy Storage Module, ESM) für den nichtflüchtigen Speicher
- In einen Anhang verschobene Tabellen mit den Erläuterungen zu den Statusanzeigen und hinzugefügte Informationen zur Fehlerbehebung

- Hinzugefügte Informationen dazu, wann die Batterie der 1756-L6*x*S-Steuerungen ausgetauscht werden muss
- Hinzugefügte Informationen zum Austausch einer 1756-L7*x*S-Steuerung
- Ergänzter Anhang mit der Änderungshistorie

1756-UM020F-EN-P, August 2010

- GuardLogix-Steuerungen werden in RSLogix 5000 Version 19 unterstützt
- Der Standardverbindungstyp für produzierte und konsumierte Sicherheits-Tags ist Unicast

1756-UM020E-EN-P, Januar 2010

- Ergänzung der Liste mit unterstützten RSLogix 5000-Funktionen um neue Sicherheits-Add-On-Befehle und Add-On-Befehle mit hoher Integrität
- Aktivieren der Zeitsynchronisierung
- Aktualisierte Beispiele zur Änderung der Sicherheitsnetzwerknummern (SNN) von Sicherheits-E/A-Modulen auf dem CIP Safety-Netzwerk, um EtherNet/IP-Sicherheits-E/A-Module anzuzeigen
- Verdeutlichte Informationen zur Ethernet-Adressierung
- ControlNet-Verbindungen für dezentrale E/A
- Definieren eines Tags als Konstante
- Festlegen der externen Zugriffsebene für Tag-Daten
- Aktualisierte Vorgehensweise zum Produzieren und Konsumieren von Sicherheits-Tags
- Einschränkungen bei der Zuordnung von Tags mit konstanten Werten
- Aktualisierte Tabelle der Softwareantworten während des Herunterladens
- GSV/SSV-Zugänglichkeit für AOI-Sicherheitsobjekt
- Speichern und Laden von Projekten mithilfe des nichtflüchtigen Speichers
- Aktualisierte Informationen zur Entsorgung von Batterien
- Wechsel von einer 1756 GuardLogix- zu einer 1768 Compact GuardLogix-Steuerung oder umgekehrt

1756-UM020D-EN-P, Juli 2008

- Aktualisierte Tabelle mit weiteren Publikationen, in der neue Handbücher aufgeführt sind
- Informationen zur 1756-L63S-Steuerung
- Allgemeine Informationen zur Programmierung mithilfe der Version 17 der RSLogix 5000-Software, inklusive der unterstützten Software-Versionen und Verbesserungen
- Einsatz eines 1756-EN2T-Moduls in einem GuardLogix-basierten System
- Informationen zu Guard I/O EtherNet/IP-Sicherheitsmodulen
- Aktualisierte Liste mit gültigen Datentypen für Sicherheits-Tags
- Aktionen zur Sicherheitsverriegelung und -entriegelung werden protokolliert
- Vorgänge zum Erstellen und Löschen der Sicherheitssignatur werden protokolliert

- Download-Vorgang umfasst jetzt eine Überprüfung des CST-Masters (Coordinated System Time, koordinierte Systemzeit)
- Aktualisierte Fehlercodebeschreibung für „Safety Task Inoperable“ (Sicherheits-Task nicht funktionsbereit)
- Wert der Sicherheitssignatur ist über den GSV-Befehl zugänglich
- Datentypinformationen zu Attributen sind über GSV- und SSV-Befehle zugänglich
- Zugriff auf Fehlerinformationen mithilfe des GSV-Befehls
- Aktualisierte Zertifizierungsdaten
- Aktualisierte Informationen zur geschätzten Batterielebensdauer
- Aktualisierte Informationen zur korrekten Entsorgung von Batterien

1756-UM020C-EN-P, Dezember 2006

- Erläuterung der Datenflussfunktionen einer GuardLogix-Steuerung
- Die Steuerung unterstützt keine BS-Upgrades über CompactFlash
- Die Sicherheits-Task unterstützt keine Add-On-Befehle oder Alarm- und Ereignissoftware von FactoryTalk®
- Das maximale angeforderte Paketintervall (RPI) für Sicherheitsverbindungen wurde von 500 ms auf 100 ms geändert
- Die Liste mit ungültigen Datentypen für Sicherheitsprogramme wurde durch eine Liste mit gültigen Datentypen ersetzt
- Überarbeitete Beschreibung von produzierten und konsumierten Sicherheitsverbindungen
- Überarbeitete Beschreibung der Auswirkungen auf die Sicherheitsverriegelungsfunktion und die Sicherheitssignatur beim Herunterladen
- Hinzugefügte UL NRGF-Zertifizierung
- Zu den technischen Daten der Steuerung hinzugefügte Daten zur Wahrscheinlichkeit eines Ausfalls bei Anforderung (PFD) und zur Wahrscheinlichkeit eines Ausfalls pro Stunde (PFH)

1756-UM020B-EN-P, Oktober 2005

RSLogix 5000-Programmiersoftware ab Version 14.01 vergleicht nicht länger die Hardware-Serien des Sicherheitspartners und der Primärsteuerung oder der Steuerung und der Sicherheitssignatur im Projekt.

1756-UM020A-EN-P, Januar 2005

Erstausgabe.

Ziffern

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

Kundendienst von Rockwell Automation

Rockwell Automation bietet Ihnen über das Internet Unterstützung bei der Verwendung seiner Produkte. Unter http://www.rockwellautomation.com/support/ finden Sie technische Handbücher, eine Wissensdatenbank mit Antworten auf häufig gestellte Fragen, technische Hinweise und Applikationsbeispiele, Beispielcode und Links zu Software-Servicepaketen. Außerdem finden Sie dort die Funktion „MySupport“, über die Sie diese Werkzeuge individuell an Ihre Anforderungen anpassen können.

Zusätzlichen telefonischen technischen Support für die Insatallation, Konfiguration und Fehlerbehebung erhalten Sie über die TechConnect^{SM}-Supportprogramme. Wenn Sie weitere Informationen wünschen, wenden Sie sich an den für Sie zuständigen Distributor oder Ihren Rockwell Automation-Vertreter. Sie können uns auch gern auf unserer Website http://www.rockwellautomation.com/support/ besuchen.

Unterstützung bei der Installation

Wenn in den ersten 24 Stunden nach der Installation Probleme auftreten, lesen Sie die Informationen in diesem Handbuch. Über den Kundendienst erhalten Sie Unterstützung beim Einrichten und Inbetriebnehmen Ihres Produkts.

USA oder Kanada	1.440.646.3434
Außerhalb der USA oder Kanada	Verwenden Sie den Worldwide Locator unter http://www.rockwellautomation.com/support/americas/phone_en.html, oder wenden Sie sich an Ihren lokalen Rockwell Automation-Vertreter.

Rückgabeverfahren bei neuen Produkten

Rockwell Automation testet alle Produkte, um sicherzustellen, dass sie beim Verlassen des Werks voll funktionsfähig sind. Sollte Ihr Produkt dennoch einmal nicht funktionieren, sodass Sie es einsenden müssen, gehen Sie wie folgt vor.

USA	Wenden Sie sich an Ihren Distributor. Sie müssen Ihrem Distributor eine Kundendienst-Bearbeitungsnummer angeben (diese erhalten Sie über die oben genannte Telefonnummer), damit das Rückgabeverfahren abgewickelt werden kann.
Außerhalb der USA	Bitte wenden Sie sich bei Fragen zum Rückgabevorgang an den für Sie zuständigen Vertreter von Rockwell Automation.

Feedback zur Dokumentation

Ihre Kommentare helfen uns, Ihre Dokumentationsanforderungen besser zu erfüllen. Wenn Sie Vorschläge zur Verbesserung dieses Dokuments haben, füllen Sie das entsprechende Formular aus (Publikation RA-DU002, erhältlich unter http://www.rockwellautomation.com/literature/).

www.rockwellautomation.com

Hauptverwaltung für Antriebs-, Steuerungs- und Informationslösungen

Amerika: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Naher Osten/Afrika: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgien, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asien/Australien/Pazifikraum: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, China, Tel: +852 2887 4788, Fax: +852 2508 1846

Deutschland: Rockwell Automation GmbH, Parsevalstraße 11, 40468 Düsseldorf, Tel: +49 (0)211 41553 0, Fax: +49 (0)211 41553 121
Schweiz: Rockwell Automation AG, Industriestrasse 20, CH-5001 Aarau, Tel: +41(62) 889 77 77, Fax: +41(62) 889 77 11, Customer Service – Tel: 0848 000 277
Österreich: Rockwell Automation, Kotzinastraße 9, A-4030 Linz, Tel: +43 (0)732 38 909 0, Fax: +43 (0)732 38 909 61

Publikation 1756-UM020I-DE-P – August 2012