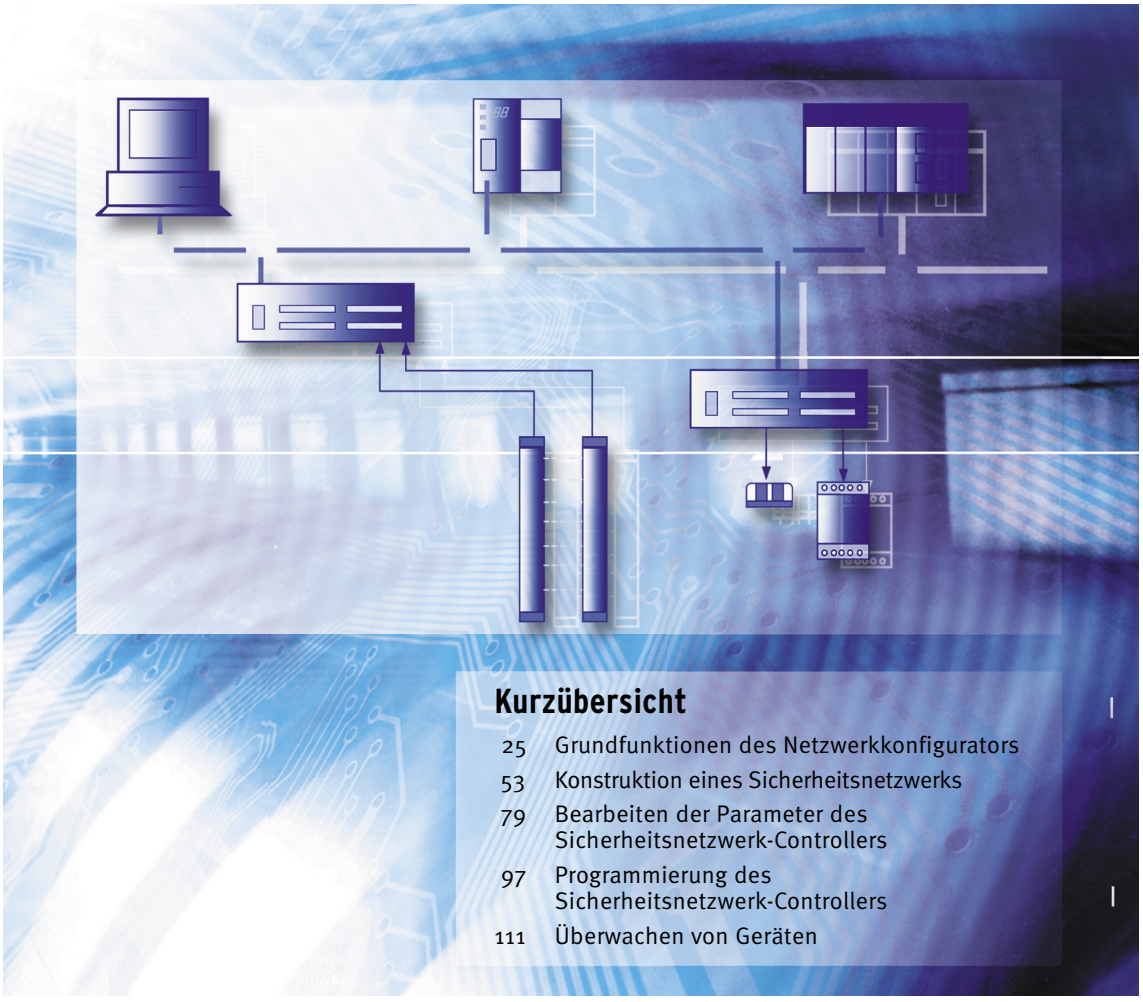
Cat. No. Z905-DE2-01

DeviceNet Safety

SYSTEMKONFIGURATIONSHANDBUCH



Kurzübersicht

Advanced Industrial Automation

OMRON

DeviceNet Safety
Systemkonfigurationshandbuch

Revisionsstand März 2005

Hinweis

OMRON-Produkte sind nur zur ordnungsgemäßen Verwendung durch qualifiziertes Personal und nur für die in diesem Handbuch beschriebenen Zwecke zugelassen.

In diesem Handbuch sind Sicherheitshinweise entsprechend der folgenden Konventionen gekennzeichnet. Beachten Sie stets die in diesen Sicherheitshinweisen enthaltenen Informationen. Ein Nichtbeachten der Sicherheitshinweise kann zu Personen- oder Sachschäden führen.

⚠ **VORSICHT**	Kennzeichnet eine potenziell gefährliche Situation, die zu leichten, mittelschweren oder schweren Verletzungen oder sogar zum Tod führen kann, wenn sie nicht vermieden wird. Außerdem können erhebliche Sachschäden verursacht werden.

	Kennzeichnet allgemeine Verbote, für die kein spezielles Symbol verwendet wird.

	Kennzeichnet unbedingt zu beachtende allgemeine Anweisungen, für die kein spezielles Symbol verwendet wird.

Verweise auf OMRON-Produkte

Alle Bezeichnungen von OMRON-Produkten werden in diesem Handbuch in Großbuchstaben geschrieben.

Die Abkürzung „SPS“ steht für speicherprogrammierbare Steuerung.

Visuelle Hilfen

Die folgenden Textsymbole in der linken Spalte dieses Handbuchs ermöglichen Ihnen das schnelle Auffinden bestimmter Informationen.

WICHTIG: Kennzeichnet wichtige Informationen zu Schritten, die zur Vermeidung von Ausfällen, Fehlfunktionen und unerwünschten Auswirkungen auf die Leistung des Produkts unbedingt vorzunehmen oder unbedingt zu unterlassen sind.

Hinweis: Kennzeichnet Informationen von besonderem Interesse für den effizienten und zweckmäßigen Einsatz des Produkts.

1,2,3… Kennzeichnet Listen, z. B. Vorgehensweisen oder Checklisten.

Marken und Copyrights

DeviceNet und DeviceNet Safety sind eingetragene Marken der Open DeviceNet Vendors Association (ODVA).

Andere Produkt- und Firmennamen, die in diesem Handbuch erwähnt werden, sind Marken oder eingetragene Marken der jeweiligen Unternehmen.

Inhaltsverzeichnis

Zu diesem Handbuch

Dieses Handbuch beschreibt die Konfiguration des DeviceNet Safety-Systems.

Lesen Sie dieses Handbuch sorgfältig durch, und vergewissern Sie sich, dass Sie die zur Verfügung gestellten Informationen verstehen, bevor Sie versuchen, ein DeviceNet Safety-System zu konfigurieren. Lesen Sie unbedingt sämtliche im folgenden Abschnitt aufgeführten Vorsichtsmaßnahmen durch.

Informationen zu DeviceNet und DeviceNet Safety finden Sie in den nachstehend aufgeführten Handbüchern.

DeviceNet Safety Systemkonfigurations-Handbuch (dieses Handbuch) (Z905)

Dieses Handbuch beschreibt die Konfiguration des DeviceNet Safety-Systems mithilfe des Network Configurators.

NE1A-SCPU01 Bedienerhandbuch für den Sicherheitsnetzwerk-Controller (Z906)

Dieses Handbuch beschreibt die technischen Daten, die Funktionen und die Anwendung des Sicherheitsnetzwerk-Controllers NE1A-SCPU01.

Bedienerhandbuch für Sicherheits-E/A-Module der Serie DST1 (Z904)

Dieses Handbuch beschreibt die technischen Daten, die Funktionen und die Anwendung der E/A-Module der Serie DST1.

DeviceNet-Bedienerhandbuch (W267)

Dieses Handbuch beschreibt den Aufbau und die Verbindungen in einem DeviceNet-Netzwerk. Es enthält detaillierte Informationen zur Installation und den technischen Daten der Kabel, Steckbindungen und anderer im Netzwerk eingesetzter Peripheriegeräte sowie der benötigten Spannungsversorgung. Bevor Sie versuchen, ein DeviceNet-System einzusetzen, müssen Sie dieses Handbuch sorgfältig durchgelesen und die darin enthaltenen Informationen in vollem Umfange verstanden haben.

⚠ VORSICHT
Falls Sie die in diesem Handbuch enthaltenen Informationen nicht durchlesen oder nicht verstehen, kann dies zur Verletzung oder zum Tod von Personen, zu einem Schaden am Produkt bzw. zu einer Fehlfunktion führen. Lesen Sie jeden Abschnitt vollständig durch, und führen Sie die vorgestellten Verfahrensweisen erst durch, wenn Sie sicher sind, dass Sie die im jeweiligen Abschnitt und den damit verbundenen Abschnitten bereitgestellten Informationen verstanden haben.

Lesen Sie dieses Handbuch sorgfältig durch

Bitte lesen Sie dieses Handbuch vor der Verwendung der Produkte sorgfältig durch, und vergewissern Sie sich sicher, dass Sie die darin enthaltenen Informationen verstanden haben. Bei Fragen oder Anmerkungen wenden Sie sich bitte an Ihre OMRON Vertretung.

Gewährleistung und Haftungsbeschränkungen

GEWÄHRLEISTUNG
OMRON gewährleistet ausschließlich, dass die Produkte frei von Material- und Produktionsfehlern sind. Diese Gewährleistung erstreckt sich (falls nicht anders angegeben) auf zwei Jahre ab Kaufdatum bei OMRON. OMRON ÜBERNIMMT KEINERLEI GEWÄHRLEISTUNG ODER ZUSAGE, WEDER EXPLIZIT NOCH IMPLIZIT, BEZÜGLICH DER NICHTVERLETZUNG VON RECHTEN DRITTER, DER MARKTTAUGLICHKEIT ODER DER EIGNUNG DER PRODUKTE FÜR EINEN BESTIMMTEN ZWECK. JEDER KÄUFER ODER BENUTZER ERKENNT AN, DASS DER KÄUFER ODER BENUTZER ALLEINE BESTIMMT HAT, OB DIE JEWEILIGEN PRODUKTE FÜR DEN VORGESEHENEN VERWENDUNGSZWECK GEEIGNET SIND. OMRON SCHLIESST ALLE ÜBRIGEN IMPLIZITEN UND EXPLIZITEN GEWÄHRLEISTUNGEN AUS.

HAFTUNGSBESCHRÄNKUNGEN
OMRON ÜBERNIMMT KEINE VERANTWORTUNG FÜR SPEZIELLE, INDIREKTE ODER FOLGESCHÄDEN, GEWINNAUSFÄLLE ODER KOMMERZIELLE VERLUSTE, DIE IN IRGENDEINER WEISE MIT DEN PRODUKTEN IN ZUSAMMENHANG STEHEN, UNABHÄNGIG DAVON, OB SOLCHE ANSPRÜCHE AUF VERTRÄGEN, GARANTIEN, VERSCHULDUNGS- ODER GEFÄHRDUNGSHAFTUNG BASIEREN. OMRON ist in keinem Fall haftbar für jedwede Ansprüche, die über den jeweiligen Kaufpreis des Produkts hinausgehen, für das der Haftungsanspruch geltend gemacht wird. OMRON ÜBERNIMMT IN KEINEM FALL DIE VERANTWORTUNG FÜR GEWÄHRLEISTUNGS- ODER INSTANDSETZUNGSANSPRÜCHE IM HINBLICK AUF DIE PRODUKTE, SOWEIT DIE UNTERSUCHUNG DURCH OMRON NICHT ERGEBEN HAT, DASS DIE PRODUKTE ORDNUNGSGEMÄSS GEHANDHABT, GELAGERT, INSTALLIERT UND GEWARTET WURDEN UND KEINERLEI BEEINTRÄCHTIGUNG DURCH VERSCHMUTZUNG, MISSBRAUCH, UNSACHGEMÄSSE VERWENDUNG ODER UNSACHGEMÄSSE MODIFIKATION ODER INSTANDSETZUNG AUSGESETZT WAREN.

Anwendungshinweise

EIGNUNG

OMRON übernimmt keinerlei Verantwortung für die Einhaltung der für die konkrete Anwendung oder Kombination der Produkte (Maschinen, Anlagen usw.) geltenden Normen, Standards usw.

Auf Kundenwunsch stellt OMRON geeignete Zertifizierungsunterlagen Dritter zur Verfügung, aus denen Nennwerte und Anwendungsbeschränkungen der jeweiligen Produkte hervorgehen. Diese Informationen allein sind nicht ausreichend für die vollständige Eignungsbestimmung der Produkte in Kombination mit Endprodukten, Maschinen, Systemen oder anderen Anwendungsbereichen.

Es folgen einige Anwendungsbeispiele, denen besondere Beachtung zu schenken ist. Es handelt sich nicht um eine umfassende Liste aller Verwendungsmöglichkeiten der Produkte. Diese Liste ist auch nicht so zu verstehen, dass Produkte für die angegebenen Verwendungsmöglichkeiten geeignet sind.

- Verwendung im Freien, Verwendung mit potenziellen chemischen Verunreinigungen oder elektrischer Beeinflussung oder Bedingungen oder Verwendungen, die nicht in diesem Handbuch beschrieben werden.
- Nukleartechnik, Verbrennungsanlagen, Schienenverkehr, Luftfahrt, Medizintechnik, Spielautomaten, Sicherheitseinrichtungen und andere Anlagen, die speziellen industriellen und/oder behördlichen Anforderungen und Auflagen unterliegen.
- Systeme, Maschinen und Geräte, die eine Gefahr für Leben und Sachgüter darstellen können.

Machen Sie sich bitte mit allen Einschränkungen im Hinblick auf die Verwendung dieser Produkte vertraut, und halten Sie diese ein.

VERWENDEN SIE DAS PRODUKT NIEMALS FÜR ANWENDUNGEN, DIE EINE GEFAHR FÜR LEBEN ODER EIGENTUM DARSTELLEN, OHNE SICHERZUSTELLEN, DASS DAS GESAMTSYSTEM UNTER BERÜCKSICHTIGUNG DER JEWEILIGEN RISIKEN KONZIPIERT UND DAS OMRON PRODUKT HINSICHTLICH DER BEABSICHTIGTEN VERWENDUNG IN DER GESAMTANLAGE BZW. DES GESAMTSYSTEMS ORDNUNGSGEMÄSS EINGESTUFT UND INSTALLIERT WIRD.

PROGRAMMIERBARE PRODUKTE

OMRON übernimmt für die Programmierung eines programmierbaren Produkts durch den Benutzer und alle daraus resultierenden Konsequenzen keine Verantwortung.

Haftungsausschlüsse

ÄNDERUNG DER TECHNISCHEN DATEN

Im Zuge der technischen Weiterentwicklung und aus anderen Gründen können jederzeit Änderungen an den technischen Daten und den verfügbaren Zubehörteilen des Produkts erfolgen.

Üblicherweise ändern wir die Modellnummern, wenn veröffentlichte Nennwerte oder Funktionen geändert oder signifikante Konstruktionsänderungen vorgenommen werden. Manche technischen Daten der Produkte werden möglicherweise ohne Mitteilung geändert. Im Zweifelsfall können auf Anfrage spezielle Modellnummern zugewiesen werden, um für Ihre Anwendung wesentliche technische Daten zu fixieren.
Bei Fragen zu technischen Daten erworbener Produkte können Sie sich jederzeit an den OMRON Vertrieb wenden.

ABMESSUNGEN UND GEWICHT

Die Angaben zu Abmessungen und Gewicht sind Nennwerte, die nicht für Fertigungszwecke bestimmt sind, auch wenn Toleranzen angegeben sind.

LEISTUNGSDATEN

Die in diesem Handbuch genannten Leistungsdaten dienen als Anhaltspunkte zur Beurteilung der Eignung durch den Benutzer und werden nicht garantiert. Die Daten können auf Testbedingungen von OMRON basieren und müssen vom Benutzer auf die tatsächliche Anwendungssituation übertragen werden.
Die tatsächliche Leistung unterliegt der Garantie und Haftungsbeschränkung von OMRON.

FEHLER UND AUSLASSUNGEN

Die in diesem Handbuch enthaltenen Informationen wurden sorgfältig geprüft und sind unserer Ansicht nach korrekt. OMRON übernimmt jedoch keine Verantwortung für evtl. trotz sorgfältiger Durchsicht verbliebene Tipp- oder Schreibfehler oder Auslassungen.

Sicherheitshinweise

1 Zielgruppe

Dieses Handbuch richtet sich an folgende Personen, die sich mit elektrischen Anlagen auskennen müssen (z. B. Elektroingenieure oder -techniker):

- Das für die Einrichtung von Automatisierungs- und Sicherheitssystemen in Produktionsstätten zuständige Personal
- Das für die Konstruktion von Automatisierungs- und Sicherheitssystemen zuständige Personal
- Das für die Verwaltung von Automatisierungs-Systemen zuständige Personal
- Das aufgrund seiner Qualifikation, Autorität und Verantwortlichkeit für die Gewährleistung der Sicherheit in den Produktphasen „Mechanischer Entwurf“, „Installation“, „Betrieb“, „Wartung“ und „Entsorgung“ zuständige Personal.

2 Allgemeine Sicherheitshinweise

Der Benutzer muss das Produkt gemäß den in diesem Handbuch beschriebenen Leistungsspezifikationen betreiben.

Wenden Sie sich vor der Verwendung dieses Produktes an Ihren OMRON-Vertreter, sofern Sie das Produkt unter Bedingungen einsetzen, die nicht im Handbuch aufgeführt sind bzw. wenn Sie das Produkt im Bereich der Nukleartechnik, im Eisenbahnverkehr, in der Luftfahrt, in Fahrzeugen, in Verbrennungssystemen, in medizinischen Geräten, in Spielautomaten, in Sicherheitsausrüstungen oder anderen Systemen, Geräten oder Ausrüstungen verwenden möchten, bei denen bei fehlerhafter Verwendung die Gefahr von Personen- oder Sachschäden besteht.

Achten Sie darauf, dass die Nenn- und Leistungsdaten des Produkts für die jeweiligen Systeme, Maschinen und Anlagen angemessen sind, und statten Sie die Systeme, Maschinen und Anlagen mit redundanten Sicherheitsmechanismen aus.

Dieses Handbuch enthält Informationen zu Programmierung und Betrieb des Produkts. Lesen Sie dieses Handbuch vor Verwendung des Produkts durch, und halten Sie dieses Handbuch während des Betriebs zu Referenzzwecken immer griffbereit.

⚠ VORSICHT

Dieses Handbuch beschreibt die Konfiguration von DeviceNet Safety-Systemen. Berücksichtigen Sie bei der Konstruktion des Systems die folgenden Aspekte, um sicherzustellen, dass die sicherheitsrelevanten Komponenten so konfiguriert werden, dass ein sicherer Betrieb der Systemfunktionen möglich ist.

Risikobeurteilung

Die in diesem Handbuch beschriebene ordnungsgemäße Anwendung der Sicherheitseinrichtungen in Hinsicht auf die Installationsbedingungen und die mechanischen Leistungsdaten und Funktionen muss unbedingt eingehalten werden. Bei der Auswahl und Anwendung von Sicherheitseinrichtungen muss bereits bei der Entwicklung der Anlage oder Installation eine Risikobeurteilung durchgeführt werden, um mögliche gefährdende Faktoren der Anlage oder Installation, in der die Sicherheitseinrichtung eingesetzt wird, zu identifizieren. Die Auswahl geeigneter Sicherheitseinrichtungen muss unter der Anleitung eines hinreichenden Risikobeurteilungssystems erfolgen. Ein unzureichendes Risikobeurteilungssystem kann zur Auswahl ungeeigneter Sicherheitseinrichtungen führen.

- Entsprechende internationale Normen (Auswahl): ISO 14121: Sicherheit von Maschinen – Leitsätze zur Risikobeurteilung

Sicherheitsvorkehrungen

Die Anwendung von Sicherheitseinrichtungen für die Konstruktion von Systemen mit sicherheitsrelevanten Komponenten für Anlagen oder Installationen muss in völliger Übereinstimmung mit internationalen Normen wie den im Folgenden aufgeführten und/oder den Normen der jeweiligen Industrie erfolgen.

- Entsprechende internationale Normen (Auswahl): ISO/DIS 12100: Sicherheit von Maschinen – Grundbegriffe, Allgemeine Gestaltungsleitsätze
  IEC 61508: Sicherheitsnorm für sicherheitsbezogene Systeme (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen)

Die Rolle von Sicherheitseinrichtungen

Sicherheitseinrichtungen sind mit den in den relevanten Normen festgelegten Sicherheitsfunktionen und -mechanismen ausgestattet. Durch geeignete Konstruktion muss jedoch sichergestellt werden, dass diese Funktionen und Mechanismen im Rahmen der Systemkonstruktion mit sicherheitsrelevanten Komponenten ordnungsgemäß operieren. Ein umfassendes Verständnis um das Funktionsprinzip dieser Funktionen und Mechanismen ist für die Konstruktion von Systemen, die diese ordnungsgemäß anwenden, unerlässlich.

- Entsprechende internationale Normen (Auswahl): ISO 14119: Sicherheit von Maschinen – Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen – Leitsätze für Gestaltung und Auswahl

Installation von Sicherheitseinrichtungen

Die Konstruktion und Installation von Systemen mit sicherheitsrelevanten Komponenten für Anlagen und Installationen muss durch entsprechend geschulte Techniker erfolgen.

- Entsprechende internationale Normen (Auswahl): ISO/DIS 12100: Sicherheit von Maschinen – Grundbegriffe, Allgemeine Gestaltungsleitsätze
  IEC 61508: Sicherheitsnorm für sicherheitsbezogene Systeme (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen)

Übereinstimmung mit Gesetzen und Richtlinien

Die Sicherheitseinrichtungen entsprechen den relevanten Richtlinien und Normen, jedoch muss sichergestellt werden, dass sie in Übereinstimmung mit den für die jeweilige Anlage oder Installation geltenden lokalen Richtlinien und Normen eingesetzt werden.

- Entsprechende internationale Normen (Auswahl): EN 60204: Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen

Beachtung der Anwendungshinweise

Beim konkreten Einsatz der ausgewählten Sicherheitseinrichtungen müssen die in diesem Handbuch und in dem der Sicherheitseinrichtung beiliegenden Bedienerhandbuch aufgeführten technischen Daten und Vorsichtsmaßnahmen beachtet werden. Der Einsatz der Produkte auf eine im Widerspruch zu diesen technischen Daten und Vorsichtsmaßnahmen stehende Art und Weise kann aufgrund unzureichender Betriebsfunktionen der sicherheitsrelevanten Komponenten zu unerwarteten Ausfällen der Anlagen und Geräte und zu entsprechenden aus solchen Ausfällen resultierenden Schäden führen.

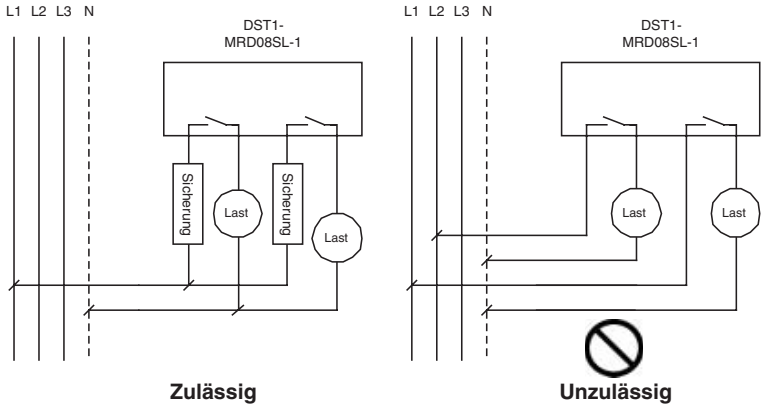
Verlagerung oder Weiterveräußerung von Geräten und Anlagen

Bei der Verlagerung oder Weiterveräußerung von Geräten und Anlagen sind die entsprechenden Dokumentationen wie beispielsweise dieses Handbuch ebenfalls an den Empfänger weiterzugeben, um diesem den ordnungsgemäßen Betrieb des Systems zu ermöglichen.

- Entsprechende internationale Normen (Auswahl): ISO/DIS 12100: Sicherheit von Maschinen – Grundbegriffe, Allgemeine Gestaltungsleitsätze IEC 61508: Sicherheitsnorm für sicherheitsbezogene Systeme (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen)

3 Sicherheitsvorkehrungen

⚠ VORSICHT	
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen die Testausgänge eines Produkts nicht als Sicherheitsausgänge benutzt werden.	⊘
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen DeviceNet-Standard-E/A-Daten oder Daten expliziter Meldungen nicht als Sicherheitssignale verwendet werden.	⊘
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen die Anzeigen eines Produkts nicht für Sicherheitsfunktionen benutzt werden.	⊘
Beim Ausfall von Sicherheits- oder Testausgängen besteht die Gefahr von schweren Verletzungen. Es dürfen keine Lasten an die Sicherheits- oder Testausgänge angeschlossen werden, die den Nennwert übersteigen.	⊘
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen die Ausgangsleitungen und die 24-VDC-Spannungsversorgungsleitungen so geführt werden, dass diese einander nicht berühren können, um zu verhindern, dass eine Last aufgrund eines Kurzschlusses zwischen einer Ausgangsleitung und einer 24 VDC führenden Leitung eingeschaltet wird.	❗
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, muss der 0-V-Ausgang der externen Spannungsversorgung geerdet werden, um zu verhindern, dass ein Ausgang aufgrund eines Masseschlusses in einem Sicherheits- oder Testausgang eingeschaltet wird.	❗
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, dürfen die Relaisausgänge des Sicherheits-E/A-Moduls DST1-MRD08SL-1 nur mit einer Phase beschaltet werden.	❗



Zulässig **Unzulässig**

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, muss jede Ausgangsklemme des Sicherheits-E/A-Moduls DST1-MRD08SL-1 mit einer 3,15-A-Sicherung (oder schwächer) abgesichert werden, um ein Verschweißen der Kontakte der Sicherheitsausgänge zu verhindern. Informieren Sie sich beim Sicherungshersteller, ob die von Ihnen getroffene Wahl für die angeschlossene Last geeignet ist.	❗
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen alte Konfigurationsdaten vor dem Anschluss eines Geräts an das Netzwerk gelöscht werden.	❗
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen vor dem Anschluss eines Geräts an das Netzwerk die Knotenadresse und die Baudrate konfiguriert werden.	❗
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen vor Inbetriebnahme des Systems geeignete Tests durchgeführt werden, um die Korrektheit der Konfigurationsdaten und der Funktionen aller Geräte sicherzustellen.	❗
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, muss beim Austausch von Geräten darauf geachtet werden, dass das Austauschgerät ordnungsgemäß konfiguriert ist und einwandfrei funktioniert.	❗
Beim Ausfall der erforderlichen Sicherheitsfunktionen besteht die Gefahr von schweren Verletzungen. Bei der Auswahl von Komponenten und Geräten müssen die in der folgenden Tabelle aufgeführten Anforderungen Berücksichtigung finden.	❗

Steuerungsgerät	Anforderungen
NOT-AUS-Taster	Verwenden Sie zugelassene Schaltgeräte mit Zwangsöffnungsmechanismus gemäß IEC/EN 60947-5-1.
Verriegelungs- oder Positionsschalter für Schutztüren	Verwenden Sie zugelassene Schaltgeräte mit Zwangsöffnungsmechanismus gemäß IEC/EN 60947-5-1, die Mikrolasten von 4 mA bei 24 VDC schalten können.
Sicherheitssensoren	Verwenden Sie zugelassene Schaltgeräte, die die Anforderungen der einschlägigen Produktstandards, Vorschriften und Gesetze im entsprechenden Land erfüllen.
Sicherheitsrelais mit zwangsgeführten Kontakten	Verwenden Sie zugelassene Schaltgeräte mit zwangsgeführten Kontakten, die EN 50205 entsprechen. Zu Rückführzwecken müssen Schaltgeräte mit Kontakten verwendet werden, die Mikrolasten von 4 mA bei 24 V DC schalten können.
Schütze	Verwenden Sie Schütze mit zwangsgeführten Kontakten, und überwachen Sie den Hilfsöffnerkontakt, um Ausfälle von Schützen erkennen zu können. Zur Rückführzwecken müssen Schaltgeräte mit Kontakten verwendet werden, die Mikrolasten von 4 mA bei 24 VDC schalten können.
Andere Geräte	Beurteilen Sie, ob die verwendeten Geräte den Anforderungen der Steuerungskategorie entsprechen.

4 Hinweise zur sicheren Verwendung

Behandlung

Lassen Sie die Geräte nicht fallen, und setzen Sie sie keinen starken Stößen oder Vibrationen aus. Andernfalls besteht die Gefahr von Fehlfunktionen.

Installation und Lagerung

Lagern oder installieren Sie die Produkte nicht an den folgenden Orten:

- Orte, an denen die Produkte direkter Sonneneinstrahlung ausgesetzt sind.
- Orte, an denen Temperaturen oder Luftfeuchtigkeit außerhalb der in den technischen Daten angegebenen Bereiche herrschen.
- Orte, die starken Temperaturschwankungen und damit Kondensation ausgesetzt sind.
- Orte, an denen die Produkte korrosiven oder entzündlichen Gasen ausgesetzt sind.
- Orte, die dem Einfluss von Stäuben (besonders Eisenstaub) oder Salzen ausgesetzt sind.
- Orte, an denen die Produkte dem Einfluss von Wasser, Öl oder Chemikalien ausgesetzt sind.
- Orte, an denen Stöße oder Vibrationen außerhalb der in den technischen Daten angegebenen Bereiche auftreten können.

Ergreifen Sie bei der Installation von Systemen an folgenden Orten angemessene und geeignete Maßnahmen. Unangemessene oder unzureichende Maßnahmen können zu Fehlfunktionen führen.

- Orte mit statischer Aufladung und anderen Störungen.
- Orte, an denen starke elektromagnetische Felder auftreten.
- Orte, die dem Einfluss von Radioaktivität ausgesetzt sein könnten.
- Orte in der Nähe von Spannungsversorgungen.

Montage

Vor der Installation und Montage sind die in den Bedienerhandbüchern der jeweiligen Produkte aufgeführten Hinweise und Anregungen zum Betrieb zu konsultieren.

Verdrahtung

- Zum Anschließen externer E/A-Geräte an die Produkte müssen die folgenden Drähte/Litzen eingesetzt werden:

Volldraht	0,2 bis 2,5 mm² (AWG 24 bis AWG 12)
Litze	0,34 bis 2,5 mm² (AWG 22 bis AWG 16) Litzen müssen vor Verwendung mit Adernendhülsen mit isolierendem Plastikkragen nach DIN 46228-4 versehen werden.

- Vor allen Verdrahtungsarbeiten muss die Spannungsversorgung ausgeschaltet werden. Andernfalls kann es zum unerwarteten Anlaufen der an die Produkte angeschlossenen externen Geräte kommen.
- Legen Sie an die Eingänge der Produkte nur die spezifizierten Spannungen an. Das Anlegen einer falschen Gleichspannung oder einer beliebigen Wechselspannung kann zu einer Beeinträchtigung der Sicherheitsfunktionen, einer Beschädigung der Produkte und/oder zu Bränden führen.
- Halten Sie Leitungen für Kommunikations- und E/A-Signale getrennt von Strom- oder Hochspannungsleitungen.
- Achten Sie beim Anbringen von Steckverbindern an den Anschlüssen der Produkte darauf, Ihre Finger nicht einzuklemmen.
- Ziehen Sie den DeviceNet-Stecker mit einem Drehmoment von 0,25 bis 0,3 Nm fest.
- Unsachgemäße Verdrahtung kann zu einer Beeinträchtigung der Sicherheitsfunktionen führen. Führen Sie alle Verdrahtungsarbeiten ordnungsgemäß durch, und kontrollieren Sie vor der Verwendung der Produkte die Funktion der Verdrahtung.
- Entfernen Sie nach Abschluss der Verdrahtungsarbeiten die Staubschutzfolie, um eine ordnungsgemäße Wärmeableitung zu gewährleisten.

Auswahl der Spannungsversorgung

Verwenden Sie eine Gleichspannungsversorgung, die die nachstehenden Anforderungen erfüllt:

- Die Gleichspannungsversorgung verwendet eine Schutzisolierung oder verstärkte Isolierung zwischen Primär- und Sekundärkreis.
- Die Gleichspannungsversorgung muss die Anforderungen für Stromkreise der Klasse 2 oder Stromkreise mit begrenzten Spannungs-/Stromwerten gemäß UL 508 erfüllen.
- Bei einem Ausfall der Versorgungsspannung muss die Ausgangsspannung für mindestens 20 ms gehalten werden.

Periodische Inspektion und Wartung

- Vor dem Austausch von Produkten muss die Versorgungsspannung ausgeschaltet werden. Andernfalls kann es zum unerwarteten Anlaufen der an die Produkte angeschlossenen externen Geräte kommen.
- Die Produkte dürfen nicht zerlegt, repariert oder modifiziert werden. Bei Widerhandlung besteht die Gefahr einer Beeinträchtigung der Sicherheitsfunktionen.

Entsorgung

- Wenn Sie die Produkte für die Entsorgung zerlegen müssen, gehen Sie mit entsprechender Vorsicht vor, um Verletzungen zu vermeiden.

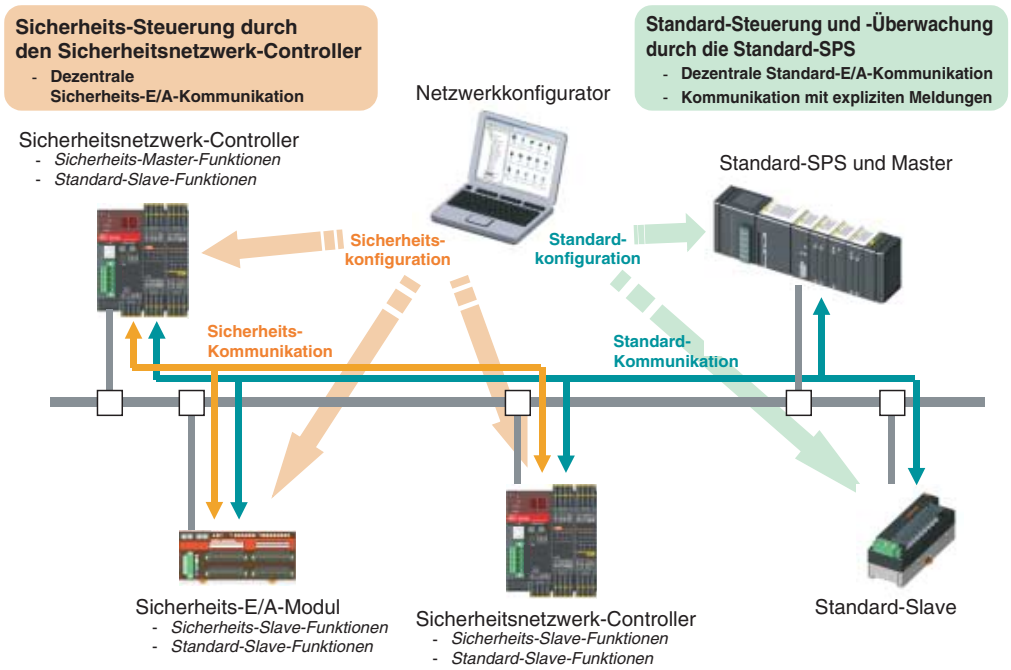
1-1 DeviceNet Safety Systemübersicht

1-1-1 DeviceNet Safety

DeviceNet ist ein der offenes herstellerunabhängiges Multi-Bit-Netzwerk, das die Steuerungen in der Maschine miteinander verknüpft. Das DeviceNet Safety-Netzwerk erweitert das konventionelle Standard-DeviceNet-Kommunikationsprotokoll um Sicherheitsfunktionen. Das DeviceNet Safety-Konzept wurde durch eine unabhängige Organisation (TÜV Rheinland) geprüft und anerkannt.

Ebenso wie bei DeviceNet können auch an DeviceNet Safety-Netzwerke DeviceNet Safety-Geräte von Drittanbietern angeschlossen werden. Darüber hinaus können DeviceNet- und DeviceNet Safety-Geräte kombiniert und an ein und dasselbe Netzwerk angeschlossen werden.

Die Kombination von DeviceNet Safety-Produkten ermöglicht den Aufbau einer Sicherheitssteuerung/eines Netzwerksystems, die/das den Anforderungen für die unter IEC 61508 (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen) definierte Sicherheitsintegritätsstufe 3 und den Anforderungen der Steuerungskategorie 4 gemäß EN 954-1 entsprechen.



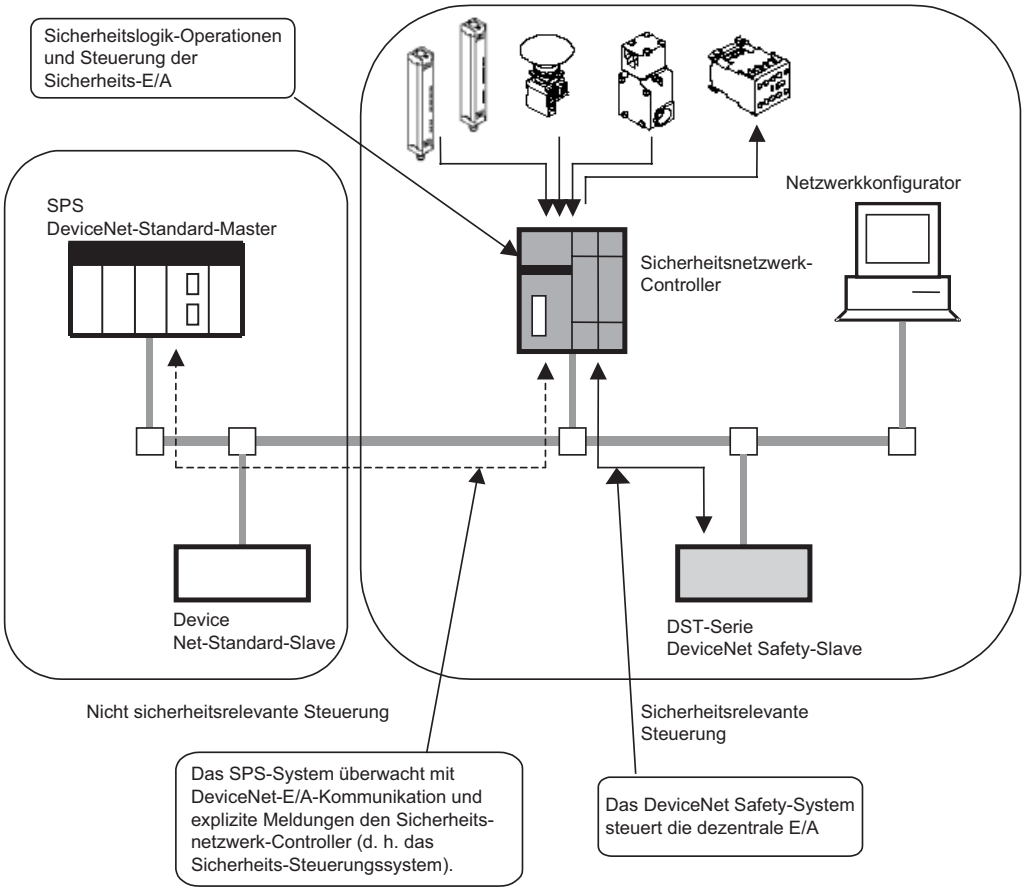
1-2 Übersicht über den Sicherheitsnetzwerk-Controller

1-2-1 Sicherheitsnetzwerk-Controller NE1A

Der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) stellt verschiedene Funktionen wie Sicherheitslogik-Operationen, Sicherheits-E/A-Steuerung und ein DeviceNet Safety-Protokoll bereit. Der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) ermöglicht den Aufbau einer Sicherheitssteuerung/eines Netzwerksystems, die/das den Anforderungen für die unter IEC 61508 (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen) definierte Sicherheitsintegritätsstufe 3 und den Anforderungen der Sicherheitskategorie 4 gemäß EN 954-1 entsprechen.

In dem unten dargestellten Beispielsystem wird das mit dem Sicherheitsnetzwerk-Controller NE1A implementierte Sicherheits-Steuerungssystem und das mit der Standard-SPS implementierte Überwachungssystem in demselben Netzwerk realisiert.

- Als Sicherheitslogik-Controller führt der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) Sicherheitslogik-Operationen aus und steuert die lokale E/A.
- Als Sicherheits-Master steuert der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) die dezentrale E/A von Sicherheits-Slaves.
- Als Standard-Slave kommuniziert der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) mit dem Standard-Master.



1-2-2 Funktionsmerkmale des Sicherheitsnetzwerk-Controllers

Sicherheitslogik-Operationen

Ergänzend zu den grundlegenden Logik-Funktionen wie AND und OR unterstützt der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) Anwendungs-Funktionsblöcke wie die Überwachung von NOT-AUS-Tastern und Schutztüren, die die Realisierung der verschiedensten Sicherheitsanwendungen ermöglichen.

Lokale Sicherheits-E/A

- Insgesamt werden 24 lokale Sicherheits-E/A-Punkte unterstützt: 16 Eingänge und 8 Ausgänge.
- Fehler in der externen Verdrahtung können aufgedeckt werden.
- Paare zusammengehöriger lokaler Eingänge können im Zweikanal-Modus betrieben werden. In diesem Modus kann der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) die Eingangsdaten-Muster und die Zeitabweichungen zwischen den Eingangssignalen analysieren.
- Paare zusammengehöriger lokaler Ausgänge können im Zweikanal-Modus betrieben werden. In diesem Modus kann der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) die Ausgangsdaten-Muster analysieren.

DeviceNet Safety-Kommunikation

- Als Sicherheits-Master kann der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) Sicherheits-Kommunikation über bis zu 16 Verbindungen mit bis zu 16 Bytes je Verbindung durchführen.
- Als Sicherheits-Slave kann der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) Sicherheits-Kommunikation über bis zu 16 Verbindungen mit bis zu 16 Bytes je Verbindung durchführen.

DeviceNet-Kommunikation

Als Standard-Slave kann der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) Standard-Kommunikation mit einem Standard-Master über bis zu zwei Verbindungen mit bis zu 16 Bytes je Verbindung durchführen.

Standalone-Controller-Modus

Der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) kann nach Deaktivierung der DeviceNet-Kommunikation auch als Standalone-Controller eingesetzt werden.

Konfiguration mit einem grafischen Tool

- Die Netzwerkkonfiguration und die Logik-Programmierung erfolgen mithilfe eines grafischen Tools. Dieses ermöglicht eine problemlose Konfiguration und Programmierung.
- Ein Logikeditor kann vom Netzwerkkonfigurator aus aktiviert werden.
- Konfigurationsdaten können herauf- und heruntergeladen werden, und Geräte können online über DeviceNet, USB oder die periphere Schnittstelle einer OMRON-SPS überwacht werden.

Systemstart und Unterstützung für das Wiederaufsetzen nach Fehlern (Error Recovery)

- Das Fehlerprotokoll und die Anzeigen an der Front des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) vereinfachen die Fehlersuche.
- Die internen Statusinformationen des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) können von einer Standard-SPS aus überwacht werden, indem diese Informationen im Standard-Master zugeteilt werden. Auf die gleiche Weise können diese Informationen von einer Sicherheits-SPS aus überwacht werden, indem diese Informationen im Sicherheits-Master zugeteilt werden.

Zugangsbeschränkung durch Kennwort

- Die Konfigurationsdaten des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) sind durch ein Kennwort geschützt.
- Mithilfe des Netzwerkkonfigurators erstellte Netzwerkkonfigurationsdateien (Projektdateien) sind ebenfalls durch ein Kennwort geschützt.

1-2-3 Standardmodelle

Produkt-bezeichnung	Beschreibung	Anzahl der E/A-Punkte		
		Sicherheits-eingänge	Testausgänge	Sicherheits-ausgänge
NE1A-SCPU01	Sicherheitsnetzwerk-Controller (NE1A-SCPU01)	16	4	8

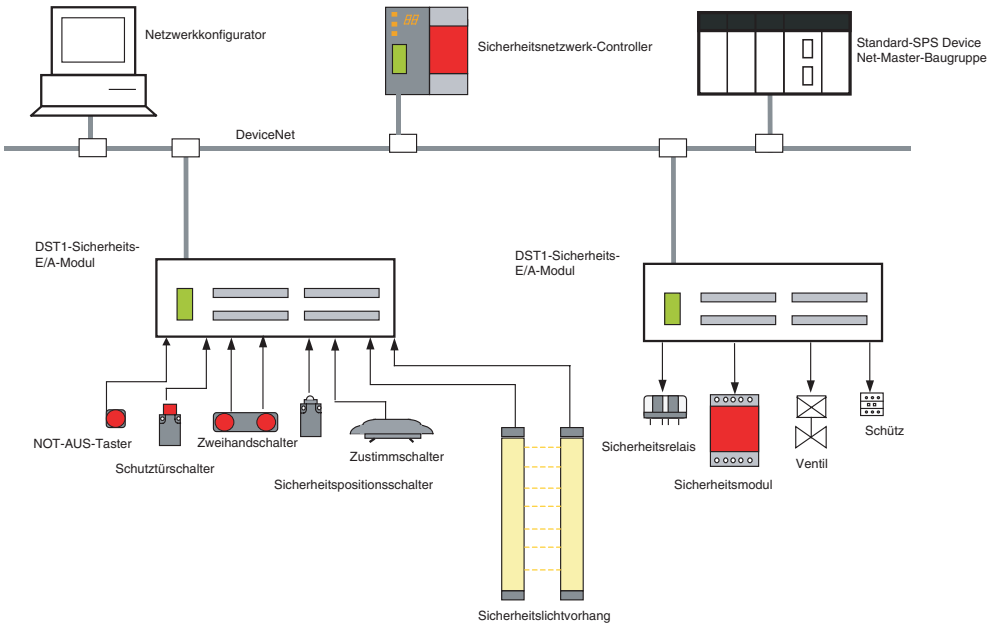
1-3 Übersicht über das Sicherheits-E/A-Modul

1-3-1 DST1-Sicherheits-E/A-Module

Die DST1-Sicherheits-E/A-Module unterstützen das DeviceNet Safety-Protokoll und steuern verschiedene Funktionen für ein Sicherheitssystem bei. Die Sicherheits-E/A-Module ermöglichen den Aufbau einer Sicherheitssteuerung/eines Netzwerksystems, die/das den Anforderungen für die unter IEC 61508 (Funktionale Sicherheit von elektrischen/elektronischen/programmierbaren Sicherheitssystemen) definierte Sicherheitsintegritätsstufe 3 und den Anforderungen der Steuerungskategorie 4 gemäß EN 954-1 entsprechen.

Die E/A-Daten der DST1-Sicherheits-E/A-Module werden über eine dem DeviceNet Safety-Protokoll entsprechende Sicherheits-E/A-Kommunikation übertragen, und die Datenverarbeitung erfolgt im Sicherheitsnetzwerk-Controller (NE1A-SCPU01).

Außerdem kann der Status der Sicherheits-E/A-Daten in einem vorhandenen DeviceNet-Netzwerk mittels Standard-E/A-Kommunikation oder Kommunikation durch explizite Meldungen mit einer Standard-SPS überwacht werden.



1-3-2 Funktionsmerkmale der Sicherheits-E/A-Module

Sicherheitseingänge

- Die Sicherheitseingänge ermöglichen den Anschluss von Halbleiterausgängen (z. B. Lichtgitter) und Kontaktausgängen (z. B. NOT-AUS-Taster) gleichermaßen.
- Fehler in der externen Verdrahtung können aufgedeckt werden.
- Eingangsverzögerungen (Einschalt- und Ausschaltverzögerungen) können eingerichtet werden.
- Paare zusammengehöriger lokaler Eingänge können im Zweikanal-Modus betrieben werden, um den Anforderungen der Kategorie 4 zu genügen.
  In diesem Modus können die Eingangsdaten-Muster und die Zeitabweichungen zwischen den Eingangssignalen analysiert werden.

Testausgänge

- Vier unabhängige Testausgänge stehen zur Verfügung.
- Der Ausfall einer externen Signalleuchte kann aufgedeckt werden. (Kann nur für die Klemme T3 eingestellt werden.)
- Die Testausgänge können als Spannungsversorgung für Geräte mit geringer Stromaufnahme (z. B. Sensoren) genutzt werden.
- Testausgänge können als Standardausgänge für Überwachungsausgänge genutzt werden.

Sicherheitsausgänge

- **Halbleiterausgänge**
  - Paare zusammengehöriger lokaler Ausgänge können im Zweikanal-Modus betrieben werden, um den Anforderungen der Kategorie 4 zu genügen.
    In diesem Modus können die Ausgangsdaten-Muster analysiert werden.
  - Der Nennausgangsstrom beträgt max. 0,5 A je Ausgang.

- **Relaisausgänge**
  - Paare zusammengehöriger Ausgangsklemmen können im Zweikanal-Modus betrieben werden, um den Anforderungen der Kategorie 4 zu genügen.
    In diesem Modus können die Ausgangsdaten-Muster analysiert werden.
  - Der Nennausgangsstrom beträgt max. 2 A je Ausgangsklemme.
  - Die Sicherheitsrelais können ausgetauscht werden.

DeviceNet Safety-Kommunikation

Als Sicherheits-Slave kann das Sicherheits-E/A-Modul Sicherheits-Kommunikation über bis zu vier Verbindungen durchführen.

DeviceNet-Kommunikation

Als Standard-Slave kann das Sicherheits-E/A-Modul Standard-E/A-Kommunikation mit einem Standard-Master über bis zu zwei Verbindungen durchführen.

Systemstart und Unterstützung für das Wiederaufsetzen nach Fehlern (Error Recovery)

- Das Fehlerprotokoll und die Anzeigen an der Front des Sicherheits-E/A-Moduls vereinfachen die Fehlersuche.
- Die internen Statusinformationen des Sicherheits-E/A-Moduls können von einer Standard-SPS aus überwacht werden, indem diese Informationen im Standard-Master alloziiert werden. Auf die gleiche Weise können diese Informationen von einer Sicherheits-SPS aus überwacht werden, indem diese Informationen im Sicherheits-Master zugeteilt werden.

Zugangsbeschränkung durch Kennwort

Die Konfigurationsdaten des Sicherheits-E/A-Moduls sind durch ein Kennwort geschützt.

E/A-Steckverbinder

- Die E/A-Steckverbinder können vom Sicherheits-E/A-Modul gelöst und wieder angeschlossen werden.
- Die E/A-Steckverbinder sind so konstruiert, dass sie nicht falsch angeschlossen werden können.

Zugfederklemmenverdrahtung

Die Verdrahtung erfolgt ohne Anziehen von Schrauben.

Wartungsfunktionen

Die Sicherheits-E/A-Module verfügen über Wartungsfunktionen wie Schalthäufigkeitszähler und Überwachung der kumulativen Betriebsdauer und der Betriebszeit.

1-3-3 Standardmodelle

Die DST1-Serie umfasst die folgenden drei Typen von Sicherheits-E/A-Modulen: Sicherheits-Eingangsmodul, Sicherheits-E/A-Modul mit Halbleiterausgängen und Sicherheits-E/A-Modul mit Relaisausgängen.

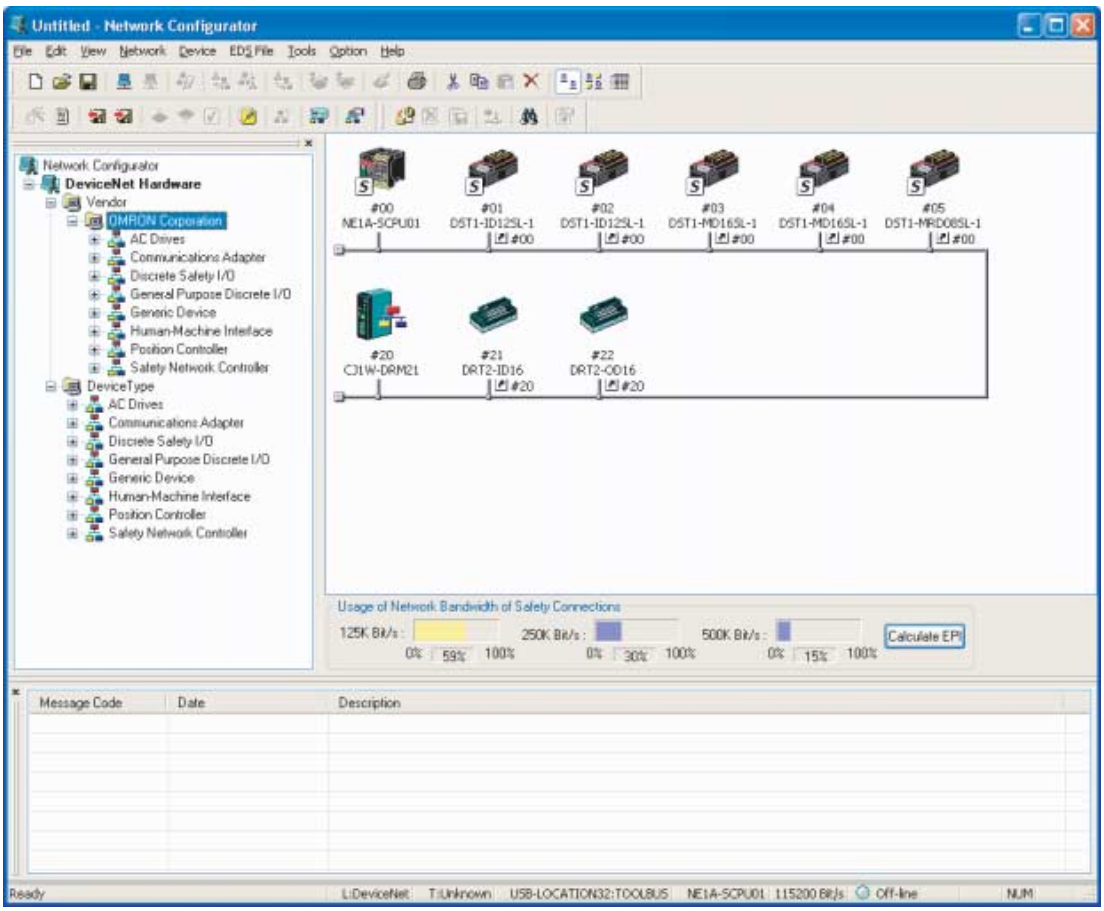
Produktbezeichnung	Beschreibung	Anzahl der E/A-Punkte			
		Sicherheitseingänge	Testausgänge	Sicherheitsausgänge	
				Halbleiterausgänge	Relaisausgänge
DST1-ID12SL-1	Sicherheits-Eingangsmodul	12	4	-	-
DST1-MD16SL-1	Sicherheits-E/A-Modul (Halbleiterausgänge)	8	4	8	-
DST1-MRD08SL-1	Sicherheits-E/A-Modul (Relaisausgänge)	4	4	-	4

1-4 Übersicht über den Netzwerkkonfigurator

1-4-1 Netzwerkkonfigurator

Bei dem Netzwerkkonfigurator (WS02-CFSC1-E) handelt es sich um eine Support Software mit grafischer Oberfläche für das Konfigurieren, Einstellen und Verwalten von DeviceNet Safety-Netzwerken.

Der Netzwerkkonfigurator kann verwendet werden, um ein virtuelles DeviceNet Safety-Netzwerk zu konfigurieren (im Netzwerkkonfigurationsfenster) und die Konfiguration und Parameter der einzelnen Sicherheits- und Standardgeräte zu überwachen.



1-4-2 Funktionsmerkmale des Netzwerkkonfigurators

Verwendbar für DeviceNet Standard- und DeviceNet Safety-Netzwerke

Der Netzwerkkonfigurator kann für die Konfiguration und Überwachung von DeviceNet Safety-Geräten und vorhandenen Standard-DeviceNet-Geräten gleichermaßen eingesetzt werden. Der Netzwerkkonfigurator unterstützt somit die verschiedensten Systemkonfigurationen: Standardsysteme, Sicherheitssysteme und Mischsysteme mit Standard- und Sicherheitsgeräten.

Programmierung des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01)

Der Netzwerkkonfigurator ist mit einem Programmier-Tool für die Sicherheitslogik-Programmierung des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) ausgestattet. DeviceNet Safety-Anwendungen können mit dem Netzwerkkonfigurator unabhängig erstellt werden.

Aufwärtskompatibilität mit dem DeviceNet-Konfigurator

Alle Funktionen des DeviceNet-Konfigurators werden unterstützt. Außerdem können alle mithilfe des DeviceNet-Konfigurators erstellten Dateien ohne Modifizierung verwendet werden.

1-4-3 Systemvoraussetzungen

Für die Verwendung des Netzwerkkonfigurators müssen folgende Systemanforderungen erfüllt sein.

Komponente	Anforderungen
Computer	IBM-PC mit mindestens 300 MHz CPU-Takt 128 MB 40 MB verfügbarer Festplattenspeicher SVGA-Anzeige CD-ROM-Laufwerk
Betriebs-system	Windows® 2000 oder Windows® XP
Serielle Schnittstelle	Es wird eine der folgenden seriellen Schnittstellen benötigt: • USB-Schnittstelle: Für eine Verbindung über die USB-Schnittstelle (USB 1.1) des Sicherheitsnetzwerk-Controllers NE1A-SCPU01. • DeviceNet-Schnittstellenkarte (3G8E2-DRM21-V1): Für eine DeviceNet-Verbindung

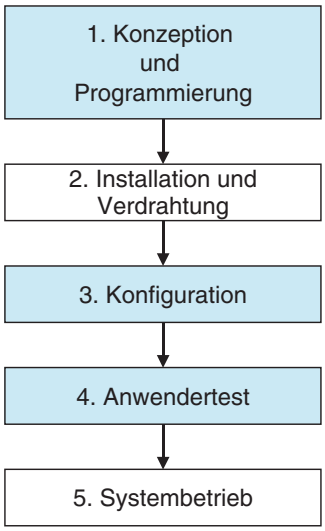
1-4-4 Standardmodelle

Produkt-bezeichnung	Beschreibung	Komponente	Kompatible Computer	Betriebssystem
WS02-CFSC1-E	Netzwerk-konfigurator	Installationsdaten-träger (CD-ROM)	IBM-PC	Windows® 2000 oder Windows® XP

1-5 Prinzipielle Vorgehensweise bei der Implementierung eines DeviceNet Safety-Netzwerks

Dieses Handbuch stellt die grundlegenden Schritte für die Implementierung und Inbetriebnahme eines Sicherheitssystems vor. Dabei wird den folgenden Schritten besondere Aufmerksamkeit gewidmet:

– Konzeption und Programmierung
– Konfiguration
– Test



1-5-1 Konzeption und Programmierung

In diesem Schritt wird ein optimales Sicherheitssystem bestimmt. Gehen Sie dazu im Einzelnen wie folgt vor:

(1) Wählen Sie basierend auf den geforderten Leistungsdaten des Sicherheitssystems die Sicherheitsgeräte aus, ordnen Sie diese an, und bestimmen Sie die den einzelnen Geräten zuzuweisenden Sicherheitsfunktionen.

(2) Konfigurieren Sie das Netzwerk im Netzwerkkonfigurator als virtuelles Netzwerk.
- Registrieren Sie alle Geräte. Handelt es sich bei dem Sicherheitssystem um ein gemischtes System mit Standard- und Sicherheitsgeräten, müssen sowohl die Sicherheitsgeräte als auch die Standardgeräte registriert werden.
- Stellen Sie die Parameter aller Geräte ein.
- Überprüfen Sie, welcher Prozentsatz der Netzwerkbandbreite verwendet wird, und unterziehen Sie die Parameter einer kritischen Prüfung.
- Erstellen Sie das Programm für den Sicherheitsnetzwerk-Controller (NE1A-SCPU01).
- Verifizieren Sie die System-Reaktionszeit aller Sicherheitsketten.

Die Auslastung der Netzwerkbandbreite und die System-Reaktionszeit werden durch verschiedene Faktoren (z. B. die Netzwerkkonfiguration, die Parametereinstellungen des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) und der Sicherheits-E/A-Module sowie das Programm des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01)) beeinflusst. Wiederholen Sie daher die obigen Schritte, bis Sie zu einer Systemkonfiguration gelangt sind, die den an das System gestellten Anforderungen genügt.

Anweisungen zur Verwendung des Netzwerkkonfigurators finden Sie in den folgenden Abschnitten:

- Registrierung von Geräten
  - Siehe *2-4 Erstellen eines virtuellen Netzwerks* (Seite 34).
- Bearbeiten von Geräteparametern
  - Siehe *2-7 Geräteparameter und -eigenschaften* (Seite 41).
  - Siehe *Kapitel 4: Bearbeiten der Parameter von Sicherheits-E/A-Modulen* (Seite 69).
  - Siehe *Kapitel 5: Bearbeiten der Parameter des Sicherheitsnetzwerk-Controllers* (Seite 79).
- Überprüfen der Auslastung der Netzwerkbandbreite
  - Siehe *3-2 Überprüfung der benötigten Netzwerkbandbreite* (Seite 59).
- Berechnung der Reaktionszeit
  - Siehe *3-3 Berechnung und Überprüfung der maximalen Reaktionszeit* (Seite 63).

WICHTIG: Weisen Sie jedem Sicherheitsnetzwerk oder Sicherheitssubnetzwerk eine eindeutige Sicherheitsnetzwerknummer zu.

1-5-2 Installation und Verdrahtung

In diesem Schritt erfolgt die Installation und Verdrahtung der einzelnen Geräte. Gehen Sie dazu wie folgt vor:

- Installieren Sie alle Geräte, und stellen Sie die Knotenadressen und Baudraten ein.
- Schließen Sie die E/A-Geräte an.
- Schließen Sie die Spannungsversorgungen an.
- Verdrahten Sie das DeviceNet.

- Verdrahten Sie die USB-Leitung.

Details zu Installation und Verdrahtung finden Sie in den folgenden Handbüchern:

Arbeitsschritt	Titel des Handbuchs	Kat.- Nr.
DeviceNet-Installation	DeviceNet-Bedienerhandbuch	W267
Installation des Sicherheitsnetzwerk-Controllers NE1A-SCPU01	NE1A-SCPU01 Bedienerhandbuch für den Sicherheitsnetzwerk-Controller	Z906
Installation der DeviceNet-Sicherheits-E/A-Module	Bedienerhandbuch für DeviceNet-Sicherheits-E/A-Module	Z904
Installation der sonstigen Geräte	Bedienerhandbuch des jeweiligen Geräts	?

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen alte Konfigurationsdaten vor dem Anschluss eines Geräts an das Netzwerk gelöscht werden.

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen vor dem Anschluss eines Geräts an das Netzwerk die Knotenadresse und die Baudrate eingestellt werden.

1-5-3 Konfiguration

In diesem Schritt werden die vom Netzwerkkonfigurator für die einzelnen Geräte erstellten Parameter in das jeweilige Gerät heruntergeladen, um die Betriebsbereitschaft des Systems herzustellen.

Führen Sie mit dem Netzwerkkonfigurator die folgenden Schritte durch:

(1) Herunterladen
Die im virtuellen Netzwerk des Netzwerkkonfigurators eingestellten Parameter werden in die konkreten Geräte heruntergeladen und in diesen gespeichert.

(2) Überprüfung
Überprüfen Sie die Einstellungen der Sicherheitsgeräte.
Kontrollieren Sie, ob die in den einzelnen Geräten gespeicherten Parameter und Sicherheitssignaturen korrekt sind.

Anweisungen zur Verwendung des Netzwerkkonfigurators finden Sie in den folgenden Abschnitten:

- Herunterladen
  - Siehe *2-7 Geräteparameter und -eigenschaften* (Seite 41).
- Überprüfung
  - Siehe *2-8 Verifizierung der Parameter* (Seite 45).

WICHTIG:
- Überprüfen Sie nach dem Herunterladen der Geräteparameter die Parameter, um sicherzustellen, dass die in den einzelnen Geräten gespeicherten Parameter und Sicherheitssignaturen korrekt sind.
- Wenn Sie für die Einstellung „Open Type“ der Sicherheitsverbindung die Einstellung „Open Only“ verwenden, müssen Sie überprüfen, dass der Sicherheits-Master und der Sicherheits-Slave ordnungsgemäß konfiguriert sind.

1-5-4 Anwendertest

In diesem Schritt überprüft der Anwender selbst den Programmbetrieb und führt Funktionstests durch.
Der Anwendertest muss stets durchgeführt werden, da die Überprüfung des Systembetriebs in der Verantwortlichkeit des Anwenders liegt. Beim Anwendertest werden die Korrektheit aller in die einzelnen Sicherheitsgeräte heruntergeladenen Parameter sowie die Sicherheitssignaturen der einzelnen Geräte überprüft. Aktivieren Sie nach Abschluss des Anwendertests den Konfigurationsschutz. Der aktivierte Konfigurationsschutz zeigt an, dass alle Parameter und Sicherheitssignaturen korrekt sind.

Details zur Aktivierung des Konfigurationsschutzes mithilfe des Netzwerkkonfigurators finden Sie unter *2-9 Konfigurationsschutz* (Seite 48).

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen vor Inbetriebnahme des Systems geeignete Tests durchgeführt werden, um die Korrektheit der Konfigurationsdaten aller Geräte und deren ordnungsgemäße Funktion sicherzustellen.

WICHTIG:
- Nach der Konfiguration aller Geräte muss ein Anwendertest durchgeführt werden, um die Konfigurationsdaten aller Geräte und deren ordnungsgemäße Funktion zu überprüfen. Weiterhin werden im Rahmen des Anwendertests die Sicherheitssignaturen der einzelnen Geräte überprüft.
- Nach erfolgreichem Abschluss des Anwendertests muss der Konfigurationsschutz aktiviert werden.

Kapitel 2: Grundfunktionen des Netzwerkkonfigurators

2-1 Aufruf und Hauptfenster des Netzwerkkonfigurators

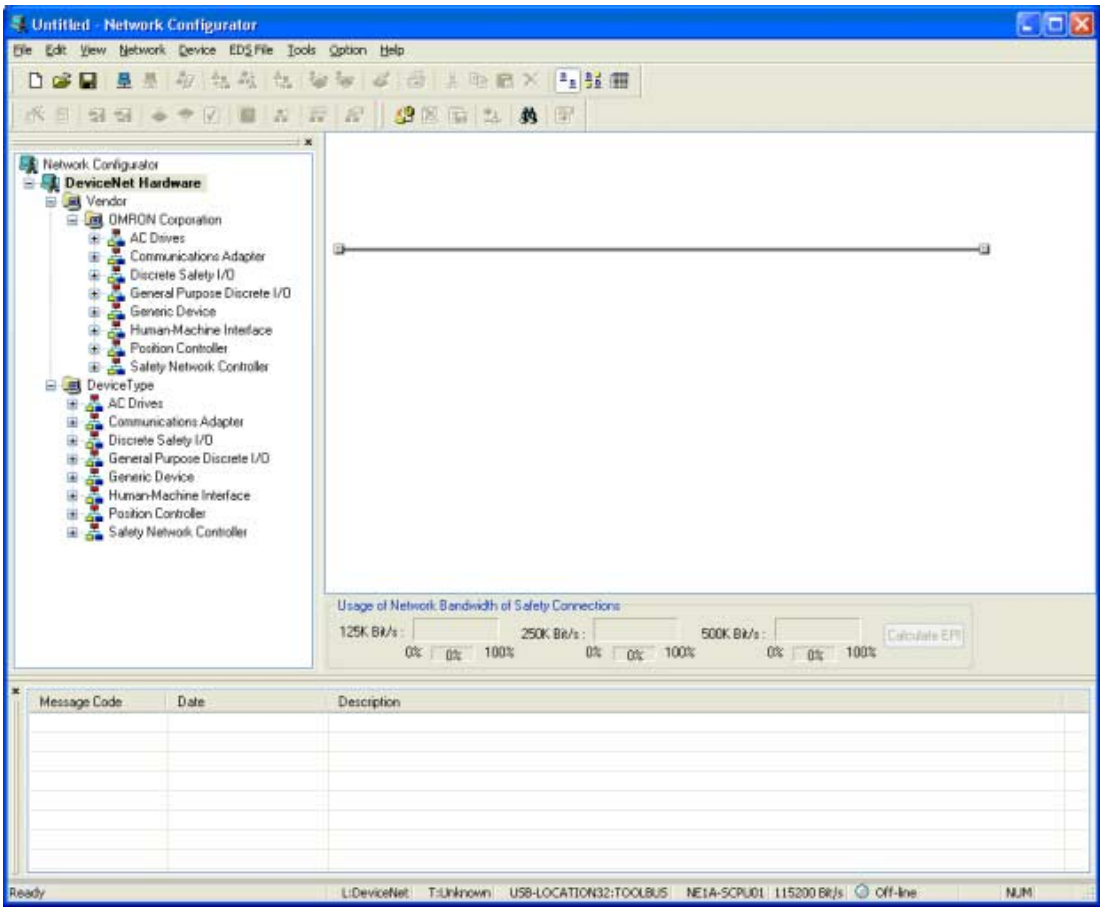
Dieser Abschnitt erläutert das Aufrufen und das Beenden des Netzwerkkonfigurators, erläutert, wie Sie die Version des Netzwerkkonfigurators bestimmen können, und erklärt das Hauptfenster.

2-1-1 Aufrufen und Beenden des Netzwerkkonfigurators

Aufruf

Wählen Sie im Windows-Startmenü ***Programme OMRON Network Configurator for DeviceNet Safety - Network Configurator*** (Verwendung der Standardnamen für die Programmordner vorausgesetzt).

Nun startet der Netzwerkkonfigurator und das folgende Fenster wird angezeigt.



Beenden

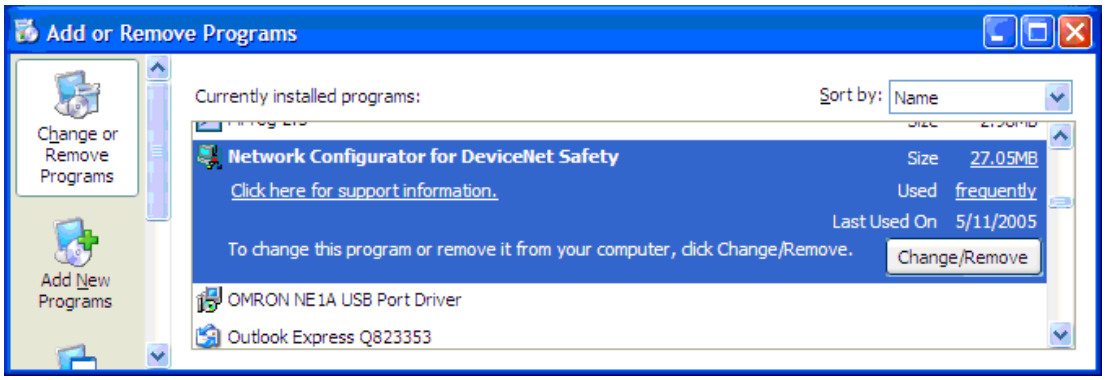
Wählen Sie im Hauptfenster den Menübefehl ***File - Exit***.

Nun wird der Netzwerkkonfigurator geschlossen.

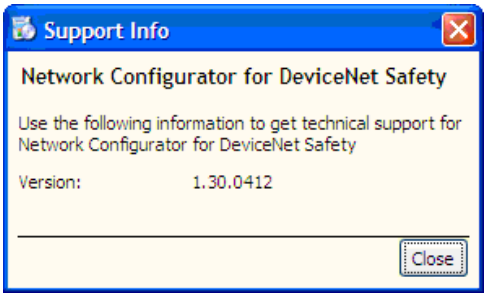
2-1-2 Bestimmung der Version

Zur Bestimmung der Version des Netzwerkkonfigurators gehen Sie folgendermaßen vor:

1. Wählen Sie im Windows-Startmenü **Systemsteuerung** (Windows XP) bzw. **Einstellungen Systemsteuerung** (Windows 2000).
2. Wählen Sie **Software**.
3. Wählen Sie aus der Liste der zurzeit installierten Programme den Eintrag **Network Configurator for DeviceNet Safety** aus, und klicken Sie auf **Supportinformationen**.

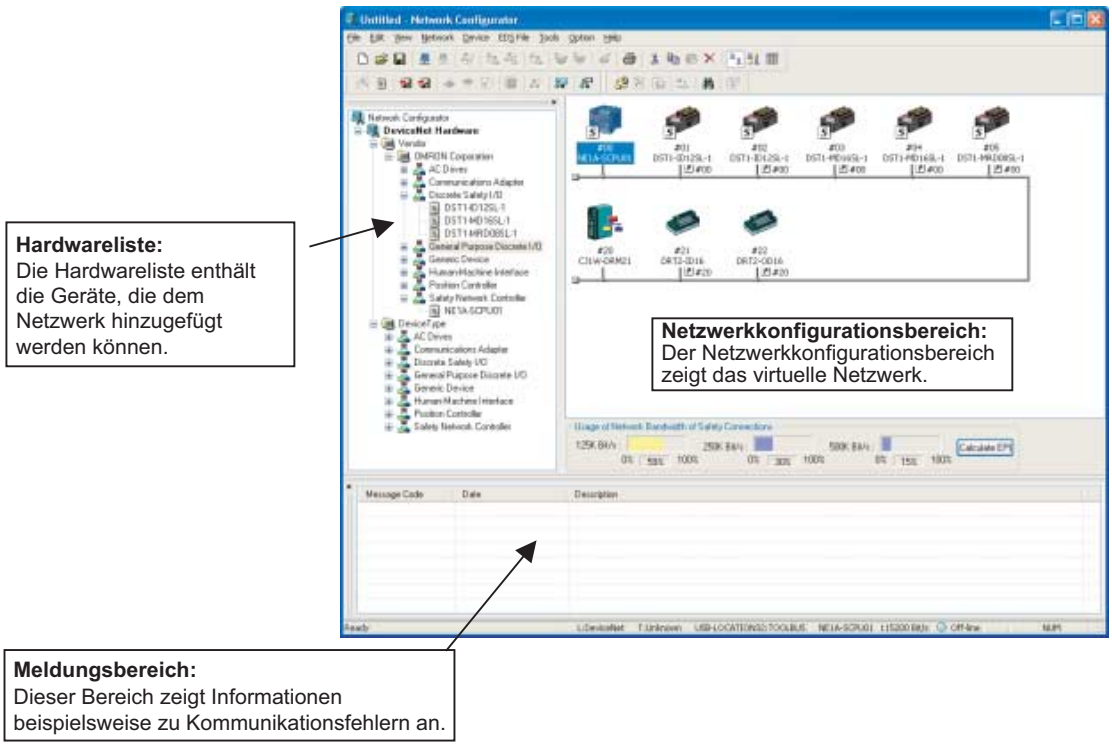


4. Im Fenster mit den Supporthinweisen werden die Versionsinformationen angezeigt.



2-1-3 Hauptfenster

Das Hauptfenster besteht aus der Hardwareliste, dem Netzwerkkonfigurationsbereich und dem Meldungsbereich.



2-2 Menüliste

Dieser Abschnitt beschreibt die Funktion der einzelnen Menübefehle des Netzwerkkonfigurators.

„Online“ bezeichnet hierbei den Zustand, dass der Netzwerkkonfigurator mit dem Netzwerk verbunden ist, „Offline“ entsprechend den Zustand, dass der Netzwerkkonfigurator nicht mit dem Netzwerk verbunden ist.

2-2-1 Menü „File“

Untermenü		Beschreibung	Offline	Online
New		Erstellen einer neuen Netzwerkkonfiguration.	O	O
Open		Öffnen einer bestehenden Netzwerkkonfigurationsdatei.	O	O
Save		Speichern der aktuellen Netzwerkkonfiguration in einer Datei.	O	O
Save As		Benennen und Speichern der aktuellen Netzwerkkonfiguration.	O	O
External Data	Export	Exportieren der Netzwerkkonfiguration in eine CSV-Datei.	O	O
	Import	Importieren einer mit dem DeviceNet-Konfigurator Version 1 oder 2 erstellten Netzwerkkonfigurationsdatei.	O	O
Change Password		Ändern des Kennworts der Netzwerkkonfigurationsdatei.	O	O
Report		Erstellen eines Berichts zu dem spezifizierten Gerät.	O	O
Print		Drucken der Geräteparameter- und E/A-Kommentar-Liste.	O	O
Setup Printer		Einrichten des Druckers.	O	O
Exit		Beenden des Netzwerkkonfigurators.	O	O
O: Unterstützt ×: Nicht unterstützt				

2-2-2 Menü „Edit“

Untermenü	Beschreibung	Offline	Online
Cut	Löschen und Kopieren der ausgewählten Geräte in die Zwischenablage.	O	O
Copy	Kopieren der ausgewählten Geräte in die Zwischenablage.	O	O
Paste	Einfügen der Geräte in der Zwischenablage an der aktuellen Cursor-Position.	O	O
Delete	Löschen der ausgewählten Geräte.	O	O
Select All	Auswählen aller Geräte.	O	O
Clear Message Report	Löschen einer Meldung im Meldungsbereich.	O	O
O: Unterstützt ×: Nicht unterstützt			

2-2-3 Menü „View“

Untermenü	Beschreibung	Offline	Online
Toolbar	Ein- und Ausblenden der Werkzeugleiste.	O	O
Status Bar	Ein- und Ausblenden der Statuszeile.	O	O
Message Report	Ein- und Ausblenden des Meldungsbereichs.	O	O
Large Icons	Umschalten auf die Netzwerkanzeige.	O	O
Large Icons - Maintenance Mode	Ein- und Ausblenden der Wartungsinformationen.	O	O
Details	Umschalten auf die Detailanzeige.	O	O
Hardwareliste	Ein- und Ausblenden der Hardwareliste.	O	O
O: Unterstützt ×: Nicht unterstützt			

2-2-4 Menü „Network“

Untermenü	Beschreibung	Offline	Online
Connect	Verbinden des Netzwerkkonfigurators mit dem Netzwerk.	O	×
Disconnect	Trennen des Netzwerkkonfigurators vom Netzwerk.	×	O
Change Connect Network Port	Ändern des Zielnetzwerk-Ports.	×	O
Move Network	Wechsel des Netzwerks, mit dem der Netzwerkkonfigurator verbunden ist.	×	O
O: Unterstützt ×: Nicht unterstützt			

Untermenü		Beschreibung	Offline	Online
Wireless Network	Move to Upper Network	Anzeigen des Netzwerks eine Schicht oberhalb des aktuellen Netzwerks in den drahtlosen Netzwerken.	×	O
	Move to Lower Network	Anzeigen des Netzwerks eine Schicht unterhalb des aktuellen Netzwerks in den drahtlosen Netzwerken.	×	O
Upload		Hochladen aller Geräteparameter im Netzwerk in den Netzwerkkonfigurator.	×	O
Download		Herunterladen aller Geräteparameter aus dem Netzwerkkonfigurator in die Geräte im Netzwerk.	×	O
Verify Structure		Überprüfen, ob die aktuelle Netzwerkkonfiguration des Netzwerkkonfigurators mit der konkreten Netzwerkkonfiguration des online verbundenen Zielnetzwerks übereinstimmt.	×	O
Update Maintenance Information		Aktualisieren der Wartungsinformationen der einzelnen Geräte auf den aktuellsten Stand.	×	O
Check Connection		Überprüfen der Konsistenz aller Verbindungen.	O	O
Property		Anzeigen der Netzwerkeigenschaften. Der Netzwerkname und die Sicherheitsnetzwerknummer können eingestellt werden.	O	O
			O: Unterstützt ×: Nicht unterstützt	

2-2-5 Menü „Device“

Untermenü		Beschreibung	Offline	Online
Parameter	Wizard	Konfigurieren der Geräteparameter mithilfe eines Assistenten. Diese Funktion wird nicht von allen Geräten unterstützt.	O	O
	Edit	Bearbeiten der Geräteparameter.	O	O
	Read	Auslesen der Parameter aus der Geräteparameterdatei.	O	O
	Save As	Speichern der Geräteparameter in einer Geräteparameterdatei.	O	O
	Upload	Hochladen der Geräteparameter eines Geräts im Netzwerk.	×	O
	Download	Herunterladen der Geräteparameter in ein Gerät im Netzwerk.	×	O
	Verifizieren	Verifizieren des Geräts und der Geräteparameter im Netzwerk.	×	O
	Lock	Schützen der Konfiguration eines Geräts im Netzwerk.	×	O
	Unlock	Aufheben des Schutzes der Konfiguration eines Geräts im Netzwerk.	×	O
Monitor		Überwachen der Parameter und des Status eines Geräts im Netzwerk. Diese Funktion wird nicht von allen Geräten unterstützt.	×	O
Reset		Zurücksetzen eines Geräts im Netzwerk.	×	O
Change Mode		Ändern des Status eines Geräts im Netzwerk. Diese Funktion wird nicht von allen Geräten unterstützt.	×	O
Change Password		Ändern des Kennworts eines Geräts im Netzwerk.	×	O
Maintenance Information		Anzeigen der Wartungsinformationen eines Geräts im Netzwerk.	×	O
Register to Another Device		Registrieren eines Geräts bei einem anderen Gerät.	O	O
External Data	Export	Exportieren von E/A-Kommentaren oder Geräteparametern in einem anderen Dateiformat. Diese Funktion wird nicht von allen Geräten unterstützt.	O	O
	Import	Importieren einer mit dem DeviceNet-Konfigurator Version 1 oder 2 erstellten Geräteparameterdatei. Diese Funktion wird nicht von allen Geräten unterstützt.	O	O
Change Node Address		Ändern der Knotenadresse eines Geräts.	O	O
Change Device Comment		Ändern des Namens eines Geräts.	O	O
Edit I/O Comment		Bearbeiten des E/A-Kommentars.	O	O
Property		Anzeigen der Eigenschaften eines Geräts.	O	O
			O: Unterstützt ×: Nicht unterstützt	

Hinweis: Durch Rechtsklicken im Netzwerkkonfigurationsbereich können die Menüs „Device“ und „Edit“ partiell angezeigt werden.

2-2-6 Menü „EDS File“

Untermenü	Beschreibung	Offline	Online
Install	Installieren einer EDS-Datei und Hinzufügen eines Geräts zur Hardwareliste.	O	O
Create	Erstellen einer neuen EDS-Datei und Hinzufügen eines Geräts zur Hardwareliste.	O	O
Delete	Löschen eines Geräts aus der Hardwareliste. Die installierte EDS-Datei wird ebenfalls gelöscht.	O	O
Save As	Benennen und Speichern der EDS-Datei eines Geräts in der Hardwareliste.	O	O
Find	Suchen nach einer bestimmten EDS-Datei in der Hardwareliste.	O	O
Add to Network	Hinzufügen eines Geräts aus der Hardwareliste zum virtuellen Netzwerk.	O	O
Property	Anzeigen der Eigenschaften einer EDS-Datei.	O	O
O: Unterstützt ×: Nicht unterstützt			

Hinweis: Das Menü „EDS File“ kann durch Rechtsklicken in der Hardwareliste aufgerufen werden.

2-2-7 Menü „Tools“

Untermenü	Beschreibung	Offline	Online
Setup Parameters	Einrichten der Parameter durch Kommunikation mit expliziten Meldungen.	×	O
Setup Node Address/ Baud Rate	Einrichten der Knotenadresse und Baudrate eines Geräts im Netzwerk.	×	O
O: Unterstützt ×: Nicht unterstützt			

2-2-8 Menü „Options“

Untermenü	Beschreibung	Offline	Online
Select Interface	Auswählen der vom Netzwerkkonfigurator für die Netzwerkverbindung verwendeten Schnittstelle.	O	O
Edit Configuration File	Bearbeiten verschiedener Konfigurationsdateien.	O	O
Setup Monitor Refresh Timer	Einstellung der Zeitwerte für die Überwachungsaktualisierung (Überwachungszyklus bei der Geräteüberwachung).	O	O
Install Extend Module	Installieren eines Erweiterungsmoduls.	O	O
Install Interface Module	Installieren eines Schnittstellenmoduls.	O	O
Parameter Auto Update when Configuration Changed	Bei Aktivierung dieser Option wird die im Master registrierte Slave-E/A-Größe automatisch aktualisiert, wenn diese Größe geändert wird. Standardmäßig ist diese Option deaktiviert (keine automatische Aktualisierung). Unter normalen Anwendungsbedingungen sollte diese Option deaktiviert bleiben.	O	O
O: Unterstützt ×: Nicht unterstützt			

2-2-9 Menü „Help“

Untermenü	Beschreibung	Offline	Online
Topic	Anzeigen der Hilfethemen.	O	O
About	Anzeigen der Versionsinformationen zum Netzwerkkonfigurator.	O	O

2-3 Verbinden mit dem Netzwerk

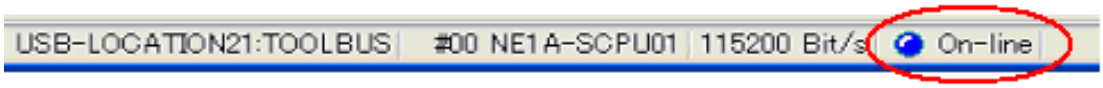
Operationen, die nur im Online-Modus durchgeführt werden können (zum Beispiel der Abruf der Netzwerkkonfiguration eines konkreten Netzwerks oder das Herunterladen der konfigurierten Geräteparameter in die Geräte im Netzwerk), erfordern, dass der Netzwerkkonfigurator mit dem Netzwerk verbunden ist.

Dieser Abschnitt erläutert, wie der Netzwerkkonfigurator über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) oder über eine im Computer installierte DeviceNet-Schnittstellenkarte mit dem Netzwerk verbunden wird. Im Anhang finden Sie Informationen zu weiteren Möglichkeiten, den Netzwerkkonfigurator mit dem Netzwerk zu verbinden.

2-3-1 Netzwerkverbindung über eine USB-Schnittstelle

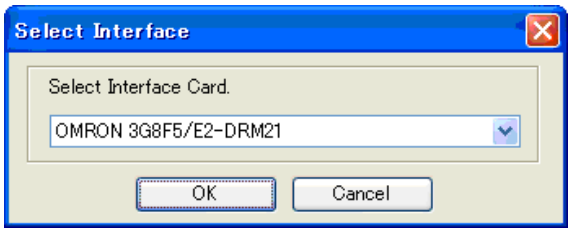
1. Schalten Sie die Spannungsversorgung des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) ein, und schließen Sie diesen an eine USB-Schnittstelle des Computers an.
2. Wählen Sie in der Menüleiste ***Option - Select Interface - NE1A USB Port***, und wählen Sie den gewünschten Modus aus.
3. Wählen Sie in der Menüleiste ***Network - Connect***.

Wurde die Verbindung mit dem Netzwerk erfolgreich hergestellt, wird in der Statuszeile am unteren Rand des Fensters On-line angezeigt.

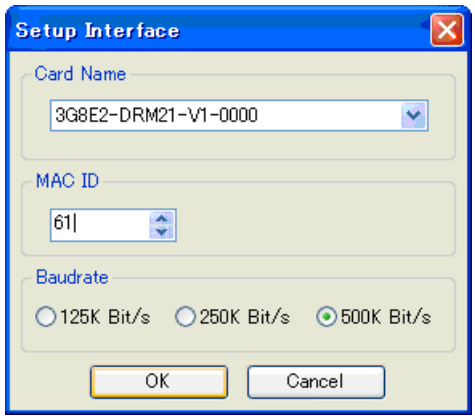


2-3-2 Netzwerkverbindung über eine DeviceNet-Schnittstellenkarte

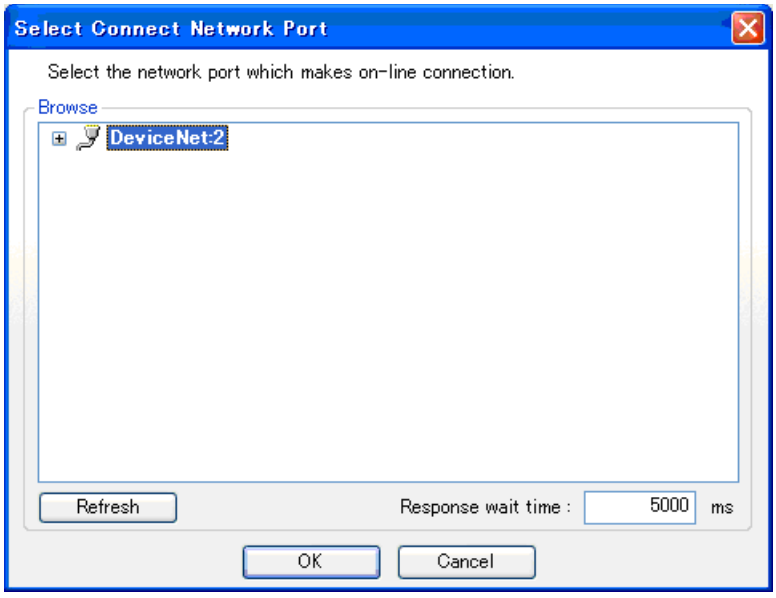
1. Wählen Sie ***Option - Select Interface - DeviceNet I/F***.
2. Wählen Sie ***Network - Connect***.
   Nun wird das Dialogfeld **Select - Interface** angezeigt.



3. Wählen Sie die Schnittstellenkarte aus, und klicken Sie auf **OK**.
   Nun wird das Dialogfeld **Setup Interface** angezeigt.
   Das Erscheinungsbild dieses Dialogfelds hängt vom Typ der ausgewählten Schnittstellenkarte ab. Dieses Beispiel zeigt das Dialogfeld für die DeviceNet PCMCIA-Karte (3G8E2-DRM21-V1). Wenn Sie eine andere Schnittstellenkarte verwenden, so ziehen Sie das Bedienerhandbuch für diese Karte zu Rate.



4. Stellen Sie die MAC ID (Knotenadresse) und die Baudrate ein, und klicken Sie auf **OK**.
   Nun wird das Dialogfeld **Select Connect Network Port** angezeigt.



   Bei der ersten Netzwerkverbindung wird automatisch eine Netzwerksuche durchgeführt, wobei dieses Dialogfeld angezeigt wird. Warten Sie, bis die Suche für alle Adressen durchgeführt wurde. Nach der Suche werden die Netzwerke angezeigt, mit denen eine Verbindung hergestellt werden kann.
   Die automatische Suche nach Netzwerken wird nur beim ersten Mal durchgeführt, später nicht mehr.
5. Wählen Sie das Netzwerk, mit dem eine Verbindung hergestellt werden soll, und klicken Sie auf **OK**.
   Wurde die Verbindung mit dem Netzwerk erfolgreich hergestellt, wird in der Statuszeile am unteren Rand des Fensters *On-line* angezeigt.

2-4 Erstellen eines virtuellen Netzwerks

Zum Einstellen der Geräteparameter und zum Programmieren des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) erstellen Sie im Netzwerkkonfigurator ein virtuelles Netzwerk, stellen Sie die Geräteparameter im virtuellen Netzwerk ein, und laden Sie dann die Parameter in die im Netzwerk vorhandenen Geräte herunter.

In diesem Abschnitt wird das Erstellen eines virtuellen Netzwerks beschrieben.

2-4-1 Erstellen eines neuen virtuellen Netzwerks

Beim Start des Netzwerkkonfigurators kann ein neues virtuelles Netzwerk erstellt werden.

Mit dem Netzwerkkonfigurator kann immer nur ein virtuelles Netzwerk zur gleichen Zeit bearbeitet werden. Verwenden Sie eine der folgenden Methoden, wenn Sie ein weiteres virtuelles Netzwerk erstellen möchten.

(1) Wählen Sie in der Menüleiste ***File - New***.

(2) Klicken Sie in der Werkzeugleiste auf **New**.

Hinweis: Beim Erstellen eines neuen virtuellen Netzwerks werden die momentan im Netzwerkkonfigurator angezeigten/bearbeiteten Informationen gelöscht. Werden diese Informationen noch benötigt, müssen die Daten vor dem Erstellen eines neuen virtuellen Netzwerks gespeichert werden.

2-4-2 Netzwerknummern

Die Netzwerknummer (d. h. die Netzwerkadresse) ist die für jede Netzwerk-Domäne separat eingestellte Nummer. Alle an einem Netzwerk angeschlossenen Geräte müssen auf dieselbe Netzwerknummer eingestellt sein.

Der Netzwerkkonfigurator kombiniert die Netzwerknummer mit der Knotenadresse zu einem eindeutigen Knotenbezeichner (UNID) und speichert diesen im Gerät. Die UNID ermöglicht die Identifizierung eines Geräts aus allen Netzwerk-Domänen.

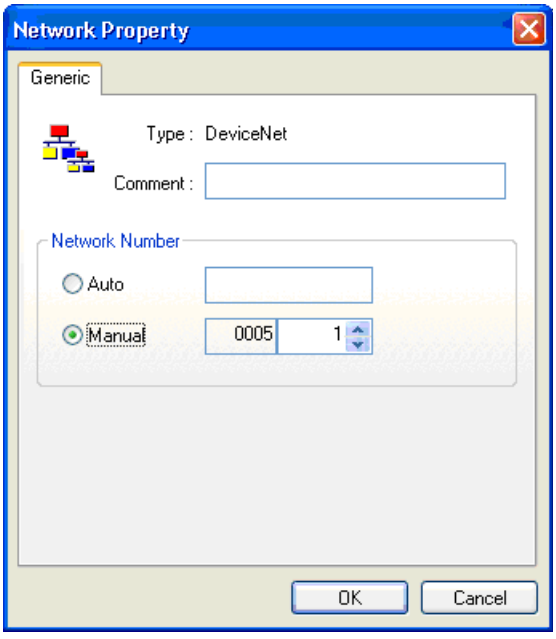
Der Netzwerkkonfigurator generiert die Netzwerknummer automatisch basierend auf dem Datum und der Uhrzeit des Zeitpunkts, zu dem die neue Netzwerkkonfigurationsdatei erstellt wird. Unter normalen Umständen muss sich der Anwender nicht um die Generierung der Netzwerknummer kümmern.

Hinweis: Beim Herunterladen der Parameter in die Geräte wird die Netzwerknummer gemeinsam mit den Parametern als UNID übertragen und in den Geräten gespeichert. Wird daher ein Gerät eingesetzt, dessen Parameter bereits für eine andere Netzwerk-Domäne eingestellt wurden, muss **Reset Type** auf **Return to the out-of-box configuration, and then emulate cycling power** gesetzt und das Gerät anschließend zurückgesetzt werden, um die UNID zu löschen.

Gehen Sie wie folgt vor, um die Netzwerknummer einzustellen.

(1) Wählen Sie in der Menüleiste ***Network - Property***.

(2) Aktivieren Sie im Bereich **Network Number** die Option **Manual**, und geben Sie die Netzwerknummer ein.



WICHTIG: Weisen Sie bei der Einrichtung jedem Netzwerk oder Subnetzwerk eine eindeutige Netzwerknummer zu.

Ist die Netzwerknummer nicht richtig eingestellt, wird möglicherweise eine Verbindung zu einem anderen Gerät hergestellt. Für jede Netzwerk-Domäne muss eine andere Netzwerknummer eingestellt werden, und alle Geräte derselben Domäne müssen auf dieselbe Netzwerknummer eingestellt werden.

2-4-3 Hinzufügen von Geräten

Es gibt zwei Möglichkeiten, dem virtuellen Netzwerk Geräte hinzuzufügen:

(1) Hinzufügen aus der Hardwareliste.

(2) Hochladen der Netzwerkkonfiguration aus dem tatsächlichen Netzwerk.

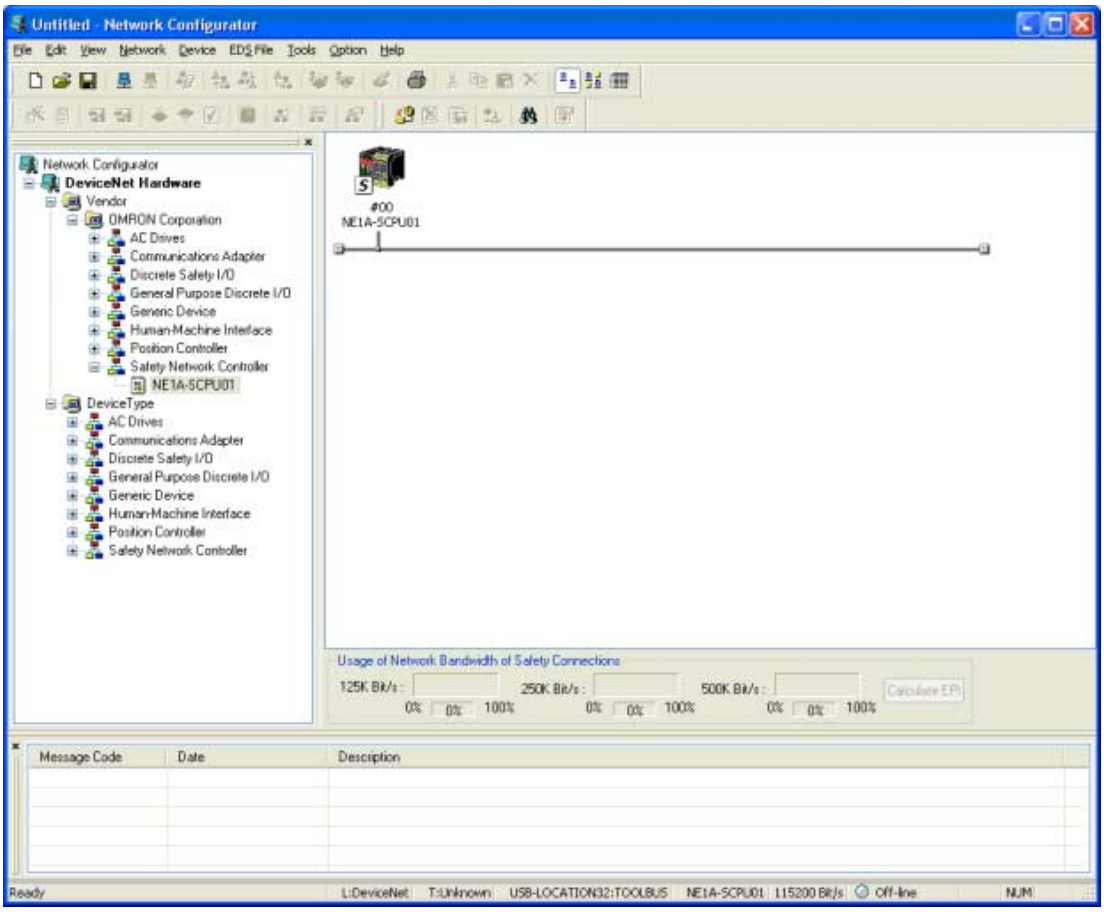
Hinzufügen von Geräten aus der Hardwareliste

Es gibt zwei Möglichkeiten, dem virtuellen Netzwerk Geräte aus der Hardwareliste hinzuzufügen:

(1) Doppelklicken in der Hardwareliste auf das gewünschte Gerät.

(2) Auswählen des Geräts in der Hardwareliste und Ziehen in den Netzwerkkonfigurationsbereich.

Wurde ein Gerät registriert, wird es folgendermaßen angezeigt:



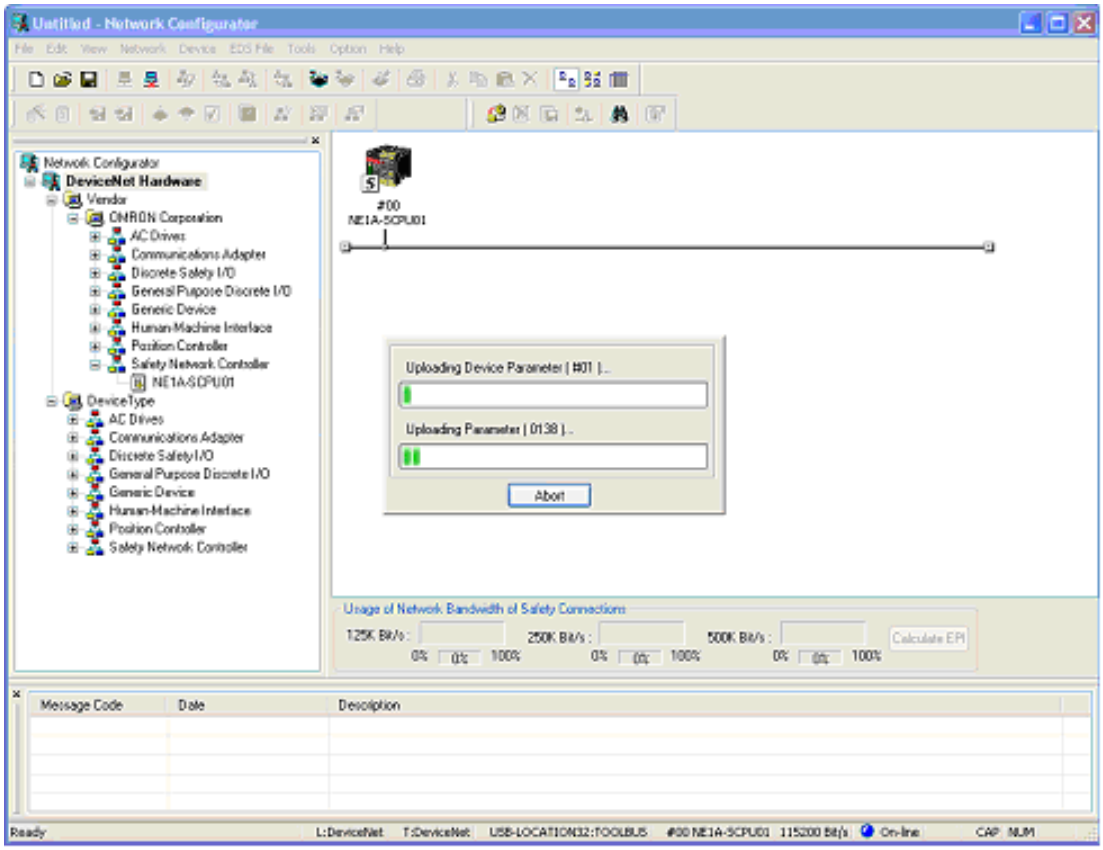
Hochladen der Netzwerkkonfiguration aus dem tatsächlichen Netzwerk

Die Netzwerkkonfiguration kann aus dem tatsächlichen Netzwerk ausgelesen werden, um ein identisch konfiguriertes virtuelles Netzwerk zu erstellen. Verbinden Sie den Netzwerkkonfigurator mit dem Netzwerk, und laden Sie die Netzwerkkonfiguration aus dem Netzwerk hoch.

(1) Wählen Sie in der Menüleiste ***Network - Upload***.

(2) Klicken Sie in der Werkzeugleiste auf ***Upload from Network***. Nun startet das Hochladen der Netzwerkkonfiguration, und die erkannten Geräte werden der Reihe nach angezeigt.

(3) Klicken Sie im Netzwerkkonfigurationsbereich mit der rechten Maustaste, ohne dabei ein Gerät auszuwählen, und wählen Sie den Kontextmenübefehl ***Upload***.



Muss nach Abschluss des Hochladens der Netzwerkkonfiguration ein Gerät hinzugefügt werden, so gehen Sie dazu wie oben unter „Hinzufügen von Geräten aus der Hardwareliste“ beschrieben vor.

WICHTIG: Vor dem Hochladen der Netzwerkkonfiguration muss die Master-Funktionalität eventuell im Netzwerk vorhandener CS/CJ-Serie DeviceNet-Baugruppen deaktiviert werden. Ist die Master-Funktionalität aktiviert, kann das Hochladen der Geräteparameter scheitern.

Hinweis:
- Beim Hochladen der Netzwerkkonfiguration werden die momentan im Netzwerkkonfigurator angezeigten/bearbeiteten Informationen gelöscht. Werden diese Informationen noch benötigt, müssen die Daten vor dem Hochladen der Netzwerkkonfiguration gespeichert werden.
- Wird die Netzwerkkonfiguration eines Netzwerkes hochgeladen, dessen Geräten bereits eine Netzwerknummer zugewiesen wurde, wird dieser Wert als Netzwerknummer für das virtuelle Netzwerk verwendet.

2-4-4 Entfernen von Geräten

Es gibt zwei Möglichkeiten, Geräte aus dem virtuellen Netzwerk zu entfernen:

(1) Wählen Sie das zu entfernende Gerät aus, und wählen Sie in der Menüleiste ***Edit - Delete***.

(2) Wählen Sie das zu entfernende Gerät aus, und klicken Sie in der Werkzeugleiste auf **Delete**.

(3) Wählen Sie das zu entfernende Gerät aus, klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät, und wählen Sie den Kontextmenübefehl ***Delete***.

Vor dem Entfernen des Geräts aus dem virtuellen Netzwerk wird ein Bestätigungsdialogfeld angezeigt. Zum Entfernen des Geräts aus dem virtuellen Netzwerk klicken Sie auf **Delete**.

2-4-5 Ändern der Knotenadresse

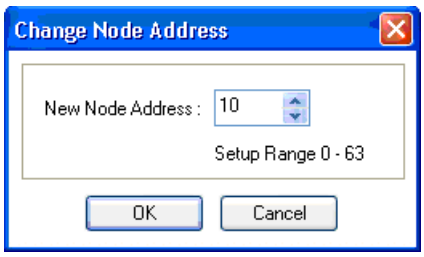
Beim Hinzufügen von Geräten aus der Hardwareliste wird dem Gerät automatisch in der Reihenfolge des Hinzufügens der Geräte eine nicht verwendete Knotenadresse von 0 bis 63 zugeordnet.

Sie können diese automatisch zugeordnete Knotenadresse auf zweierlei Weise ändern:

(1) Wählen Sie das Gerät aus, und wählen Sie in der Menüleiste ***Device - Change Node Address***.

(2) Wählen Sie das Gerät aus, klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät, und wählen Sie den Kontextmenübefehl ***Change Node Address***.

Das folgende Dialogfeld wird angezeigt. Ändern Sie die Knotenadresse, und klicken Sie auf **OK**.



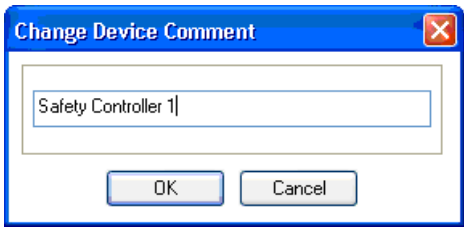
2-4-6 Ändern der Gerätekommentare

Beim Hinzufügen von Geräten aus der Hardwareliste wird als Kommentar zunächst der Gerätetyp angezeigt. Dieser Kommentar kann auf zweierlei Weise geändert werden:

(1) Wählen Sie das Gerät aus, und wählen Sie in der Menüleiste ***Device - Change Device Comment***.

(2) Wählen Sie das Gerät aus, klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät, und wählen Sie den Kontextmenübefehl ***Change Device Comment***.

Das folgende Dialogfeld wird angezeigt. Geben Sie den gewünschten Gerätekommentar ein, und klicken Sie auf OK.



2-5 Speichern und Laden von Netzwerkkonfigurationsdateien

Die Netzwerkkonfiguration des erstellten virtuellen Netzwerks kann in einer Datei gespeichert werden. Die so erstellte Datei kann geöffnet, modifiziert und in die an das Netzwerk angeschlossenen Geräte heruntergeladen werden.

2-5-1 Kennwortschutz für Netzwerkkonfigurationsdateien

Netzwerkkonfigurationsdateien können mit einem Kennwortschutz versehen werden. Das eingestellte Kennwort wird verschlüsselt und in der Datei gespeichert. Mithilfe des Kennwortschutzes können Sie Netzwerkkonfigurationsdateien vor unbeabsichtigter Änderung und nicht autorisierter Verwendung schützen.

Folgende Operationen im Netzwerkkonfigurator erfordern die Eingabe des Kennworts der Netzwerkkonfigurationsdatei:

- Speichern der Netzwerkkonfigurationsdatei
- Öffnen der Netzwerkkonfigurationsdatei
- Ändern des Kennworts der Netzwerkkonfigurationsdatei

Zum Speichern der Datei muss das korrekte Kennwort eingegeben werden. Wird beim Öffnen der Datei nicht das richtige Kennwort eingegeben, wechselt der Netzwerkkonfigurator in den Schutzmodus. In diesem Modus sind bestimmte Operationen des Netzwerkkonfigurators eingeschränkt.

Die Festlegung des Kennworts einer Netzwerkkonfigurationsdatei erfolgt beim erstmaligen Speichern der Datei. Das Kennwort muss aus 6 bis 16 alphanumerischen Zeichen bestehen. Wenn Sie kein Kennwort einrichten möchten, machen Sie im Dialogfeld **Assign Password** keine Eingabe, sondern klicken Sie nur auf **OK**.

Zum Ändern des Kennworts einer Netzwerkkonfigurationsdatei wählen Sie in der Menüleiste ***File - Change Password***. Nach der Änderung des Kennworts müssen die Datei und das Kennwort jedoch gespeichert werden, damit die Kennwortänderung wirksam wird.

WICHTIG:

- Aus Sicherheitsgründen wird empfohlen, Kennwörter für Netzwerkkonfigurationsdateien zu vergeben.
- Vergessen Sie das eingestellte Kennwort nicht. Haben Sie das Kennwort einer Netzwerkkonfigurationsdatei vergessen, können Sie diese nicht mehr öffnen.

2-5-2 Speichern der Netzwerkkonfigurationsdatei

Netzwerkkonfigurationsdateien können auf verschiedene Arten gespeichert werden:

(1) Wählen Sie in der Menüleiste ***File - Save*** oder ***File - Save As***.

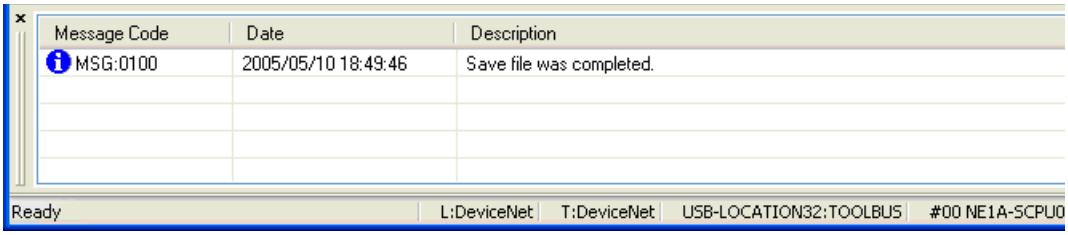
(2) Klicken Sie in der Werkzeugleiste auf **Save**.

Anschließend wird das Windows-Standarddialogfeld für das Speichern von Dateien angezeigt. Wählen Sie den Ordner für die Speicherung der Datei aus, geben Sie der Datei einen Namen, und klicken Sie auf **Speichern**.

Beim erstmaligen Speichern einer Datei wird das Dialogfeld **Assign Password** angezeigt. In diesem legen Sie das Kennwort für die Netzwerkkonfigurationsdatei fest.

Bei allen folgenden Speichervorgängen wird das Dialogfeld **Password Confirmation** angezeigt. Hier müssen Sie das aktuelle Kennwort für die Netzwerkkonfigurationsdatei eingeben.

Wurde die Datei erfolgreich gespeichert, wird im Meldungsbereich die folgende Meldung angezeigt:



2-5-3 Laden von Netzwerkkonfigurationsdateien

Gespeicherte Netzwerkkonfigurationsdateien können auf zweierlei Weise in den Netzwerkkonfigurator geladen werden:

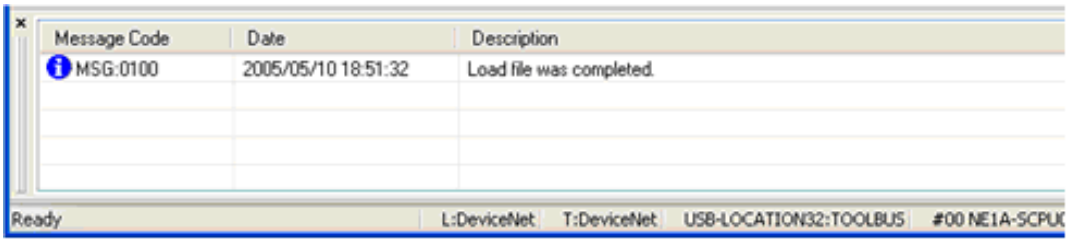
(1) Wählen Sie in der Menüleiste **File - Open**.

(2) Klicken Sie in der Werkzeugleiste auf **Open**.

Bei beiden Varianten wird das Windows-Standarddialogfeld **Öffnen** angezeigt. Wählen Sie die gewünschte Datei aus, und klicken Sie auf **Öffnen**.

Als nächstes wird das Dialogfeld **Check Password** angezeigt. Hier müssen Sie das aktuelle Kennwort für die Netzwerkkonfigurationsdatei eingeben.

Wurde die Datei erfolgreich geöffnet, wird im Meldungsbereich die folgende Meldung angezeigt:

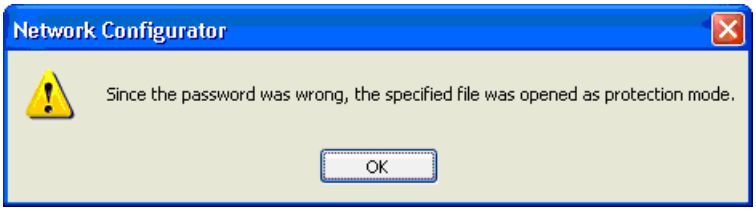


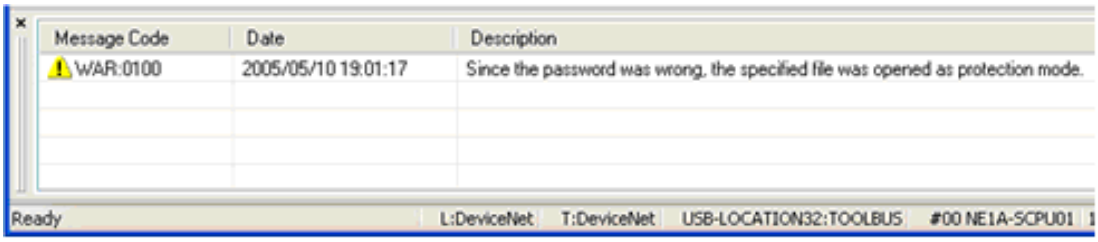
Hinweis: Wurde nicht das richtige Kennwort eingegeben, öffnet der Netzwerkkonfigurator die Datei im Schutzmodus. Im Schutzmodus sind bestimmte Operationen wie das Speichern der Datei, das Herunterladen von Parametern und das Ändern des Gerätestatus nicht möglich. Detaillierte Informationen hierzu finden Sie unter *2-5-4 Schutzmodus* (Seite 39).

2-5-4 Schutzmodus

Wurde beim Öffnen der Netzwerkkonfigurationsdatei nicht das richtige Kennwort eingegeben, öffnet der Netzwerkkonfigurator die Datei im Schutzmodus.

Wurde nicht das richtige Kennwort eingegeben, wird in einem Dialogfeld und im Meldungsbereich die folgende Meldung angezeigt:





Die folgenden Operationen können im Schutzmodus nicht durchgeführt werden:

- Speichern der Netzwerkkonfigurationsdatei
- Ändern des Kennworts der Netzwerkkonfigurationsdatei
- Herunterladen der Netzwerkkonfiguration in Geräte im Netzwerk
- Herunterladen der Parameter in Geräte im Netzwerk
- Zurücksetzen von Geräten im Netzwerk
- Ändern des Kennworts von Geräten im Netzwerk
- Senden von Anforderungen als explizite Meldungen an Geräte im Netzwerk
- Festlegen der Knotenadresse von Geräten im Netzwerk
- Festlegen der Baudrate von Geräten im Netzwerk

2-6 Kennwortschutz für Geräte

Sicherheitsgeräte können intern ein Kennwort speichern. Das Einrichten eines Kennworts für ein Sicherheitsgerät hindert unbefugte Personen am Ändern der Parameter oder des Status des Sicherheitsgeräts.

2-6-1 Einstellen eines Gerätekennworts

Die folgenden Operationen im Netzwerkkonfigurator erfordern die Eingabe des Gerätekennworts.
Bei Eingabe eines falschen Kennworts können diese Operationen nicht ausgeführt werden.

- Herunterladen der Netzwerkkonfiguration
- Herunterladen von Parametern
- Schutz der Konfiguration
- Aufheben des Konfigurationsschutzes
- Zurücksetzen
- Ändern des Status
- Ändern des Kennworts

Das Einrichten eines Kennworts für ein Gerät kann auf verschiedene Arten erfolgen. Erforderlich ist jedoch auf jeden Fall, dass der Netzwerkkonfigurator online, d. h. mit dem Netzwerk verbunden ist.

(1) Wählen Sie das Gerät aus, und wählen Sie in der Menüleiste ***Device - Change Password***.

(2) Wählen Sie das Gerät aus, klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät, und wählen Sie den Kontextmenübefehl ***Change Password***.

Nun wird das im Folgenden abgebildete Dialogfeld **Change Password** angezeigt. Geben Sie das aktuelle und das neue Kennwort ein, und klicken Sie auf **OK**. Das Kennwort muss aus 6 bis 16 alphanumerischen Zeichen bestehen.

Gerätekennwörter werden nicht in der Netzwerkkonfigurationsdatei gespeichert. Die Standardeinstellungen eines Geräts enthalten kein Kennwort. Wird daher der die Rücksetzvariante eines Geräts auf *Return to the out-of-box configuration, and then emulate cycling power* gesetzt und das Gerät anschließend zurückgesetzt, ist das Gerät nicht mehr durch ein Kennwort geschützt. Zum Zurücksetzen des Geräts ist jedoch die Eingabe des aktuellen Kennworts erforderlich. Vergessen Sie daher das eingestellte Gerätekennwort nicht.

WICHTIG: Aus Sicherheitsgründen wird empfohlen, Gerätekennwörter einzurichten.

Hinweis: Wenn Sie für verschiedene Geräte dasselbe Kennwort vergeben haben und eine Operation durchführen, die die Eingabe eines Kennworts erfordert, genügt es, das Kennwort einmalig für alle Geräte einzugeben. Aktivieren Sie hierzu im Dialogfeld **Password Input** das Kontrollkästchen **Use this password for all device**.

2-6-2 Vorgehensweise im Fall eines vergessenen Gerätekennworts

Wenn Sie ein Gerätekennwort vergessen haben, wenden Sie sich bitte an Ihre OMRON-Vertretung. Von dieser erhalten Sie ein Ersatzkennwort, das Sie in das im Netzwerkkonfigurator enthaltene Password Recovery Tool eingeben können, um den Kennwortschutz des Geräts aufzuheben.

Die folgenden Informationen werden benötigt, um dieses Ersatzkennwort generieren zu können. Sie können diese Informationen mithilfe des Password Recovery Tools aus dem Gerät abrufen. Detaillierte Informationen hierzu finden Sie in Anhang 5: „Verwendung des Password Recovery Tools“.

- Vendor ID
- Seriennummer
- Zählerstand

2-7 Geräteparameter und -eigenschaften

Die Eigenschaften registrierter Geräte können im virtuellen Netzwerk ohne jegliche Beschränkung bearbeitet werden. Als Netzwerkkonfigurationsdatei gespeicherte Parameter können zu einem späteren Zeitpunkt wieder geladen und unverändert oder mit Modifikationen in die Geräte heruntergeladen werden.

2-7-1 Bearbeiten von Geräteparametern

Geräteparameter können auf verschiedene Arten bearbeitet werden:

(1) Doppelklicken Sie auf das Gerätesymbol.
(2) Wählen Sie das Gerät aus, und wählen Sie in der Menüleiste ***Device Parameter - Edit***.
(3) Wählen Sie das Gerät aus, und klicken Sie in der Werkzeugleiste auf ***Edit Parameter***.
(4) Wählen Sie das Gerät aus, klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät, und wählen Sie den Kontextmenübefehl ***Parameter - Edit***.

Das Erscheinungsbild des nun angezeigten Bearbeitungsfensters für die Geräteparameter hängt vom jeweiligen Gerät ab. Informationen zur Bearbeitung der Geräteparameter von DST1-Sicherheits-E/A-Modulen finden Sie in *Kapitel 4* (Seite 69). Information zur Bearbeitung der Geräteparameter von Sicherheitsnetzwerk-Controllern (NE1A-SCPU01) finden Sie in *Kapitel 5* (Seite 79).

2-7-2 Hochladen von Geräteparametern

Die Parameter aller Geräte im Netzwerk können aus dem Netzwerk in den Netzwerkkonfigurator hochgeladen werden. Die Parameter aller Geräte im Netzwerk können aus dem Netzwerk in den Netzwerkkonfigurator hochgeladen werden. Diese Funktion erfordert, dass der Netzwerkkonfigurator online, d. h. mit dem Netzwerk verbunden ist.

(1) Wählen Sie ein oder mehrere Geräte aus, und wählen Sie in der Menüleiste ***Device - Parameter Upload***.
(2) Wählen Sie ein oder mehrere Geräte aus, und klicken Sie in der Werkzeugleiste auf **Upload from Device**.
(3) Wählen Sie ein oder mehrere Geräte aus, klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte, und wählen Sie den Kontextmenübefehl ***Parameter - Upload***.

WICHTIG: Vor dem Hochladen der Netzwerkkonfiguration muss die Master-Funktionalität eventuell im Netzwerk vorhandener CS/CJ-Serie DeviceNet-Baugruppen deaktiviert werden. Ist die Master-Funktionalität aktiviert, kann das Hochladen der Geräteparameter scheitern.

Hinweis: Information zum Hochladen der Netzwerkkonfiguration finden Sie unter „Hochladen der Netzwerkkonfiguration aus dem tatsächlichen Netzwerk“ im Abschnitt *2-4-3 Hinzufügen von Geräten* (Seite 35).

2-7-3 Herunterladen von Geräteparametern

Für das Herunterladen der Parameter in ein Gerät gibt es zweierlei Möglichkeiten: Gezieltes Herunterladen der Geräteparameter in ausgewählte Geräte oder sequenzielles Herunterladen der Geräteparameter aller Geräte im Netzwerk. Beide Methoden sind gleichermaßen zulässig. Stellen Sie doch sicher, dass die Parameter aller Geräte heruntergeladen werden.

Diese Funktion erfordert, dass der Netzwerkkonfigurator online, d. h. mit dem Netzwerk verbunden ist. Das Herunterladen der Parameter erfordert außerdem die Eingabe der Gerätekennwörter.

Herunterladen der Parameter in bestimmte Geräte

Das Herunterladen der Parameter in bestimmte Geräte kann auf verschiedene Arten erfolgen:

(1) Wählen Sie ein oder mehrere Geräte aus, und wählen Sie in der Menüleiste ***Device - Parameter Download***.
(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf ***Download to Device***.
(3) Wählen Sie ein oder mehrere Geräte aus, klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte, und wählen Sie den Kontextmenübefehl ***Parameter Download***.

Nun wird das Fenster für die Eingabe des Gerätekennworts angezeigt. Geben Sie das Kennwort für die ausgewählten Geräte ein, und klicken Sie auf **OK**.

Wenn Sie für verschiedene Geräte dasselbe Kennwort vergeben haben, können Sie im folgenden Dialogfeld das Kontrollkästchen **Use this password for all device** aktivieren. Auf diese Weise ersparen Sie sich die Eingabe des Kennworts für alle anderen Geräte.

Herunterladen der Parameter in alle Geräte im Netzwerk

Das Herunterladen der Parameter in alle Geräte im Netzwerk kann auf verschiedene Arten erfolgen:

(1) Wählen Sie in der Menüleiste ***Network - Upload***.

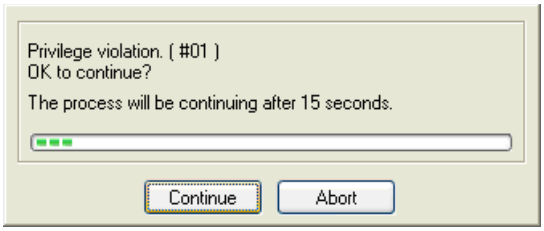
(2) Klicken Sie in der Werkzeugleiste auf **Download to Network**.

(3) Klicken Sie im Netzwerkkonfigurationsbereich mit der rechten Maustaste, ohne dabei ein Gerät auszuwählen, und wählen Sie den Kontextmenübefehl ***Download***.

Nun wird das Fenster für die Eingabe des Gerätekennworts angezeigt. Geben Sie das wie unter Herunterladen der Parameter in bestimmte Geräte beschrieben das Kennwort für die Geräte ein, und klicken Sie auf **OK**.

Fehler beim Herunterladen

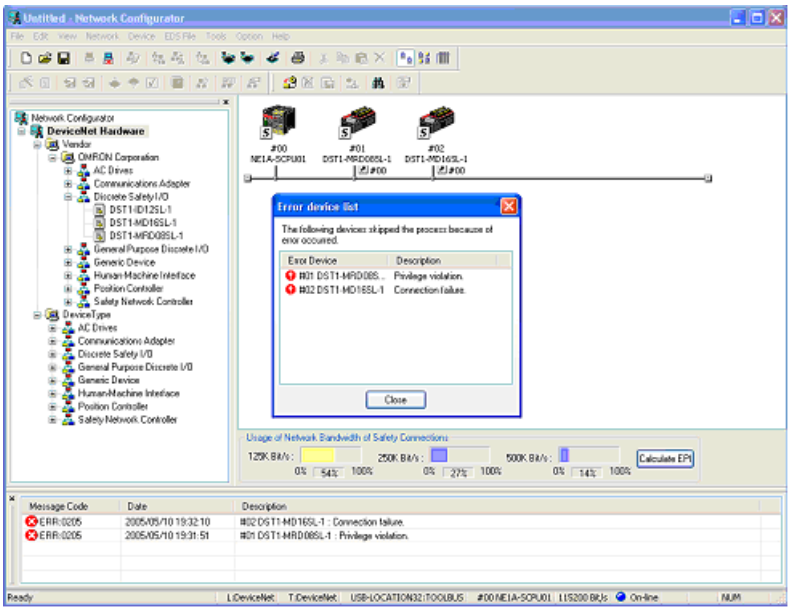
Tritt beim sequenziellen Herunterladen der Geräteparameter in mehrere Geräte ein Fehler auf, wird das folgende Dialogfeld angezeigt.



Wurde nach 15 Sekunden auf keine der Schaltflächen geklickt, setzt der Netzwerkkonfigurator das Herunterladen der Geräteparameter fort. Möchten Sie sofort mit dem Herunterladen der Geräteparameter in das nächste Gerät fortfahren, so klicken Sie auf **Continue**.

Wenn Sie stattdessen auf **Abort** klicken, wird das Herunterladen der Geräteparameter abgebrochen. Die Parameter der nachfolgenden Geräte werden folglich nicht in diese heruntergeladen.

Nach Abschluss des Prozesses wird der aufgetretene Fehler aufgeführt und im Meldungsbereich angezeigt.



2-7-4 Geräteeigenschaften

Im Dialogfeld Property des jeweiligen Geräts können Sie die Geräteinformationen, die Art der Sicherheits- und der Standard-E/A-Punkte sowie die Sicherheitssignaturen einsehen.

Dieses Dialogfeld kann auf verschiedene Arten aufgerufen werden:

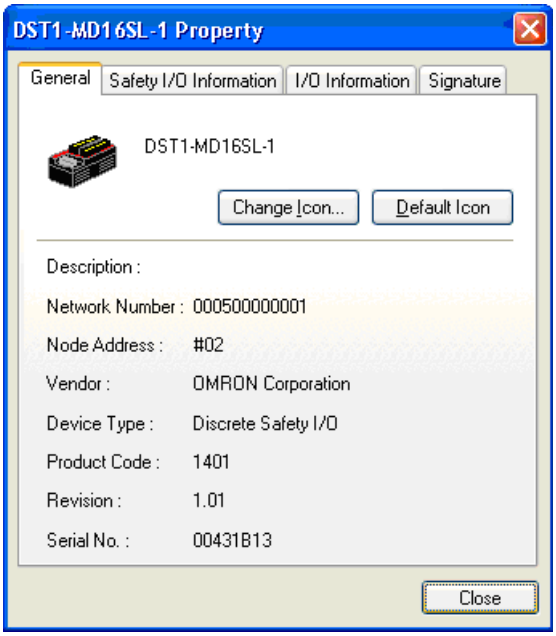
(1) Wählen Sie das Gerät aus, und wählen Sie in der Menüleiste ***Device - Property***.

(2) Wählen Sie das Gerät aus, und klicken Sie in der Werkzeugleiste auf **Device Property**.

(3) Wählen Sie ein Gerät aus, klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät, und wählen Sie den Kontextmenübefehl ***Property***.

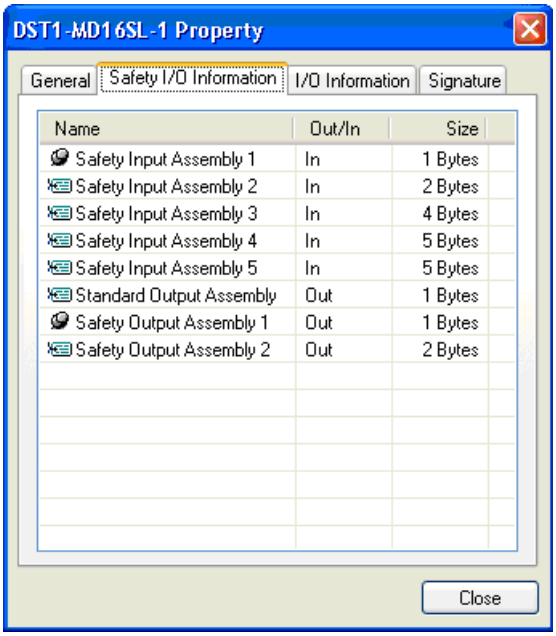
Registerkarte „General“

Auf dieser Registerkarte werden die Geräteinformationen angezeigt. Hier können Sie auch das Symbol ändern, das im Netzwerkkonfigurationsbereich für dieses Gerät angezeigt wird.



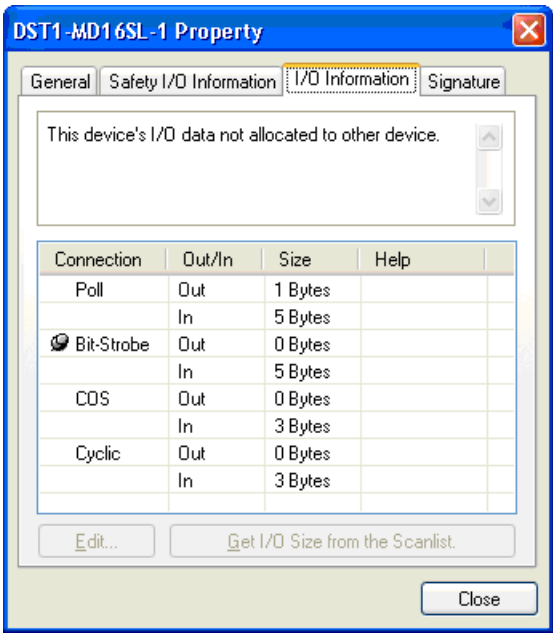
Registerkarte „Safety I/O Information“

Auf dieser Registerkarte werden Klassifizierungsinformationen zur Sicherheits-E/A des Geräts angezeigt.



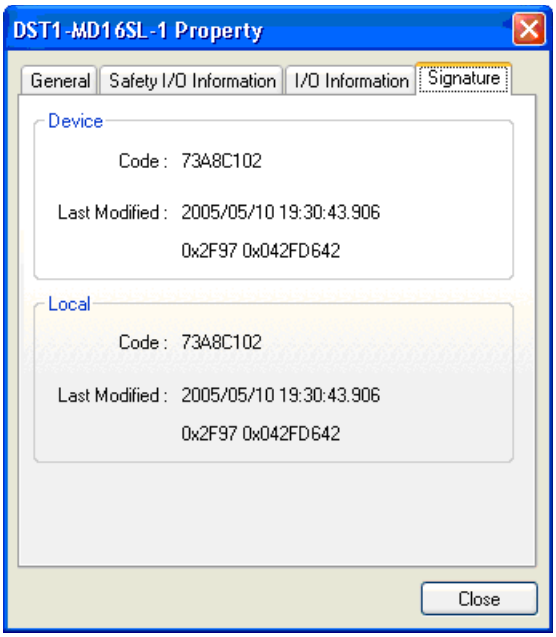
Registerkarte „I/O Information“

Auf dieser Registerkarte werden Klassifizierungsinformationen zur Standard-E/A des Geräts angezeigt.



Registerkarte „Signature“

Auf dieser Registerkarte werden die vom Netzwerkkonfigurator generierte und die im Gerät tatsächlich gespeicherte Sicherheitssignatur angezeigt.



2-8 Verifizierung der Parameter

Nach dem Herunterladen der Parameter in ein Gerät muss eine Verifizierung der Parameter durchgeführt werden, um zu kontrollieren, ob die vom Anwender eingetragenen Daten auch ordnungsgemäß in das Gerät heruntergeladen wurden. Der Anwender muss diese Verifizierung für Sicherheitsgeräte durchführen.

2-8-1 Überprüfung der Geräteparameter

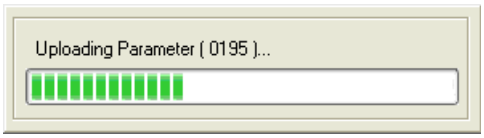
Überprüfen Sie die Parameter nach dem Herunterladen in die Geräte auf eine der folgenden Arten. Dazu ist es erforderlich, dass der Netzwerkkonfigurator online, d. h. mit dem Netzwerk verbunden ist.

(1) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste **Device - Parameter - Verify**.

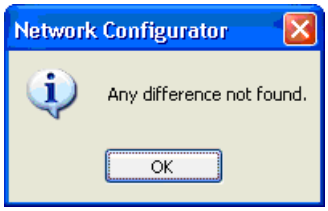
(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Verify Parameter**.

(3) Wählen Sie das Gerät aus, klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät, und wählen Sie den Kontextmenübefehl **Parameter - Verify**.

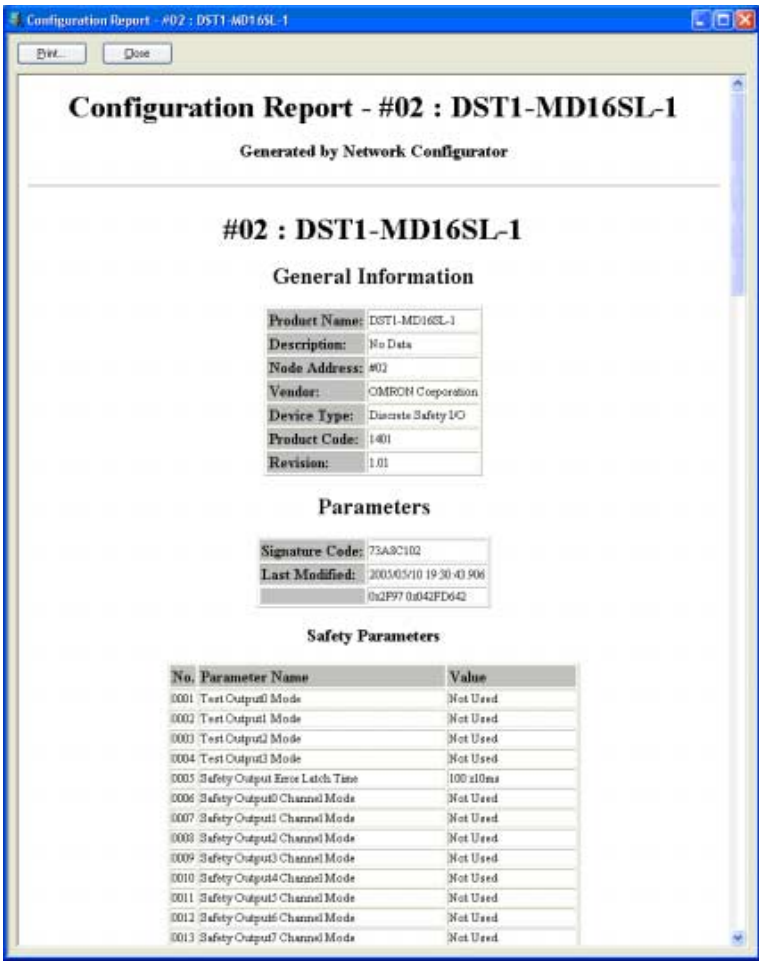
Nun werden die Geräteparameter hochgeladen.



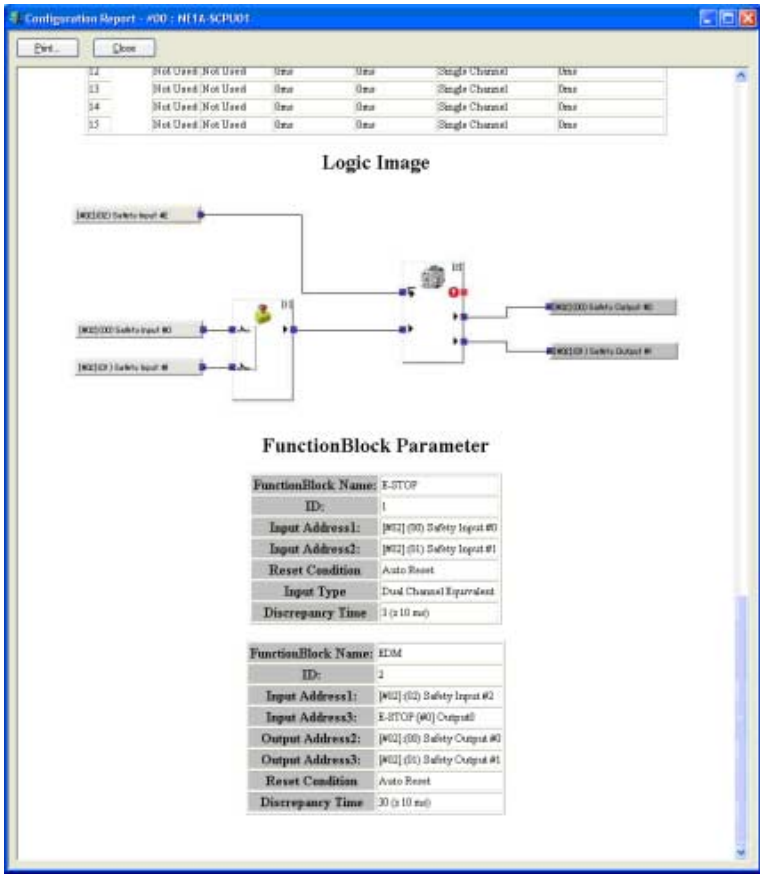
Der Netzwerkkonfigurator überprüft zunächst selbst, ob die hochgeladenen Parameter von den Parametern im virtuellen Netzwerk abweichen. Liegen keine Abweichungen vor, wird das folgende Dialogfeld angezeigt:



Sobald Sie auf **OK** klicken, werden die hochgeladenen Parameter angezeigt.



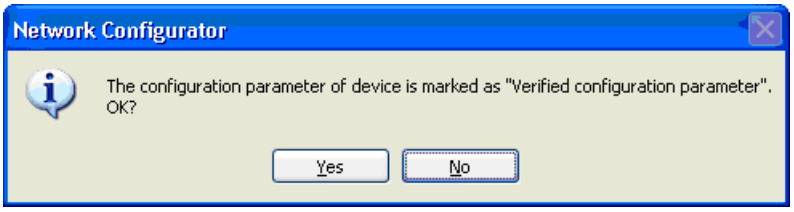
Sie müssen nun überprüfen, ob die angezeigten Parameter Ihren Eingabewerten entsprechen. Handelt es sich bei dem Gerät um einen Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01), wird wie im folgenden Fenster auch das Logikprogramm angezeigt. Kontrollieren Sie, ob das Logikprogramm Ihren Eingaben entspricht.



Hinweis: Die angezeigten Parameter und das Logikprogramm können auch ausgedruckt werden. Klicken Sie zum Ausdrucken auf die Schaltfläche **Print** am oberen linken Rand des Fensters.

Klicken Sie nach Abschluss der Verifizierung auf die Schaltfläche **Close** am oberen linken Rand des Fensters, um das Fenster zu schließen.

Nun wird das folgende Dialogfeld angezeigt:



Stimmen die Parameter mit Ihren Eingaben über ein, so klicken Sie auf **Yes**.

Nach der Überprüfung ändert das zu dem Gerätesymbol im virtuellen Netzwerk gehörende Sicherheitssymbol seine Farbe nach Grün. Dies zeigt an, dass die Überprüfung durchgeführt wurde.

WICHTIG: Überprüfen Sie nach dem Herunterladen der Konfigurationsdaten die Parameter, und überprüfen Sie die Korrektheit der im Gerät gespeicherten Parameter und der Sicherheitssignatur.

Hinweis:
- Nachdem Sie die Parameter aller Geräte überprüft haben, sollten Sie die Netzwerkkonfigurationsdatei unbedingt speichern.
- Das Symbol *Verified configuration parameter* gewährleistet die Korrektheit der in der Netzwerkkonfigurationsdatei enthaltenen Geräteparameter. Diese Information wird in der Netzwerkkonfigurationsdatei gespeichert, nicht jedoch im Gerät selbst. Wird daher eine Netzwerkkonfiguration aus dem Netzwerk hochgeladen, wird das Symbol *Verified configuration parameter* nicht angezeigt, auch wenn die Parameter des Geräts bereits verifiziert wurden.
- Wenn Sie bereits überprüfte Parameter bearbeiten, verschwindet das Symbol *Verified configuration parameter*. In diesem Fall müssen die Geräteparameter erneut verifiziert werden.

Parameterabweichungen

Stellt der Netzwerkkonfigurator bei der Verifizierung der Parameter eine Abweichung fest, wird wie im folgenden Fenster abgebildet der abweichende Parameter gemeinsam mit der Sicherheitssignatur angezeigt.

Überprüfen Sie die Parameterwerte, und wiederholen Sie das Herunterladen der Parameter.

2-9 Konfigurationsschutz

Führen Sie nach dem Verifizieren der Geräteparameter einen Anwendertest durch. Durch Überprüfung aller Funktionen des Geräts im Rahmen des Anwendertests wird sichergestellt, dass die Geräteparameter durch den Anwender überpüft wurden.

Das Konfigurationsschutz-Symbol zeigt die erfolgreiche Durchführung des Anwendertests an.

2-9-1 Schutz der Gerätekonfiguration

Gehen Sie nach dem Anwendertest auf eine der im Folgenden beschriebenen Weisen vor, um die Konfiguration zu schützen. Dazu ist es erforderlich, dass der Netzwerkkonfigurator online, d. h. mit dem Netzwerk verbunden ist. Weiterhin muss die Verifizierung der Geräteparameter durchgeführt worden sein, bevor die Konfiguration geschützt werden kann.

(1) Wählen Sie ein oder mehrere Geräte aus, und wählen Sie in der Menüleiste ***Device - Parameter - Lock***.

(2) Wählen Sie ein oder mehrere Geräte aus, klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte, und wählen Sie den Kontextmenübefehl ***Parameter - Lock***.

Nun wird das Fenster für die Eingabe des Gerätekennworts angezeigt. Geben Sie das Kennwort für die ausgewählten Geräte ein, und klicken Sie auf **OK**.

Wenn Sie für verschiedene Geräte dasselbe Kennwort vergeben haben, können Sie im folgenden Dialogfeld das Kontrollkästchen **Use this password for all device** aktivieren. Auf diese Weise ersparen Sie sich die Eingabe des Kennworts für alle anderen Geräte.

Nach dem Schutz der Konfiguration wird das zu dem Gerätesymbol im virtuellen Netzwerk gehörende Sicherheitssymbol als Schloss angezeigt. Dies zeigt an, dass die Konfiguration geschützt wurde.

WICHTIG: Vom den Schützen der Konfiguration muss der Betrieb des Geräts überprüft werden.

Hinweis:
- Nachdem Sie die Konfiguration aller Geräte geschützt haben, sollten Sie die Netzwerkkonfigurationsdatei unbedingt speichern.
- Das Konfigurationsschutz-Symbol zeigt die erfolgreiche Durchführung des Gerätetests an. Diese Information wird sowohl im Gerät selbst als auch in der Netzwerkkonfigurationsdatei gespeichert.
- Nach dem Schützen der Konfiguration können keine Parameter mehr in das Gerät heruntergeladen werden. Zum Ändern der Parameter muss zunächst der Konfigurationsschutz aufgehoben werden.
- Wenn Sie bereits verifizierte Geräteparameter bearbeiten, verschwindet das Symbol **Verified configuration parameter**. In diesem Fall müssen die Geräteparameter erneut verifiziert werden.

2-9-2 Aufheben des Konfigurationsschutzes

Für die Änderung der Parameter von Geräten, für die ein Konfigurationsschutz eingerichtet wurde, muss zuvor dieser Konfigurationsschutz aufgehoben werden. Das Aufheben des Konfigurationsschutzes kann auf verschiedene Arten erfolgen. Dazu ist es erforderlich, dass der Netzwerkkonfigurator online, d. h. mit dem Netzwerk verbunden ist.

(1) Wählen Sie ein oder mehrere Geräte aus, und wählen Sie in der Menüleiste ***Device - Parameter Unlock***.

(2) Wählen Sie ein oder mehrere Geräte aus, klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte, und wählen Sie den Kontextmenübefehl ***Parameter - Unlock***.

Nun wird das Fenster für die Eingabe des Gerätekennworts angezeigt. Geben Sie wie unter *2-9-1 Schutz der Gerätekonfiguration* (Seite 48) beschrieben das Kennwort für die ausgewählten Geräte ein, und klicken Sie auf **OK**.

Nach Aufhebung des Konfigurationsschutzes wird das zu dem Gerätesymbol im virtuellen Netzwerk gehörende Sicherheitssymbol wieder wie zuvor (Verified Configuration Parameter-Symbol) angezeigt.

Hinweis: Nach der Änderung der Geräteparameter müssen diese zunächst wieder verifiziert werden, bevor die Konfiguration wieder geschützt werden kann.

2-10 Zurücksetzen des Geräts und Änderung des Gerätestatus

In diesem Abschnitt wird erläutert, wie Sicherheitsgeräte zurückgesetzt werden und ihr Status geändert wird. Manche Geräte unterstützen möglicherweise keine Statusänderung.

2-10-1 Möglichkeiten zum Zurücksetzen von Geräten

Es existieren drei Varianten zum Zurücksetzen von Sicherheitsgeräten.

Rücksetzvariante	Beschreibung
Emulate cycling power.	Zurücksetzen wie beim Aus- und Wiedereinschalten der Spannungsversorgung.
Return to the out-of-box configuration, and then emulate cycling power.	Zurücksetzen der im nichtflüchtigen Speicher des Geräts enthaltenen Informationen auf die Standardeinstellungen mit anschließendem Neustart.
Return information except for specified parameters to the out-of-box configuration, and then emulate cycling power.	Zurücksetzen der im nichtflüchtigen Speicher des Geräts enthaltenen Informationen mit Ausnahme der anwenderdefinierten Daten auf die Standardeinstellungen mit anschließendem Neustart.

Im nichtflüchtigen Speicher des Schutzgeräts sind die folgenden Informationen gespeichert:

Typ	Standard-einstellung	Zeitpunkt des Einstellung	Beschreibung
Geräteparameter	Nicht konfiguriert	Herunterladen der Parameter	Vom Anwender erstellte Programme und Parametereinstellungen
Knotenadresse (Software-einstellung)	63	Änderung der Knotenadresse	Knotenadresse beim Einschalten des Geräts mit aktivierter Softwareeinstellung
Baudrate (Software-einstellung)	125 Kbit/s	Änderung der Baudrate	Baudrate beim Einschalten des Geräts mit aktivierter Softwareeinstellung (nur NE1A-SCPU01)
TUNID (Target Unique Node Identifier)	Nicht eingestellt	Erstmaliges Herunterladen der Parameter	Der Bezeichner des lokalen Knotens im Safety Netzwerk in Kombination mit der Netzwerknummer und der Knotenadresse
Kennwort	Kein Kennwort	Änderung des Kennworts	Für ein Gerät eingestelltes Kennwort
CFUNID (Configuration Owning UNID)	Nicht eingestellt	Erstmaliges Herunterladen der Parameter	Eindeutiger Bezeichner (UNID) der Konfigurationsquelle
OCPUNID (Output Connection Point Owning UNID)	Nicht eingestellt	Beim Start der ersten Sicherheits-kommunikation	UNID des Sicherheits-Masters, der eine Sicherheitsausgangsverbindung öffnet

Die oben aufgeführten Informationen sind im nichtflüchtigen Speicher des Geräts gespeichert und werden daher – nachdem sie einmal eingestellt wurden – beim Aus- und Wiedereinschalten der Spannungsversorgung nicht gelöscht. Zum Löschen der Informationen, d. h. zur Rückkehr zu den Standardeinstellungen, wählen Sie eine der Optionen *Return to the out-of-box configuration, and then emulate cycling power* oder *Return to the out-of-box configuration except to preserve the following parameters, and then emulate cycling power*.

⚠ VORSICHT

Werden alte Konfigurationsdaten vor dem Anschluss des Geräts an das Netzwerk nicht gelöscht, kann dies zu einem Ausfall der Sicherheitsfunktionen, Verletzungen und Todesfällen führen.

2-10-2 Zurücksetzen von Geräten

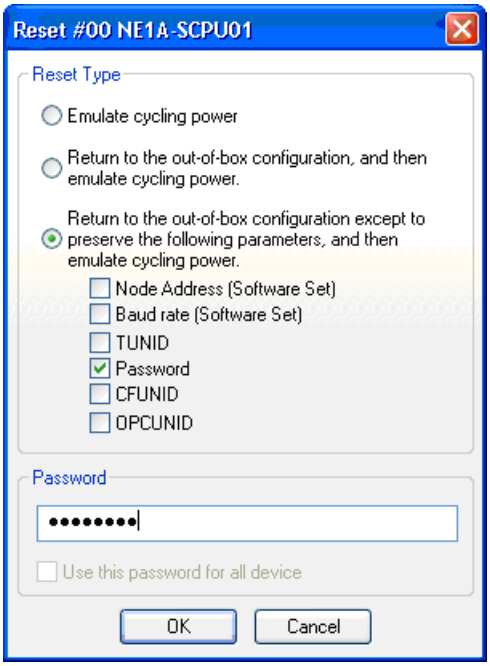
Das Zurücksetzen von Geräten kann auf verschiedene Arten erfolgen. Dazu ist es erforderlich, dass der Netzwerkkonfigurator online, d. h. mit dem Netzwerk verbunden ist.

(1) Wählen Sie ein oder mehrere Geräte aus, und wählen Sie in der Menüleiste ***Device - Reset***.

(2) Wählen Sie ein oder mehrere Geräte aus, klicken Sie mit der rechten Maustaste auf die ausgewählten Geräte, und wählen Sie den Kontextmenübefehl ***Reset***.

Nun wird das Dialogfeld **Reset** für die einzelnen Geräte angezeigt (siehe nachstehendes Beispiel). Wählen Sie die gewünschte Rücksetzvariante aus, geben Sie das Gerätekennwort ein, und klicken Sie dann auf **OK**.

Um beispielsweise die aktuelle Kennworteinstellung mehrerer Geräte mit demselben Kennwort zu erhalten, aber die anderen Informationen auf die Standardeinstellungen zurückzusetzen, wählen Sie die folgenden Einstellungen:



2-10-3 Rücksetzvarianten und Gerätestatus

Welche der Rücksetzvarianten gewählt werden kann, hängt vom aktuellen Gerätestatus ab:

Rücksetzvariante	**Gerätestatus**			
	Sicherheitsverbindung hergestellt und Konfiguration geschützt	Sicherheitsverbindung hergestellt und Konfiguration geschützt	Sicherheitsverbindung nicht hergestellt und Konfiguration geschützt	Sicherheitsverbindung nicht hergestellt und Konfiguration geschützt
Emulate cycling power	Zurücksetzen nicht möglich	Zurücksetzen nicht möglich	Zurücksetzen möglich	Zurücksetzen möglich
Return to the out-of-box configuration, and then emulate cycling power.	Zurücksetzen nicht möglich	Zurücksetzen nicht möglich	Zurücksetzen nicht möglich	Zurücksetzen möglich
Return information except for specified parameters to the out-of-box configuration, and then emulate cycling power.	Zurücksetzen nicht möglich	Zurücksetzen nicht möglich	Zurücksetzen nicht möglich	Zurücksetzen möglich

2-10-4 Ändern des Gerätestatus

Die Änderung des Gerätestatus wird nicht von allen Geräten unterstützt.

Der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) kann zwischen den beiden Betriebsarten IDLE und RUN umschalten. Detailinformationen zu den Betriebsarten des Sicherheitsnetzwerk-Controllers finden Sie im NE1A-SCPU01 Bedienerhandbuch für den Sicherheitsnetzwerk-Controller (Z906).

Bei DST1-Sicherheits-E/A-Modulen besteht keine Notwendigkeit zur Änderung der Betriebsart.

Die Änderung der Betriebsart eines Geräts kann auf verschiedene Arten erfolgen. Dazu ist es erforderlich, dass der Netzwerkkonfigurator online, d. h. mit dem Netzwerk verbunden ist.

(1) Wählen Sie das Gerät aus, und wählen Sie in der Menüleiste **Device - Change Mode**, gefolgt von der gewünschten Betriebsart.

(2) Wählen Sie das Gerät aus, klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät, und wählen Sie den Kontextmenübefehl **Change Mode**, gefolgt von der gewünschten Betriebsart.

Nun wird das Fenster für die Eingabe des Gerätekennworts angezeigt. Geben Sie das Kennwort für die ausgewählten Geräte ein, und klicken Sie auf **OK**.

3-1 Anwendungen

Dieses Kapitel erläutert die Konstruktion eines DeviceNet Safety Netzwerks für die beiden folgenden Fälle:

(1) Konstruktion eines neuen Sicherheitsnetzwerks

(2) Modifizieren eines bestehenden Sicherheitsnetzwerks

3-1-1 Konstruktion eines neuen Sicherheitsnetzwerks

Dieser Abschnitt erläutert die Vorgehensweise für die Einrichtung eines Systems durch Konzeption eines neuen Sicherheitsnetzwerks mithilfe des Netzwerkkonfigurators und anschließendem Herunterladen der Parameter in die Geräte im Netzwerk.

Konzeption und Programmierung

1. Aufrufen des Netzwerkkonfigurators

   Rufen Sie den Netzwerkkonfigurator auf.

   Siehe *2-1-1 Aufrufen und Beenden des Netzwerkkonfigurators* (Seite 27).

2. Erstellen des virtuellen Netzwerks

   Erstellen Sie durch Hinzufügen von Geräten aus der Hardwareliste das virtuelle Netzwerk. Legen Sie außerdem bei Bedarf die Netzwerknummer fest.

   Siehe *2-4 Erstellen eines virtuellen Netzwerks* (Seite 34).

3. Bearbeiten und Programmieren von Geräteparametern

   Legen Sie die Parameter für die im virtuellen Netzwerk konfigurierten DST1-Sicherheits-E/A-Module fest.

   Siehe *Kapitel 4: Bearbeiten der Parameter von Sicherheits-E/A-Modulen* (Seite 69) und *Bedienerhandbuch für Sicherheits-E/A-Module der Serie DST1 (Z904)*.

   Legen Sie die Parameter für den im virtuellen Netzwerk konfigurierten Sicherheitsnetzwerk-Controller NE1A-SCPU01 fest.

   Siehe *Kapitel 5: Bearbeiten der Parameter des Sicherheitsnetzwerk-Controllers* (Seite 79) und *NE1A-SCPU01 Bedienerhandbuch für den Sicherheitsnetzwerk-Controller (Z906)*.

   Programmieren Sie den im virtuellen Netzwerk konfigurierten Sicherheitsnetzwerk-Controller NE1A-SCPU01.

   Siehe *Kapitel 6: Programmierung des Sicherheitsnetzwerk-Controllers* (Seite 97) und *NE1A-SCPU01 Bedienerhandbuch für den Sicherheitsnetzwerk-Controller (Z906)*.

4. Überprüfung der benötigten Netzwerkbandbreite

   Kontrollieren Sie, dass die für die Sicherheits-E/A-Kommunikation benötigte Bandbreite die zulässige Bandbreite des Netzwerks nicht überschreitet. Sollte die zulässige Bandbreite des Netzwerks überschritten werden, ist eine Neuauslegung der Netzwerkkonfiguration, beginnend mit Schritt 2, erforderlich.

   Siehe *3-2 Überprüfung der benötigten Netzwerkbandbreite* (Seite 59).

5. Berechnung und Überprüfung der maximalen Reaktionszeit

   Berechnen Sie die maximale Reaktionszeit aller Sicherheitsketten, und stellen Sie sicher, dass diese den Anforderungen an das System genügt. Sollten die Anforderungen an das System nicht erfüllt sein, ist eine Neuauslegung der Netzwerkkonfiguration, beginnend mit Schritt 2, erforderlich.

   Siehe *3-3 Berechnung und Überprüfung der maximalen Reaktionszeit* (Seite 63).

6. Speichern der Netzwerkkonfigurationsdatei

   Speichern Sie die Netzwerkkonfigurationsdatei mit dem abgeschlossenen Netzwerkentwurf.

   Siehe *2-5-2 Speichern der Netzwerkkonfigurationsdatei* (Seite 38).

7. Beenden des Netzwerkkonfigurators

   Beenden Sie den Netzwerkkonfigurator.

   Die folgenden Operationen erfolgen nach Installation und Verdrahtung des Netzwerks. Hierzu muss der Netzwerkkonfigurator mit dem Netzwerk verbunden werden.

WICHTIG: Weisen Sie jedem Sicherheitsnetzwerk oder Sicherheitssubnetzwerk eine eindeutige Sicherheitsnetzwerknummer zu.

Konfiguration

8. Aufrufen des Netzwerkkonfigurators und Verbinden des Netzwerkkonfigurators mit dem Netzwerk.

   Rufen Sie den Netzwerkkonfigurator auf, und verbinden Sie ihn über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) oder über eine DeviceNet-Schnittstellenkarte mit dem Netzwerk.

   Siehe *2-3 Verbinden mit dem Netzwerk* (Seite 32).

9. Laden der Netzwerkkonfigurationsdatei

   Laden Sie die Netzwerkkonfigurationsdatei mit dem abgeschlossenen Netzwerkentwurf.

   Siehe *2-5-3 Laden von Netzwerkkonfigurationsdateien* (Seite 39).

10. Zurücksetzen von Geräten

    Bei einer Änderung der Konfiguration aufgrund der Ergebnisse des Anwendertests oder beim erneuten Herunterladen der Parameter muss vor dem Herunterladen der neuen Parameter die vorherige Konfiguration gelöscht werden. Setzen Sie dazu das Gerät zurück, indem Sie die Rücksetzvariante auf **Return to the out-of-box configuration, and then emulate cycling power** setzen.

Siehe *3-1-2 Modifizieren eines bestehenden Sicherheitsnetzwerks* (Seite 56).

11. Herunterladen von Geräteparametern

    Laden Sie die Parameter in alle Geräte herunter.

    Siehe *2-7-3 Herunterladen von Geräteparametern* (Seite 41).

12. Verifizierung der heruntergeladenen Geräteparameter und der Sicherheitssignaturen

    Verifizieren Sie die Parameter aller Geräte, und kontrollieren Sie, ob die von Ihnen eingegebenen Geräteparameter und Programme korrekt heruntergeladen und in den Geräten gespeichert wurden.

    Siehe *2-8 Verifizierung der Parameter* (Seite 45).

13. Speichern der Netzwerkkonfigurationsdatei

    Speichern Sie die Netzwerkkonfigurationsdatei, nachdem Sie die Parameter aller Geräte verifiziert haben.

    Siehe *2-5-2 Speichern der Netzwerkkonfigurationsdatei* (Seite 38).

14. Beenden des Netzwerkkonfigurators

    Beenden Sie den Netzwerkkonfigurator.

WICHTIG:
- Verifizieren Sie nach dem Herunterladen der Geräteparameter die Parameter, um sicherzustellen, dass die in den einzelnen Geräten gespeicherten Parameter und Sicherheitssignaturen korrekt sind.
- Wenn Sie für die Einstellung **Open Type** der Sicherheitsverbindung die Einstellung **Open Only** verwenden, müssen Sie kontrollieren, dass der Sicherheits-Master und der Sicherheits-Slave ordnungsgemäß konfiguriert sind.

Anwendertest

15. Anwendertest

    Der Anwender muss persönlich die Geräteparameter und die Operation der Geräte verifizieren, um zu bestätigen, dass die Anforderungen an das Sicherheitssystem erfüllt sind.

16. Aufrufen des Netzwerkkonfigurators und Verbinden des Netzwerkkonfigurators mit dem Netzwerk.

    Rufen Sie den Netzwerkkonfigurator auf, und verbinden Sie ihn über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) oder über eine DeviceNet-Schnittstellenkarte mit dem Netzwerk.

    Siehe *2-3 Verbinden mit dem Netzwerk* (Seite 32).

17. Laden der Netzwerkkonfigurationsdatei

    Laden Sie die Netzwerkkonfigurationsdatei mit den bereits überprüften Parametern.

    Siehe *2-5-3 Laden von Netzwerkkonfigurationsdateien* (Seite 39).

18. Konfigurationsschutz

    Schützen Sie die Konfiguration aller Geräte, um dadurch anzuzeigen, dass die Parameter verifiziert worden sind, und um die Parameter vor irrtümlichen Überschreiben zu schützen.

    Siehe *2-9-1 Schutz der Gerätekonfiguration* (Seite 48).

19. Speichern der Netzwerkkonfigurationsdatei

    Speichern Sie die Netzwerkkonfigurationsdatei mit der geschützten Konfiguration.

    Siehe *2-5-2 Speichern der Netzwerkkonfigurationsdatei* (Seite 38).

20. Beenden des Netzwerkkonfigurators

    Beenden Sie den Netzwerkkonfigurator.

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen vor Inbetriebnahme des Systems geeignete Tests durchgeführt werden, um die Korrektheit der Konfigurationsdaten aller Geräte und deren ordnungsgemäße Funktion sicherzustellen.

WICHTIG:
- Nach der Konfiguration aller Geräte muss ein Anwendertest durchgeführt werden, um die Konfigurationsdaten aller Geräte und deren ordnungsgemäße Funktion zu überprüfen. Weiterhin werden im Rahmen des Anwendertests die Sicherheitssignaturen der einzelnen Geräte überprüft.
- Nach erfolgreichem Abschluss des Anwendertests muss der Konfigurationsschutz aktiviert werden.

Starten des Systems

21. Starten des Systems

    Starten Sie das System.

3-1-2 Modifizieren eines bestehenden Sicherheitsnetzwerks

Dieser Abschnitt erläutert die Vorgehensweise zum Modifizieren eines Sicherheitsnetzwerks nach der Inbetriebnahme des Systems.

Modifizieren des Systems

1. Anhalten des Systems

   Schalten Sie die Spannungsversorgung sich bewegender Systemkomponenten (z. B. Motoren) aus, und halten Sie das System an. Belassen Sie die Spannungsversorgung des Netzwerks und des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) eingeschaltet.
2. Aufrufen des Netzwerkkonfigurators und Verbinden des Netzwerkkonfigurators mit dem Netzwerk.

   Rufen Sie den Netzwerkkonfigurator auf, und verbinden Sie ihn über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) oder über eine DeviceNet-Schnittstellenkarte mit dem Netzwerk.

   Siehe *2-1-1 Aufrufen und Beenden des Netzwerkkonfigurators* (Seite 27) und *2-3 Verbinden mit dem Netzwerk* (Seite 32).
3. Hochladen der Netzwerkkonfiguration

   Laden Sie die Netzwerkkonfiguration hoch, um die aktuelle Netzwerkkonfiguration zu ermitteln.

   Siehe *2-4 Erstellen eines virtuellen Netzwerks* (Seite 34).
4. Aufheben des Konfigurationsschutzes

   Heben Sie den Konfigurationsschutz aller Geräte auf, um die Netzwerkkonfiguration ändern zu können.

   Siehe *2-9-2 Aufheben des Konfigurationsschutzes* (Seite 48).
5. Zurücksetzen von Geräten

   Löschen Sie die Konfiguration eines Geräts, bevor Sie die Geräteparameter und die Knotenadresse ändern. Setzen Sie dazu das Gerät zurück, indem Sie die Rücksetzvariante auf **Return to the out-of-box configuration, and then emulate cycling power** setzen.
6. Beenden des Netzwerkkonfigurators

   Beenden Sie den Netzwerkkonfigurator.
7. Modifizieren des Systems

   Nehmen Sie die der gewünschten Systemmodifikation entsprechenden Änderungen an dem Netzwerk, der Verdrahtung, den Knotenadressen und den Geräten im Netzwerk vor. Neu hinzugefügte Schutzgeräte müssen vorab konfiguriert werden.

⚠ VORSICHT
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen alte Konfigurationsdaten vor dem Anschluss eines Geräts an das Netzwerk gelöscht werden.

⚠ VORSICHT
Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen vor dem Anschluss eines Geräts an das Netzwerk die Knotenadresse und die Baudrate eingestellt werden.

Hinweis: Für die Verwendung der gespeicherten Netzwerkkonfigurationsdatei besteht keinerlei Notwendigkeit, da im Rahmen dieser Vorgehensweise der Konfigurationsschutz der Geräte aufgehoben wird und die Geräte auf ihre Standardkonfiguration zurückgesetzt werden.

Neukonzeption des Systems

8. Aufrufen des Netzwerkkonfigurators

   Rufen Sie den Netzwerkkonfigurator auf, um das Netzwerk neu zu konzipieren.
9. Laden der Netzwerkkonfigurationsdatei

   Laden Sie die gespeicherte Netzwerkkonfigurationsdatei mit der geschützten Konfiguration.

   Siehe *2-5-3 Laden von Netzwerkkonfigurationsdateien* (Seite 39).
10. Modifizieren des virtuellen Netzwerks

    Nehmen Sie durch Änderung der Knotenadressen und Hinzunahme oder Löschen von Geräten die der gewünschten Systemmodifikation entsprechenden Änderungen vor.

    Siehe *2-4 Erstellen eines virtuellen Netzwerks* (Seite 34).
11. Ändern der Geräteparameter und des Programms

    Führen Sie die der gewünschten Systemmodifikation entsprechenden Änderungen der Parameter der im virtuellen Netzwerk konfigurierten DST1-Sicherheits-E/A-Module durch.

    Siehe *Kapitel 4: Bearbeiten der Parameter von Sicherheits-E/A-Modulen* (Seite 69) und *Bedienerhandbuch für Sicherheits-E/A-Module der Serie DST1 (Z904)*.

Führen Sie die der gewünschten Systemmodifikation entsprechenden Änderungen der Parameter des im virtuellen Netzwerk konfigurierten Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) durch.

Siehe *Kapitel 5: Bearbeiten der Parameter des Sicherheitsnetzwerk-Controllers* (Seite 79) und *NE1A-SCPU01 Bedienerhandbuch für den Sicherheitsnetzwerk-Controller (Z906)*.

Führen Sie die der gewünschten Systemmodifikation entsprechenden Änderungen des Programms des im virtuellen Netzwerk konfigurierten Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) durch.

Siehe *Kapitel 6: Programmierung des Sicherheitsnetzwerk-Controllers* (Seite 97) und *NE1A-SCPU01 Bedienerhandbuch für den Sicherheitsnetzwerk-Controller (Z906)*.

12. Verifizierung der benötigten Netzwerkbandbreite

    Kontrollieren Sie, dass die für die Sicherheits-E/A-Kommunikation benötigte Bandbreite die zulässige Bandbreite des Netzwerks nicht überschreitet. Sollte die zulässige Bandbreite des Netzwerks überschritten werden, ist die gewünschte Systemmodifikation einer erneuten kritischen Prüfung zu unterziehen.

    Siehe *3-2 Überprüfung der benötigten Netzwerkbandbreite* (Seite 59).

13. Neuberechnung und Überprüfung der maximalen Reaktionszeit

    Berechnen Sie die maximale Reaktionszeit aller Sicherheitsketten, und stellen Sie sicher, dass diese den Anforderungen an das System genügt. Sollten die Anforderungen an das System nicht erfüllt sein, ist die gewünschte Systemmodifikation einer erneuten kritischen Prüfung zu unterziehen.

    Siehe *3-3 Berechnung und Überprüfung der maximalen Reaktionszeit* (Seite 63).

14. Speichern der Netzwerkkonfigurationsdatei

    Speichern Sie die Netzwerkkonfigurationsdatei mit den durchgeführten Änderungen.

    Siehe *2-5-2 Speichern der Netzwerkkonfigurationsdatei* (Seite 38).

15. Beenden des Netzwerkkonfigurators

    Beenden Sie den Netzwerkkonfigurator.

    Die folgenden Operationen erfolgen nach Durchführung der Änderungen an dem Netzwerksystem. Hierzu muss der Netzwerkkonfigurator mit dem Netzwerk verbunden werden.

WICHTIG:
- Weisen Sie bei der Einrichtung jedem Netzwerk oder Subnetzwerk eine eindeutige Netzwerknummer zu.
- Werden die Parameter eines Sicherheits-Slaves oder eines Standard-Slaves geändert, entsprechen die Parameterinformationen nicht mehr denen im Sicherheits-Master oder Standard-Master, in dem der Slave registriert ist. Aus diesem Grund wird ein gelbes Ausrufezeichensymbol [!] neben dem Symbol für den Slave angezeigt. Wird dieses Symbol angezeigt, müssen Sie die Slave-Informationen überprüfen. Öffnen Sie dazu für den Master das Dialogfeld **Edit Parameter**. Weisen Sie bei der Einrichtung jedem Netzwerk oder Subnetzwerk mit Sicherheits-Slaves eine eindeutige Netzwerknummer zu.

Hinweis: Werden die Geräteparameter einer geschützten Konfiguration geändert, ändert sich die Farbe des Schlüsselsymbols nach Gelb.

Neukonfiguration

16. Aufrufen des Netzwerkkonfigurators und Verbinden des Netzwerkkonfigurators mit dem Netzwerk.

    Rufen Sie den Netzwerkkonfigurator auf, und verbinden Sie ihn über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) oder über eine DeviceNet-Schnittstellenkarte mit dem Netzwerk.

    Siehe *2-3 Verbinden mit dem Netzwerk* (Seite 32).

17. Laden der Netzwerkkonfigurationsdatei

    Laden Sie die Netzwerkkonfigurationsdatei mit den abgeschlossenen Konzeptänderungen.

    Siehe *2-5-3 Laden von Netzwerkkonfigurationsdateien* (Seite 39).

18. Herunterladen von Geräteparametern

    Laden Sie die Parameter in alle Geräte herunter.

    Siehe *2-7-3 Herunterladen von Geräteparametern* (Seite 41).

19. Verifizierung der heruntergeladenen Geräteparameter und der Sicherheitssignaturen

    Verifizieren Sie die Parameter aller Geräte, bei denen ein Symbol anzeigt, dass die Parameter noch nicht verifiziert wurden, und kontrollieren Sie, ob die von Ihnen eingegebenen Geräteparameter und Programme korrekt heruntergeladen und in den Geräten gespeichert wurden.

    Siehe *2-8 Verifizierung der Parameter* (Seite 45).

20. Speichern der Netzwerkkonfigurationsdatei

    Speichern Sie die Netzwerkkonfigurationsdatei, nachdem Sie die Parameter aller Geräte verifiziert haben.

    Siehe *2-5-2 Speichern der Netzwerkkonfigurationsdatei* (Seite 38).

21. Beenden des Netzwerkkonfigurators

    Beenden Sie den Netzwerkkonfigurator.

WICHTIG:
- Überprüfen Sie nach dem Herunterladen der Geräteparameter die Parameter, um sicherzustellen, dass die in den einzelnen Geräten gespeicherten Parameter und Sicherheitssignaturen korrekt sind.
- Wenn Sie für die Einstellung **Open Type** der Sicherheitsverbindung die Einstellung **Open Only** verwenden, müssen Sie kontrollieren, dass der Sicherheits-Master und der Sicherheits-Slave ordnungsgemäß konfiguriert sind.

Hinweis:
- Im Netzwerkkonfigurationsbereich wird die Konfiguration des Geräts als geschützt angezeigt, jedoch wurde der Konfigurationsschutz des tatsächlichen Geräts bereits aufgehoben, so dass die Parameter runterladen werden können.
- Beim Herunterladen von Parametern in ein Gerät, bei dem die Farbe des Schlüsselsymbols aufgrund von Parameteränderungen nach Gelb gewechselt ist, muss das Symbol anschließend wieder den Status vor der Überprüfung annehmen (weißes Symbol [S]).
- Beim Herunterladen von Parametern in ein Gerät, bei dem die Farbe des Schlüsselsymbols nicht gewechselt ist, da keine Parameteränderungen aufgetreten sind, muss das Symbol anschließend wieder den Status annehmen, der den erfolgreichen Abschluss der Überprüfung anzeigt (grünes Symbol [S]).

Zusätzliche Anwendertests

22. Anwendertest

    Der Anwender muss persönlich die Geräteparameter und die Operation der Geräte überprüfen, um zu bestätigen, dass die Anforderungen an das Sicherheitssystem erfüllt sind.
23. Aufrufen des Netzwerkkonfigurators und Verbinden des Netzwerkkonfigurators mit dem Netzwerk.

    Rufen Sie den Netzwerkkonfigurator auf, und verbinden Sie ihn über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) oder über eine DeviceNet-Schnittstellenkarte mit dem Netzwerk.

    Siehe *2-3 Verbinden mit dem Netzwerk* (Seite 32).
24. Laden der Netzwerkkonfigurationsdatei

    Laden Sie die gespeicherte Netzwerkkonfigurationsdatei mit den überprüften Parametern.

    Siehe *2-5-3 Laden von Netzwerkkonfigurationsdateien* (Seite 39).
25. Konfigurationsschutz

    Schützen Sie die Konfiguration aller Geräte, um dadurch anzuzeigen, dass die Parameter überprüft worden sind, und um die Parameter vor irrtümlichen Überschreiben zu schützen.

    Siehe *2-9-1 Schutz der Gerätekonfiguration* (Seite 48).
26. Speichern der Netzwerkkonfigurationsdatei

    Speichern Sie die Netzwerkkonfigurationsdatei mit der geschützten Konfiguration.

    Siehe *2-5-2 Speichern der Netzwerkkonfigurationsdatei* (Seite 38).
27. Beenden des Netzwerkkonfigurators

    Beenden Sie den Netzwerkkonfigurator.

⚠ VORSICHT

Um eine Beeinträchtigung der Sicherheitsfunktionen mit der damit verbundenen Gefahr schwerer Verletzungen zu vermeiden, müssen vor Inbetriebnahme des Systems geeignete Tests durchgeführt werden, um die Korrektheit der Konfigurationsdaten aller Geräte und deren ordnungsgemäße Funktion sicherzustellen.

WICHTIG:
- Nach der Konfiguration aller Geräte muss ein Anwendertest durchgeführt werden, um die Konfigurationsdaten aller Geräte und deren ordnungsgemäße Funktion zu überprüfen. Weiterhin werden im Rahmen des Anwendertests die Sicherheitssignaturen der einzelnen Geräte überprüft.
- Nach erfolgreichem Abschluss des Anwendertests muss der Konfigurationsschutz aktiviert werden.

Neustart des Systems

28. Starten des Systems

    Starten Sie das System.

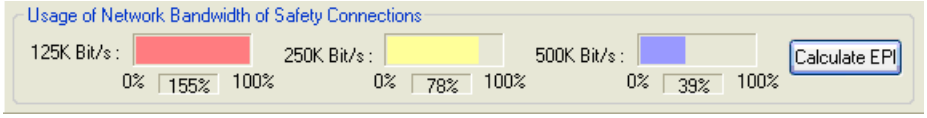
3-2 Überprüfung der benötigten Netzwerkbandbreite

Annähernd 100 % der Netzwerkbandbreite von DeviceNet können tatsächlich verwendet werden. Führen die Einstellungen zu einer Überschreitung der zulässigen Bandbreite, kommt es jedoch zum Auftreten von Zeitüberschreitungsfehlern.

Dieser Abschnitt erläutert die Vorgehensweise zur Überprüfung der für die Sicherheits-E/A-Kommunikation im konzipierten Netzwerk verwendeten Netzwerkbandbreite und zur Berechnung des EPIs (Nenn-Paketintervall) anhand des Bandbreitennutzungsfaktors.

3-2-1 Überprüfung der für die Sicherheits-E/A-Kommunikation benötigten Netzwerkbandbreite

Im unteren Abschnitt des Netzwerkkonfigurationsbereichs zeigt der Netzwerkkonfigurator den für die Sicherheits-E/A-Kommunikation der im virtuellen Netzwerk eingerichteten Verbindungen verwendeten prozentualen Anteil an der Netzwerkbandbreite an.



Die Anzeige des verwendeten prozentualen Anteils der Netzwerkbandbreite erfolgt separat für alle Baudraten.

Ausschließliche Verwendung von Sicherheits-E/A-Kommunikation

Bei ausschließlicher Verwendung von Sicherheits-E/A-Kommunikation kann der für die Sicherheits-E/A-Kommunikation verwendete prozentuale Anteil der Netzwerkbandbreite problemlos bis zu ca. 90 % betragen.

Überschreitet der prozentuale Anteil 90 %, so bestimmen Sie das durchschnittliche EPI (siehe nachstehenden Abschnitt), und verwenden Sie diesen Wert als Referenz für das Festlegen der Verbindungen.

WICHTIG: Behalten Sie für das Herstellen von Verbindungen und für die Kommunikationsaktivität des Netzwerkkonfigurators mindestens 10 % der Netzwerkbandbreite in Reserve. Verwendet die Anwendung Kommunikation mit expliziten Meldungen, wird zusätzliche Netzwerkbandbreite benötigt. Bestimmen Sie in diesem Fall basierend auf der Menge der Daten und der Häufigkeit der Kommunikation die erforderliche Netzwerkbandbreite für die Kommunikation mit expliziten Meldungen.

Gemeinsame Verwendung von Sicherheits- und Standard-E/A-Kommunikation

Finden im Netzwerk sowohl Sicherheits- als auch Standard-E/A-Kommunikation statt, muss die erforderliche Netzwerkbandbreite für jede dieser Kommunikationsarten separat bestimmt werden. In diesem Fall müssen Sie kontrollieren, dass die für die Sicherheits-E/A-Kommunikation benötigte Bandbreite den bestimmten Wert nicht überschreiten.

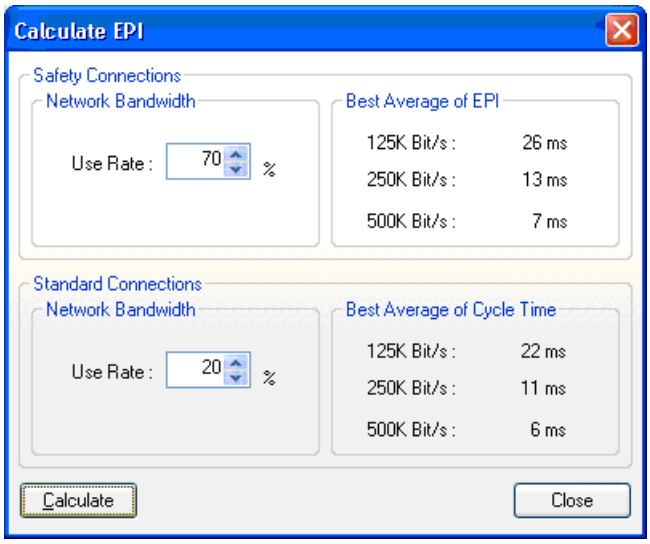
Der Netzwerkkonfigurator kann das durchschnittliche EPI berechnen. Hierfür müssen Sie die für die verschiedenen Kommunikationsarten benötigte Netzwerkbandbreite eingeben.

3-2-2 Zuteilung von Netzwerkbandbreite

Die Berechnung des mittleren EPIs für die Sicherheits- und die Standard-E/A-Kommunikation erfolgt durch die Eingabe des Bandbreitennutzungsfaktors für die beiden Kommunikationsarten in den Netzwerkkonfigurator.

Gehen Sie zum Berechnen des EPIs wie folgt vor:

1. Richten Sie mithilfe des Netzwerkkonfigurators das vorgesehene virtuelle Netzwerk ein.
2. Klicken Sie im unteren Abschnitt des Netzwerkkonfigurationsbereichs auf **EPI Calculation**.
3. Geben Sie die für die Sicherheits-E/A-Kommunikation und die für die Standard-E/A-Kommunikation benötigte Netzwerkbandbreite ein, und klicken Sie auf **Calculate**.
4. Für jede einzelne Baudrate wird nun das mittlere EPI für alle Verbindungen der Sicherheits-E/A-Kommunikation sowie die Kommunikationszykluszeit für die Standard-E/A-Kommunikation angezeigt. Überprüfen Sie das EPI für die Sicherheits-E/A-Kommunikation sowie die Kommunikationszykluszeit des Standard-Masters für die verwendete Baudrate.



WICHTIG:

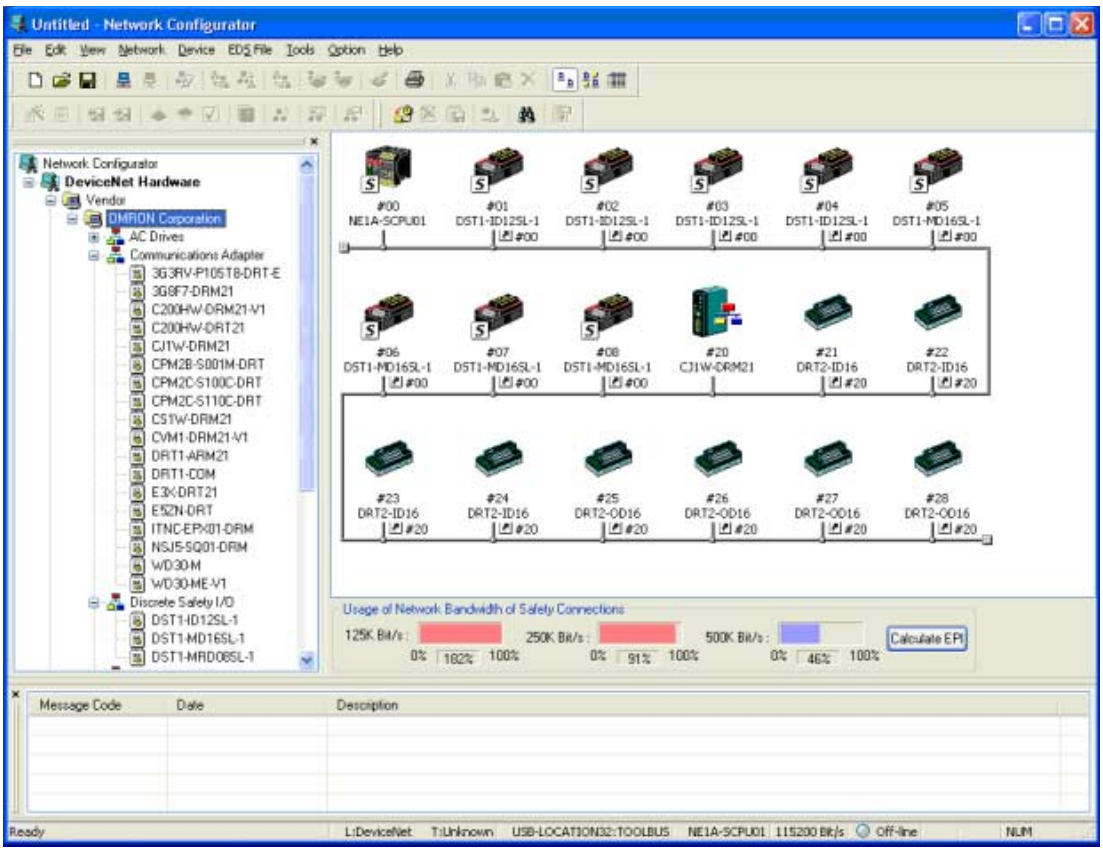
- Behalten Sie für das Herstellen von Verbindungen und für die Kommunikationsaktivität des Netzwerkkonfigurators mindestens 10 % der Netzwerkbandbreite in Reserve. Verwendet die Anwendung Kommunikation mit expliziten Meldungen, wird zusätzliche Netzwerkbandbreite benötigt. Bestimmen Sie in diesem Fall basierend auf der Menge der Daten und der Häufigkeit der Kommunikation die erforderliche Netzwerkbandbreite für die Kommunikation mit expliziten Meldungen.
- Bei dem Ergebnis dieser Berechnung handelt es sich um einen Mittelwert für alle Sicherheitsverbindungen. Verwenden Sie diesen Wert als Anhaltswert. Passen Sie das EPI für das gesamte Netzwerk an, indem Sie das EPI für Verbindungen, die eine kurze Reaktionszeit erfordern, verkürzen, und das EPI für Verbindungen, die keine derart schnelle Reaktion erfordern, verlängern.
- Kontrollieren Sie, dass der im unteren Abschnitt des Netzwerkkonfigurationsbereichs angezeigte Nutzungsfaktor den zugeteilten Wert nicht überschreitet, wenn Sie basierend auf den Ergebnissen der Berechnung das EPI für das gesamte Netzwerk anpassen. Wird die berechnete Bandbreite nicht ordnungsgemäß den Standardverbindungen zugewiesen, kann es zum Auftreten von Zeitüberschreitungsfehlern bei der Kommunikation kommen, da die Sicherheits-E/A-Kommunikation Vorrang vor der Standard-E/A-Kommunikation hat.
- Die insgesamt für Sicherheits- und die Standardverbindungen verwendete Netzwerkbandbreite darf maximal 90 % des Maximalwerts betragen, d. h., mindestens 10 % der verfügbaren Bandbreite müssen für die Kommunikation mit expliziten Meldungen reserviert bleiben.
- Führen Sie einen Anwendertest durch, um sicherzustellen, dass es mit den eingestellten Werten keine Probleme gibt.

Hinweis:

- Soll im Netzwerk keine Standard-E/A-Kommunikation stattfinden, setzen Sie die für Standardverbindungen verwendete Netzwerkbandbreite auf Null.
- Die Auflösung für das EPI beträgt 1 ms. Bei Verwendung des berechneten Werts ist die zu verwendende Netzwerkbandbreite daher möglicherweise kleiner als der zugeteilte Wert.

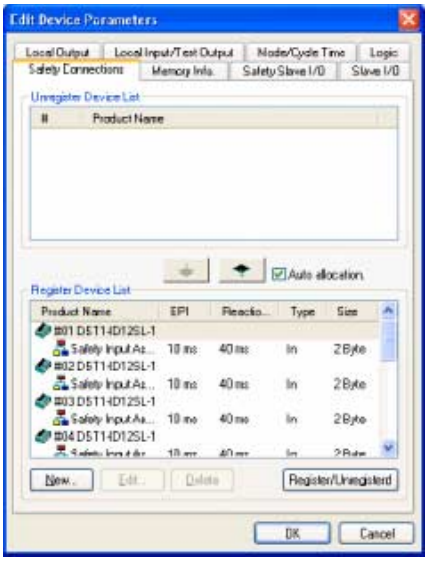
3-2-3 EPI-Berechnung – Ein Beispiel

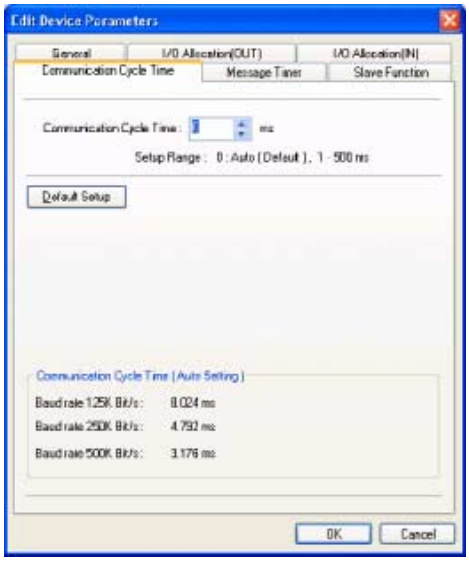
Anhand der folgenden Netzwerkkonfiguration wird exemplarisch die Berechnung des EPIs demonstriert. Die Baudrate beträgt 500 Kbit/s.



Der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) richtet Sicherheitsverbindungen zwischen vier Sicherheits-Eingangsmodulen DST1-ID12SL-1 und vier Sicherheits-E/A-Modulen DST1-MD16SL-1 ein. Für alle Sicherheitsverbindungen werden die Standardwerte verwendet, das EPI beträgt 10 ms.

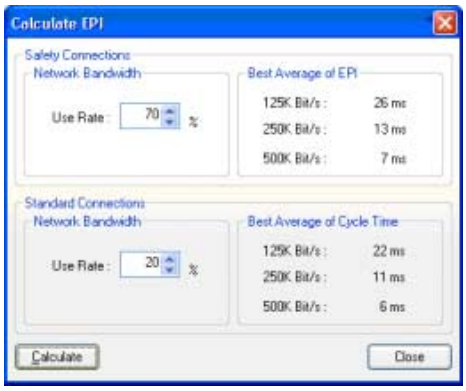
Weiterhin richtet die Standard-SPS CJ1W-DRM21 Standardverbindungen zwischen vier Eingangsmodulen DRT2-ID16 und vier Ausgangsmodulen DRT2-OD16 ein. Für alle Standardverbindungen werden die Standardwerte verwendet; die Kommunikationszykluszeit der Standard-SPS CJ1W-DRM21 wird automatisch gesetzt, jedoch versucht die SPS, mit einer Zykluszeit von ca. 3,2 ms zu operieren.



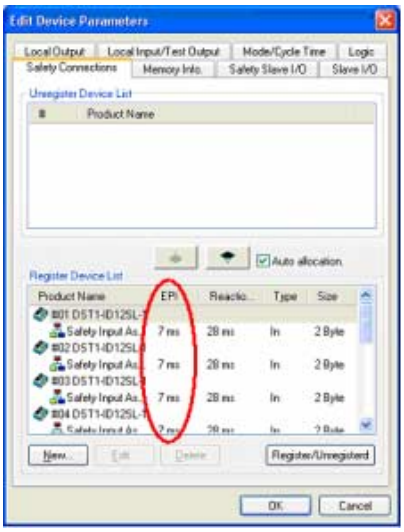


In diesem Fall teilen wir 70 % der verfügbaren Netzwerkbandbreite für Sicherheitsverbindungen und 20 % für Standardverbindungen zu.

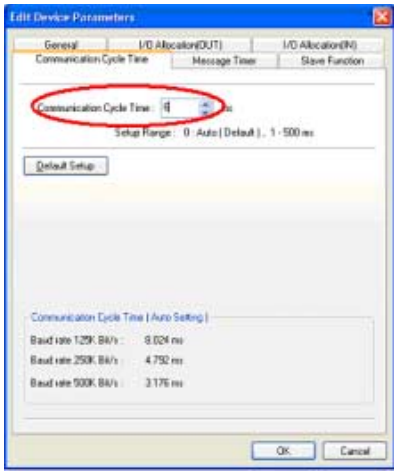
Den Berechnungsergebnissen können Sie entnehmen, dass das EPI für die Sicherheitsverbindungen auf 7 ms und der Kommunikationszyklus des Standard-Masters auf 6 ms eingestellt werden kann.



Setzen Sie entsprechend der Berechnungsergebnisse das EPI aller durch den Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) unterhaltenen Sicherheitsverbindungen auf 7 ms.



Setzen Sie analog die Kommunikationszykluszeit der Standard-SPS CJ1W-DRM21 auf 6 ms.



3-3 Berechnung und Überprüfung der maximalen Reaktionszeit

Der letzte Schritt bei der Konzeption des Netzwerks besteht aus der Berechnung der Reaktionszeit der Sicherheitsketten. Der Anwender muss persönlich überprüfen, dass die Reaktionszeit aller Sicherheitsketten den Anforderungen an das System genügt.

3-3-1 Reaktionszeit – Das Konzept

Die Reaktionszeit ist die maximale Zeitspanne zwischen dem Ansprechen eines Eingangsgeräts und der Betätigung (Ein- oder Ausschalten) des Ausgangsgeräts unter Berücksichtigung von Fehlern und Ausfällen in den Sicherheitsketten. Die Reaktionszeit ist der maßgebliche Faktor für die Berechnung des Sicherheitsabstands.

Die Reaktionszeit wird für jede einzelne Sicherheitskette berechnet. Im Folgenden finden Sie einige typische Beispiele für Sicherheitsketten:

(1) Standalone-System (Sicherheitsnetzwerk-Controller NE1A-SCPU01)

(2) Dezentrale Eingabe / Lokale Ausgabe am Sicherheitsnetzwerk-Controller NE1A-SCPU01

(3) Lokale Eingabe am Sicherheitsnetzwerk-Controller NE1A-SCPU01 / Dezentrale Ausgabe

(4) Dezentrale Eingabe / Dezentrale Ausgabe

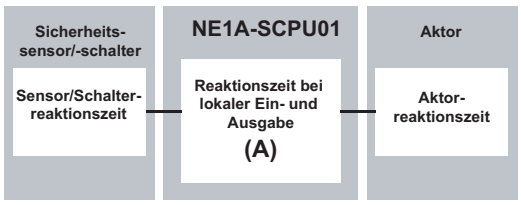
Hinweis: Selbst beim Auftreten von Fehlern und Ausfällen in den Sicherheitsketten ist die maximale Reaktionszeit durch die Ausgangs-Ausschaltzeit nach oben beschränkt.

3-3-2 Berechnung der maximalen Reaktionszeit

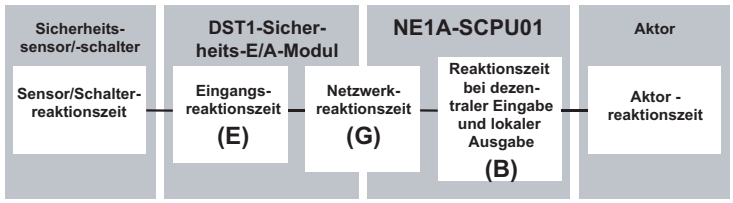
Komponenten der Reaktionszeit

Im Folgenden finden Sie eine Aufstellung über die Komponenten, aus denen sich die Reaktionszeit der einzelnen Sicherheitsketten zusammensetzt.

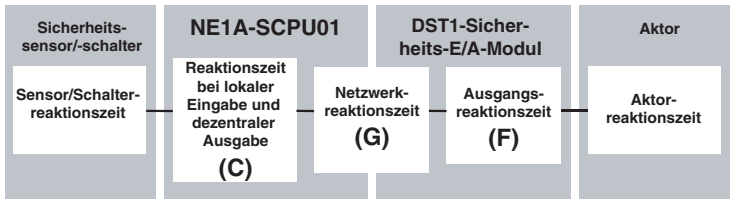
(1) Standalone-System (Sicherheitsnetzwerk-Controller NE1A-SCPU01)



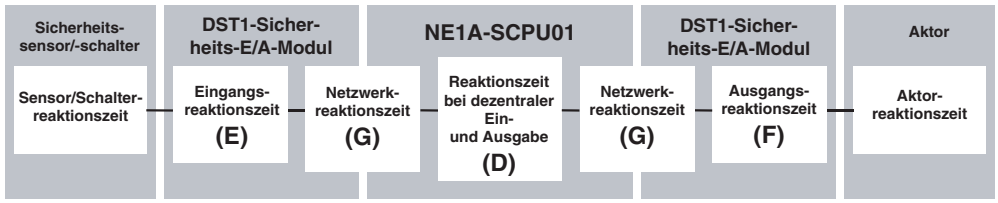
(2) Dezentrale Eingabe / Lokale Ausgabe am Sicherheitsnetzwerk-Controller NE1A-SCPU01



(3) Lokale Eingabe am Sicherheitsnetzwerk-Controller NE1A-SCPU01 / Dezentrale Ausgabe



(4) Dezentrale Eingabe / Dezentrale Ausgabe



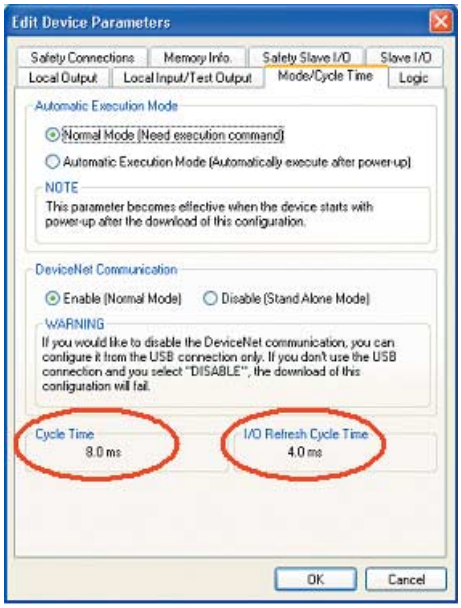
Formeln für die Berechnung der maximalen Reaktionszeit

	Komponente	Formel
A	Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei lokaler Ein- und Ausgabe (ms)	Ein-/Ausschaltverzögerung + E/A-Aktualisierungs-zykluszeit + 2 * Zykluszeit des Sicherheitsnetz-werk-Controllers NE1A-SCPU01 + 2,5
B	Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei dezentraler Eingabe und lokaler Ausgabe (ms)	Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 + 2,5
C	Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei lokaler Eingabe und dezentraler Ausgabe (ms)	Ein-/Ausschaltverzögerung + E/A-Aktualisierungs-zykluszeit + 2 * Zykluszeit des Sicherheitsnetz-werk-Controllers NE1A-SCPU01
D	Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei dezentraler Ein- und Ausgabe (ms)	Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01
E	Eingangsreaktionszeit des DST1-Sicherheits-E/A-Moduls (ms)	Ein-/Ausschaltverzögerung + 16,2
F	Ausgangsreaktionszeit des DST1-Sicherheits-E/A-Moduls (ms)	6,2 + Relaisansprechzeit (nur DST1-MRD08SL-1)
G	Netzwerkreaktionszeit (ms)	Berechnungsergebnis des Netzwerkkonfigurators

WICHTIG: Wird der Ausgang eines Funktionsblocks in einem Sicherheitsnetzwerk-Controller-Programm zur Eingangsseite des Funktionsblocks zurückgeführt, muss die Zykluszeit des Sicherheits-netzwerk-Controllers NE1A-SCPU01 zur Reaktionszeit der Sicherheitskette addiert werden.

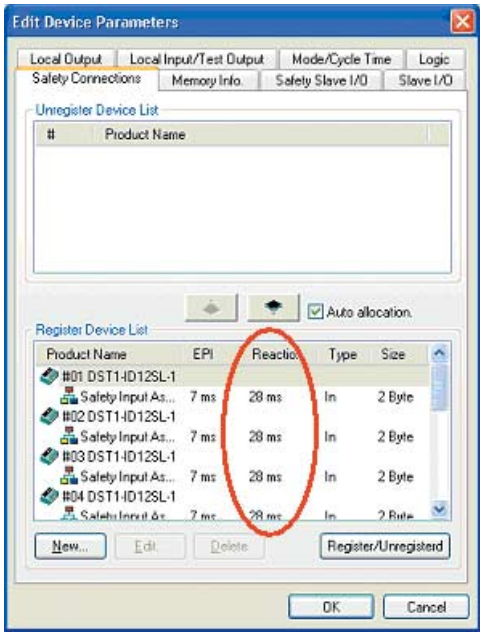
Überprüfen Sie die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01, die E/A-Aktualisierungs-zykluszeit und die Netzwerkreaktionszeit im Netzwerkkonfigurator.

Überprüfen Sie auf der Registerkarte **Mode/Cycle Time** des Dialogfelds **Edit Device Parameters** für den



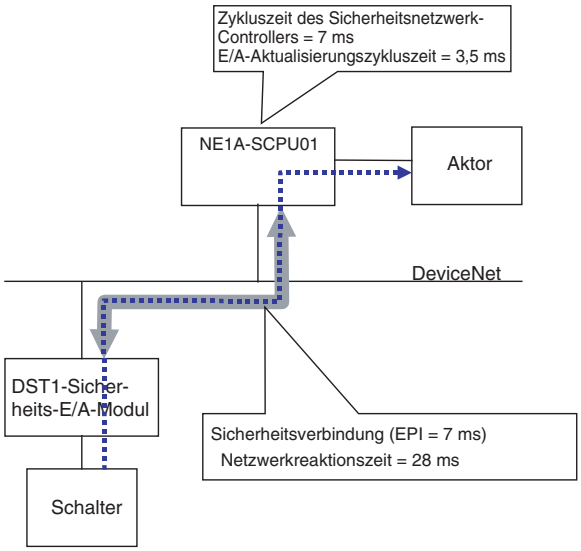
Sicherheitsnetzwerk-Controller NE1A-SCPU01 die Zykluszeit und die E/A-Aktualisierungszeit.

Überprüfen Sie auf der Registerkarte **Safety Connection** des Dialogfelds **Edit Device Parameters** für den Sicherheitsnetzwerk-Controller NE1A-SCPU01 die Netzwerkreaktionszeit.



Berechnung der maximalen Reaktionszeit – Ein Beispiel

Beispiel 1: Dezentrale Eingabe / Lokale Ausgabe am Sicherheitsnetzwerk-Controller NE1A-SCPU01



Maximale Reaktionszeit (ms)

= Schalterreaktionszeit

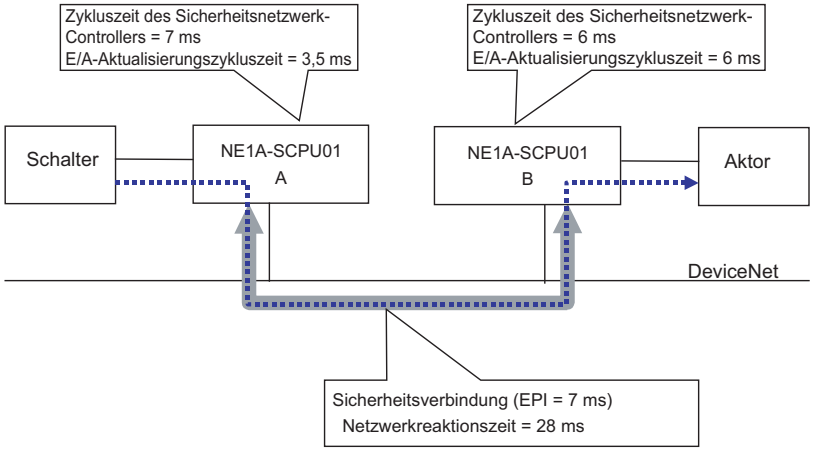
- \+ Eingangsreaktionszeit des DST1-Sicherheits-E/A-Moduls
- \+ Netzwerkreaktionszeit
- \+ Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei dezentraler Eingabe und lokaler Ausgabe
- \+ Aktorreaktionszeit

= Schalterreaktionszeit

- \+ Ein-/Ausschaltverzögerung (DST1-Sicherheits-E/A-Modul) + 16,2
- \+ 28
- \+ 7 + 2,5
- \+ Aktorreaktionszeit

= 53.7 + Ein-/Ausschaltverzögerung + Schalterreaktionszeit + Aktorreaktionszeit

Beispiel 2: Lokale Eingabe / Dezentrale Ausgabe



Maximale Reaktionszeit (ms)

= Schalterreaktionszeit
- \+ Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 bei lokaler Eingabe und dezentraler Ausgabe
- \+ Netzwerkreaktionszeit
- \+ Reaktionszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01-B bei dezentraler Eingabe und lokaler Ausgabe
- \+ Aktorreaktionszeit

= Schalterreaktionszeit
- \+ Ein-/Ausschaltverzögerung (NE1A-SCPU01) + 3,5 + 7 2
- \+ 28
- \+ 6 + 2,5
- \+ Aktorreaktionszeit

= 54,0 + Ein-/Ausschaltverzögerung + Schalterreaktionszeit + Aktorreaktionszeit

3-3-3 Überprüfung der maximalen Reaktionszeit

Kontrollieren Sie, dass die berechnete maximale Reaktionszeit aller Sicherheitsketten den Anforderungen an das System entspricht. Sollte die Reaktionszeit die Systemanforderungen nicht erfüllen, muss der Netzwerkentwurf einer kritischen Prüfung unterzogen werden. Die folgenden Aspekte können dazu beitragen, dass die maximale Reaktionszeit den Anforderungen an das System entspricht.

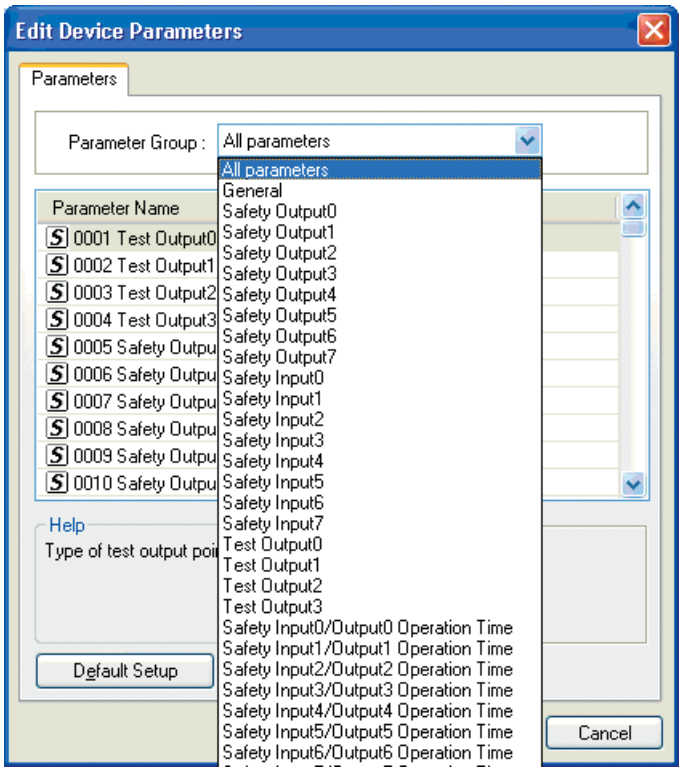
- Eine Verkürzung des EPIs führt zu einer Verkürzung der Netzwerkreaktionszeit. Eine Verkürzung des EPIs führt allerdings auch zu einer Einschränkung der für andere Verbindungen zur Verfügung stehenden Netzwerkbandbreite.
- Die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) wird ausgehend von der Programmgröße, der Anzahl der Verbindungen usw. automatisch berechnet. Für Sicherheitsketten, die beispielsweise eine schnellere Reaktionszeit erfordern, können auch andere Ausführungen des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) eingesetzt werden.

Kapitel 4: Bearbeiten der Parameter von Sicherheits-E/A-Modulen

4-1 Bearbeiten von Parametern

4-1-1 Parametergruppen

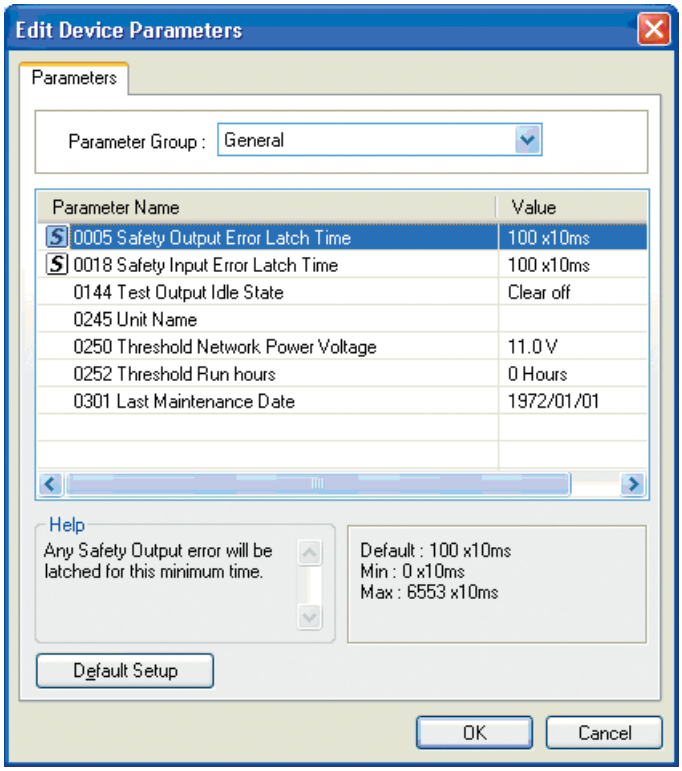
Die Parameter für DST1-Sicherheits-E/A-Module werden in verschiedene Gruppen unterteilt: allgemeine Parameter, Parameter für die einzelnen Sicherheitseingänge, Parameter für die einzelnen Testausgänge, Parameter für die einzelnen Sicherheitsausgänge und Betriebszeitparameter. Der Wechsel zwischen den angezeigten und zu bearbeitenden Parametergruppen erfolgt mithilfe des Listenfelds *Parameter Group*. Aufgrund der Vielfalt der Parameter der DST1-Sicherheits-E/A-Module erleichtert die separate Darstellung der einzelnen Parametergruppen das Bearbeiten der Parameter.



Parameter, bei denen das Symbol S angezeigt wird, sind für Sicherheitsanwendungen von Bedeutung.

4-1-2 Parametergruppe „General“

In diesem Abschnitt werden die Parameter der Parametergruppe „General“ erläutert.



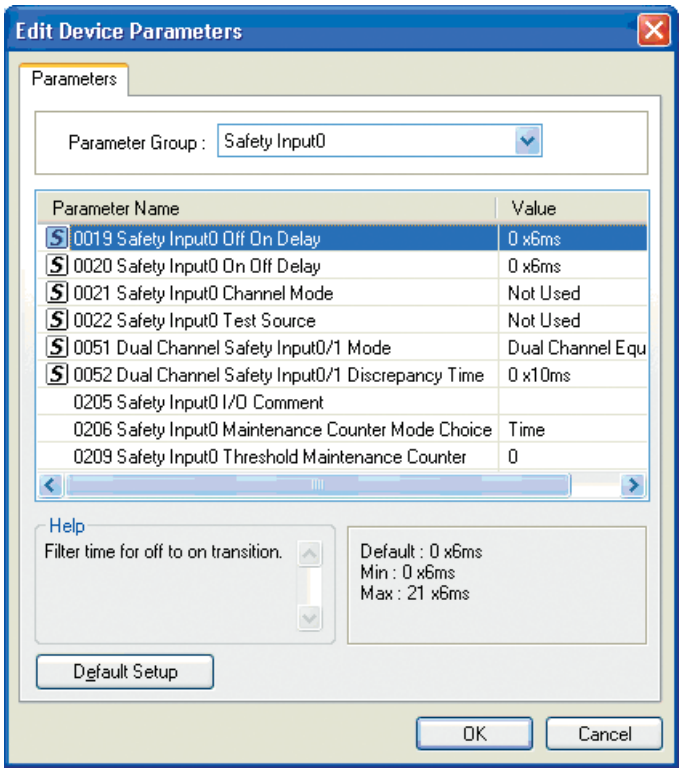
	Parameter	Einstellungen	Beschreibung	Standard-einstellung
S	Output Error Latch Time	0 bis 65.530 ms (in Schritten von 10 ms)	Dieser Parameter ist allen Sicherheits-ausgängen gemeinsam. Er bestimmt die Zeitdauer, für die der Fehlerzustand aktiviert wird, wenn ein Fehler in einem dieser Ausgänge auf-tritt. Auch nach Behebung der Fehler-ursache bleibt der Fehlerzustand für die hier eingestellte Zeitdauer aktiviert.	1.000 ms
S	Input Error Latch Time	0 bis 65.530 ms (in Schritten von 10 ms)	Dieser Parameter ist allen Sicherheits-eingängen und Testausgängen gemeinsam. Er bestimmt die Zeitdauer, für die der Fehlerzustand aktiviert wird, wenn ein Fehler in einem dieser Ein- bzw. Ausgänge auftritt. Auch nach Behebung der Fehlerursache bleibt der Fehlerzustand für die hier eingestellte Zeitdauer aktiviert.	1.000 ms
	Test Output Idle State	Clear off	Dieser Parameter ist allen Testaus-gängen gemeinsam, bei denen der Parameter *Test Output Mode* auf *Standard Output* eingestellt ist. Er bestimmt den Ausgangszustand des Testausgangs beim Empfangen von Leerlaufdaten.	Clear off
		Keep output data		
	Unit Name	max. 32 Zeichen	Mithilfe dieses Parameters kann ein anwenderdefinierter Name für das Sicherheits-E/A-Modul festgelegt wer-den. Der eingestellte Name wird im Sicherheits-E/A-Modul gespeichert und in der Netzwerkkonfiguration angezeigt.	Keine Standard-einstellung

	Parameter	Einstellungen	Beschreibung	Standard-einstellung
	Threshold Network Power Voltage	8,0 bis 30,0 V	Dieser Parameter definiert den Grenzwert für die Versorgungsspannung des Netzwerks. Fällt die Spannung unter diesen Grenzwert, wird das entsprechende Bit im allgemeinen Status auf EIN gesetzt.	11,0 V
	Threshold Run Hours	0 bis 429.496.729 Stunden	Dieser Parameter definiert den Grenzwert für die Betriebsdauer des Moduls. Überschreitet die Betriebsdauer des Moduls den hier eingestellten Grenzwert, wird das entsprechende Bit im allgemeinen Status auf EIN gesetzt.	0 Stunden
	Last Maintenance Date	1.1.1972 bis 19.1.2039	Dieser Parameter enthält das Datum der letzten Wartung des Sicherheits-E/A-Moduls.	1.1.1972

4-1-3 Parametergruppen für die einzelnen Sicherheitseingänge

In diesem Abschnitt werden die Parameter der Parametergruppen für die einzelnen Sicherheitseingänge erläutert.

Hierbei werden die Parameter jeweils eines Sicherheitseingangs zu einer Gruppe zusammengefasst.



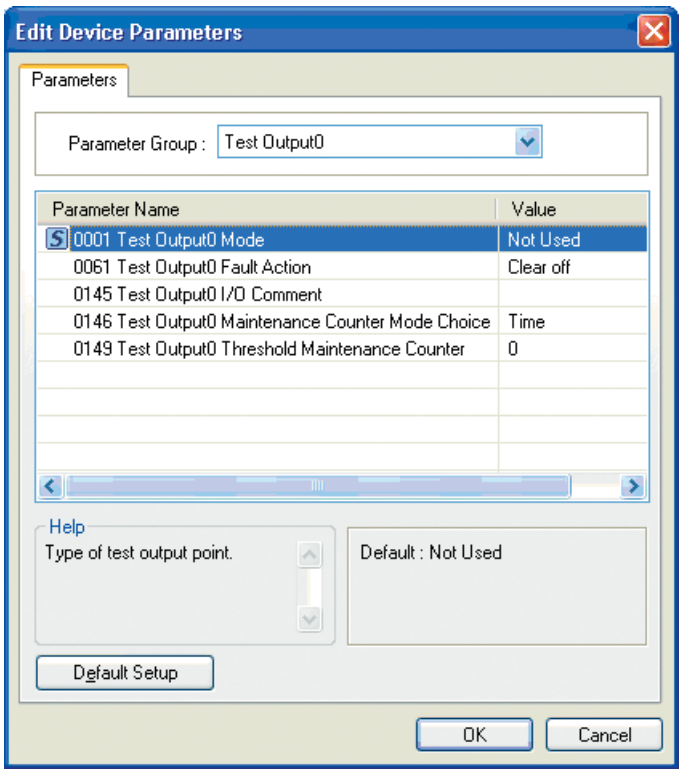
	Parameter	Einstellungen	Beschreibung	Standard-einstellung
S	Off On Delay	0 bis 126 ms (in Schritten von 6 ms)	Eingangseinschaltverzögerungszeit.	0 ms
S	Off On Delay	0 bis 126 ms (in Schritten von 6 ms)	Eingangsausschaltverzögerungszeit.	0 ms
S	Safety Input Channel Mode	Not used.	Dieser Sicherheitseingang wird nicht verwendet. (Es ist kein externes Eingangsgerät angeschlossen.)	Not used.
		Test pulse from test out	Anschluss eines Geräts mit einem Kontaktausgang in Kombination mit einem Testausgang. Bei Auswahl dieses Modus muss außerdem für den Parameter *Test Source* der als Testquelle zu verwendende Testausgang ausgewählt und der Parameter *Test Output Mode* dieses Testausgangs auf *Pulse Test Output* eingestellt werden. Diese Option ermöglicht es, Verbindungen zwischen der Eingangssignalleitung und der Spannungsversorgung (+) sowie Querschlüsse mit anderen Eingangssignalleitungen zu erkennen.	
		Used as a safety input.	Anschluss eines Sicherheitsgeräts mit Halbleiterausgang (z. B. Sicherheitslichtgitter).	
		Used as a standard input.	Anschluss eines Standardgeräts (d. h. eines nicht sicherheitsrelevanten Geräts).	

	Parameter	Einstellungen	Beschreibung	Standard-einstellung
S	Test Source	Not used.	Ist der Parameter *Safety Input Channel Mode* eines Sicherheitseingangs auf *Test Pulse from Test Out* eingestellt, muss dieser Parameter auf den in Verbindung mit dem Sicherheitseingang zu verwendenden Testausgang eingestellt werden. Der Parameter *Test Output Mode* des betreffenden Testausgangs muss auf *Pulse Test Output* gesetzt werden.	Not used.
		Test Output 0		
		Test Output 1		
		Test Output 2		
		Test Output 3		
S	Dual Channel Safety Input Mode	Single Channel	Betrieb des Sicherheitseingangs im Einkanalmodus. Wird dieser Parameter eines Sicherheitseingangs auf *Single Channel* gesetzt, wird der für den Zweikanalmodus zugeordnete zweite Sicherheitseingang automatisch ebenfalls im Einkanalmodus betrieben.	Dual Channel Equivalent
		Dual Channel Equivalent	Betrieb des Sicherheitseingangs in Verbindung mit einem zweiten Sicherheitseingang im Zweikanal-Äquivalenzmodus.	
		Dual Channel Complementary	Betrieb des Sicherheitseingangs in Verbindung mit einem zweiten Sicherheitseingang im Zweikanal-Komplementärmodus.	
S	Dual Channel Safety Input Discrepancy Time	0 bis 65.530 ms (in Schritten von 10 ms)	Grenzwert für die Laufzeitunterschiede zwischen den beiden Eingängen im Zweikanalmodus.	0 ms
	E/A-Kommentar	max. 32 Zeichen	E/A-Kommentar für den Sicherheitseingang. Der hier eingegebene E/A-Kommentar wird im Logik-Editor als E/A-Tag verwendet.	Kein E/A-Kommentar
	Maintenance Counter Mode Choice	Time	Betriebsart des Wartungszählers.	Time
		Count		
	Threshold Maintenance Counter	0 bis 4.294.967.295 Stunden	Grenzwert für den Wartungszähler.	0

WICHTIG: Wird der Parameter *Safety Input Channel Mode* auf *Test Pulse from Test Out* gesetzt, muss außerdem für den Parameter *Test Source* der als Testquelle zu verwendende Testausgang ausgewählt und der Parameter *Test Output Mode* dieses Testausgangs auf *Pulse Test Output* eingestellt werden.

4-1-4 Parametergruppen für die einzelnen Testausgänge

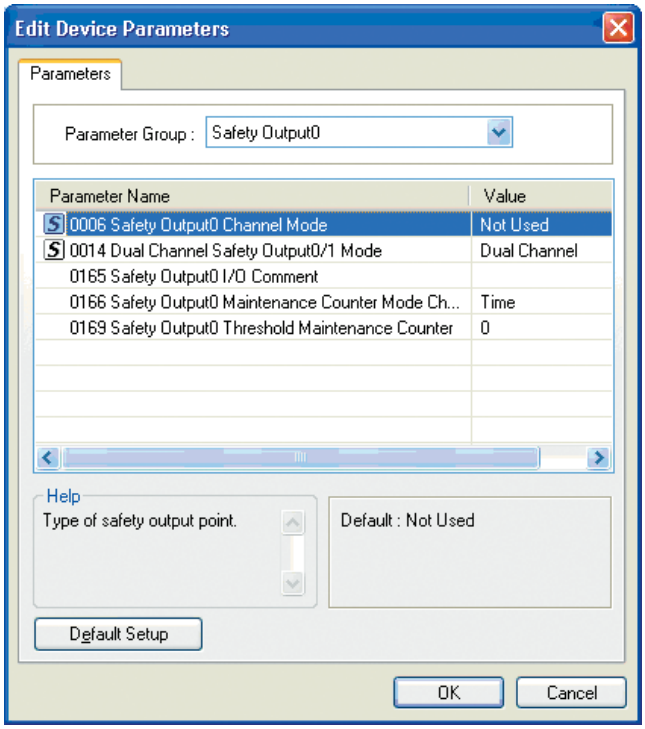
In diesem Abschnitt werden die Parameter der Parametergruppen für die einzelnen Testausgänge erläutert. Hierbei werden die Parameter jeweils eines Testausgangs zu einer Gruppe zusammengefasst.



	Parameter	Einstellungen	Beschreibung	Standard-einstellung
S	Test Output Mode	Not used.	Dieser Testausgang wird nicht verwendet.	Not used.
		Standard Output	Der Testausgang ist an den Eingang einer Muting-Lampe oder einer SPS angeschlossen und fungiert als Überwachungsausgang.	
		Pulse Test Output	Anschluss eines Geräts mit einem Kontaktausgang in Kombination mit einem Testausgang.	
		Power Supply Output	Der Testausgang fungiert als Spannungsversorgung für einen Sicherheitssensor. Es werden die über den Testausgang an die E/A-Spannungsversorgung geleiteten Spannungen ausgegeben.	
		Muting Lamp Output (diese Einstellung wird nur für die Klemme T3 unterstützt)	Der Testausgang ist an den Eingang einer Muting-Lampe angeschlossen. Ist der Ausgang auf EIN gesetzt, kann eine Unterbrechung der Verbindung zur Muting-Lampe festgestellt werden.	
	Fault Action	Clear off	Bestimmt den Ausgangszustand des Testausgangs beim Auftreten eines Kommunikationsfehlers. Dieser Parameter ist nur dann aktiviert, wenn der Parameter *Test Output Mode* auf *Standard Output* oder *Muting Lamp* eingestellt ist.	Clear off
		Hold last data		
	I/O Comment	max. 32 Zeichen	E/A-Kommentar für den Testausgang. Der hier eingegebene E/A-Kommentar wird im Logik-Editor als E/A-Tag verwendet.	Kein E/A-Kommentar
	Maintenance Counter Mode Choice	Time	Betriebsart des Wartungszählers.	Time
		Count		
	Threshold Maintenance Counter	0 bis 4.294.967.295 Stunden	Grenzwert für den Wartungszähler.	0

4-1-5 Parametergruppen für die einzelnen Sicherheitsausgänge

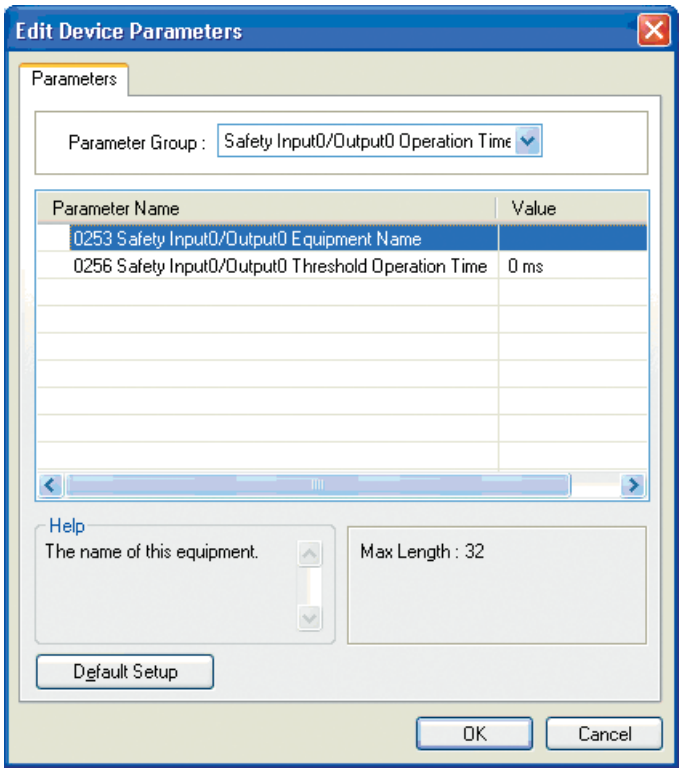
In diesem Abschnitt werden die Parameter der Parametergruppen für die einzelnen Sicherheitsausgänge erläutert.
Hierbei werden die Parameter jeweils eines Sicherheitsausgangs zu einer Gruppe zusammengefasst.



	Parameter	Einstellungen	Beschreibung	Standard-einstellung
S	Safety Output Channel Mode	Not used.	Dieser Sicherheitsausgang wird nicht verwendet. (Es ist kein externes Ausgangsgerät angeschlossen.)	Not used.
		Safety	Bei dieser Einstellung wird der Testimpuls nicht ausgegeben, wenn der Ausgang auf EIN gesetzt ist. Bei Verwendung dieser Einstellung können Querschlüsse zwischen der Ausgangs-Signalleitung und der Spannungsversorgung (+) – wenn der Ausgang auf AUS gesetzt ist – sowie Masseschlüsse erkannt werden.	
		Safety Pulse Test (diese Einstellung wird nur beim Sicherheits-E/A-Modul DST1-MD16SL-1 unterstützt)	Bei dieser Einstellung wird der Testimpuls ausgegeben, wenn der Ausgang auf EIN gesetzt ist. Bei Verwendung dieser Einstellung können Querschlüsse zwischen der Ausgangs-Signalleitung und der Spannungsversorgung und Kurzschlüsse mit anderen Ausgangs-Signalleitungen erkannt werden.	
S	Dual Channel Safety Output Mode	Single Channel	Betrieb des Sicherheitsausgangs im Einkanalmodus. Wird dieser Parameter eines Sicherheitsausgangs auf *Single Channel* gesetzt, wird der für den Zweikanalmodus zugeordnete zweite Sicherheitsausgang automatisch ebenfalls im Einkanalmodus betrieben.	Dual Channel
		Dual Channel	Betrieb des Sicherheitsausgangs im Zweikanalmodus. Wenn die beiden in Verbindung zu verwendenden Sicherheitsausgänge Normal-Status haben, können die Ausgänge eingeschaltet werden.	
	I/O Comment	max. 32 Zeichen	E/A-Kommentar für den Sicherheitsausgang. Der hier eingegebene E/A-Kommentar wird im Logik-Editor als E/A-Tag verwendet.	Kein E/A-Kommentar
	Maintenance Counter Mode Choice	Time	Betriebsart des Wartungszählers.	Time
		Count		
	Threshold Maintenance Counter	0 bis 4.294.967.295 Stunden	Grenzwert für den Wartungszähler.	0

4-1-6 Parametergruppe für die Betriebszeiten

In diesem Abschnitt werden die Parameter der Parametergruppen für die Betriebszeiten der Sicherheitseingänge und -ausgänge erläutert. Hierbei werden die Parameter jeweils eines Eingangs-/Ausgangspaars zu einer Gruppe zusammengefasst.



	Parameter	Einstellungen	Beschreibung	Standard-einstellung
	Equipment Name	max. 32 Zeichen	Kommentar für die zu überwachende Betriebszeit.	Kein Kommentar
	Threshold Response Time	0 bis 65.535 ms (in Schritten von 1 ms)	Grenzwert für die Betriebszeit.	0 ms

Kapitel 5: Bearbeiten der Parameter des Sicherheitsnetzwerk-Controllers

5-1 Einstellungen für Sicherheitsverbindungen

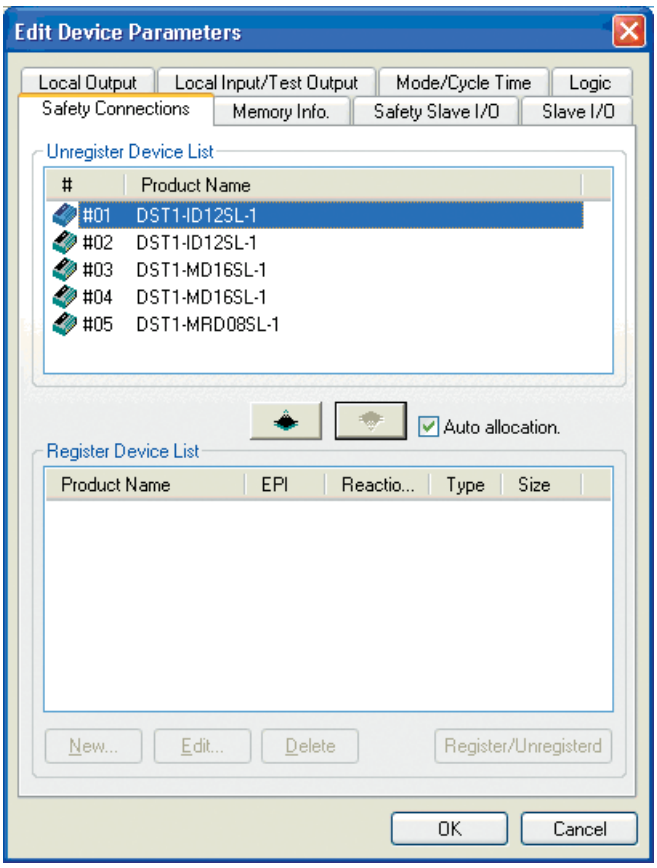
Öffnen Sie das Dialogfeld *Edit Device Parameters* für den Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01), und klicken Sie auf die Registerkarte **Safety Connections**. Auf dieser Registerkarte können Sie die Sicherheits-Slaves (z. B. DST1-Sicherheits-E/A-Module), mit denen eine Sicherheitskommunikation stattfindet, registrieren, und die Kommunikationsparameter einstellen.

Hinweis: Erfolgt der Betrieb des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) im Standalone-Modus, erübrigt sich das Einstellen der Parameter auf dieser Registerkarte.

5-1-1 Registrieren von Sicherheits-Slaves

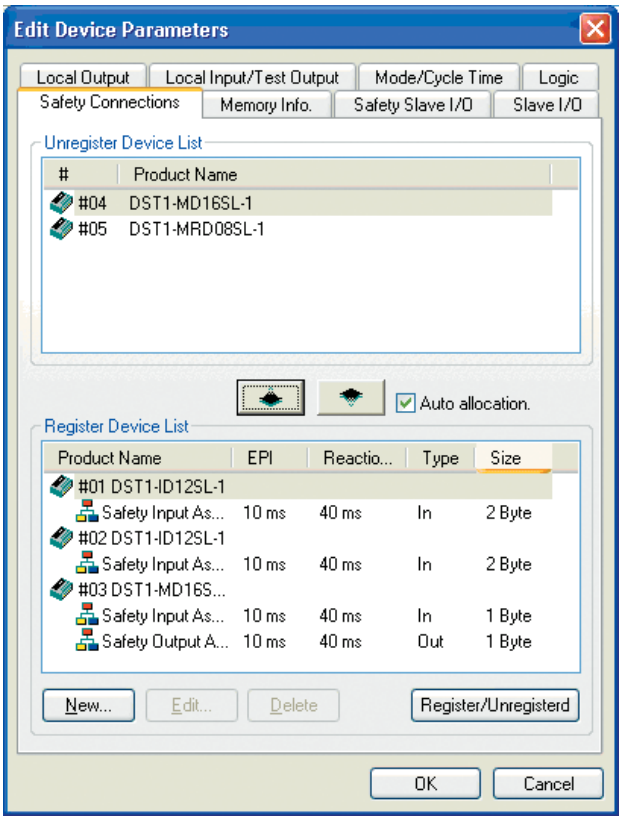
Gehen Sie wie folgt vor, um Sicherheits-Slaves als Kommunikationsziele zu registrieren:

1. Im oberen Bereich werden die nicht registrierten Geräte aufgeführt, im unteren Bereich die registrierten Geräte.



2. Wählen Sie einen zu registrierenden Sicherheits-Slave in der Liste *Unregister Device List* aus, und klicken Sie auf die Schaltfläche .
3. Der in Schritt 2 ausgewählte Sicherheits-Slave wird nun registriert.

Ist beim Registrieren des Sicherheits-Slaves das Kontrollkästchen *Auto Allocation* aktiviert, werden die Standardverbindungen und Parameter wie in der folgenden Abbildung gezeigt automatisch zugeteilt.



Die Liste *Register Device List* enthält die folgenden Informationen:

Spalte	Angezeigte Informationen
Product Name	Die Bezeichnung des registrierten Sicherheits-Slaves (Symbol) oder der in der Sicherheitsverbindung verwendeten E/A-Konfiguration (Symbol).
EPI	Das EPI für die Sicherheitsverbindung. Detailinformationen zum EPI finden Sie unter *5-1-2 Festlegen der Einstellungen für Sicherheitsverbindungen* (Seite 82).
Reaktionszeit	Die Netzwerkreaktionszeit für die Sicherheitsverbindung.
Type	Der Typ der in der Sicherheitsverbindung verwendeten E/A-Konfiguration.
Size	Die Datengröße der in der Sicherheitsverbindung verwendeten E/A-Konfiguration.

4. In der Liste *Register Device* können Sie Verbindungen hinzufügen und löschen und die Verbindungsparameter bearbeiten.
   - Zum Hinzufügen einer Verbindung wählen Sie den Sicherheits-Slave aus, dem Sie die Verbindung hinzufügen möchten, und klicken auf **New**. Informationen zum Einstellen der Verbindungsparameter finden Sie unter *5-1-2 Festlegen der Einstellungen für Sicherheitsverbindungen* (Seite 82).
   - Zum Löschen einer Verbindung wählen Sie die zu löschende Verbindung aus und klicken auf **Delete**.
   - Zum Bearbeiten der Verbindungsparameter wählen Sie die gewünschte Verbindung aus und klikken auf **Edit**. Nun werden die Parameter der ausgewählten Verbindung angezeigt. Informationen zum Ändern der Verbindungsparameter finden Sie unter *5-1-2 Festlegen der Einstellungen für Sicherheitsverbindungen* (Seite 82).
   - Wählen Sie den Sicherheits-Slave aus, und klicken Sie auf **Register/Unregister**. Sind die Verbindungen bereits eingerichtet, werden diese beim Klicken auf diese Schaltfläche wieder aufgehoben. Andernfalls werden die Standardverbindungen und -Parameter zugeteilt.

Hinweis: – Zum Löschen eines Sicherheits-Slaves aus der Liste *Register Device* wählen Sie den zu löschenden Sicherheits-Slave aus und klicken auf *Delete*.

– Des weiteren gilt: Wenn eine der folgenden Operationen im Netzwerkkonfigurationsbereich ausgeführt wird, wird der Sicherheits-Slave mittels Auto-Zuteilung registriert:

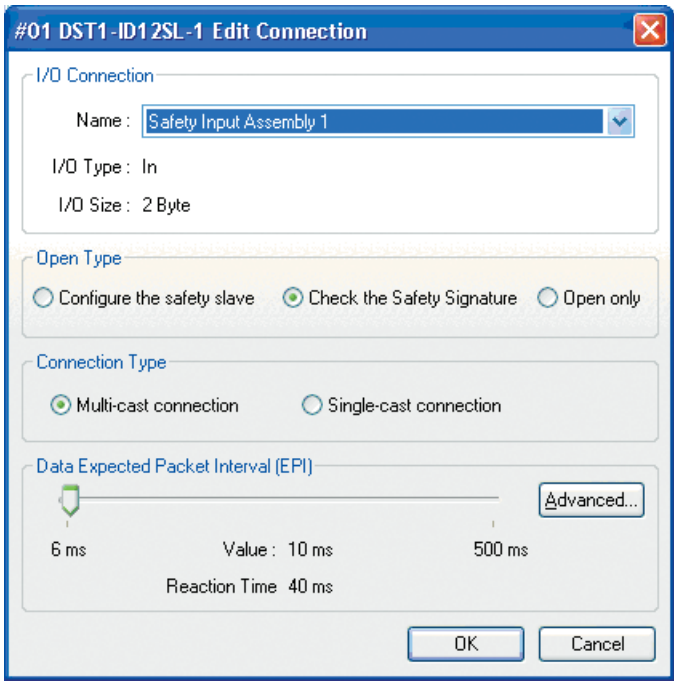
(1) Ziehen eines Slave-Geräts zum Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01).

(2) Auswahl eines Slave-Geräts und Festlegen des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) als Ziel durch Auswahl des Geräts und Auswahl des Befehls *Register to Other Device* in der Menüleiste.

WICHTIG: Eine Änderung an den Einstellungen der Sicherheitsverbindung kann Auswirkungen auf das Programm haben. Rufen Sie nach jeder Änderung von Einstellungen der Sicherheitsverbindung den Logik-Editor auf, und überprüfen Sie das Programm.

5-1-2 Festlegen der Einstellungen für Sicherheitsverbindungen

In diesem Abschnitt wird das Festlegen der Einstellungen für Sicherheitsverbindungen erläutert.



I/O Connection

Wählen Sie die verwendende E/A-Konfiguration aus den vom Ziel-Sicherheits-Slave unterstützten E/A-Konfigurationen aus.

Hinweis:
- Informationen zu den von den DST1-Sicherheits-E/A-Modulen unterstützten E/A- Konfigurationen finden Sie im Abschnitt 3-2: "Remote I/O Allocations" des *Bedienerhandbuchs für Sicherheits-E/A-Module der Serie DST1*.
- Wird die Sicherheits-Slave-Funktion des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) verwendet, muss die E/A-Konfiguration auf der Registerkarte *Safety Slave I/O* eingestellt werden. Siehe hierzu *5-2 Sicherheits-Slave-Einstellungen* (Seite 84).

Open Type

Legen Sie die Vorgehensweise beim Herstellen der Verbindung mit den Sicherheits-Slaves durch den Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) fest.

Open Type	Beschreibung
Configure the target device	Beim Herstellen der Verbindung wird der Sicherheits-Slave konfiguriert. Die einstellbaren Parameter sind auf die für die Sicherheitsanwendung relevanten Parameter beschränkt. Unter normalen Umständen sollte diese Einstellung des Parameters nicht verwendet werden.
Check the safety signature	Beim Herstellen der Verbindung sendet der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) die Sicherheitssignatur des Slaves. Die Sicherheitssignatur wird von dem Sicherheits-Slave, der die herzustellende Verbindung empfängt, überprüft. Diese Einstellung des Parameters empfiehlt sich für Verbindungen mit DST1-Sicherheits-E/A-Modulen.
Open only	Beim Herstellen der Verbindung sendet der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) die Sicherheitssignatur des Slaves nicht. Der Sicherheits-Slave akzeptiert die Verbindung ohne Überprüfung der Sicherheitssignatur. Zur Verwendung der Slave-Funktion des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) muss der Sicherheits-Slave mithilfe des Netzwerkkonfigurators ordnungsgemäß konfiguriert werden. Wird der Sicherheits-Slave nicht ordnungsgemäß konfiguriert, wird keine Verbindung hergestellt, daher besteht auch keine Notwendigkeit, dass der Sicherheits-Master die Sicherheitssignatur zur Prüfung an den Sicherheits-Slave sendet. Handelt es sich bei dem Sicherheits-Slave um einen Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01), muss diese Einstellung des Parameters gewählt werden.

WICHTIG: Wenn Sie für den Parameter *Open Type* der Sicherheitsverbindung die Einstellung *Open Only* verwenden, müssen Sie sicherstellen, dass der Sicherheits-Master und der Sicherheits-Slave ordnungsgemäß konfiguriert sind.

Hinweis: Wenn Sie für den Parameter *Open Type* der Sicherheitsverbindung die Einstellung *Configure the target device* verwenden und der Sicherheits-Slave nicht konfiguriert ist, konfiguriert der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) den Sicherheits-Slave und stellt dann eine Verbindung her. Daher kann bei einem Austausch des Sicherheits-Slaves die Verbindung ohne Verwendung des Netzwerkkonfigurators wieder neu hergestellt werden, indem der Slave einfach wieder ans Netzwerk angeschlossen wird. In der aktuellen Version sind die einstellbaren Parameter jedoch auf die für die Sicherheitsanwendung relevanten Parameter beschränkt. Müssen die Standardparameter nicht eingestellt werden, kann diese Einstellung des Parameters gewählt werden. Die Fähigkeit zum Einstellen der Standardparameter ist für künftige Gerätegenerationen geplant.

Connection Type

Festlegen der Art der zu verwendenden Verbindung zwischen dem Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) und dem Sicherheits-Slave.

Connection Type	Beschreibung
Multi-cast connection	Diese Verbindungsart kann nur verwendet werden, wenn es sich bei dem Slave um ein Sicherheits-Eingangs-Modul handelt. Bei Verwendung einer Multicast-Verbindung kann ein Sicherheits-Eingangs-Modul die Eingangsdaten an maximal 15 Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) übertragen. Richten mehrere Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) eine Multicast-Verbindung zu ein und demselben Sicherheits-Slave ein, werden diese als eine Multicast-Gruppe klassifiziert. Die unter *I/O Connection* festgelegte E/A-Konfiguration und das EPI müssen für alle diese Sicherheitsnetzwerk-Controller identisch sein. Diese Verbindungsart kann auch gewählt werden, wenn nur ein Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) im Netzwerk vorliegt.
Single-cast connection	Diese Verbindungsart kann für Eingangs- wie für Ausgangsverbindungen ausgewählt werden. Der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) stellt mit dem Sicherheits-Slave eine 1:1-Verbindung für die Übertragung von Sicherheitsdaten her.

EPI (Expected Packet Interval)

Das EPI ist das Intervall, mit dem der Sicherheits-Slave Sicherheitsdaten mit dem Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) austauscht. Der eingestellte Wert muss größer als die Zykluszeit des Ziel-Sicherheits-Slaves und des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) sein.

Die Zykluszeit aller DST1-Sicherheits-E/A-Module beträgt 6 ms. Die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 können Sie nach Abschluss der Parametereinstellungen und der Programmierung auf der Registerkarte *Mode/Cycle Time* des Dialogfelds *Edit Device Parameters* des Sicherheitsnetzwerk-Controllers NE1A-SCPU01 einsehen.

Die hier eingestellte Zeit hat Auswirkungen auf die Netzwerkbandbreite und auf die Netzwerkreaktionszeit. Informationen zur Netzwerkbandbreite finden Sie unter *3-2 Überprüfung der benötigten Netzwerkbandbreite* (Seite 59), Informationen zur Netzwerkreaktionszeit unter *3-3 Berechnung und Überprüfung der maximalen Reaktionszeit* (Seite 63).

Advanced

Die Schaltfläche **Advanced** ermöglicht die Änderung weiterer Kommunikationsparameter. Diese Parameter haben Auswirkungen auf den Systembetrieb und sollten unter normalen Umständen nicht geändert werden.

5-2 Sicherheits-Slave-Einstellungen

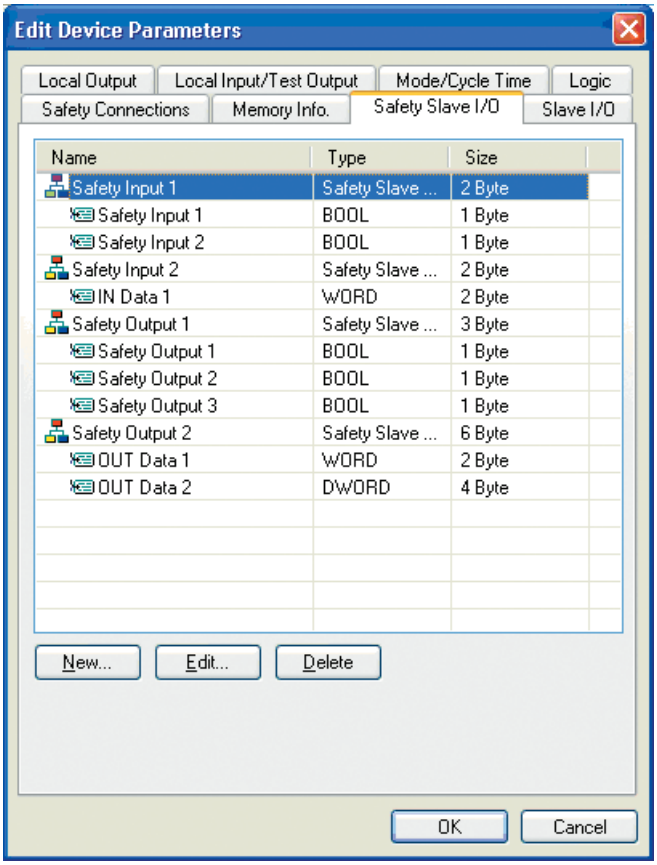
Auf der Registerkarte **Safety Slave I/O** können Sie die für den Betrieb des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) als Sicherheits-Slave erforderliche E/A-Konfiguration einstellen. Die auf dieser Registerkarte eingestellte E/A-Konfiguration wird auf der Registerkarte *Safety Connections* des als Sicherheits-Master fungierenden Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) angezeigt und kann dort ausgewählt werden.

Die E/A-Tags finden im Logik-Editor Verwendung.

Hinweis: Wird der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) nicht als Sicherheits-Slave eingesetzt, müssen die Parameter auf dieser Registerkarte nicht eingestellt werden.

5-2-1 Registrieren von E/A-Konfigurationen für Sicherheits-Slaves

Registrieren Sie die E/A-Konfigurationen für die Verwendung des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) als Sicherheits-Slave.



Auf dieser Registerkarte werden die folgenden Informationen angezeigt.

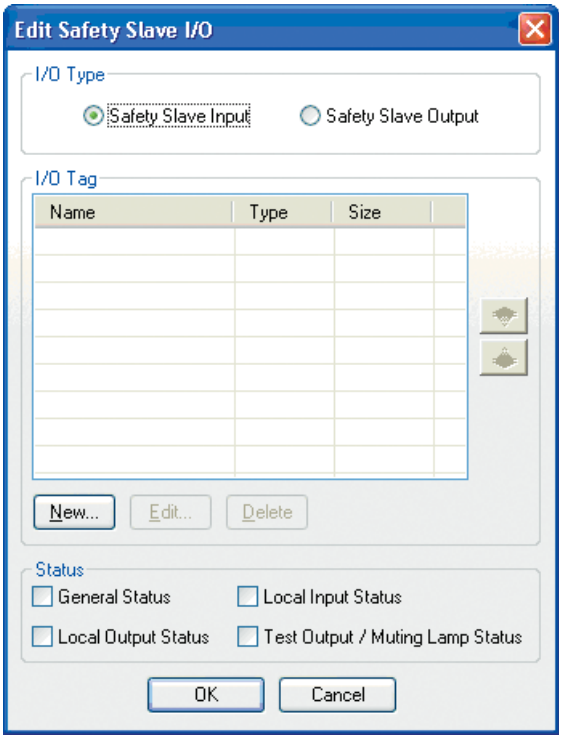
Parameter	Angezeigte Informationen
Name	Der registrierte Name der E/A-Konfiguration (Symbol) und die in der Konfiguration definierten E/A-Tags (Symbol).
Type	Der Typ der E/A-Konfiguration (Eingang/Ausgang) und die Datentypen für die E/A-Tags.
Size	Die Datengröße der E/A-Konfiguration und der E/A-Tags.

Auf dieser Registerkarte können Sie E/A-Konfigurationen für den Sicherheits-Slave hinzufügen, ändern und löschen. Sie können bis zu vier E/A-Konfigurationen registrieren.

- Zum Hinzufügen einer E/A-Konfiguration klicken Sie auf **New**. Nun wird das Dialogfeld *Edit Safety Slave I/O* angezeigt. Legen Sie wie unter *5-2-2 Einstellen der Daten einer E/A-Konfiguration* (Seite 85) erläutert die Daten der E/A-Konfiguration fest.
- Zum Ändern der Daten der E/A-Konfiguration wählen Sie die zu bearbeitende E/A-Konfiguration aus und klicken auf **Edit**. Nun wird das Dialogfeld *Edit Safety Slave I/O* angezeigt. Ändern Sie wie unter *5-2-2 Einstellen der Daten einer E/A-Konfiguration* (Seite 85) erläutert die Daten der E/A-Konfiguration.
- Zum Löschen einer E/A-Konfiguration wählen Sie die zu löschende E/A-Konfiguration aus und klicken auf **Delete**.

5-2-2 Einstellen der Daten einer E/A-Konfiguration

Dieser Abschnitt erläutert das Einstellen der Daten einer E/A-Konfiguration.



I/O Type

Wählen Sie den einzustellenden Datentyp aus. Für Sicherheitsdaten stehen die folgenden Übertragungsrichtungen zur Verfügung:

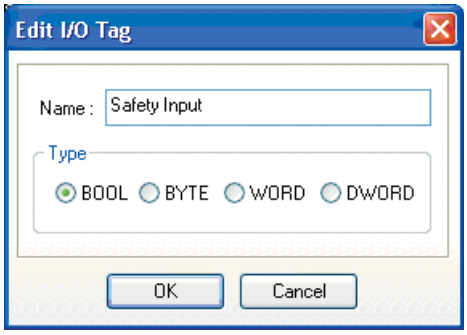
Sicherheits-Slave-Eingang: NE1A-SCPU01 (Sicherheits-Slave) → Sicherheits-Master

Sicherheits-Slave-Ausgang: Sicherheits-Master → NE1A-SCPU01 (Sicherheits-Slave)

I/O Tag

Für eine E/A-Konfiguration können verschiedene E/A-Tags definiert werden. Die hier definierten E/A-Tags können im Logik-Editor eingesetzt werden.

- Zur Definition eines neuen E/A-Tags klicken Sie auf **New** und legen den Namen und den Datentyp fest. Je E/A-Konfiguration können E/A-Tags für bis zu 16 Bytes definiert werden.



- Zum Ändern eines bereits definierten E/A-Tags wählen Sie das zu bearbeitende E/A-Tag aus und klikken auf **Edit I/O Tag**.
- Zum Löschen eines bereits definierten E/A-Tags wählen Sie das zu löschende E/A-Tag aus und klicken auf **Delete**.

Status

Ist der Parameter *I/O Type* auf *Target Input* gesetzt, kann die E/A-Konfiguration auch die Statusinformationen des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) beinhalten. Für die Statusinformationen werden automatisch die folgenden Tags generiert:

Status	Tag
Allgemeiner Status	General Status
Status der Sicherheitseingänge	Safety Input Status

Status	Tag
Status der Sicherheitsausgänge	Safety Output Status
Status der Testausgänge/Muting-Lampe	Test Output/Muting Lamp Status

5-3 Standard-Slave-Einstellungen

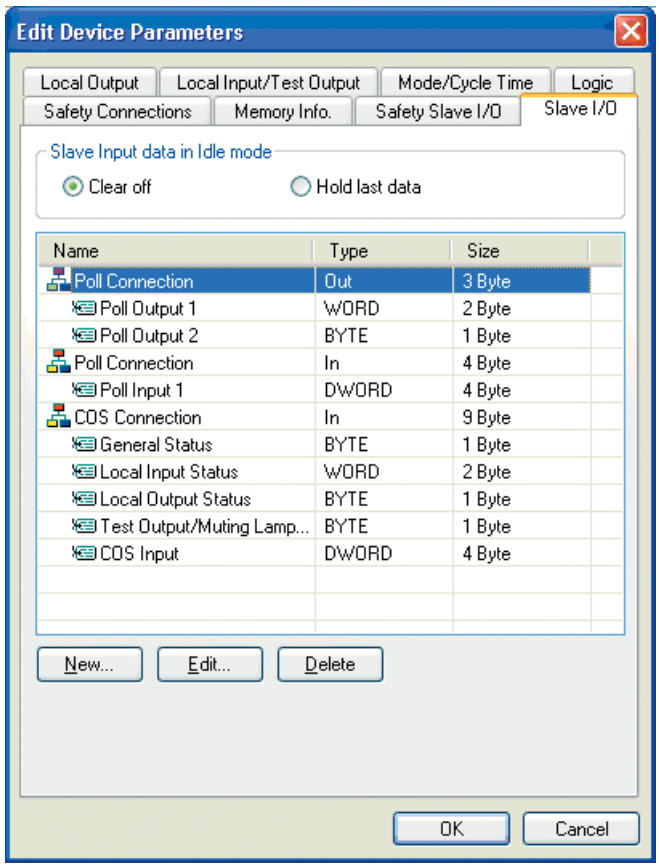
Auf der Registerkarte **Slave I/O** können Sie die für den Betrieb des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) als Standard-Slave erforderliche E/A-Konfiguration einstellen. Die auf dieser Registerkarte eingestellte E/A-Konfiguration wird im entsprechenden Fenster/Dialogfeld der als Standard-Master fungierenden CS/CJ-Serie SPS angezeigt.

Die für die E/A-Konfiguration definierten E/A-Tags können im Logik-Editor eingesetzt werden.

Hinweis: Wird der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) nicht als Standard-Slave eingesetzt, müssen die Parameter auf dieser Registerkarte nicht eingestellt werden.

5-3-1 Registrieren von E/A-Konfigurationen für Standard-Slaves

Registrieren Sie die E/A-Konfigurationen für die Verwendung des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) als Standard-Slave.



Auf dieser Registerkarte werden die folgenden Informationen angezeigt.

Spalte	Angezeigte Informationen
Name	Der registrierte Name der E/A-Konfiguration (Symbol) und die in der Konfiguration definierten E/A-Tags (Symbol).
Type	Der Typ der E/A-Konfiguration (Eingang/Ausgang) und die Datentypen für die E/A-Tags.
Size	Die Datengröße der E/A-Konfiguration und der E/A-Tags.

Auf dieser Registerkarte können Sie E/A-Konfigurationen für den Standard-Slave hinzufügen, ändern und löschen. Für jede Standardverbindung können Eingangs- und Ausgangs-Konfigurationen registriert werden.

- Zum Hinzufügen einer E/A-Konfiguration klicken Sie auf **New**. Nun wird das Dialogfeld *Edit Slave I/O* angezeigt. Legen Sie wie unter *5-3-3 Einstellen der Daten einer E/A-Konfiguration* (Seite 88) erläutert die Daten der E/A-Konfiguration fest.
- Zum Ändern der Daten der E/A-Konfiguration wählen Sie die zu bearbeitende E/A-Konfiguration aus und klicken auf **Edit**. Nun wird das Dialogfeld *Edit Slave I/O* angezeigt. Legen Sie wie unter *5-3-3 Einstellen der Daten einer E/A-Konfiguration* (Seite 88) erläutert die Daten der E/A-Konfiguration fest.
- Zum Löschen einer E/A-Konfiguration wählen Sie die zu löschende E/A-Konfiguration aus und klicken auf **Delete**.

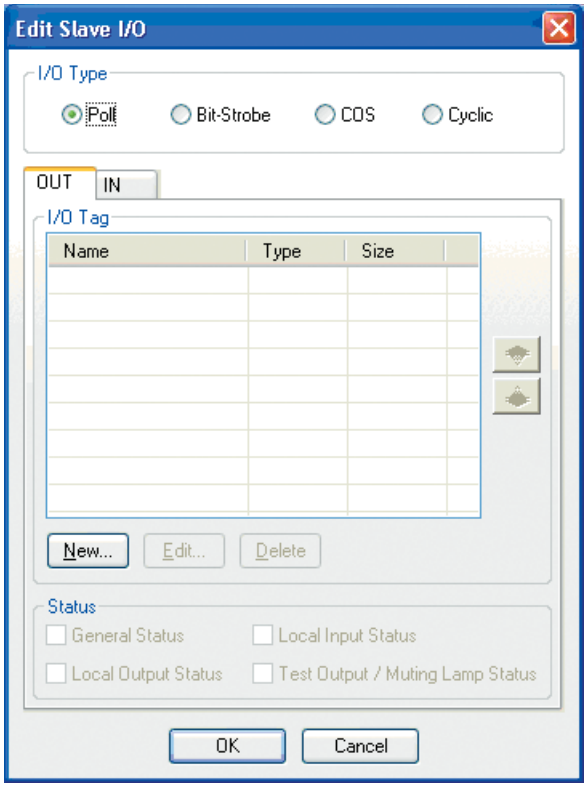
5-3-2 Einstellung des Parameter „Slave Input Data in Idle Mode“

Mit diesem Parameter legen Sie fest, ob die letzten Daten gehalten oder gelöscht werden, wenn bei Verwendung des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) als Standard-Slave mit einer Eingangs-E/A-Konfiguration einer der folgenden Fälle eintritt:

- Wechsel der Betriebsart des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) von RUN nach IDLE.
- Auftreten eines Fehlers (beispielsweise eines Kommunikationsfehlers in einer Sicherheitskette).

5-3-3 Einstellen der Daten einer E/A-Konfiguration

Dieser Abschnitt erläutert das Einstellen der Daten einer E/A-Konfiguration.



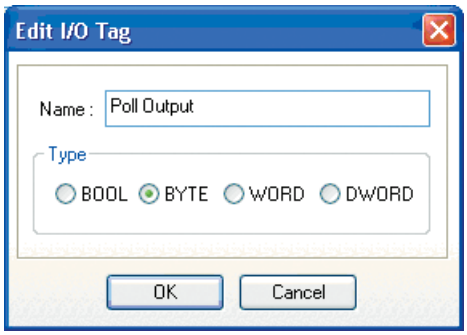
I/O Type

Für die E/A-Konfiguration verwendeter Verbindungstyp. Für jede Verbindung können Eingangs- und Ausgangs-Konfigurationen registriert werden. Wird jedoch der Verbindungstyp *Bit-Strobe* ausgewählt, können keine Ausgangs-Konfigurationen registriert werden, da die Daten vom Standard-Master nicht ausgegeben werden können.

I/O Tag

Für eine E/A-Konfiguration können verschiedene E/A-Tags definiert werden. Die hier definierten E/A-Tags können im Logik-Editor eingesetzt werden.

- Zur Definition eines neuen E/A-Tags klicken Sie auf **New** und legen den Namen und den Datentyp fest. Je E/A-Konfiguration können E/A-Tags für bis zu 16 Bytes definiert werden.



- Zum Ändern eines bereits definierten E/A-Tags wählen Sie das zu bearbeitende E/A-Tag aus und klikken auf **Edit I/O Tag**.
- Zum Löschen eines bereits definierten E/A-Tags wählen Sie das zu löschende E/A-Tag aus und klicken auf **Delete**.

Status

Ist der Parameter I/O Type auf *Input* gesetzt, kann die E/A-Konfiguration auch die Statusinformationen des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) beinhalten. Für die Statusinformationen werden automatisch die folgenden Tags generiert:

Status	Tag
Allgemeiner Status	General Status
Status der Sicherheitseingänge	Safety Input Status
Status der Sicherheitsausgänge	Safety Output Status
Status der Testausgänge/Muting-Lampe	Test Output/Muting Lamp Status

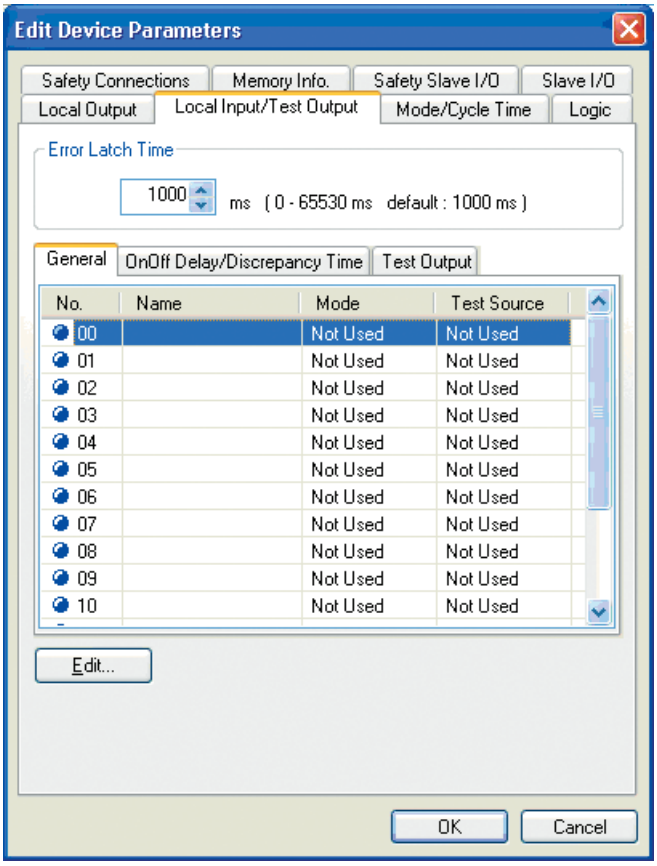
5-4 Lokale E/A-Einstellungen

Auf den Registerkarten **Local Output** und **Local Input/Test Output** können Sie die lokalen E/A-Einstellungen des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) festlegen.

Hinweis: Standardmäßig ist der Parameter *Mode* aller Ein- und Ausgänge auf *not used* gesetzt. Wenn Sie die lokale E/A des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) nicht verwenden, müssen die Parameter auf diesen Registerkarten nicht eingestellt werden.

5-4-1 Einstellen der Sicherheitseingänge

Zum Konfigurieren der Sicherheitseingänge klicken Sie auf die Registerkarte **Local Input/Test Output** und dort auf die Registerkarte **General**.



Hinweis: Sicherheitseingänge verfügen über eine Vielzahl von Parametern, daher ist die Registerkarte **Local Input/Test Output** weiter in die Registerkarten **General** und **On-Off Delay/Discrepancy Time** unterteilt.

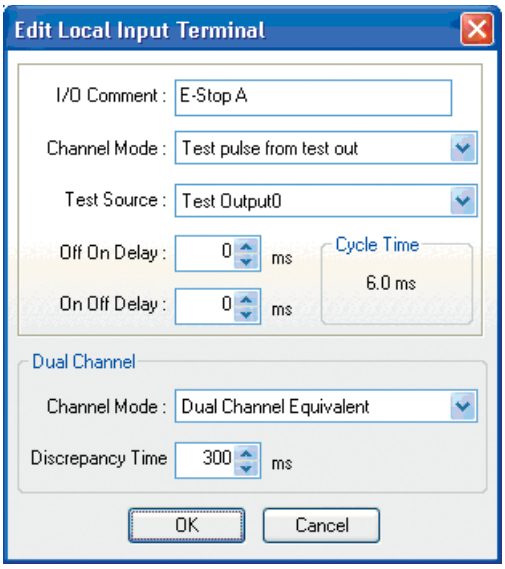
Error Latch Time

Dieser Parameter ist allen Sicherheitseingängen und Testausgängen gemeinsam. Er bestimmt die Zeitdauer, für die der Fehlerzustand aktiviert wird, wenn ein Fehler in einem dieser Ein- bzw. Ausgänge auftritt.

Auch nach Behebung der Fehlerursache bleibt der Fehlerzustand für die hier eingestellte Zeitdauer aktiviert. Diese Zeitspanne kann auf einen Wert zwischen 0 und 65.530 ms eingestellt werden.

Einstellungen für individuelle Sicherheitseingänge

Doppelklicken Sie auf die Zeile mit dem einzustellenden Sicherheitseingang, oder wählen Sie die Zeile aus, und klicken Sie auf **Edit**.



I/O Comment

Für jeden Sicherheitseingang kann ein E/A-Kommentar zur Bezeichnung der Klemme eingegeben werden. Der hier eingegebene E/A-Kommentar wird im Logik-Editor als E/A-Tag verwendet.

Channel Mode

Kanalmodus für den Sicherheitseingang

Einstellung	Beschreibung
Not Used	Dieser Sicherheitseingang wird nicht verwendet. (Der Sicherheitseingang ist mit keinem externen Eingabegerät verbunden.)
Test pulse from test out	Anschluss eines Geräts mit einem Kontaktausgang in Kombination mit einem Testausgang. Bei Auswahl dieses Modus muss außerdem für den Parameter *Test Source* der als Testquelle zu verwendende Testausgang ausgewählt und der Parameter *Test Output Mode* dieses Testausgangs auf *Pulse Test Output* eingestellt werden. Diese Option ermöglicht es, Verbindungen zwischen der Eingangssignalleitung und der Spannungsversorgung (+) sowie Querschlüsse mit anderen Eingangssignalleitungen zu erkennen.
Used as safety input	Anschluss eines Sicherheitsgeräts mit Halbleiterausgang (z. B. Sicherheitslichtgitter).
Used as standard input	Anschluss eines Standardgeräts (d. h. eines nicht sicherheitsrelevanten Geräts).

Test Source

Ist der Parameter *Channel Mode* eines Sicherheitseingangs auf *Test Pulse from Test Out* eingestellt, muss dieser Parameter auf den in Verbindung mit dem Sicherheitseingang zu verwendenden Testausgang eingestellt werden.

Der Parameter *Test Output Mode* des hier ausgewählten Testausgangs wird automatisch auf *Pulse Test Output* gesetzt.

Hinweis: Der Parameter *Test Output Mode* des betreffenden Testausgangs muss auf *Pulse Test Output* gesetzt werden.

Off On Delay und On Off Delay

Diese Parameter bestimmen die Einschalt- und Ausschaltverzögerungszeit des Sicherheitseingangs. Der Einstellbereich liegt zwischen 0 und 128 ms, muss jedoch ein Vielfaches der Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) betragen. Überprüfen Sie die angezeigte Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01), und stellen Sie die Verzögerungszeiten entsprechend ein.

WICHTIG:
- Der optimale Wert für die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) wird ausgehend von den Parametereinstellungen und dem Programm automatisch berechnet. Aus diesem Grund müssen die Einschalt- und Ausschaltverzögerungszeiten der Sicherheitseingänge als letztes festgelegt werden.
- Verwenden Sie für die Einschalt- und Ausschaltverzögerungszeiten der Sicherheitseingänge ganzzahlige Vielfache der Zykluszeit. Bei fehlerhafter Einstellung der Einschalt- und Ausschaltverzögerungszeiten wird eine Fehlermeldung angezeigt, wenn Sie das Dialogfeld *Edit Device Parameter* schließen.

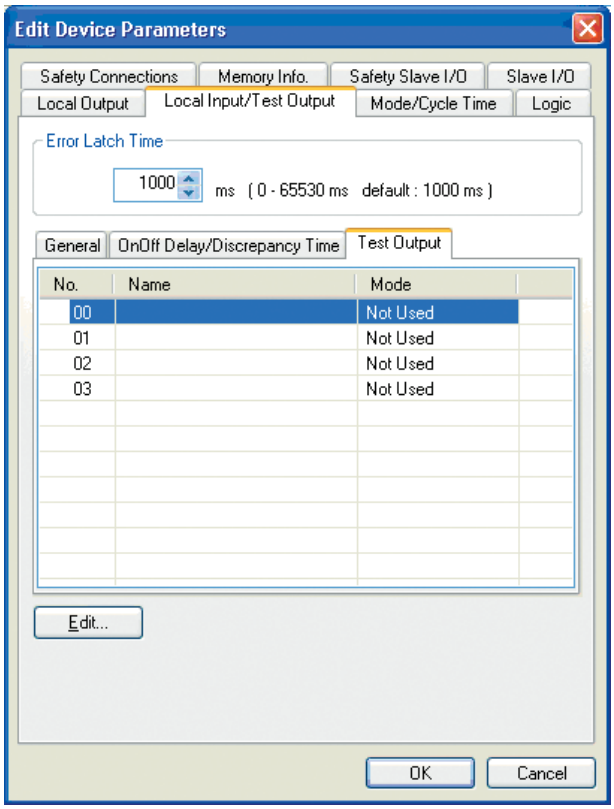
Dual Channel

Stellen Sie hier den Zweikanal-Sicherheitseingangs-Modus und die zulässige Verzögerungszeit ein. Die nachstehende Tabelle führt die möglichen Einstellungen für den Zweikanal-Sicherheitseingangs-Modus auf. Die zulässige Verzögerungszeit kann zwischen 0 und 65.530 ms in Schritten von 10 ms eingestellt werden.

Einstellung	Beschreibung
Single Channel	Betrieb des Sicherheitseingangs im Einkanalmodus. Wird Parameter *Channel Mode* eines Sicherheitseingangs auf *Single Channel* gesetzt, wird der für den Zweikanalmodus zugeordnete zweite Sicherheitseingang automatisch ebenfalls im Einkanalmodus betrieben.
Dual Channel Equivalent	Betrieb des Sicherheitseingangs in Verbindung mit einem zweiten Sicherheitseingang im Zweikanal-Äquivalenzmodus.
Dual Channel Complementary	Betrieb des Sicherheitseingangs in Verbindung mit einem zweiten Sicherheitseingang im Zweikanal-Komplementärmodus.

5-4-2 Einstellen der Testausgänge

Zum Konfigurieren der Testausgänge klicken Sie auf die Registerkarte **Local Input/Test Output** und dort auf die Registerkarte **Test Output**.

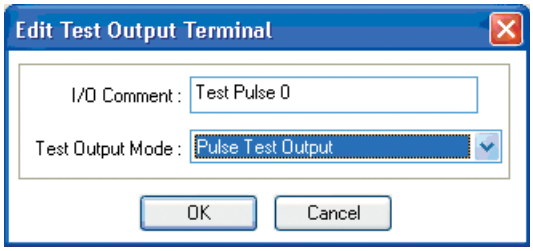


Error Latch Time

Der Testausgang wird in Verbindung mit einem Sicherheitseingang verwendet. Die Einstellung dieses Parameters gilt daher für alle Sicherheitseingänge und Testausgänge. Detaillierte Informationen hierzu finden Sie in unter *Error Latch Time* im Abschnitt *5-4-1 Einstellen der Sicherheitseingänge* (Seite 90).

Einstellungen für individuelle Testausgänge

Doppelklicken Sie auf die Zeile mit dem einzustellenden Testausgang, oder wählen Sie die Zeile aus, und klicken Sie auf **Edit**.



I/O Comment

Hier können Sie einen E/A-Kommentar für den Testausgang eingeben. Der hier eingegebene E/A-Kommentar wird im Logik-Editor als E/A-Tag verwendet.

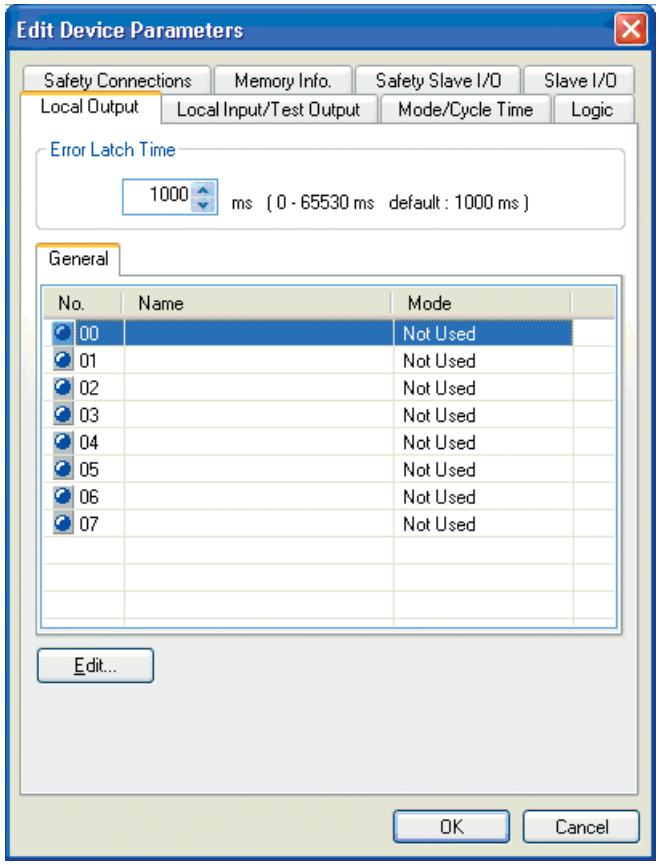
Test Output Mode

Kanalmodus für den Testausgang.

Einstellung	Beschreibung
Not Used	Dieser Testausgang wird nicht verwendet.
Standard Output	Der Testausgang ist an den Eingang einer Muting-Lampe oder einer SPS angeschlossen und fungiert als Überwachungsausgang.
Pulse Test Output	Anschluss eines Geräts mit einem Kontaktausgang in Kombination mit einem Sicherheitseingang.
Power Supply Output	Der Testausgang fungiert als Spannungsversorgung für einen Sicherheitssensor. Die ausgegebene Spannung der Test Output Klemme entspricht der E/A Spannungsversorgung (V, G).
Muting Lamp Output	Der Testausgang ist an den Eingang einer Muting- Lampe angeschlossen (diese Einstellung wird nur für die Klemme T3 unterstützt). Ist der Ausgang auf EIN gesetzt, kann eine Unterbrechung der Verbindung zur Muting-Lampe festgestellt werden.

5-4-3 Einstellen der Sicherheitsausgänge

Zum Einstellen der Sicherheitsausgänge klicken Sie auf die Registerkarte **Local OUT**.



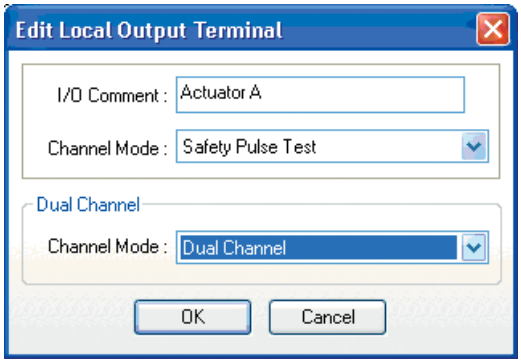
Error Latch Time

Dieser Parameter ist allen Sicherheitsausgängen gemeinsam. Er bestimmt die Zeitdauer, für die der Fehlerzustand aktiviert wird, wenn ein Fehler in einem der Sicherheitsausgänge auftritt.

Auch nach Behebung der Fehlerursache bleibt der Fehlerzustand für die hier eingestellte Zeitdauer aktiviert. Diese Zeitspanne kann auf einen Wert zwischen 0 und 65.530 ms eingestellt werden.

Einstellungen für individuelle Sicherheitsausgänge

Doppelklicken Sie auf die Zeile mit dem einzustellenden Sicherheitsausgang, oder wählen Sie die Zeile aus, und klicken Sie auf **Edit**.



I/O Comment

Hier können Sie einen E/A-Kommentar für den Sicherheitsausgang einstellen. Der hier eingegebene E/A-Kommentar wird im Logik-Editor als E/A-Tag verwendet.

Channel Mode

Kanalmodus für den Sicherheitsausgang.

Einstellung	Beschreibung
Not Used	Dieser Sicherheitsausgang wird nicht verwendet. (Es ist kein externes Ausgangsgerät angeschlossen.)
Safety	Bei dieser Einstellung wird der Testimpuls nicht ausgegeben, wenn der Ausgang auf EIN gesetzt ist. Bei Verwendung dieser Einstellung können Querschlüsse zwischen der Ausgangs-Signalleitung und der Spannungsversorgung (+) – wenn der Ausgang auf AUS gesetzt ist – sowie Masseschlüsse erkannt werden.
Safety Pulse Test	Bei dieser Einstellung wird der Testimpuls ausgegeben, wenn der Ausgang auf EIN gesetzt ist. Bei Verwendung dieser Einstellung können Querschlüsse zwischen der Ausgangs-Signalleitung und der Spannungsversorgung und Querschlüsse mit anderen Ausgangs-Signalleitungen erkannt werden.

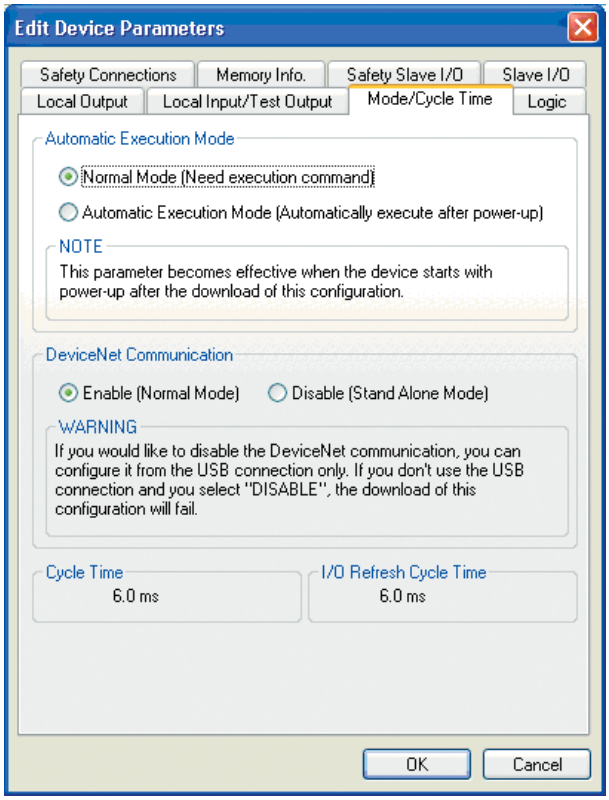
Dual Channel / Channel Mode

Die nachstehende Tabelle führt die möglichen Einstellungen für den Zweikanal-Sicherheitsausgangs-Modus auf.

Einstellung	Beschreibung
Single Channel	Betrieb des Sicherheitsausgangs im Einkanalmodus. Wird Parameter *Channel Mode* eines Sicherheitsausgangs auf *Single Channel* gesetzt, wird der für den Zweikanalmodus zugeordnete zweite Sicherheitsausgang automatisch ebenfalls im Einkanalmodus betrieben.
Dual Channel	Betrieb des Sicherheitsausgangs im Zweikanalmodus. Wenn die beiden in Verbindung zu verwendenden Sicherheitsausgänge Normal-Status haben, können die Ausgänge eingeschaltet werden.

5-5 Einstellen der Betriebsarten und Bestätigen der Zykluszeit

Auf der Registerkarte **Mode/Cycle Time** können Sie die Betriebsarten des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) festlegen und die Zykluszeit überprüfen.



5-5-1 Einstellen der Betriebsarten des Sicherheitsnetzwerk-Controllers NE1A

Automatic Execution Mode

Die Einstellung des automatischen Ausführungsmodus des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) darf erst nach der Konfiguration des Systems, d. h. nach dem Herunterladen der Geräteparameter Parameter erfolgen.

Einstellung	Beschreibung
Normal Mode	Nach dem Einschalten der Spannungsversorgung startet die Baugruppe in der IDLE-Betriebsart. Die Umschaltung in die RUN-Betriebsart erfolgt durch eine explizite Änderung der Betriebsart mithilfe des Netzwerkkonfigurators. Solange die Geräteparameter nicht verifiziert wurden, muss diese Betriebsart eingestellt sein.
Automatic Execution Mode	Nach dem Einschalten der Spannungsversorgung startet die Baugruppe in der RUN-Betriebsart, sofern die folgenden Bedingungen erfüllt sind: • Die Konfiguration wurde geschützt. • Die Baugruppe arbeitete vor dem Ausschalten der Spannungsversorgung in der RUN-Betriebsart.

WICHTIG: Selbst wenn für den Parameter *Automatic Execution Mode* die Einstellung *Automatic Execution Mode* gewählt und die Konfiguration geschützt wurde, startet die Baugruppe beim Einschalten der Spannungsversorgung nicht in der RUN-Betriebsart, wenn sie beim vorherigen Ausschalten der Spannungsversorgung in der IDLE-Betriebsart arbeitete. Damit die Baugruppe in der RUN-Betriebsart startet, muss die Spannungsversorgung zuvor in der RUN-Betriebsart ausgeschaltet worden sein.

Einstellen der DeviceNet-Kommunikation

Wird der Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) als Standalone-Controller eingesetzt, kann die DeviceNet-Kommunikation deaktiviert werden. Die Deaktivierung der DeviceNet-Kommunikation führt zu einer Verkürzung der Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01), jedoch können dann keine DeviceNet-Kommunikationsfunktionen verwendet werden.

WICHTIG: Ist die DeviceNet-Kommunikation deaktiviert, muss der Netzwerkkonfigurator über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) angeschlossen werden. Erfolgt die Deaktivierung der DeviceNet-Kommunikation durch das Herunterladen von Parametern über eine DeviceNet-Schnittstellenkarte, kommt es zum Auftreten eines Fehlers im Netzwerkkonfigurator, da die DeviceNet-Kommunikation des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) deaktiviert wurde.

5-5-2 Bestätigen der Zykluszeit

Zykluszeit

Die Zykluszeit des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) wird ausgehend von den eingestellten Parametern und dem im Logik-Editor erstellten Programm automatisch berechnet und angezeigt.

Die Zykluszeit wird bei der Berechnung der Reaktionszeit und der Auswahl der Einstellungen für die Einschalt- und Ausschaltverzögerungszeiten verwendet. Überprüfen Sie den Wert nach dem Einstellen aller Parameter und Programme.

E/A-Aktualisierungszykluszeit

Der E/A-Aktualisierungszyklus dient der Aktualisierung der lokalen E/A. Die E/A-Aktualisierungszykluszeit wird automatisch berechnet und angezeigt.

Die E/A-Aktualisierungszykluszeit wird bei der Berechnung der Reaktionszeit verwendet.

Überprüfen Sie den Wert nach dem Einstellen aller Parameter und Programme.

Kapitel 6: Programmierung des Sicherheitsnetzwerk-Controllers

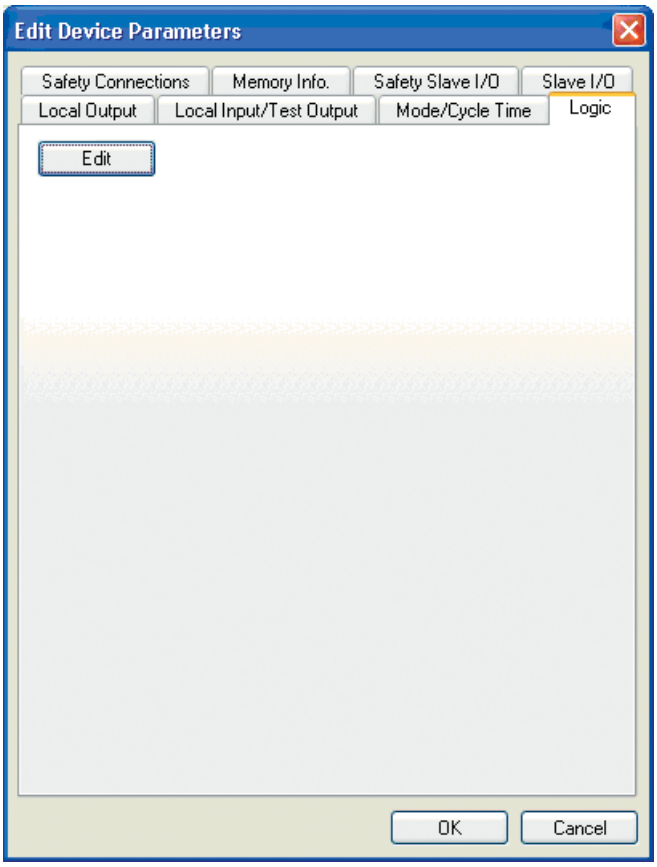
6-1 Aufrufen und Beenden des Logik-Editors

6-1-1 Aufrufen des Logik-Editors

Die Programmierung des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) erfolgt mithilfe des Logik-Editors.

Gehen Sie zum Aufrufen des Logik-Editors wie folgt vor:

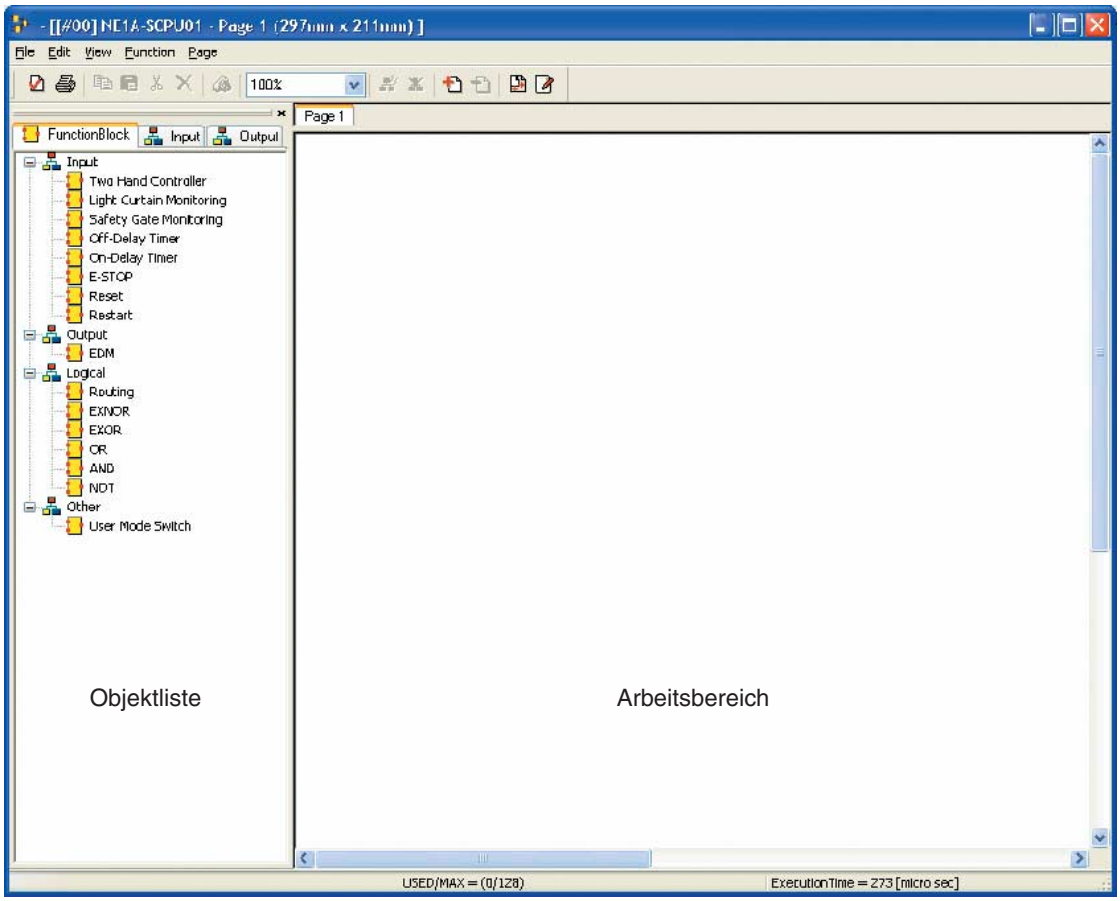
1. Klicken Sie im Dialogfeld **Edit Device Parameters** für den Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) auf die Registerkarte **Logic**.



2. Klicken Sie auf **Edit**.

Nun wird der Logik-Editor aufgerufen.

Dieser umfasst die Objektliste und den Arbeitsbereich (siehe nachstehende Abbildung).



6-1-2 Beenden des Logik-Editors

Gehen Sie zum Beenden des Logik-Editors wie folgt vor:

1. Wählen Sie im Menü **File** des Logik-Editors den Befehl ***Exit***.
   Nun wird der Logik-Editor geschlossen.
2. Klicken Sie im Dialogfeld **Edit Device Parameters** für den Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) auf **OK**.

WICHTIG:
- Um das Programm zu speichern und die Programmierung abzuschließen, müssen Sie nach dem Beenden des Logik-Editors im Dialogfeld **Edit Device Parameters** für den Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) auf **OK** klicken.
- Wenn Sie stattdessen auf **Cancel** klicken, werden die bis zu diesem Zeitpunkt eingegebenen Parametereinstellungen einschließlich des Programms nicht gespeichert. Durch Anwendung des Befehls ***File - Apply*** temporär gespeicherte Programme werden ebenfalls gelöscht.

6-2 Menübefehle

Die folgenden Befehle beschreiben die Menübefehle des Logik-Editors.

6-2-1 Menü „File“

Befehl	Beschreibung	Online	Offline
Apply	Temporäres Speichern des aktuellen Programms im Netzwerk-Konfigurator.	OK	OK
Import	Einlesen einer mithilfe des Befehls **Export** gespeicherten Datei.	OK	OK
Export	Speichern des aktuellen Programms in einer Datei. Sie können das in der Datei gespeicherte Programm in einen anderen Sicherheits-netzwerk-Controller NE1A (NE1A-SCPU01) importieren. Die Verbindungen zwischen den E/A-Tags werden jedoch nicht gespeichert.	OK	OK
Print	Drucken des Programms.	OK	OK
Page Setup	Einstellen des Seitenlayouts für den Druck.	OK	OK
Program Title	Programmtitel und Programmierer. Diese Informationen erscheinen im Ausdruck.	OK	OK
Exit	Beenden des Logik-Editors.	OK	OK

6-2-2 Menü „Edit“

Befehl	Beschreibung	Online	Offline
Cut	Ausschneiden des ausgewählten Funktionsblocks und Einfügen in die Zwischenablage.	OK	OK
Copy	Kopieren des ausgewählten Funktionsblocks in die Zwischenablage.	OK	OK
Paste	Kopieren des Funktionsblocks aus der Zwischenablage in den Arbeitsbereich.	OK	OK
Delete	Löschen des ausgewählten Elements.	OK	OK
Properties	Anzeigen der Eigenschaften des ausgewählten Funktionsblocks.	OK	OK

6-2-3 Menü „View“

Befehl	Beschreibung	Online	Offline
Object List	Ein- und Ausblenden der Objektliste.	OK	OK
Status Bar	Ein- und Ausblenden der Statuszeile.	OK	OK
Tool Bar	Ein- und Ausblenden der Werkzeugleiste.	OK	OK

6-2-4 Menü „Function“

Befehl		Beschreibung	Online	Offline
Transmission-Message Setting		Einstellen der Sendefunktion für explizite Meldungen.	OK	OK
Monitor Device		Überwachen der Werte der E/A-Tags und der Signalzustände aller Verbindungsleitungen im Logik-Editor.	OK	---
Jump Address	New	Erstellen einer neuen Sprungadresse (Sprungursprung).	OK	OK
	Select	Einfügen des Ziels der Sprungadresse in den Arbeitsbereich.	OK	OK

6-2-5 Menü „Page“

Befehl	Beschreibung	Online	Offline
Add Page	Hinzufügen einer neuen Seite hinter der letzten Seite.	OK	OK
Delete Last Page	Löschen der letzten Seite.	OK	OK
Change Page Title	Ändern des Titels der ausgewählten Seite.	OK	OK

6-3 Programmierung

6-3-1 Arbeitsbereich

Legen Sie zunächst die Größe des Arbeitsbereichs fest. Wählen Sie dazu in der Menüleiste ***File - Page Setup***.

Der Arbeitsbereich besteht aus Seiten der festgelegten Größe, die je nach Bedarf hinzugefügt und gelöscht werden können. Beim Drucken des Programms wird jede Seite mit der festgelegten Größe gedruckt.

WICHTIG: Enthält der Arbeitsbereich bereits Elemente, kann die Einrichtung der Seite nicht mehr geändert werden. Legen Sie daher zunächst mithilfe des Menübefehls ***File - Page Setup*** die Größe des Arbeitsbereichs fest.

Einschränkungen bei der Programmierung

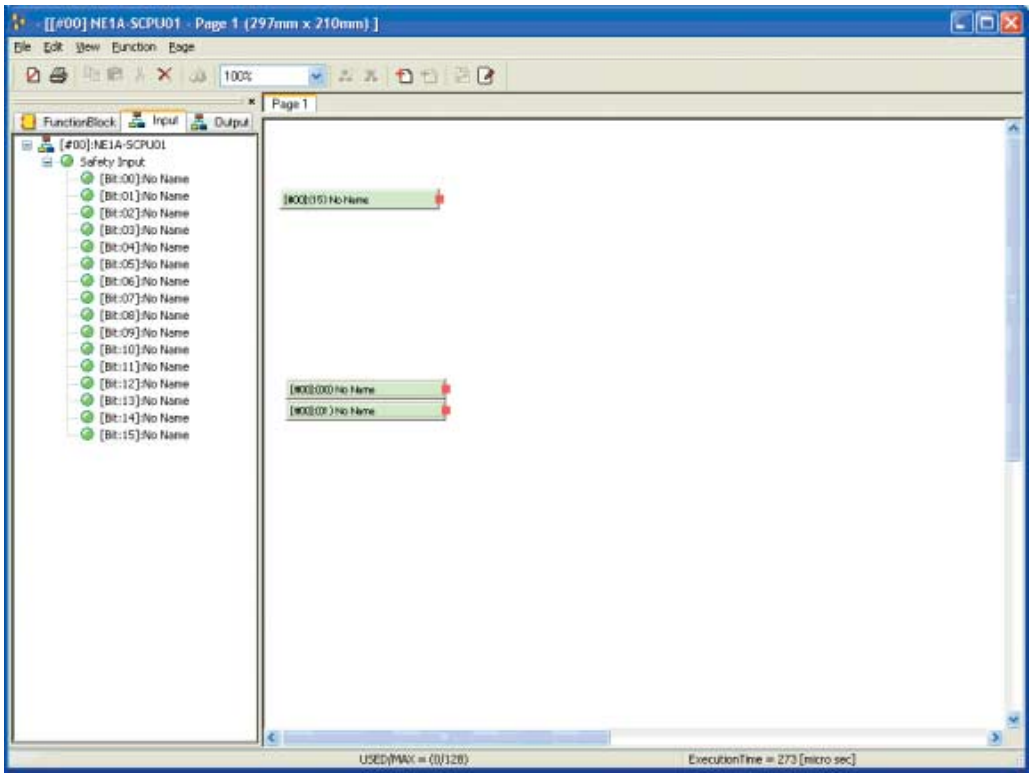
Elemente wie E/A-Tags und Funktionsblöcke können auf allen Seiten verwendet werden. Es gelten jedoch die folgenden Einschränkungen:

- Eingangs-Tags können auf mehreren Seiten verwendet werden, auf jeder Seite jedoch nur einmal.
- Ausgangs-Tags können nur ein einziges Mal auf nur einer Seite verwendet werden.
- Nur Funktionsblöcke können kopiert werden. E/A-Tags sowie Verbindungen zwischen E/A-Tags und zwischen Funktionsblöcken können nicht kopiert werden.
- Wird ein Funktionsblock eingefügt, wird er an derselben Position platziert, die der kopierte oder ausgeschnittene Funktionsblock hatte. Wenn Sie einen Funktionsblock auf derselben Seite wie den ursprünglichen Funktionsblock einfügen, müssen Sie den Ursprungs-Funktionsblock zuvor verschieben.
- Sie können maximal 128 Funktionsblöcke verwenden.
- Sie können maximal 128 Sprungadressen verwenden.
- Sie können maximal 32 Seiten verwenden.

6-3-2 Programmierung mit Funktionsblöcken

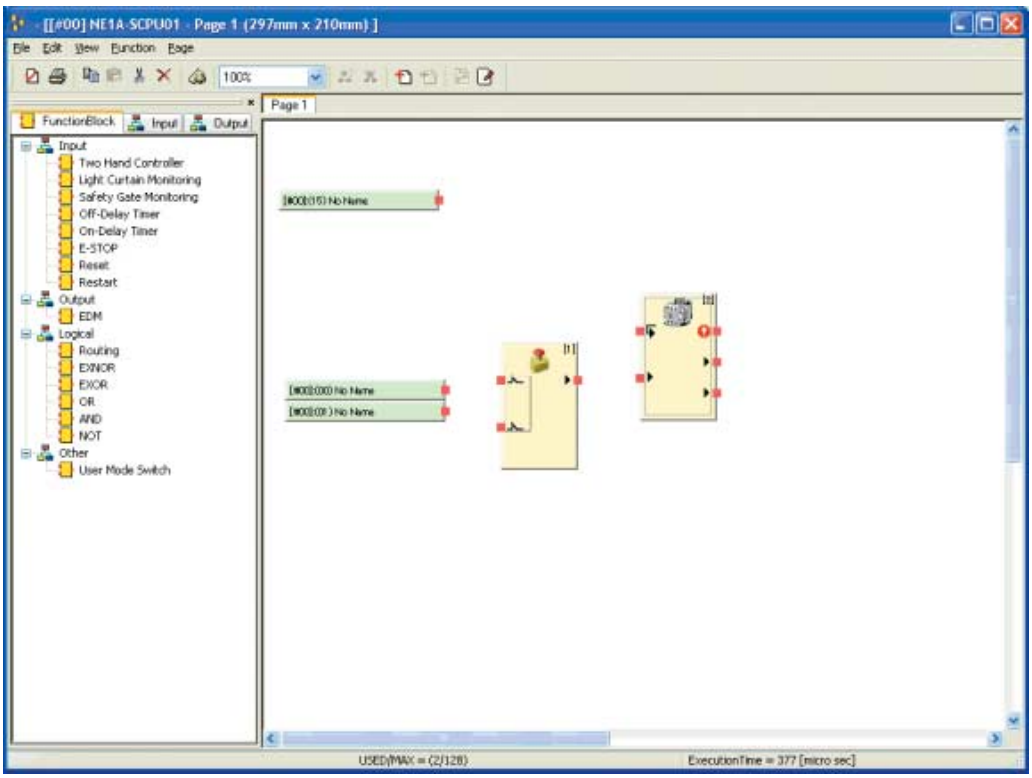
Platzieren von Eingangs-Tags

1. Klicken Sie in der Objektliste auf die Registerkarte **Input**.
2. Wählen Sie das gewünschte Eingangs-Tag aus, ziehen Sie es in den Arbeitsbereich, und legen Sie es an der gewünschten Position ab. Sie können auch mehrere Eingangs-Tags auf einmal auswählen und diese gleichzeitig im Arbeitsbereich platzieren.



Platzieren von Funktionsblöcken

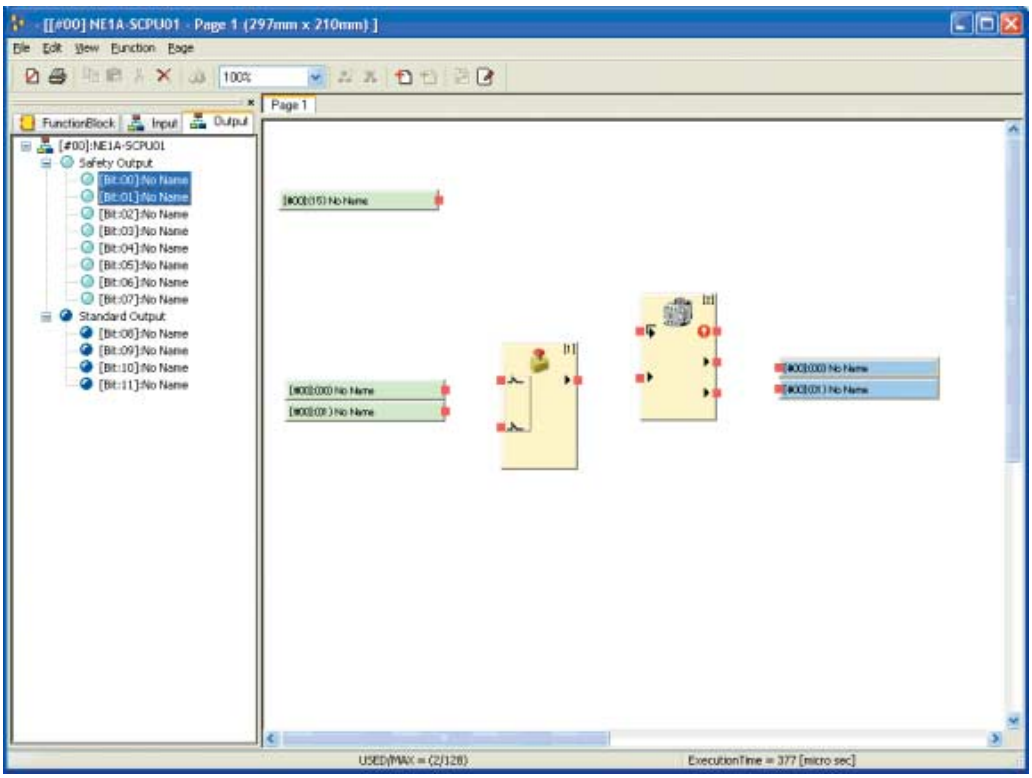
1. Klicken Sie in der Objektliste auf die Registerkarte **Function Block**.
2. Wählen Sie den gewünschten Funktionsblock aus, ziehen Sie ihn in den Arbeitsbereich, und legen Sie ihn an der gewünschten Position ab.



Platzieren von Ausgangs-Tags

1. Klicken Sie in der Objektliste auf die Registerkarte **Output**.
2. Wählen Sie das gewünschte Ausgangs-Tag aus, ziehen Sie es in den Arbeitsbereich, und legen Sie es an der gewünschten Position ab.

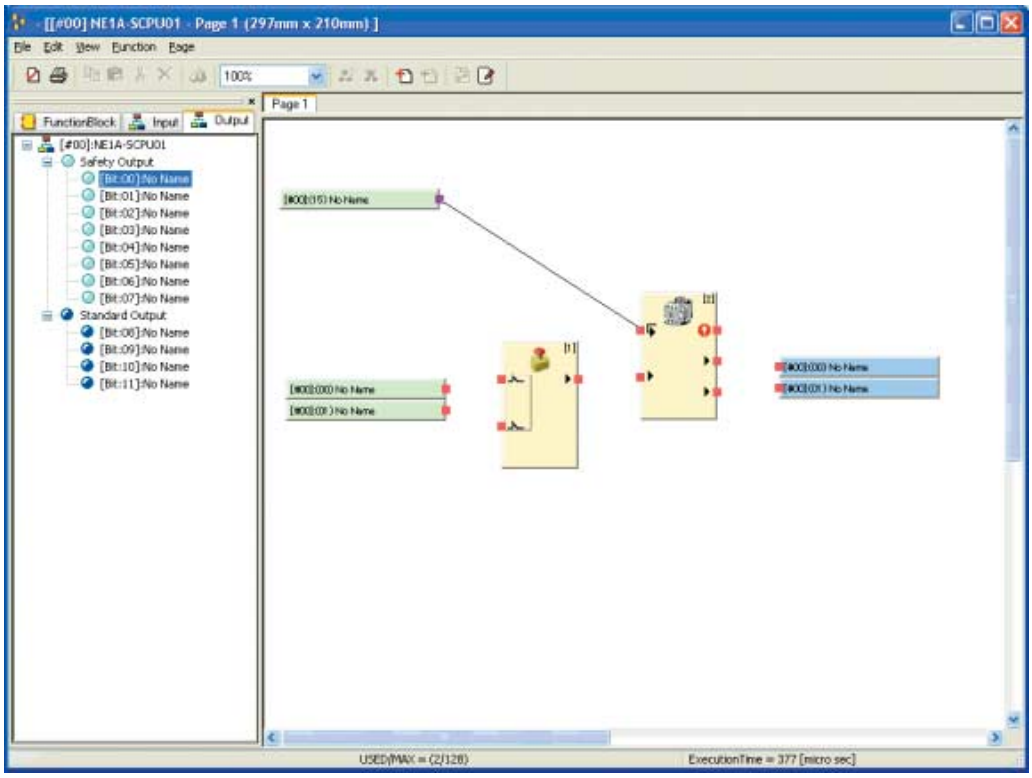
   Sie können auch mehrere Ausgangs-Tags auf einmal auswählen und diese gleichzeitig im Arbeitsbereich platzieren.



Verbindungen

Gehen Sie zum Verbinden von E/A-Tags und Funktionsblöcken folgendermaßen vor:

1. Klicken Sie auf den Quellanschluss (■), und ziehen Sie diesen zum Zielanschluss.



2. Erstellen Sie durch wiederholtes Herstellen von Verbindungen das gewünschte Programm.

Löschen von Elementen

E/A-Tags, Funktionsblöcke und Verbindungen können auf verschiedene Arten gelöscht werden:

(1) Wählen Sie das zu löschende Element aus, und wählen Sie in der Menüleiste ***Edit - Delete***.

(2) Wählen Sie das zu löschende Element aus, und klicken Sie in der Werkzeugleiste auf **Delete**.

(3) Klicken Sie mit der rechten Maustaste auf das zu löschende Element, und wählen Sie den Kontextmenübefehl ***Delete***.

(4) Wählen Sie das zu löschende Element aus, und drücken Sie die Entf-Taste oder die Rückschritttaste.

Hinzufügen und Löschen von Seiten

Hinzufügen von Seiten

Das Hinzufügen einer Seite kann auf verschiedene Arten erfolgen. Die neue Seite wird hinter der letzten Seite hinzugefügt.

(1) Wählen Sie dazu in der Menüleiste ***Page - Add Page***.

(2) Klicken Sie in der Werkzeugleiste auf **Add Page**.

Löschen von Seiten

Das Löschen einer Seite kann auf verschiedene Arten erfolgen. Die jeweils letzte Seite wird gelöscht.

(1) Wählen Sie dazu in der Menüleiste ***Page - Delete Last Page***.

(2) Klicken Sie in der Werkzeugleiste auf **Delete Last Page**.

Seitentitel

Sie können für jede Seite einen Titel festlegen. Die Eingabe dieses Titels kann beim Hinzufügen der Seite erfolgen. Zu einem späteren Zeitpunkt kann der Seitentitel auf verschiedene Arten geändert werden:

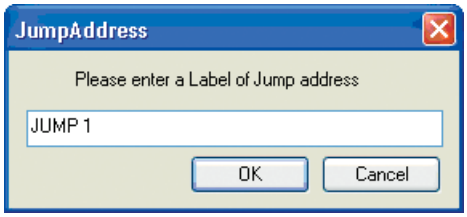
(1) Wählen Sie in der Menüleiste ***Page - Change Page Title***.

(2) Klicken Sie im Arbeitsbereich mit der rechten Maustaste auf die Registerzunge der Seite, und wählen Sie den Kontextmenübefehl ***Change Page Title***.

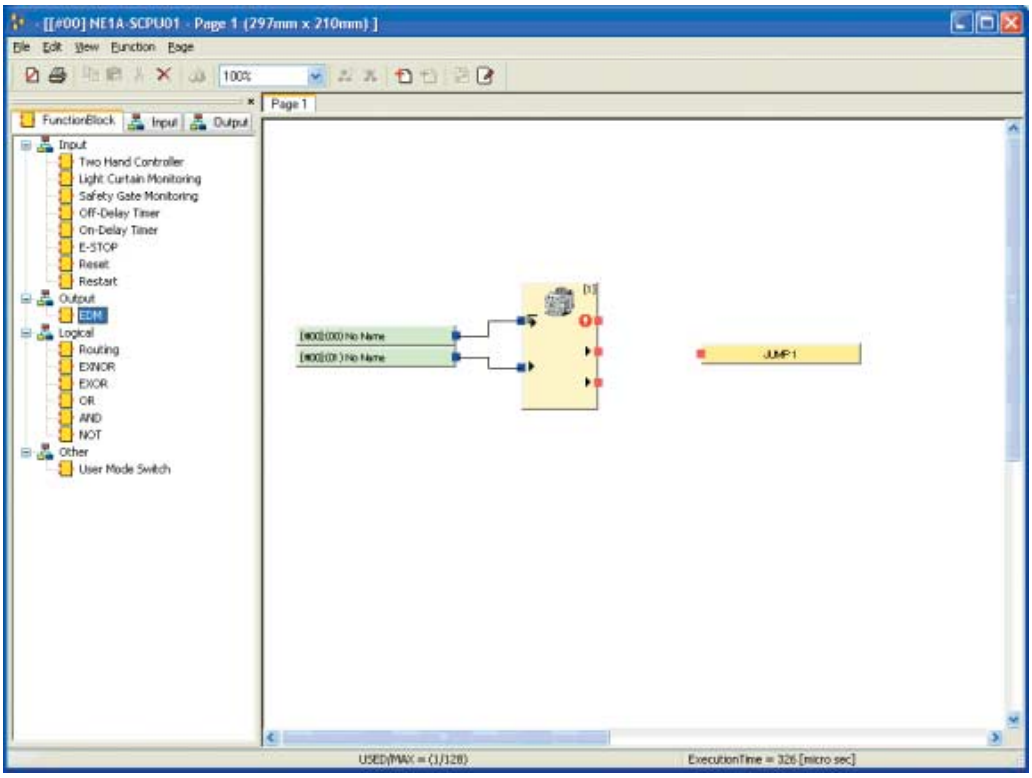
Sprungadressen

Die Sprungadressenbefehle erleichtern die Erstellung komplexer und/oder mehrere Seiten belegender Programme.

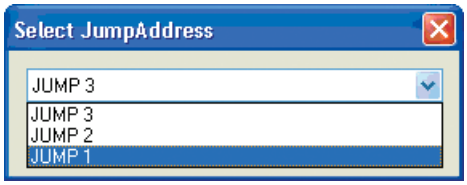
1. Legen Sie zunächst auf eine der folgenden Weisen den Sprungursprung fest;
   (1) Wählen Sie in der Menüleiste ***Function - Jump Address - New***.
   (2) Klicken Sie mit der rechten Maustaste in den Arbeitsbereich, und wählen Sie den Kontextmenübefehl ***Jump Address***.



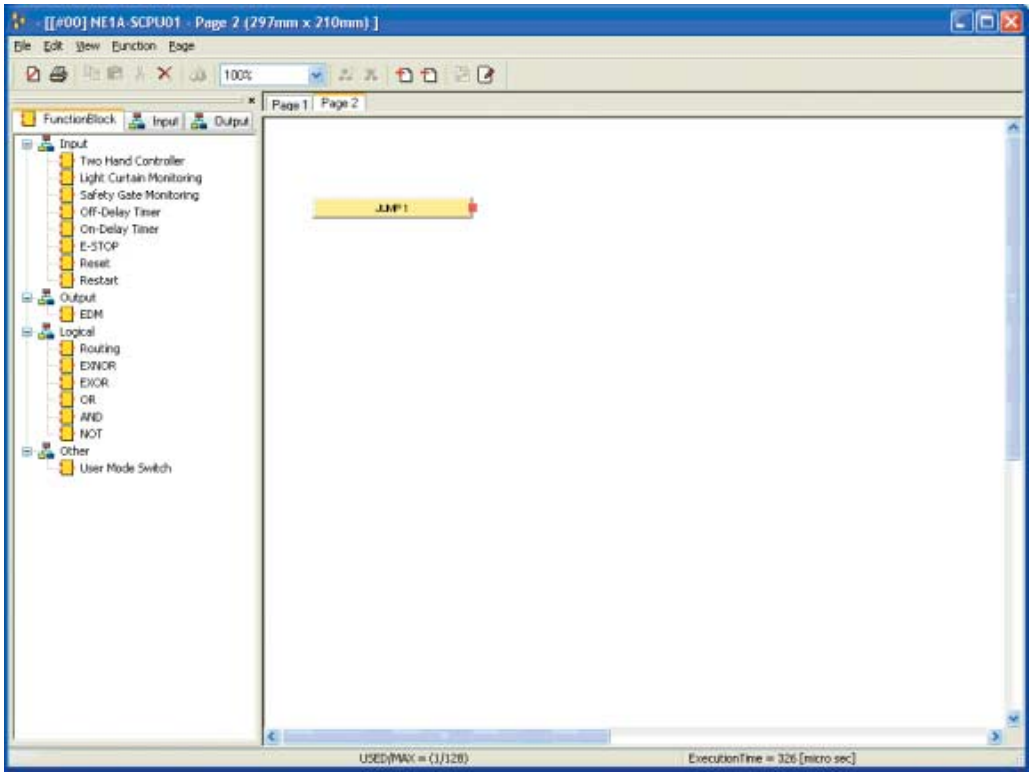
2. Geben Sie einen Namen für die Sprungadresse ein, und klicken Sie auf **OK**.
   Die Sprungadresse wird folgendermaßen angezeigt:



3. Geben Sie auf eine der folgenden Weisen das Sprungziel ein:
   (1) Wählen Sie in der Menüleiste ***Function - Jump Address - Select***.
   (2) Klicken Sie mit der rechten Maustaste in den Arbeitsbereich, und wählen Sie den Kontextmenübefehl ***Select Jump Address***.



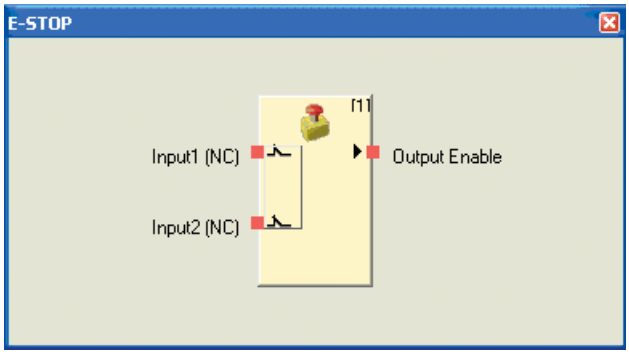
4. Wählen Sie den Namen des Sprungursprungs aus, und klicken Sie auf **OK**.
   Die Sprungadresse wird folgendermaßen angezeigt:



Funktionsblock-E/A-Information

Die E/A-Information eines Funktionsblocks kann auf eine der folgenden Weisen bestätigt werden:

- Klicken Sie mit der rechten Maustaste auf den Funktionsblock, und wählen Sie ***Detail***.



Bearbeiten von Funktionsblockparametern

Die Bearbeitung der Parameter eines Funktionsblocks erfolgt im Parameterbearbeitungsfenster. Zum Aufrufen dieses Fensters gehen Sie auf eine der folgenden Arten vor:

(1) Wählen Sie den Funktionsblock aus, und wählen Sie in der Menüleiste ***Edit Properties***.

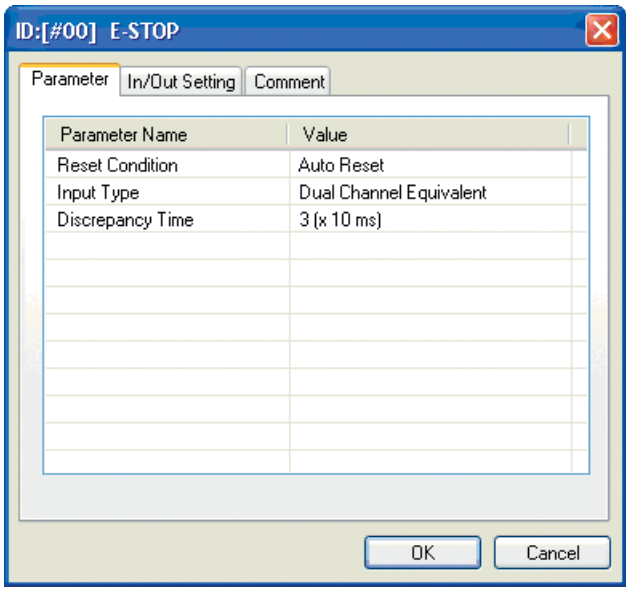
(2) Klicken Sie mit der rechten Maustaste auf den Funktionsblock, und wählen Sie den Kontextmenübefehl ***Edit***.

(3) Wählen Sie den Funktionsblock aus, und klicken Sie in der Werkzeugleiste auf ***Property***.

Hinweis: Anzahl und Art der bearbeitbaren Parameter hängen von dem jeweiligen Funktionsblock ab. Detailinformationen finden Sie im *NE1A-SCPU01 Bedienerhandbuch für den Sicherheitsnetzwerk-Controller (Cat. No. Z906-DE1)*.

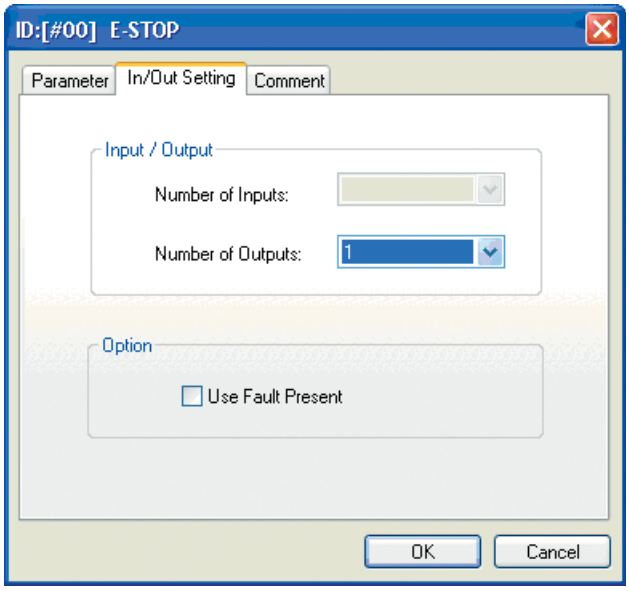
Parameter

Zum Einstellen der Parameter des Funktionsblocks klicken Sie auf die Registerkarte **Parameter**.



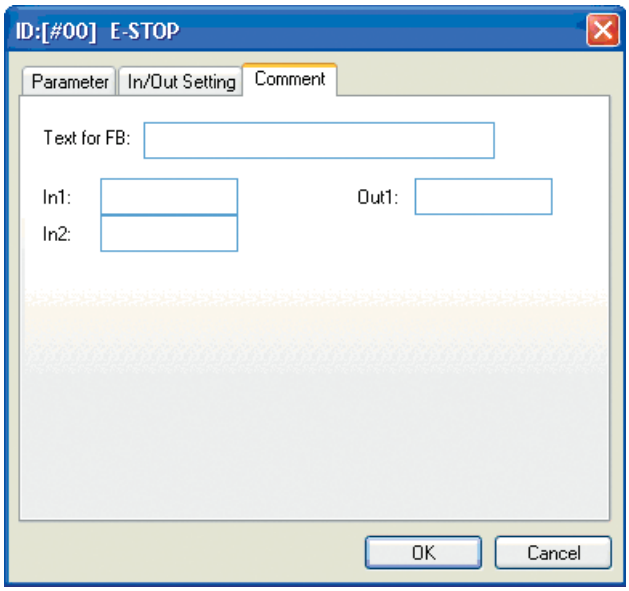
Ein-/Ausgangseinstellungen

Zum Einstellen der Zahl der Ein- und Ausgänge sowie der Option *Fault Present* klicken Sie auf die Registerkarte **In/Out Setting**.



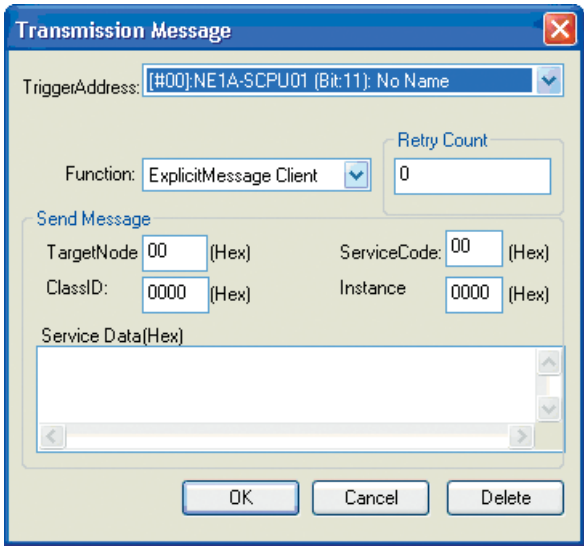
Kommentar

Zum Eingeben von Namen für den Funktionsblock oder für E/A-Signale klicken Sie auf die Registerkarte **Comment**. Die Namen der E/A-Signale werden im Fenster nicht angezeigt, wohl aber der Name des Funktionsblocks (unterhalb des Funktionsblocks). Wenn Sie das Programm drucken, werden jedoch alle in diesem Fenster eingegebenen Namen gedruckt.



Senden von expliziten Meldungen

Wird ein als Trigger definiertes Ausgangs-Tag auf EIN gesetzt, kann eine hier vorab festgelegte explizite Meldung versendet werden. Für das gesamte Programm kann nur eine explizite Meldung festgelegt werden. Wählen Sie dazu in der Menüleiste *Function TransmissionMessage Setting*.



TriggerAddress

Wählen Sie das Ausgangs-Tag aus, das als Trigger für das Versenden der expliziten Meldungfungieren soll. Jedes Mal, wenn dieses Ausgangs-Tag seinen Zustand von AUS nach EIN ändert, wird die hier festgelegte explizite Meldung versendet.

Retry Count

Legen Sie hier fest, wie oft das Senden der expliziten Meldung beim Auftreten eines Übertragungsfehlers wiederholt werden soll.

Ist dieser Parameter auf 0 eingestellt, erfolgt keine Wiederholung.

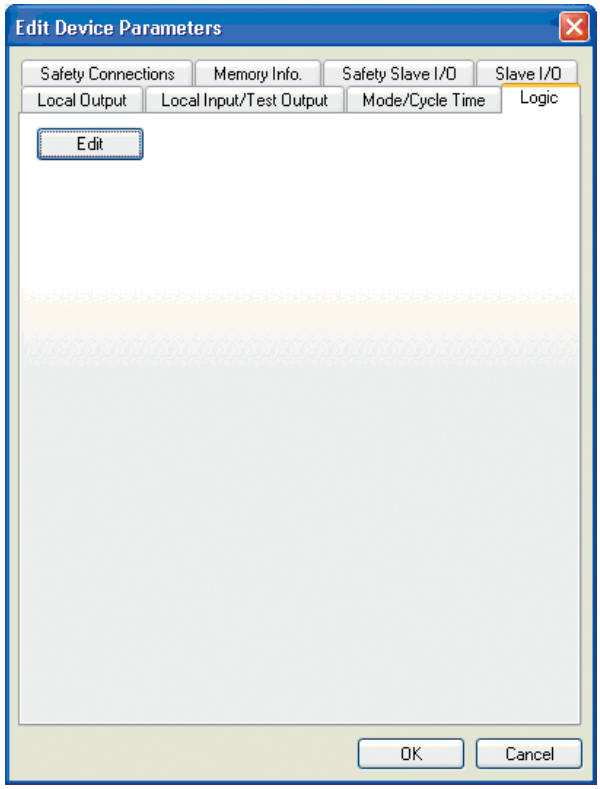
Send Message

- TargetNode
  Stellen Sie hier die Adresse (hexadezimal) des Zielknotens ein, an den die explizite Meldung gesendet werden soll.
- ServiceCode
  Stellen Sie hier den Servicecode (hexadezimal) der expliziten Meldung ein.
- ClassID
  Stellen Sie hier die Klassen-ID (hexadezimal) der expliziten Meldung ein.
- Instance
  Stellen Sie hier die Instanzen-ID (hexadezimal) der expliziten Meldung ein.
- Service Data
  Geben Sie hier beliebige Daten (hexadezimal) für die explizite Meldung ein.

6-3-3 Speichern des Programms

Gehen Sie zum Speichern des Programms wie folgt vor:

1. Wählen Sie in der Menüleiste *File - Apply*.
   Das Programm wird temporär im Netzwerk-Konfigurator gespeichert. Wenn Sie den Logik-Editor beenden, werden die Daten ebenfalls temporär gespeichert.
2. Klicken Sie nach dem Beenden des Logik-Editors im Dialogfeld **Edit Device Parameters** für den Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) auf **OK**.



3. Zum Speichern der Datei wählen Sie im Hauptfenster des Netzwerk-Konfigurators *File* und *Save* oder *Save As*.

WICHTIG:
- Um das Programm zu speichern und die Programmierung abzuschließen, müssen Sie nach dem Beenden des Logik-Editors im Dialogfeld **Edit Device Parameters** für den Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) auf **OK** klicken.
- Wenn Sie stattdessen auf **Cancel** klicken, werden die bis zu diesem Zeitpunkt eingegebenen Parametereinstellungen einschließlich des Programms nicht gespeichert. Durch Anwendung des Befehls ***File - Apply*** temporär gespeicherte Programme werden ebenfalls gelöscht.

6-3-4 Aktualisieren eines Programms

Bei einer Änderung der E/A-Tags der Sicherheits-Slaves, die die lokale E/A des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) konfigurieren (z. B. beim Hinzufügen oder Löschen von E/A-Tags), müssen Sie den Logik-Editor aufrufen und das Programm überprüfen.

Wenn Sie die Parameter ohne vorherigen Aufruf des Logik-Editors in den Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) herunterladen, tritt aufgrund der Inkonsistenz der Daten im Logik-Editor ein Herunterlade-Fehler auf. Rufen Sie in diesem Fall den Logik-Editor auf, überprüfen Sie das Programm, und nehmen Sie die erforderlichen Modifikationen vor.

6-3-5 Überwachung des Programms

Die Werte der E/A-Tags und die Signalzustände aller Verbindungen mit Funktionsblöcken können online im Logik-Editor überwacht werden. Stellen Sie sicher, dass der Netzwerk-Konfigurator mit dem Netzwerk verbunden ist und dass sich der zu überwachende Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) in der RUN-Betriebsart befindet, bevor Sie die Online-Programm-Überwachung starten.

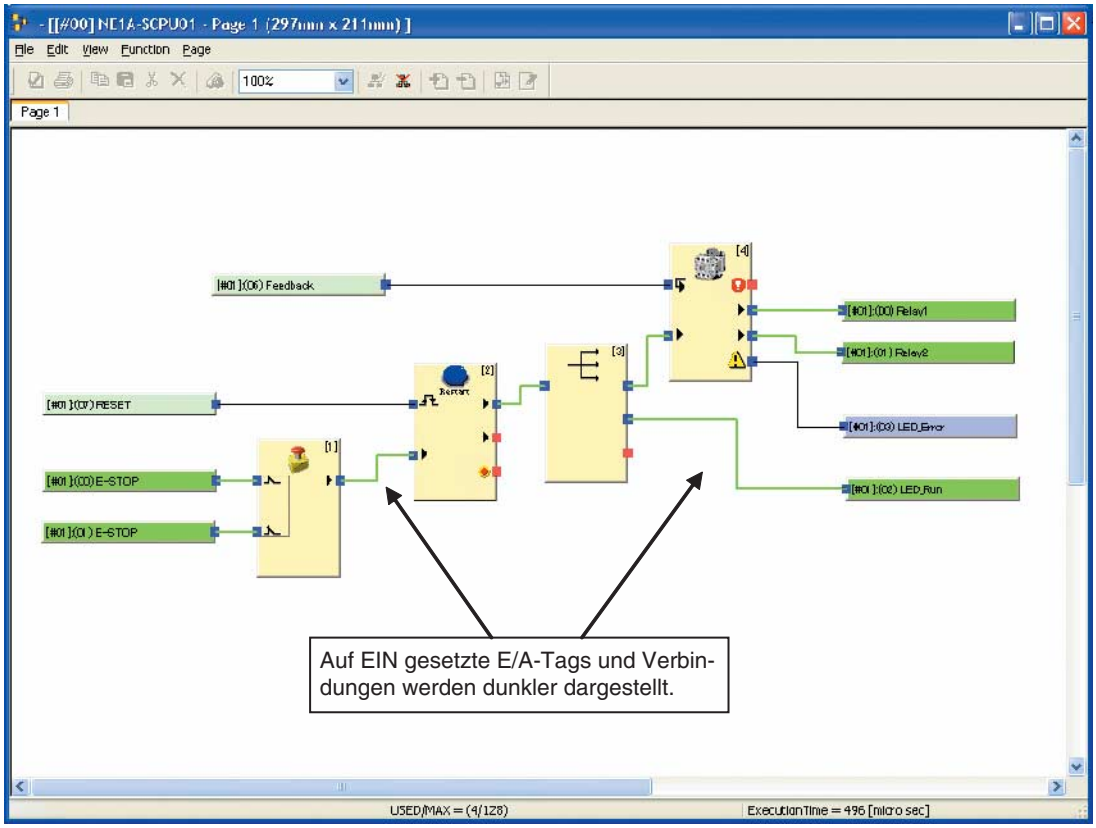
Starten der Online-Überwachung

Die Online-Überwachung kann auf die folgenden Arten gestartet werden:

(1) Wählen Sie in der Menüleiste ***Function - Monitoring***.

(2) Klicken Sie in der Werkzeugleiste auf **Monitoring**.

Bei der Überwachung werden die auf EIN gesetzten E/A-Tags und Verbindungen dunkler dargestellt.



Stoppen der Online-Überwachung

Die Online-Überwachung kann auf die folgenden Arten gestoppt werden:

(1) Wählen Sie in der Menüleiste erneut **Function - Monitoring**.

(2) Klicken Sie in der Werkzeugleiste auf **Stop Monitoring**.

7-1 Überwachungsfunktion

DeviceNet Safety-Geräte verfügen über eine Vielzahl interner Statusinformationen. Diese Informationen können mithilfe des Netzwerkkonfigurators überwacht werden.

7-1-1 Statusüberwachung

Beschreibung

Der Status von Sicherheitsnetzwerk-Controllern NE1A (NE1A-SCPU01) und DST1-Sicherheits-E/A-Modulen kann mithilfe des Netzwerkkonfigurators überwacht werden. Beim Auftreten eines Fehlers in einem Gerät kann auf detaillierte Informationen zu diesem Fehler zugegriffen werden.

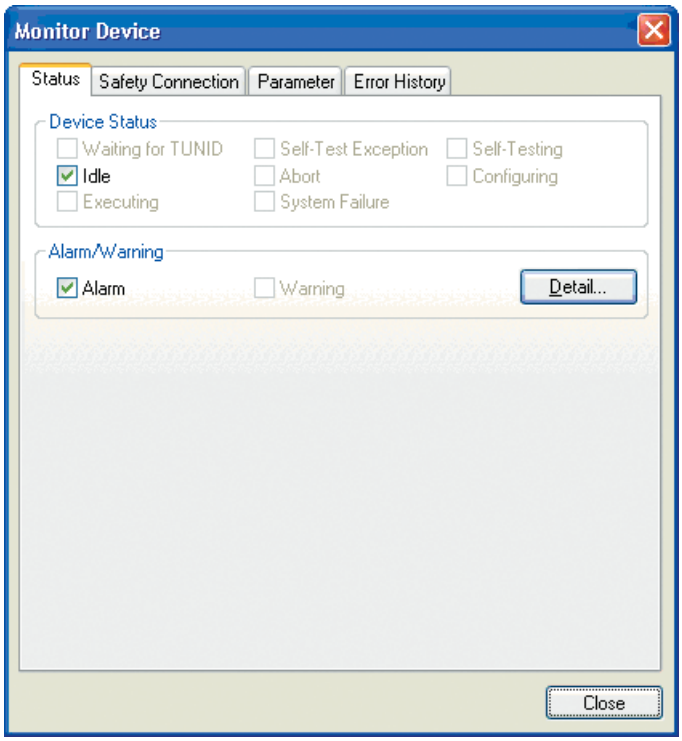
Statusüberwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zum Überwachen des Status eines Geräts auf eine der folgenden Arten vor:

(1) Wählen Sie das Gerät aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Status**.

(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Status**.

(3) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Status**.



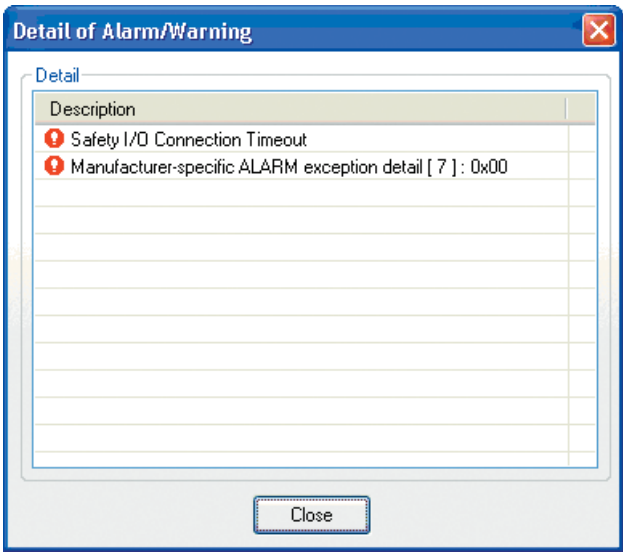
Gerätestatus

Auf der Registerkarte wird der Gerätestatus angezeigt.

Alarm/Warning

In diesem Bereich werden Fehler und Warnmeldungen angezeigt, die in dem Gerät aufgetreten sind.

Zur näheren Analyse eines Fehlers klicken Sie auf **Detail**. Das Symbol kennzeichnet Alarme, das Symbol Warnmeldungen.



7-1-2 Überwachen von Sicherheitsverbindungen

Beschreibung

Der Sicherheitsverbindungsstatus von Sicherheitsnetzwerk-Controllern NE1A (NE1A-SCPU01) kann mithilfe des Netzwerkkonfigurators überwacht werden. Auf diese Weise können Sie beim Auftreten von Fehlern in der Sicherheitskommunikation feststellen, welches Gerät und welche Sicherheitsverbindung von diesem Fehler betroffen ist. Verbindungsinformationen von DST1-Sicherheits-E/A-Modulen können nicht überwacht werden.

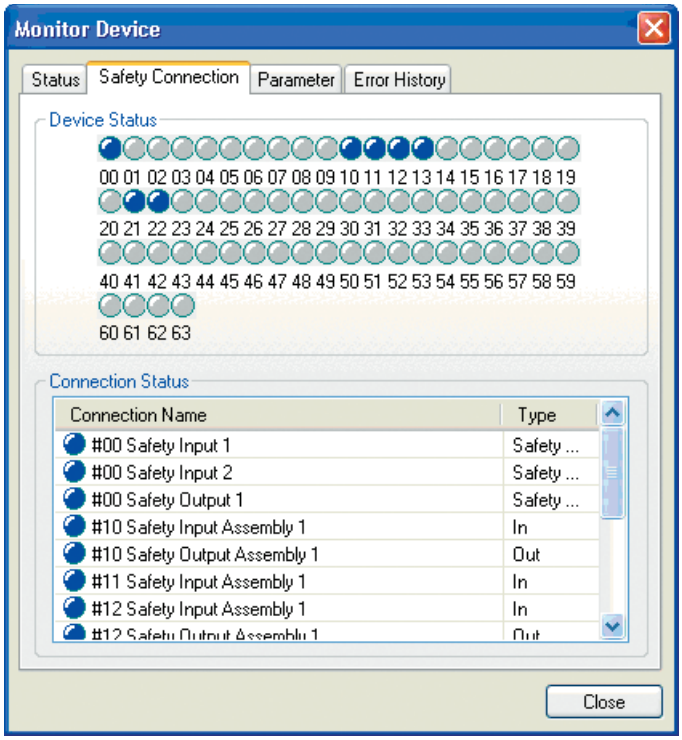
Überwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zum Überwachen des Status der Sicherheitsverbindungen auf eine der folgenden Arten vor:

(1) Wählen Sie den Sicherheitsnetzwerk-Controller (NE1A-SCPU01) aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Safety Connection**.

(2) Wählen Sie den Sicherheitsnetzwerk-Controller (NE1A-SCPU01) aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Safety Connection**.

(3) Klicken Sie mit der rechten Maustaste auf den Sicherheitsnetzwerk-Controller (NE1A-SCPU01), und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Safety Connection**.



Der Verbindungsstatus des Sicherheits-Slaves wird für die lokale Knotenadresse angezeigt. Für die anderen Knotenadressen wird der Status der für die Geräteparameter konfigurierten Sicherheitsverbindungen angezeigt.

Gerätestatus

Im Bereich **Device Status** kann der Verbindungsstatus für die einzelnen Knotenadressen überprüft werden. Der Verbindungsstatus wird durch die folgenden Farben angezeigt:

Farbe	Status
Grau	Nicht registriertes Gerät
Grün	Alle Verbindungen senden Leerlaufdaten.
Blau	Alle Verbindungen kommunizieren normal.
Gelb	Mindestens eine Verbindung ist nicht verbunden oder sendet Leerlaufdaten. (Es ist ein Fehler aufgetreten und es besteht keine Verbindung.)
Rot	In mindestens einer Verbindung ist ein Fehler aufgetreten.

Für die lokale Knotenadresse (d. h. die Knotenadresse des Sicherheits-Slaves) zeigt die Farbe Grau an, dass keine Verbindungen bestehen oder dass ein Fehler in einer Verbindung aufgetreten ist. Die Farbe Blau zeigt an, dass bei einer oder mehreren Verbindungen normale Kommunikation stattfindet.

Connection Status

Im Bereich **Connection Status** kann der Status für die einzelnen Sicherheitsverbindungen überprüft werden. Der Verbindungsstatus wird durch die folgenden Farben angezeigt:

Farbe	Status
Grau	Verbindung ist nicht hergestellt.
Grün	Es werden Leerlaufdaten übertragen.
Blau	Es findet normale Kommunikation statt.
Rot	Es ist ein Kommunikationsfehler aufgetreten.

Für die lokale Knotenadresse (d. h. die Knotenadresse des Sicherheits-Slaves) zeigt die Farbe Grau an, dass keine Verbindungen bestehen oder dass ein Fehler in der Verbindung aufgetreten ist. Die Farbe Blau zeigt normale Kommunikation an.

7-1-3 Überwachen von Parametern

Beschreibung

Der E/A-Status von Sicherheitsnetzwerk-Controllern NE1A (NE1A-SCPU01) und DST1-Sicherheits-E/A-Modulen kann mithilfe des Netzwerkkonfigurators überwacht werden. Durch Überwachung des E/A-Status können Sie beim Auftreten von Problemen mit der Konfiguration oder bei Fehlern in E/A-Punkten die Fehlerursache bestimmen.

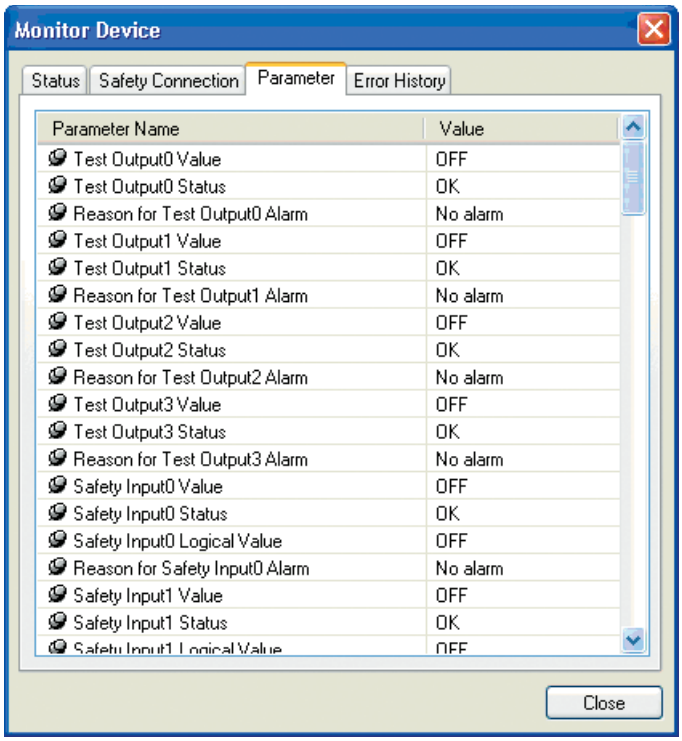
Überwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zum Überwachen der Parameter auf eine der folgenden Arten vor:

(1) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Parameter**.

(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Parameter**.

(3) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Parameter**.



Klemmenstatus von Testausgängen

Eintrag	Beschreibung
Test Output Value	Ausgangswert des Testausgangs.
Test Output Status	Bewertungsergebnis für den Testausgang. Beim Auftreten eines Fehlers wird „Alarm“ angezeigt.
Reason for Test Output Alarm	Ursache des Fehlers.

Klemmenstatus von Sicherheitseingängen

Eintrag	Beschreibung
Safety Input Value	Eingangswert des Sicherheitseingangs.
Safety Input Status	Bewertungsergebnis für den Sicherheitseingang im Einkanalmodus. Beim Auftreten eines Fehlers wird „Alarm“ angezeigt.
Safety Input Logical Value	Logisches Äquivalent des Bewertungsergebnisses.
Reason for Safety Input Alarm	Ursache des Fehlers.

Klemmenstatus von Sicherheitsausgängen

Eintrag	Beschreibung
Safety Output Value	Ausgangswert des Sicherheitsausgangs.
Safety Output Monitor Value	Überwachungswert für den Ausgang des Sicherheitsausgangs.
Safety Output Status	Bewertungsergebnis für den Sicherheitsausgang im Einkanalmodus. Beim Auftreten eines Fehlers wird „Alarm“ angezeigt.
Reason for Safety Output Alarm	Ursache des Fehlers.

Status von Sicherheitseingängen im Zweikanalmodus

Eintrag	Beschreibung
Dual Channel Safety Input Evaluation	Bewertungsergebnis für den Sicherheitseingang im Zweikanalmodus. Beim Auftreten eines Fehlers wird „Alarm“ angezeigt.

7-1-4 Überwachung der Fehlerhistorie

Beschreibung

Die Fehlerhistorie von Sicherheitsnetzwerk-Controllern NE1A (NE1A-SCPU01) und DST1-Sicherheits-E/A-Modulen kann mithilfe des Netzwerkkonfigurators überwacht werden.

Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) können intern bis zu 20 Fehlerhistoriendatensätze speichern, DST1-Sicherheits-E/A-Module bis zu 10 Fehlerhistoriendatensätze. Treten bei bereits maximal gefüllter Fehlerhistorie weitere Fehler auf, wird der jeweils älteste Datensatz überschrieben.

Informationen zu bestimmten Fehlern werden im nichtflüchtigen Speicher abgelegt und beim Ausschalten der Spannungsversorgung nicht gelöscht. Informationen zu anderen Fehlern werden im RAM abgelegt und beim Ausschalten der Spannungsversorgung gelöscht. Detaillierte Informationen hierzu finden Sie in den jeweiligen Bedienerhandbüchern.

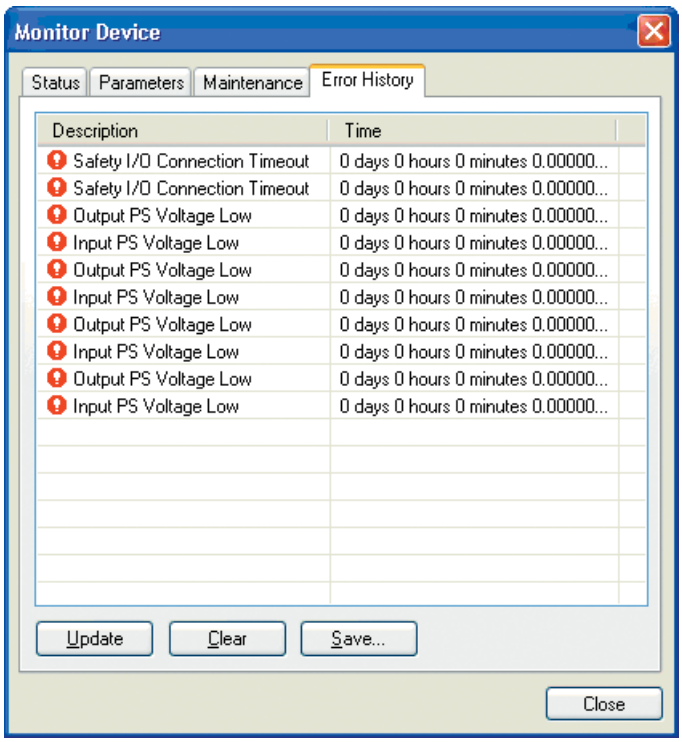
Überwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zum Überwachen der Fehlerhistorie eines Geräts auf eine der folgenden Arten vor:

(1) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Error History**.

(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Error History**.

(3) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Error History**.



Fehlerhistorieneinträge

Eintrag	Beschreibung
Description	Fehlerdetails
Time	Gesamtbetriebsdauer des Geräts zum Zeitpunkt des Auftretens des Fehlers. DST1-Sicherheits-E/A-Module unterstützen diese Funktion nicht, daher wird bei diesen in dieser Spalte stets der Wert 0 angezeigt.

Speichern der Fehlerhistorie

Die Fehlerhistorie kann im CSV-Format gespeichert werden. Klicken Sie dazu auf **Save**.

Löschen der Fehlerhistorie

Zum Löschen der im Sicherheitsnetzwerk-Controller NE1A (NE1A-SCPU01) oder DST1-Sicherheits-E/A-Modul intern gespeicherten Fehlerhistorie klicken Sie auf **Clear**.

Aktualisieren der Fehlerhistorie

Zum Aktualisieren der Fehlerhistorie klicken Sie auf **Update**.

7-2 Wartungsfunktionen für DST1-Sicherheits-E/A-Module

DST1-Sicherheits-E/A-Module unterstützen dieselben Wartungsfunktionen wie DRT2-Smart-Slaves. Bei letzteren handelt es sich um Standard-Slaves.

7-2-1 Überwachung der Netzwerk-Versorgungsspannung

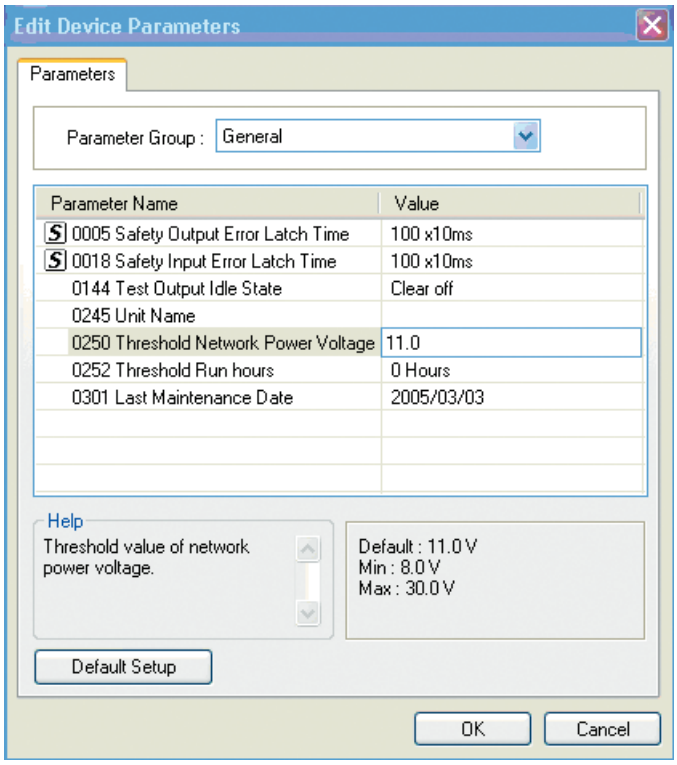
Beschreibung

DST1-Sicherheits-E/A-Module überwachen jederzeit den aktuellen Wert der Netzwerk-Versorgungsspannung und speichern Minimum und Maximum dieses Werts. Fällt die Spannung unter einen eingestellten Grenzwert ab (Standardeinstellung: 11 V), wird der Fehlermerker **Threshold Network Power Voltage** des allgemeinen Status auf EIN gesetzt. Sie können diese Information mithilfe des Netzwerkkonfigurators und expliziten Meldungen überwachen.

Hinweis:
- DeviceNet erfordert eine minimale Kommunikations-Versorgungsspannung von 11 V. Fällt die Spannung unter 11 V ab, kann der Netzwerkkonfigurator gemessene Werte möglicherweise nicht mehr lesen.
- Beim Ausschalten der Spannungsversorgung des DST1-Sicherheits-E/A-Moduls (Netzwerkspannung) werden die Angaben zur Minimum und Maximum der Versorgungsspannung gelöscht.

Einstellen des Grenzwerts für die Überwachung der Netzwerk-Versorgungsspannung mithilfe des Netzwerkkonfigurators

Die Einstellung des Grenzwerts für die Überwachung der Netzwerk-Versorgungsspannung erfolgt im Feld *Threshold Network Power Voltage* der Parametergruppe **General**.



Überwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zum Überwachen des aktuellen, des minimalen und des maximalen Werts der Netzwerk-Versorgungsspannung im allgemeinen Status auf eine der folgenden Arten vor:

(1) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Maintenance Information***.

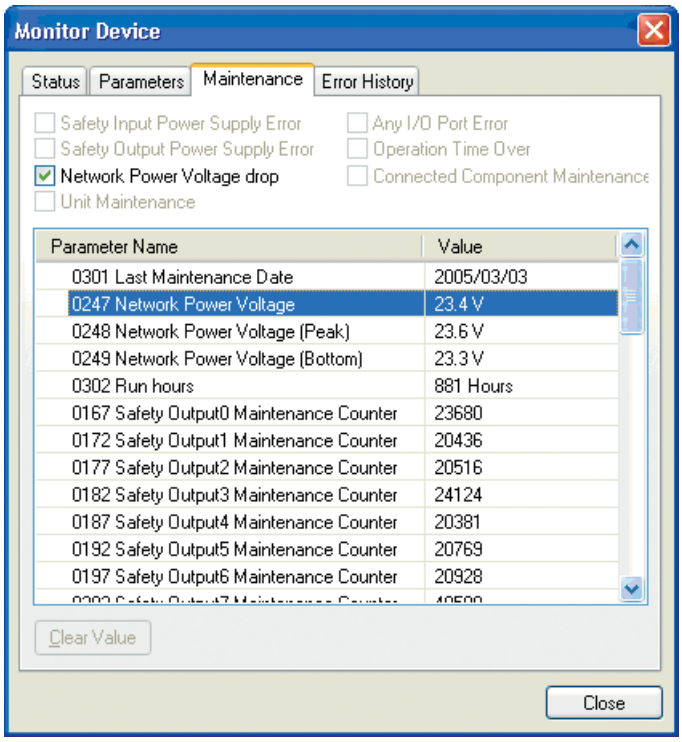
(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Maintenance Information**.

(3) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Maintenance Information***.

(4) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(5) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(6) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.



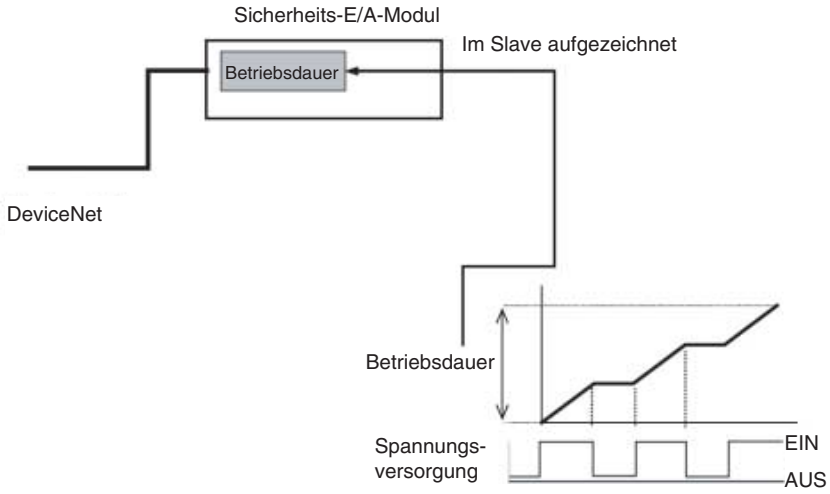
Sie können die angezeigten Werte zur maximalen und minimalen Netzwerk-Versorgungsspannung löschen. Wählen Sie dazu den jeweiligen Wert aus, und klicken Sie auf **Clear Value**.

7-2-2 Überwachung der Betriebsdauer

Beschreibung

DST1-Sicherheits-E/A-Module registrieren die Gesamtbetriebsdauer, also die Zeit, in der die Versorgungsspannung anliegt, und speichern diese im nichtflüchtigen Speicher. Erreicht diese Betriebsdauer den eingestellten Grenzwert, wird der Merker **Unit Maintenance** im allgemeinen Status auf EIN gesetzt.

- Mögliche Werte: 0 bis 429.496.729,5 Stunden (interne Repräsentation: 0000 0000 bis FFFF FFFF hex)
- Auflösung: 0,1 Stunde

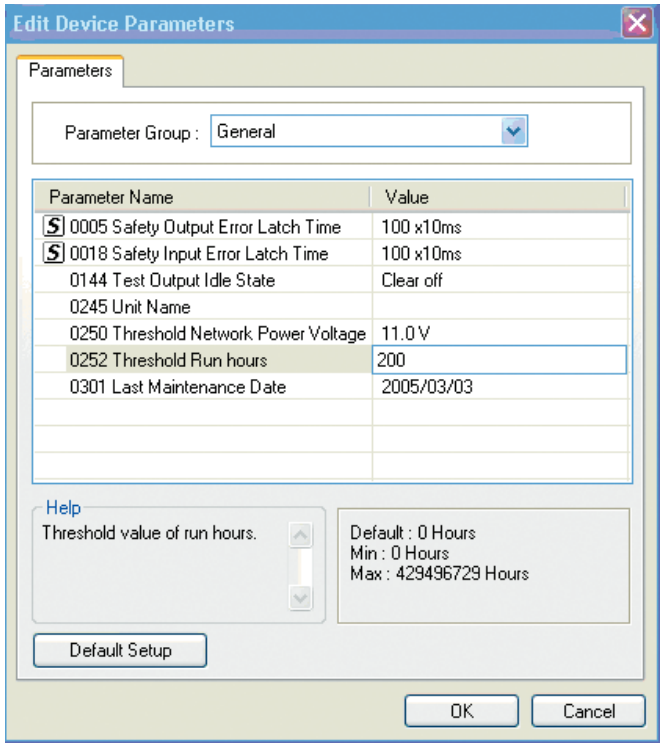


Sie können diese Information mithilfe des Netzwerkkonfigurators und expliziten Meldungen überwachen.

Hinweis:
- Die Betriebsdauerüberwachung summiert die Zeiten auf, in denen die Spannungsversorgung des DST1-Sicherheits-E/A-Moduls (Netzwerk-Spannungsversorgung) eingeschaltet ist. Die Zeiträume, in denen die Spannungsversorgung ausgeschaltet ist, werden nicht berücksichtigt.
- Die interne Aufsummierung der Betriebsdauer erfolgt bei DST1-Sicherheits-E/A-Modulen in 0,1-Stunden-Schritten. Die Eingabe des Grenzwerts für die Betriebsdauer im Netzwerkkonfigurator und die Überwachung der Gesamtbetriebsdauer auf die Überschreitung dieses Grenzwerts erfolgt jedoch in 1-Stunden-Schritten.

Einstellen des Grenzwerts für die Überwachung der Betriebsdauer mithilfe des Netzwerkkonfigurators

Die Einstellung des Grenzwerts für die Überwachung der Betriebsdauer erfolgt im Feld *Threshold Run hours* der Parametergruppe General.



Ist der Grenzwert auf 0 eingestellt, erfolgt keine Überwachung der Betriebsdauer.

Überwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zur Überwachung der Betriebsdauer im allgemeinen Status auf eine der folgenden Arten vor:

(1) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Maintenance Information***.

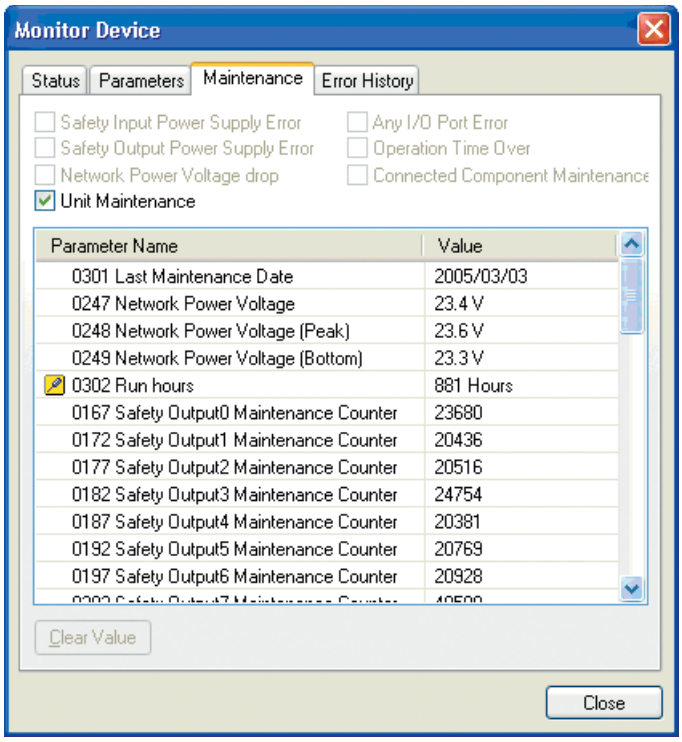
(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Maintenance Information**.

(3) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Maintenance Information***.

(4) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(5) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(6) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.



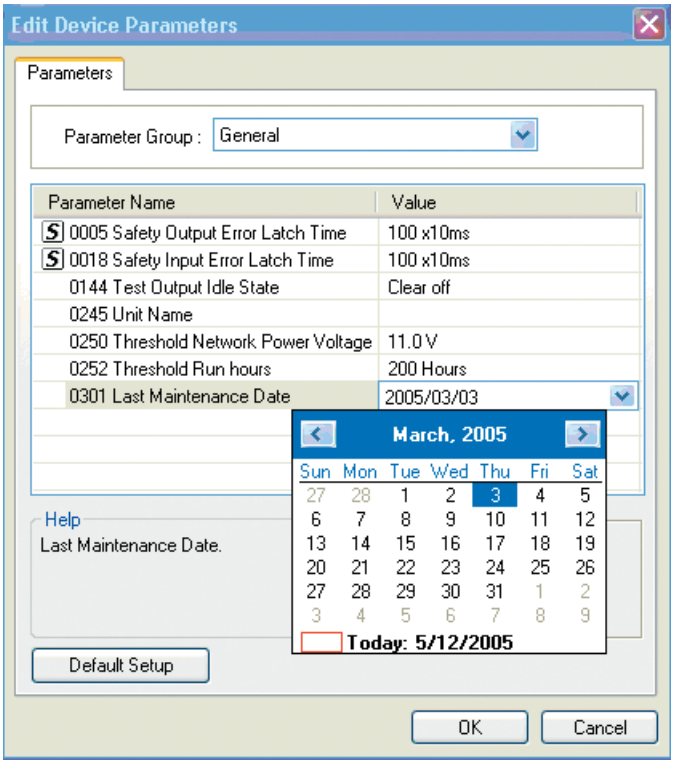
7-2-3 Letzter Wartungstermin

Beschreibung

DST1-Sicherheits-E/A-Module können den letzten Wartungstermin intern im nichtflüchtigen Speicher speichern. Anhand dieser Information können Sie leicht den nächsten Wartungstermin festlegen. Der gespeicherte Wartungstermin kann mithilfe des Netzwerkkonfigurators und expliziten Meldungen abgerufen werden.

Aufzeichnen des Wartungstermins mithilfe des Netzwerkkonfigurators

Die Aufzeichnung des letzten Wartungstermins erfolgt im Parameter **Last Maintenance Date** der Parametergruppe *General*.



Überwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zum Abrufen des letzten Wartungstermins auf eine der folgenden Arten vor:

(1) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Maintenance Information***.

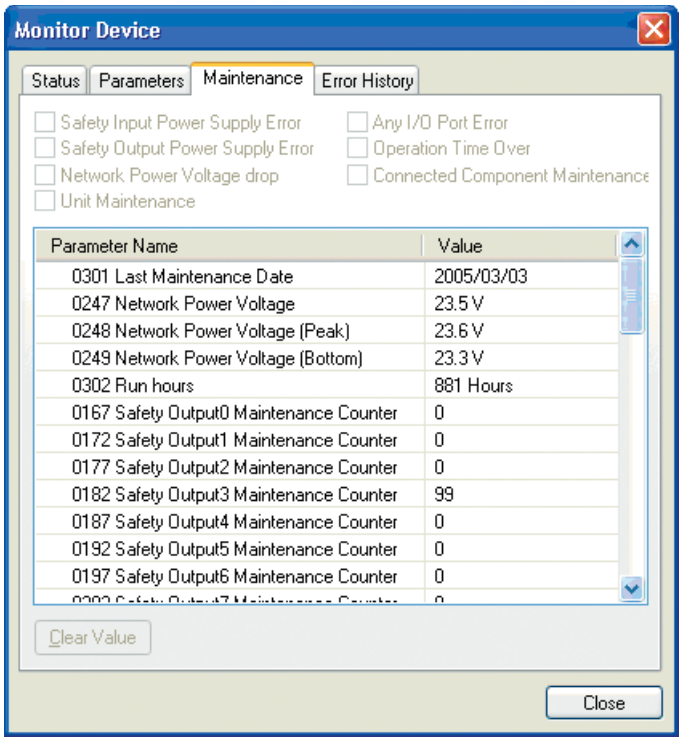
(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Maintenance Information**.

(3) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Maintenance Information***.

(4) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(5) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(6) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

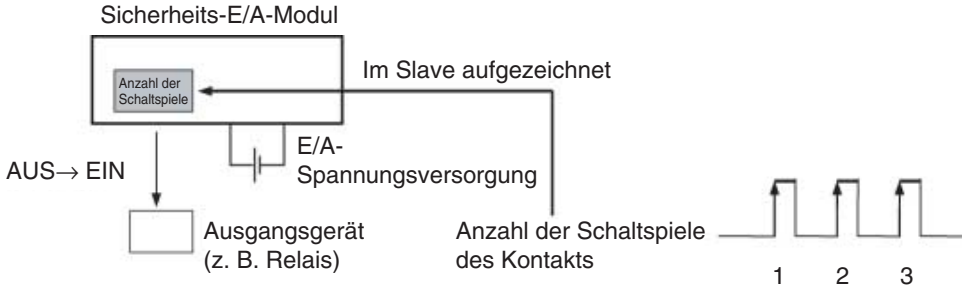


7-2-4 Überwachung des Schalthäufigkeitszählers

Beschreibung

DST1-Sicherheits-E/A-Module registrieren, wie oft jeder Sicherheitseingangs-, Testausgangs- und Sicherheitsausgangskontakt geschaltet wird, und speichern diese Informationen intern im nichtflüchtigen Speicher. Erreicht einer dieser Zähler den eingestellten Grenzwert, wird der Merker **Connected Component Maintenance** im allgemeinen Status auf EIN gesetzt.

- Wertebereich: 0 bis 4.294.967.295 Schaltspiele (interne Darstellung: 0000 0000 bis FFFF FFFF hex)
- Maßeinheit: Schaltspiele
- Maximale Auflösung: 166,7 Hz

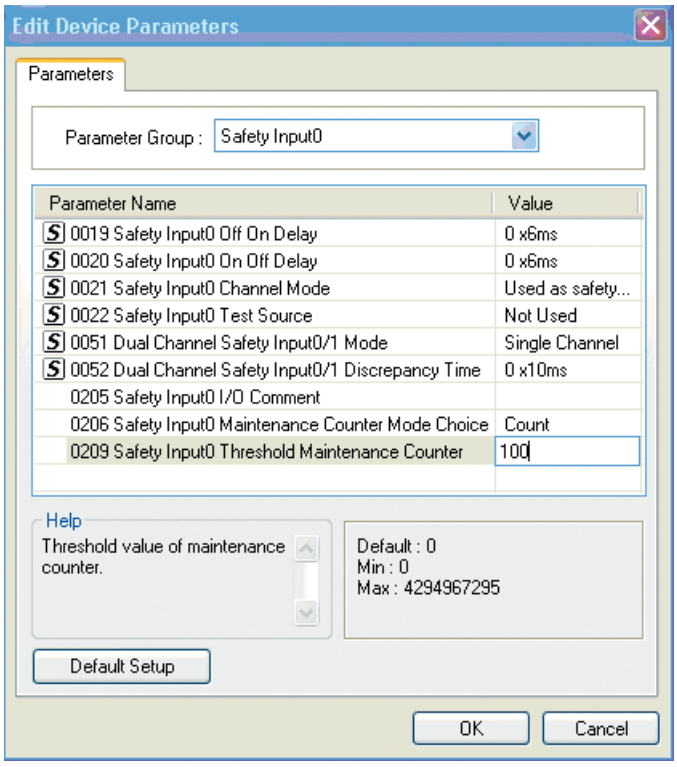


Sie können diese Information mithilfe des Netzwerkkonfigurators und expliziten Meldungen überwachen.

Hinweis:
- Wird die Anzahl der Schaltspiele eines Kontakts überwacht, kann nicht gleichzeitig auch die Gesamtschaltzeit (siehe nächsten Abschnitt) desselben Kontakts überwacht werden. Die Einstellung des Parameters *Maintenance Counter Mode Choice* bestimmt die Art der Überwachung des Kontakts.
- Wird die Einstellung des Parameters *Maintenance Counter Mode Choice* geändert, werden die intern gespeicherten Zähler- oder Zeitdaten gelöscht.
- Die Erfassung der Schaltspiele oder der Schaltzeit ist außer Funktion, wenn die E/A-Spannungsversorgung ausgeschaltet ist.

Einstellen des Grenzwerts für die Überwachung des Schalthäufigkeitszählers mithilfe des Netzwerkkonfigurators

Die Einstellung der Parameter **Maintenance Counter Mode Choice** und **Threshold Maintenance Counter** erfolgt für jeden einzelnen Sicherheitseingang, Testausgang und Sicherheitsausgang separat.



Ist der Parameter **Threshold Maintenance Counter** auf 0 gesetzt, erfolgt keine Überwachung des Grenzwerts.

Überwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zum Überwachen der Anzahl der Schaltspiele von Sicherheitseingängen, Testausgängen und Sicherheitsausgängen auf eine der folgenden Arten vor:

(1) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Maintenance Information***.

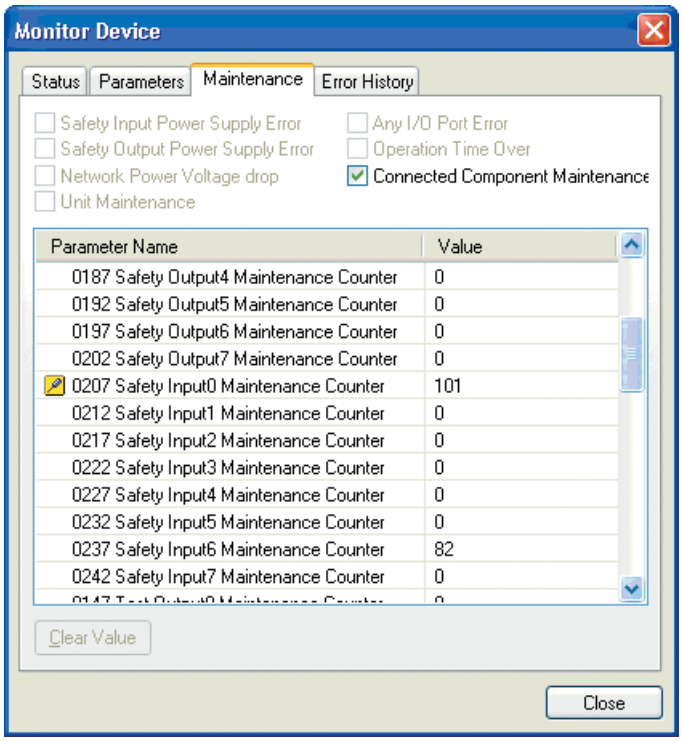
(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Maintenance Information**.

(3) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Maintenance Information***.

(4) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(5) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(6) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.



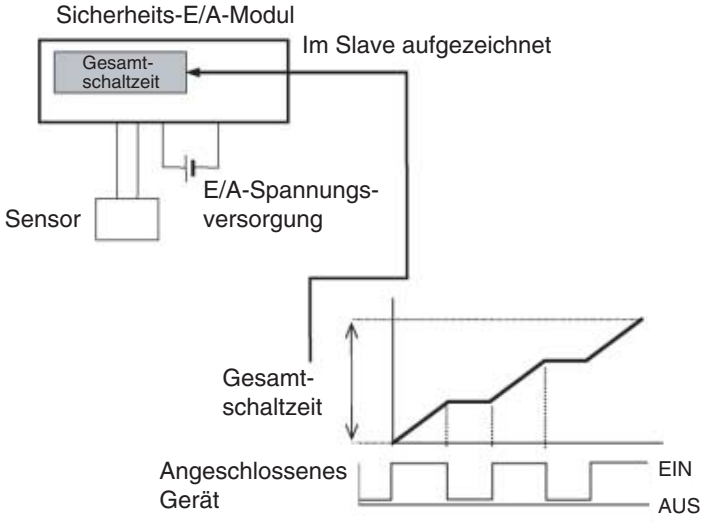
Jeder Zähler kann individuell gelöscht werden. Wählen Sie dazu den zu löschenden Zähler aus, und klicken Sie auf **Clear Value**.

7-2-5 Überwachung der Gesamteinschaltzeit

Beschreibung

DST1-Sicherheits-E/A-Module registrieren die Gesamtzeit, für die jeder einzelne Sicherheitseingangs-, Testausgangs- und Sicherheitsausgangskontakt eingeschaltet ist, und speichern diese Informationen intern im nichtflüchtigen Speicher. Erreicht einer dieser Schaltzeitzähler den eingestellten Grenzwert, wird der Merker **Connected Component Maintenance** im allgemeinen Status auf EIN gesetzt.

- Mögliche Werte: 0 bis 4.294.967.295 Sekunden (interne Darstellung: 0000 0000 bis FFFF FFFF hex)
- Auflösung: 1 Sekunde



Sie können diese Information mithilfe des Netzwerkkonfigurators und expliziten Meldungen überwachen.

Hinweis:
- Wird die Anzahl der Schaltspiele eines Kontakts (siehe vorherigen Abschnitt) überwacht, kann nicht gleichzeitig auch die Gesamteinschaltzeit desselben Kontakts überwacht werden. Die Einstellung des Parameters *Maintenance Counter Mode Choice* bestimmt die Art der Überwachung des Kontakts.
- Wird die Einstellung des Parameters *Maintenance Counter Mode Choice* geändert, werden die intern gespeicherten Zähler- oder Zeitdaten gelöscht.
- Die Erfassung der Schaltspiele oder der Schaltzeit ist außer Funktion, wenn die E/A-Spannungsversorgung ausgeschaltet ist.
- Die Überwachung der Schaltzeit überprüft etwa einmal in der Sekunde, ob der jeweilige Kontakt geschaltet ist. Dies muss beachtet werden, wenn die Schaltzeit einzelner Kontakte weniger als eine Sekunde beträgt.

Schaltdauerüberwachung bei einer Schaltzeit von 0,5 s

In *Abbildung A* beträgt die tatsächliche Schaltzeit 3 x 0,5 s = 1,5 s. Zu den Zeitpunkten, zu denen die Überprüfung des Ausgangszustands erfolgt, ist dieser jedoch nur ein einziges Mal auf EIN gesetzt, daher wird eine Schaltzeit von 1 s gemessen.

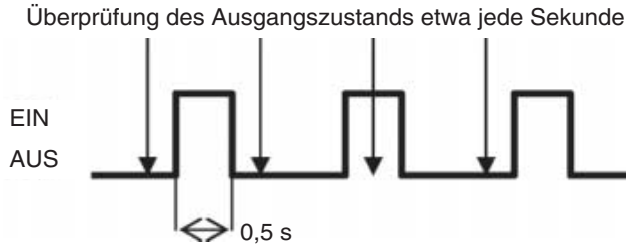


Abbildung A

In *Abbildung B* beträgt die tatsächliche Schaltzeit 3 x 0,5 s = 1,5 s. Zu den Zeitpunkten, zu denen die Überprüfung des Ausgangszustands erfolgt, ist dieser zwei Mal auf EIN gesetzt, daher wird eine Schaltzeit von 2 s gemessen.

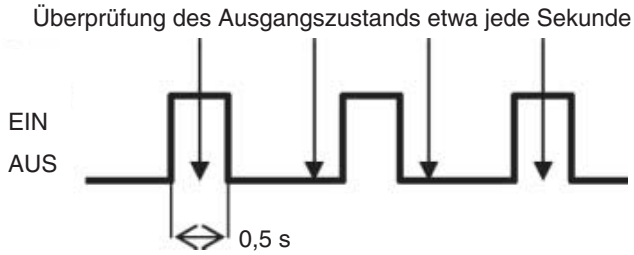


Abbildung B

Schaltzeitüberwachung bei einer Schaltzeit von 1,5 s

In *Abbildung C* beträgt die tatsächliche Schaltzeit 2 x 1,5 s = 3 s. Zu den Zeitpunkten, zu denen die Überprüfung des Ausgangszustands erfolgt, ist dieser jedoch insgesamt viermal auf EIN gesetzt, daher wird eine Schaltzeit von 4 s gemessen.

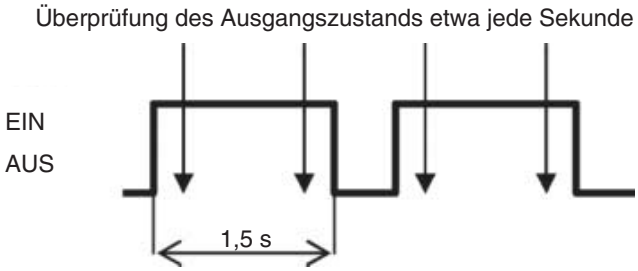
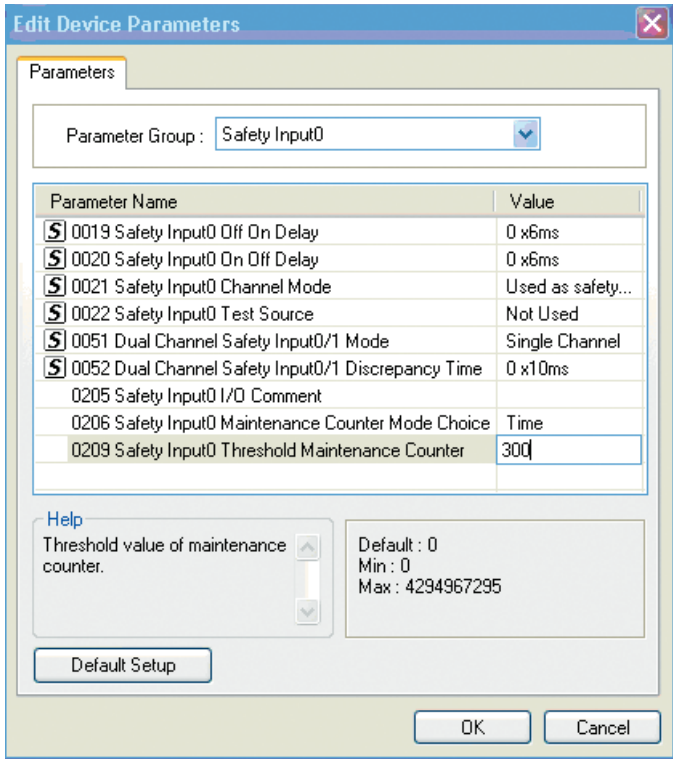


Abbildung C

Einstellen des Grenzwerts für die Überwachung der Schaltzeit mithilfe des Netzwerkkonfigurators

Die Einstellung der Parameter **Maintenance Counter Mode Choice** und **Threshold Maintenance Counter** erfolgt für jeden einzelnen Sicherheitseingang, Testausgang und Sicherheitsausgang separat.



Ist der Parameter **Threshold Maintenance Counter** auf 0 gesetzt, erfolgt keine Überwachung der Schaltzeit.

Überwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zum Überwachen der Gesamtschaltzeit von Sicherheitseingängen, Testausgängen und Sicherheitsausgängen auf eine der folgenden Arten vor:

(1) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Maintenance Information***.

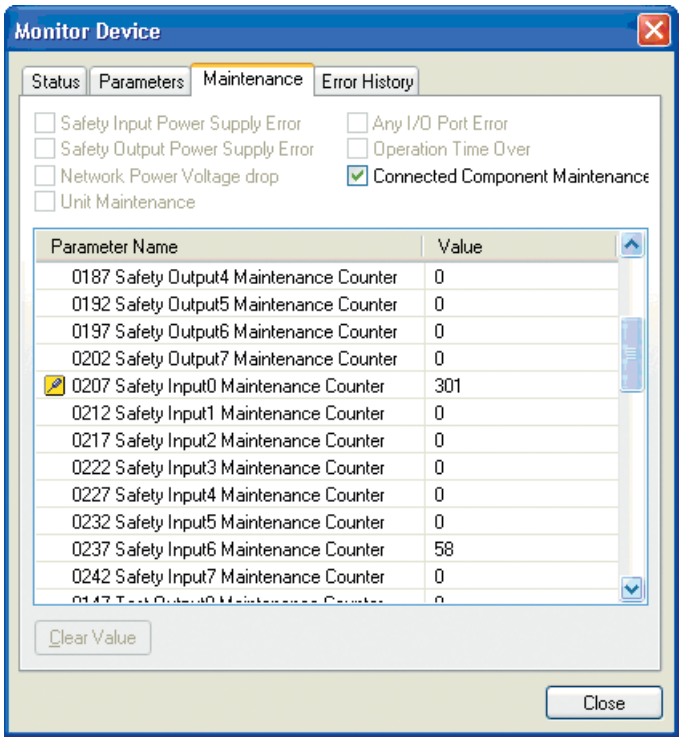
(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Maintenance Information**.

(3) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Maintenance Information***.

(4) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(5) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(6) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.



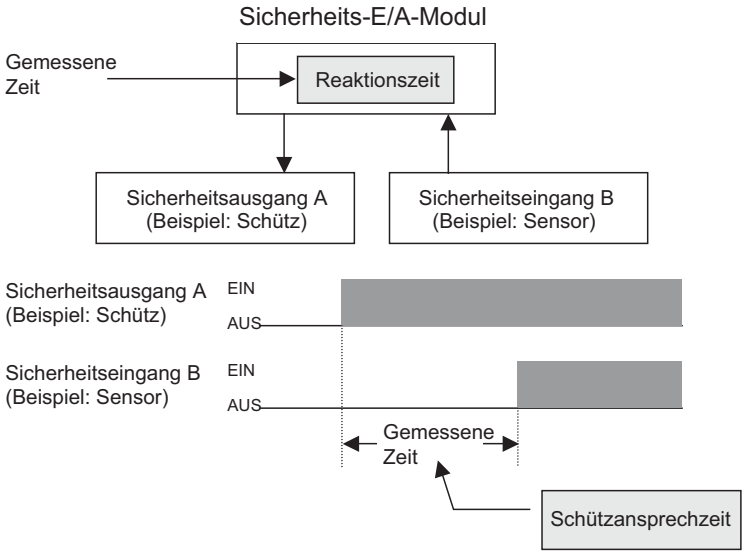
Jeder Schaltdauerzähler kann individuell gelöscht werden. Wählen Sie dazu den zu löschenden Zähler aus, und klicken Sie auf **Clear Value**.

7-2-6 Überwachung der Reaktionszeit

Beschreibung

DST1-Sicherheits-E/A-Module registrieren die Zeitspanne zwischen dem Einschalten eines Sicherheitsausgangs und dem Einschalten des zugehörigen Sicherheitseingangs und speichern diese Informationen intern im nichtflüchtigen Speicher. Überschreitet diese Reaktionszeit den eingestellten Grenzwert, wird der Merker **Threshold Response Time** im allgemeinen Status auf EIN gesetzt.

- Mögliche Werte: 0 bis 65.535 ms (interne Darstellung: 0000 bis FFFF hex)
- Auflösung: 1 ms



Bei der Bestimmung der Reaktionszeit werden die Eingangs- und Ausgangsreaktionszeit des DST1-Sicherheits-E/A-Moduls hinzuaddiert.

Maximale Eingangsreaktionszeit eines DST1-Sicherheits-E/A-Moduls

= 16,2 ms + Eingangseinschaltverzögerungszeit

Maximale Ausgangsreaktionszeit eines DST1-Sicherheits-E/A-Moduls

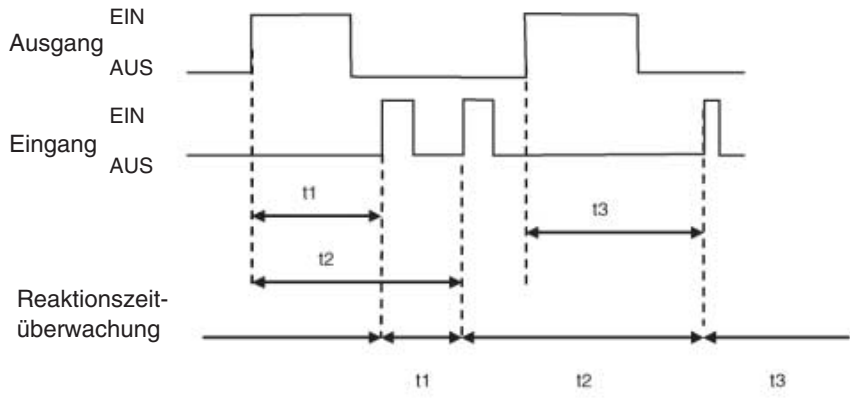
= 6,2 ms + Relaisansprechzeit (nur DST1-MRD08SI-1)

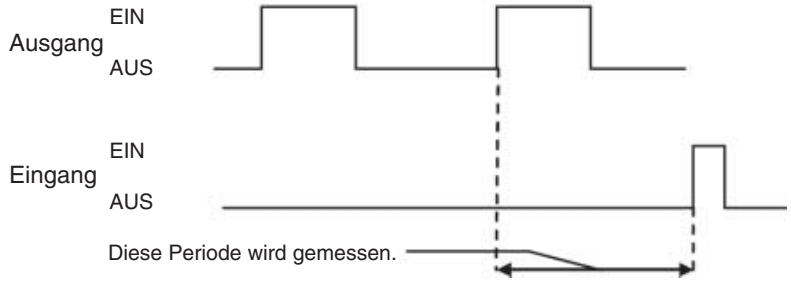
Diese Messung ist auf ±6 ms genau.

Sie können diese Information mithilfe des Netzwerkkonfigurators und expliziten Meldungen überwachen.

Hinweis:

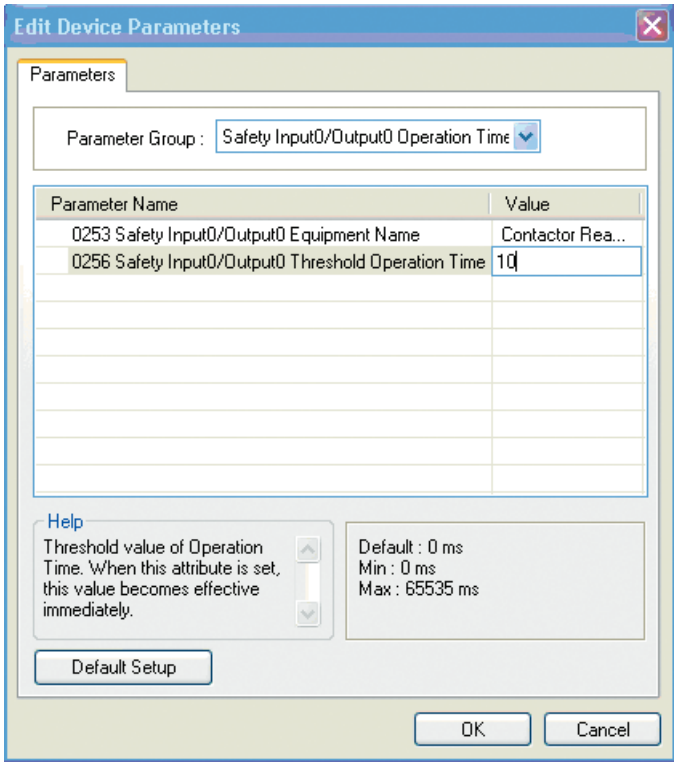
- Bei den Sicherheits-E/A-Modulen DST1-MD16SL-1 und DST1-MRD08SL-1 erfolgt die Messung der Reaktionszeit ab dem Einschalten eines Sicherheitsausgangs und dem Einschalten des Sicherheitseingangs mit derselben Nummer (zum Beispiel Sicherheitseingang 0 und Sicherheitsausgang 0).
- Bei dem Sicherheits-E/A-Modul DST1-ID12SL-1 wird die Zeit zwischen dem Einschalten der beiden gepaarten Sicherheitseingänge gemessen (zum Beispiel Sicherheitseingang 0 und Sicherheitseingang 6).
- Die Reaktionszeit wird unmittelbar nach der Bestimmung, d. h. nach dem Einschalten des Eingangs gespeichert. Die Messung wird jedoch intern fortgesetzt, bis der Ausgang das nächste Mal eingeschaltet wird. Wird der Eingang erneut eingeschaltet, bevor der Ausgang wieder eingeschaltet wird, wird die gemessene Reaktionszeit aktualisiert. Tritt im Verlauf einer pendelnden Bewegung (z. B. Kolbenhub) ein Eingangsfehler auf, wird möglicherweise der Messwert für die Reaktionszeit (Hinweg) auf dem Rückweg aktualisiert.
- Wird der Ausgang zweimal hintereinander eingeschaltet, bevor der Eingang eingeschaltet wird, erfolgt die Messung ab dem zweiten Einschalten des Ausgangs bis zum Einschalten des Eingangs.





Einstellen des Grenzwerts für die Reaktionszeitüberwachung mithilfe des Netzwerkkonfigurators

Die Einstellung des Grenzwerts für die Reaktionszeitüberwachung für die einzelnen Paare von Ausgängen und Eingängen erfolgt in der Parametergruppe **Operation Time**.



Ist der Grenzwert auf 0 eingestellt, erfolgt keine Überwachung der Reaktionszeit.

Überwachung mithilfe des Netzwerkkonfigurators

Gehen Sie zur Überwachung der Reaktionszeiten auf eine der folgenden Arten vor:

(1) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Maintenance Information***.

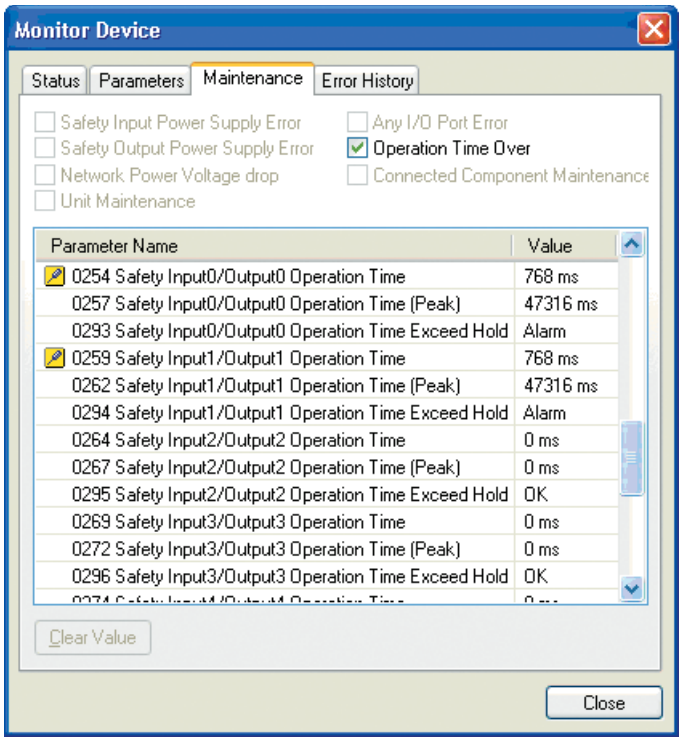
(2) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Maintenance Information**.

(3) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Maintenance Information***.

(4) Wählen Sie ein Gerät aus, und wählen Sie in der Menüleiste ***Device - Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(5) Wählen Sie ein Gerät aus, und klicken Sie in der Werkzeugleiste auf **Monitor Device**. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.

(6) Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie den Kontextmenübefehl ***Monitor***. Klicken Sie in dem nun angezeigten Dialogfeld auf die Registerkarte **Maintenance**.



- Unter *Operation Time* wird der aktuelle Wert für die Reaktionszeit angezeigt.
- Unter *Operation Time (Peak)* wird der längste aufgetretene Wert für die Reaktionszeit angezeigt.
- Ist der Grenzwert für die Reaktionszeitüberwachung gesetzt und wurde dieser Grenzwert mindestens einmal überschritten, wird unter *Operation Time Exceed Hold* „Alarm“ angezeigt.

Die unter *Operation Time (Peak)* und *Operation Time Exceed Hold* angezeigten Werte können gelöscht werden. Wählen Sie dazu den zu löschenden Wert aus, und klicken Sie auf **Clear Value**.

A Verbinden des Netzwerkkonfigurators mit dem Netzwerk mittels einer CS/CJ-Serie-SPS

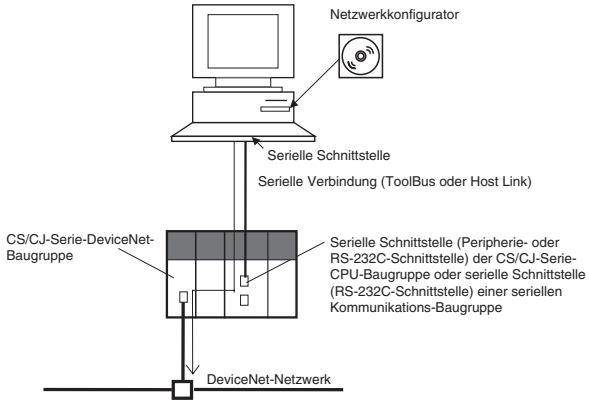
A-1 Verbinden mit dem DeviceNet-Netzwerk

Der Netzwerkkonfigurator kann wie im Folgenden dargestellt über die serielle Schnittstelle einer CS/CJ-Serie-CPU-Baugruppe oder über eine CS/CJ-Serie-Ethernet-Baugruppe mit dem DeviceNet-Netzwerk verbunden werden. Dieser Anhang erläutert die entsprechende Vorgehensweise.

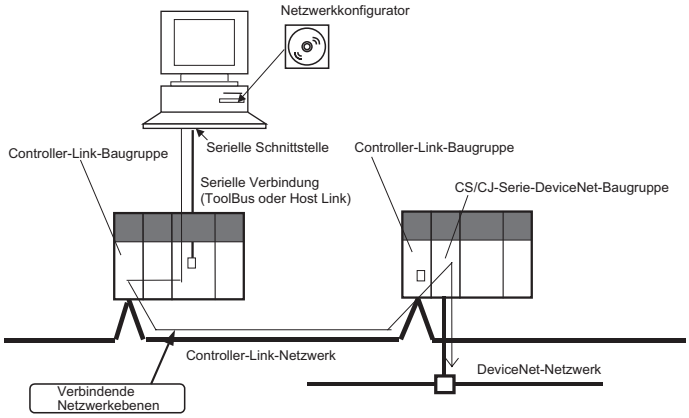
Informationen zum Anschließen des Netzwerkkonfigurators über die USB-Schnittstelle des Sicherheitsnetzwerk-Controllers NE1A (NE1A-SCPU01) oder über eine im PC installierte DeviceNet-Schnittstellenkarte finden Sie unter *2-3 Verbinden mit dem Netzwerk* (Seite 32).

1. Verbinden Sie die serielle Schnittstelle des PCs über eine Peripheriebus- (ToolBus) oder eine Host-Link-Verbindung mit der seriellen Schnittstelle einer CS/CJ-Serie-CPU-Baugruppe (d. h. der Peripherie- oder der RS-232-Schnittstelle) oder einer seriellen Kommunikations-Baugruppe (d. h. einer RS-232C- oder RS-422A/485-Schnittstelle)

   Um eine Verbindung mit dem DeviceNet-Netzwerk herstellen zu können, muss die SPS mit einer CS/CJ-Serie-DeviceNet-Baugruppe (CS1W-DRM21(-V1) oder CJ1W-DRM21) ausgestattet sein.

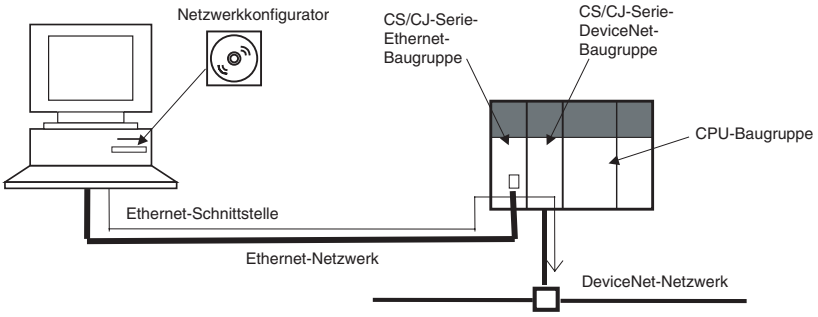


   Bei einer seriellen Verbindung kann die Verbindung zum DeviceNet über bis zu maximal drei Netzwerkebenen erfolgen (siehe nachstehende Abbildung).

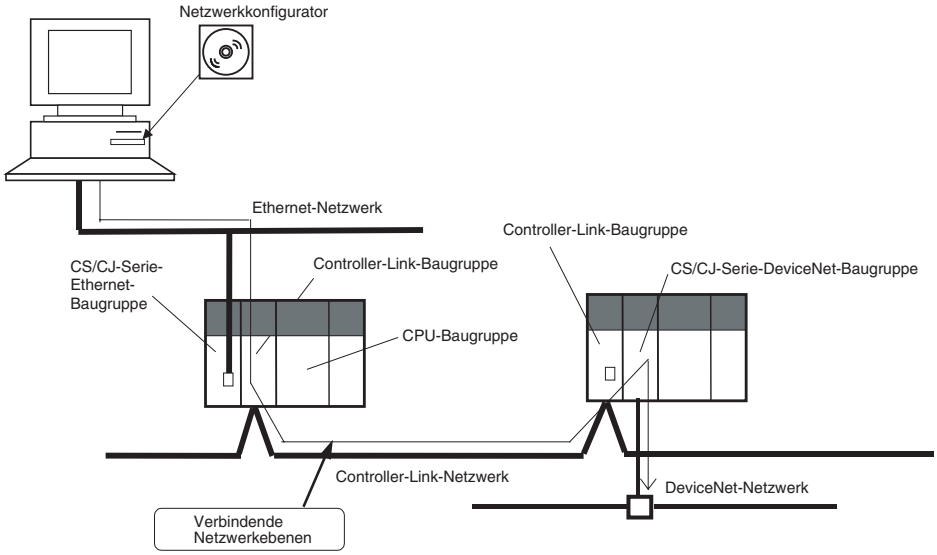


2. Verbinden Sie die Ethernet-Schnittstelle des PCs mit einer CS/CJ-Serie-Ethernet-Baugruppe.

   Um eine Verbindung mit dem DeviceNet-Netzwerk herstellen zu können, muss die SPS mit einer CS/CJ-DeviceNet-Baugruppe (CS1W-DRM21(-V1) oder CJ1W-DRM21) ausgestattet sein.



Bei einer Ethernet-Verbindung kann die Verbindung zum DeviceNet über bis zu maximal drei Netzwerkebenen erfolgen (siehe nachstehende Abbildung).



A-2 Festlegen der Schnittstelle für die Verbindung zum DeviceNet-Netzwerk

Gehen Sie wie folgt vor, um die Schnittstelle für die Verbindung zum DeviceNet-Netzwerk festzulegen.

Hinweis: Das Festlegen der Schnittstelle für die Verbindung muss bei jeder Definition einer Online-Verbindung erfolgen.

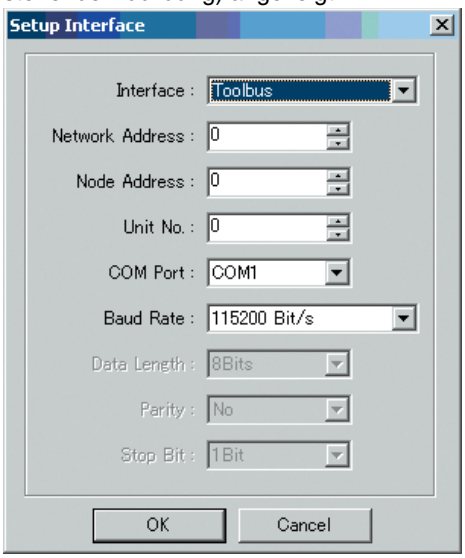
1. Wählen Sie in der Menüleiste ***Option - Select Interface***.
   (Die aktuell verwendete Schnittstelle ist ausgewählt.)
2. Wählen Sie eine der im Untermenü angebotenen Schnittstellen aus.
   - Serielle Schnittstelle: Wählen Sie ***SYSMAC CS/CJ I/F Port***.
   - Ethernet-Baugruppe: Wählen Sie ***SYSMAC CS/CJ Ethernet Unit I/F***.
3. Wählen Sie in der Menüleiste ***Network Connect***.
   Nun wird ein Dialogfeld mit den Parametern der ausgewählten Schnittstelle angezeigt.
   Detailinformationen zu den Einstellungen dieser Parameter finden Sie unter *Festlegen der seriellen Schnittstelle der SYSMAC CS/CJ-Serie-SPS als Schnittstelle für die Verbindung zum DeviceNet-Netzwerk* (Seite 137) bzw. *Festlegen der SYSMAC CS/CJ-Serie-Ethernet-Baugruppe als Schnittstelle für die Verbindung zum DeviceNet-Netzwerk* (Seite 138).

Hinweis: Solange der Netzwerkkonfigurator online, d. h. mit dem Netzwerk verbunden ist, kann die Schnittstelle nicht gewechselt werden. Wählen Sie dazu zunächst in der Menüleiste ***Network Unconnect***, um die Verbindung mit dem Netzwerk zu trennen, und wechseln Sie dann die Schnittstelle im Offline-Modus.

Festlegen der seriellen Schnittstelle der SYSMAC CS/CJ-Serie-SPS als Schnittstelle für die Verbindung zum DeviceNet-Netzwerk

(Fortsetzung von Schritt 3 auf der vorherigen Seite.)

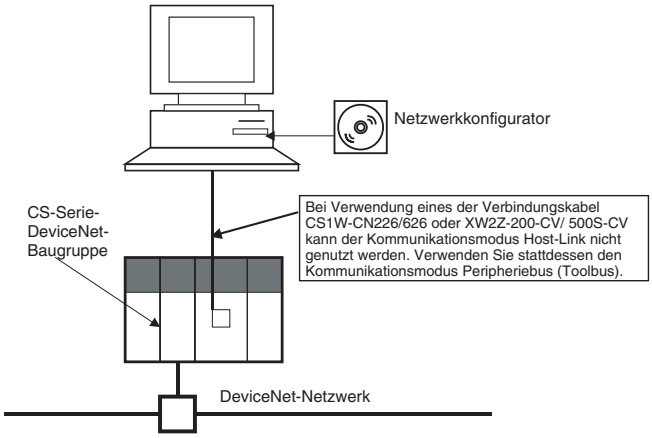
1. Bei Auswahl der Einstellung *SYSMAC CS/CJ I/F Port* als Schnittstelle wird als nächstes das Dialogfeld *Setup Interface* (siehe nachstehende Abbildung) angezeigt.



Stellen Sie die einzelnen Parameter wie im Folgenden beschrieben ein:

Interface	Wählen Sie einen der folgenden seriellen Kommunikationsmodi für die serielle Schnittstelle der CS/CJ-Serie-SPS aus: • Peripheriebus (ToolBus) • Host-Link
Network Address	Geben Sie hier die FINS-Netzwerkadresse der Ziel-DeviceNet-Baugruppe ein. Die Eingabe dieser Adresse ist erforderlich, wenn die Verbindung über mehrere Netzwerkebenen hinweg hergestellt wird. Ist die CS/CJ-Serie-SPS direkt an das DeviceNet-Netzwerk angeschlossen, so geben Sie hier den Wert 0 ein.
Node Address	Die Eingabe dieser Adresse ist erforderlich, wenn die Verbindung über mehrere Netzwerkebenen hinweg hergestellt wird. Ist die CS/CJ-Serie-SPS direkt an das DeviceNet-Netzwerk angeschlossen, so geben Sie hier den Wert 0 ein.
CPU Bus Unit Number	Geben Sie hier die Baugruppennummer (der mithilfe des Drehschalters an der Vorderseite der DeviceNet-Baugruppe eingestellte Wert) der als CPU-Bus-Baugruppe fungierenden DeviceNet-Baugruppe (CS1W-DRM21(-V1)) ein. • Die Baugruppennummer liegt zwischen 0 und 15.
Communications Port	Wählen Sie die zu verwendende serielle Schnittstelle des PCs aus, auf dem der Netzwerkkonfigurator (Version 2) ausgeführt wird. • Das Listenfeld bietet alle verfügbaren seriellen Schnittstellen des PCs an.
Baud Rate	Wählen Sie die Baudrate für die serielle Verbindung mit der CS/CJ-Serie-SPS aus: • 9.600, 19.200, 38.400 oder 115.200 Bit/s. Für die verschiedenen Kommunikationsmodi (Peripheriebus/Host-Link) stehen unterschiedliche Baudraten zur Auswahl. Detaillierte Informationen hierzu finden Sie im CS/CJ-Serie Bedienerhandbuch.
Data Length	Wählen Sie die Datenlänge für die serielle Verbindung mit der CS/CJ-Serie-SPS aus. Diese Einstellung ist nur bei Verwendung des Kommunikationsmodus Host-Link erforderlich. o 7Bits oder 8Bits
Parity	Wählen Sie die Parität für die serielle Verbindung mit der CS/CJ-Serie-SPS aus. Diese Einstellung ist nur bei Verwendung des Kommunikationsmodus Host-Link erforderlich. o No, Even oder Odd
Stop Bits	Wählen Sie die Anzahl der Stoppbits für die serielle Verbindung mit der CS/CJ-Serie-SPS aus. Diese Einstellung ist nur bei Verwendung des Kommunikationsmodus Host-Link erforderlich. o 1Bit oder 2Bits

WICHTIG: Wenn Sie mithilfe des Verbindungskabels CS1W-CN226/626 oder XW2Z-200S-CV/500S-CV eine serielle Verbindung mit einer CS-Serie-SPS mit in das CPU-Rack integrierter DeviceNet-Baugruppe CS1W-DRM21(-V1) herstellen möchten, müssen Sie den Kommunikationsmodus Peripheriebus (ToolBus) auswählen. Bei Auswahl des Kommunikationsmodus Host-Link kann keine Verbindung hergestellt werden.



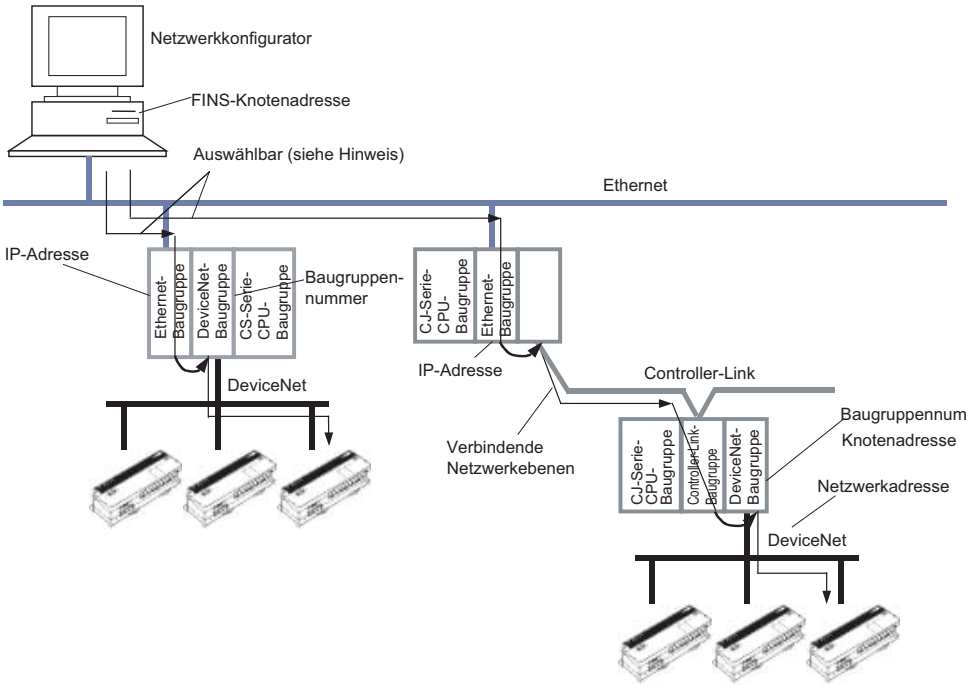
Hinweis:
- Informationen zur FINS-Knotenadresse finden Sie im *CS/CJ-Serie Bedienerhandbuch (W380)*.
- Bei Auswahl des Kommunikationsmodus ***Host link*** kann das Herunterladen aus dem Netzwerk mehrere Minuten in Anspruch nehmen. Es wird daher empfohlen, für serielle Verbindungen den Kommunikationsmodus *Peripheral Bus (ToolBus)* zu wählen.

Festlegen der SYSMAC CS/CJ-Serie-Ethernet-Baugruppe als Schnittstelle für die Verbindung zum DeviceNet-Netzwerk

Sie können den Computer (d. h. den Netzwerkkonfigurator) unter Verwendung einer CS/CJ-Serie-Ethernet-Baugruppe und einer CS/CJ-Serie-DeviceNet-Baugruppe direkt an ein Ethernet-Netzwerk anschließen und auf diese Weise mit dem DeviceNet-Netzwerk verbinden.

Hinweis: Die Verbindung über Ethernet erfordert die gleichzeitige Verwendung einer CS/CJ-Serie-Ethernet-Baugruppe und einer CS/CJ-Serie-DeviceNet-Baugruppe (Bei Verwendung von Baugruppen anderer SPS-Serien kann keine Verbindung über Ethernet hergestellt werden.)

Sind mehrere Steuerungen mit Ethernet- und DeviceNet-Baugruppen an das Ethernet-Netzwerk angeschlossen, kann die Verbindung zum gewünschten DeviceNet-Netzwerk durch Angabe der IP-Adresse der betreffenden Ethernet-Baugruppe und der Baugruppennummer der betreffenden DeviceNet-Baugruppe hergestellt werden.



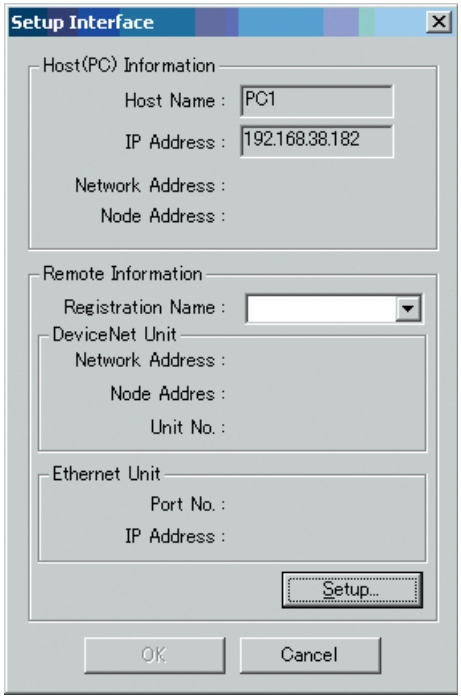
Hinweis: Durch Angabe des registrierten Namens des Ziel-DeviceNet-Netzwerks kann die Verbindung zum Ziel-DeviceNet-Netzwerk hergestellt werden. Die Registrierung des Namens des Ziel-DeviceNet-Netzwerks erfolgt durch Angabe der folgenden Daten:
- IP-Adresse und UDP-Port-Nummer der Ethernet-Baugruppe
- Netzwerkadresse, Knotenadresse und CPU-Bus-Baugruppennummer der DeviceNet-Baugruppe
- FINS-Knotenadresse des Computers (d. h. des Netzwerkkonfigurators)

Registrieren von Ziel-DeviceNet-Netzwerken

Für eine Ethernet-Verbindung muss das Ziel-DeviceNet-Netzwerk vorab registriert werden. Sie können maximal 20 DeviceNet-Netzwerke registrieren.

Gehen Sie wie folgt vor, um das Ziel-DeviceNet-Netzwerk zu registrieren:

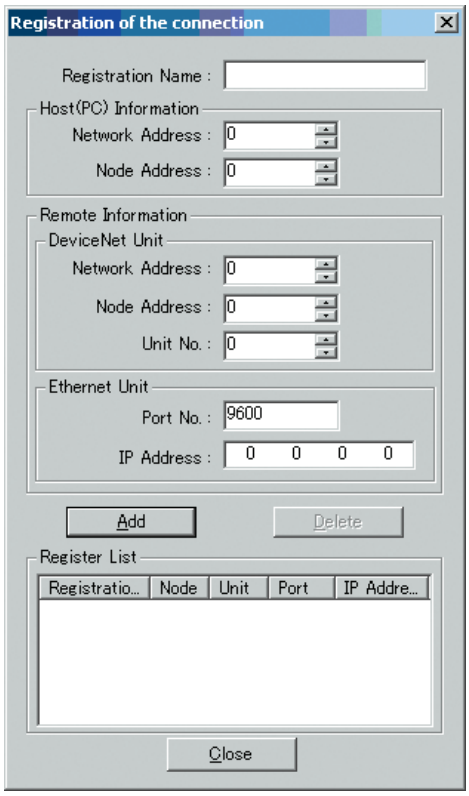
1. Wählen Sie ***Network - Connect***.
2. Nun wird das folgende Dialogfeld angezeigt:



Komponenten des Dialogfelds *Setup Interface*

Host (PC) Information	Einstellungen des Netzwerkkonfigurator-PCs	
	Host Name	Der Name des PCs wird automatisch angezeigt.
	IP Address	Die IP-Adresse des PCs wird automatisch angezeigt.
	Network Address	Die im PC eingestellte FINS-Netzwerkadresse wird automatisch angezeigt. (Hierbei handelt es sich um die im folgenden Schritt in das Dialogfeld *Registration of the connection* eingegebene Netzwerkadresse.)
	Node Address	Die im PC eingestellte FINS-Knotenadresse wird automatisch angezeigt. (Hierbei handelt es sich um die im folgenden Schritt in das Dialogfeld *Registration of the connection* eingegebene Knotenadresse.)

3. Klicken Sie auf **Setup**. Nun wird das Dialogfeld *Registration of the connection* angezeigt (siehe nachstehende Abbildung).



Komponenten des Dialogfelds *Registration of the connection*

Registration Name	Legen Sie hier den zu registrierenden Namen für das Ziel-DeviceNet-Netzwerk fest. Sie können bis zu 20 Namen registrieren. Der Name kann bis zu 25 Zeichen umfassen.		
Host (PC) Information	Einstellungen des Netzwerkkonfigurator-PCs		
	Network Address	Geben Sie hier die FINS-Netzwerkadresse des Netzwerkkonfigurator-PCs ein. Diese muss der Netzwerkadresse der Ethernet-Baugruppe entsprechen. Der Eintrag 0 entspricht keiner Netzwerkadresse.	
	Node Address	Geben Sie hier die FINS-Knotenadresse des Netzwerkkonfigurator-PCs ein.	
Remote Information	Einstellungen für die DeviceNet- und die Ethernet-Baugruppe, über die die Verbindung zum Ziel-DeviceNet-Netzwerk hergestellt wird.		
	Device-Net Unit	Network Address	Geben Sie hier die FINS-Netzwerkadresse der Ziel-DeviceNet-Baugruppe ein. Die Eingabe dieser Adresse ist erforderlich, wenn die Verbindung über mehrere Netzwerkebenen hinweg hergestellt wird. Ist die CS/CJ-Serie-SPS direkt an das DeviceNet-Netzwerk angeschlossen, so geben Sie hier den Wert 0 ein.
		Node Address	Geben Sie hier die Knotenadresse der Ziel-DeviceNet-Baugruppe ein. Die Eingabe dieser Adresse ist erforderlich, wenn die Verbindung über mehrere Netzwerkebenen hinweg hergestellt wird. Ist die CS/CJ-Serie-SPS direkt an das DeviceNet-Netzwerk angeschlossen, so geben Sie hier den Wert 0 ein.
		CPU Bus Unit Number	Geben Sie hier die Baugruppennummer der als CPU-Bus-Baugruppe fungierenden Ziel-DeviceNet-Baugruppe ein.
	Ethernet Unit	Port Number	Geben Sie hier die UDP-Port-Nummer der Ethernet-Baugruppe ein.
		IP Address	Geben Sie hier die IP-Adresse der Ethernet-Baugruppe ein.

Einstellen der Netzwerkadresse im Bereich *Host (PC) Information* des Dialogfelds

Geben Sie die FINS-Knotenadresse des Netzwerkkonfigurator-PCs ein.

Der Netzwerkkonfigurator-PC verwendet den OMRON FINS-Kommunikationsdienst, um über das Ethernet eine Verbindung zum DeviceNet-Netzwerk herzustellen. Dazu muss sowohl die FINS-Knotenadresse als auch die IP-Adresse eingegeben werden.

Verwenden Sie für die Netzwerkadresse denselben Wert wie die Ethernet-Baugruppe. Die Netzwerkadresse der Ethernet-Baugruppe wird in der Routing-Tabelle der CPU-Baugruppe festgelegt. Wird die Routing-Tabelle nicht verwendet, so geben Sie hier den Wert 0 ein.

Einstellen der Knotenadresse im Bereich *Host (PC) Information* des Dialogfelds

Geben Sie die FINS-Knotenadresse des Netzwerkkonfigurator-PCs ein.

Für diese Einstellung muss mithilfe der OMRON Ethernet-Baugruppe eine Entsprechung zwischen der Remote-IP-Adresse und der Knotenadresse festgelegt werden. Detaillierte Informationen hierzu finden Sie im *Bedienerhandbuch zur Ethernet-Baugruppe der SYSMAC CS/CJ-Serie (W420, W421 und W343)*.

Einstellen der Netzwerkadresse im Bereich *Remote Information/DeviceNet Unit* des Dialogfelds

Geben Sie die FINS-Netzwerkadresse der DeviceNet-Baugruppe ein, mit der das Ziel-DeviceNet-Netzwerk verbunden ist.

Die Eingabe dieser Adresse ist erforderlich, wenn die Verbindung über mehrere Netzwerkebenen hinweg hergestellt wird. Ist die CS/CJ-Serie-SPS direkt an das DeviceNet-Netzwerk angeschlossen, so geben Sie hier den Wert 0 ein.

Einstellen der Knotenadresse im Bereich *Remote Information/DeviceNet Unit* des Dialogfelds

Geben Sie die Knotenadresse der DeviceNet-Baugruppe ein, mit der das Ziel-DeviceNet-Netzwerk verbunden ist.

Die Eingabe dieser Adresse ist erforderlich, wenn die Verbindung über mehrere Netzwerkebenen hinweg hergestellt wird. Ist die CS/CJ-Serie-SPS direkt an das DeviceNet-Netzwerk angeschlossen, so geben Sie hier den Wert 0 ein.

Einstellen der CPU-Bus-Baugruppennummer im Bereich *Remote Information/DeviceNet Unit* des Dialogfelds

Geben Sie die Baugruppennummer (0 bis F) der als CPU-Bus-Baugruppe fungierenden DeviceNet-Baugruppe ein, mit der das Ziel-DeviceNet-Netzwerk verbunden ist.

Einstellen der Port-Nummer im Bereich *Remote Information/Ethernet Unit* des Dialogfelds

Geben Sie die Nummer des UDP-Ports ein, über den die Ethernet-Baugruppe den FINS-Kommunikationsdienst abwickelt. Stellen Sie hier denselben Wert wie in den Einstellungen im Systemeinstellungsbereich der CPU-Bus-Baugruppe ein, an die die Ethernet-Baugruppe angeschlossen ist. Normalerweise wird der Port 9600 verwendet.

Einstellen der IP-Adresse im Bereich *Remote Information/Ethernet Unit* des Dialogfelds

Geben Sie die IP-Adresse der Ethernet-Baugruppe ein.

Informationen zum Festlegen die IP-Adresse der Ethernet-Baugruppe finden Sie im Bedienerhandbuch zur Ethernet-Baugruppe der SYSMAC CS/CJ-Serie (W420, W421 und W343).

4. Klicken Sie auf *Register*. Die eingestellten Werte werden nun registriert und in der Liste *Register List* angezeigt.
   - Registration Name: Registrierungsname des Ziel-DeviceNet-Netzwerks
   - Node: FINS-Netzwerkadresse und FINS-Knotenadresse (die dritte Zahl ist immer 0) des PCs
   - Unit: FINS-Netzwerkadresse, FINS-Knotenadresse und Baugruppennummer der DeviceNet-Baugruppe
   - Port: Nummer des für die FINS-Kommunikation verwendeten Ports der Ethernet-Baugruppe
   - IP Address: IP-Adresse der Ethernet-Baugruppe
5. Klicken Sie auf *Close*, um dieses Dialogfeld zu schließen und zum Dialogfeld *Setup Interface* zurückzukehren.

Auswahl des Registrierungsnamens (Ziel-DeviceNet-Netzwerk)

Wählen Sie im Dialogfeld *Setup Interface* das gewünschte DeviceNet-Netzwerk, mit dem Sie eine Verbindung herstellen möchten, aus der Liste der Registrierungsnamen aus.

1. Wählen Sie im Bereich *Remote Information* den Registrierungsnamen des Ziel-DeviceNet-Netzwerks aus dem Listenfeld *Registration Name* aus.

   Im Bereich *Remote Information* werden die folgenden eingestellten Werte des ausgewählten Registrierungsnamens angezeigt:
   - Network Address: FINS-Netzwerkadresse der DeviceNet-Baugruppe
   - Node Address: Knotenadresse der DeviceNet-Baugruppe
   - CPU Bus Unit Number: Baugruppennummer der DeviceNet-Baugruppe
   - Port Number: Nummer des für die FINS-Kommunikation verwendeten Ports der Ethernet-Baugruppe
   - IP Address: IP-Adresse der Ethernet-Baugruppe
2. Klicken Sie auf **OK**.

   Klicken Sie im Bestätigungsdialogfeld auf **OK**.

   Nun wird die Verbindung zum gewünschten DeviceNet-Netzwerk hergestellt.

   Nach erfolgreicher Herstellung der Verbindung wird die Statusanzeige in der Statusleiste blau dargestellt; zudem wird die Statusmeldung „On-line“ angezeigt.

Hinweis: Informationen zu FINS-Netzwerkadressen und FINS-Knotenadressen finden Sie im *Bedienerhandbuch der DeviceNet-Baugruppe (W380)* sowie im *Bedienerhandbuch zur Ethernet-Baugruppe der SYSMAC CS/CJ-Serie (W420, W421 und W343)*.

B Bearbeiten der Parameter von CS/CJ-Serie-DeviceNet-Baugruppen

In diesem Abschnitt wird die Bearbeitung der Parameter einer CS/CJ-Serie-DeviceNet-Baugruppe erläutert.

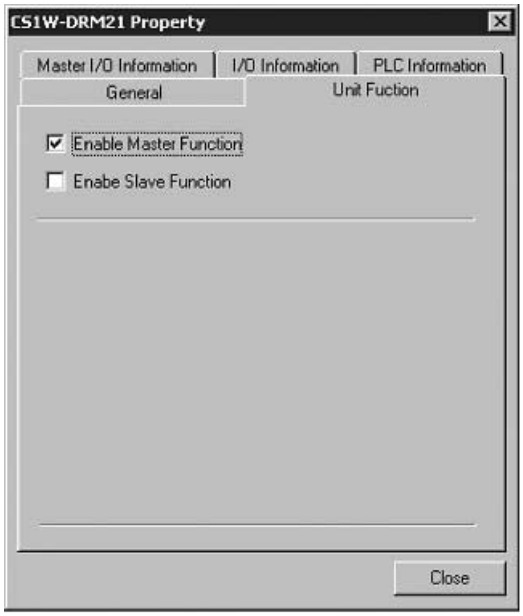
B-1 Festlegen der Baugruppen-Funktion

Die Baugruppe kann als Master und/oder als Slave fungieren.

Gehen Sie wie folgt vor, um die Baugruppen-Funktion festzulegen:

1. Markieren Sie im Netzwerkkonfigurationsbereich (rechter Bereich) das Symbol für den Master.
2. Wählen Sie den Menübefehl ***Device - Property***.

Nun wird das folgende Dialogfeld angezeigt. Klicken Sie auf die Registerkarte **Unit Function**.



3. Aktivieren Sie eines der Kontrollkästchen *Enable Master Function* oder *Enable Slave Function* (oder beide).

B-2 Übersicht über die Master-Parameter

Gehen Sie wie folgt vor, um das Dialogfeld **Edit Device Parameters** aufzurufen.

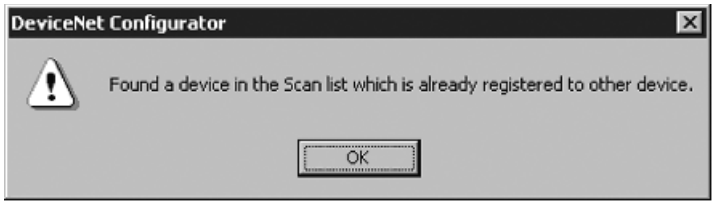
1. Markieren Sie die Baugruppe, deren Parameter Sie bearbeiten möchten.
2. Wählen Sie den Menübefehl ***Device - Parameter Edit***.
3. Nun wird das Dialogfeld **Edit Device Parameters** für den Master angezeigt.

Hinweis:

– Stimmen die E/A-Größe des im Netzwerkkonfigurationsbereich angezeigten Geräts und die E/A-Datengröße des in der Abfrageliste registrierten Geräts nicht überein, wird das folgende Warnfenster angezeigt. In diesem Fall hat die in der Abfrageliste eingestellte E/A-Größe Vorrang.

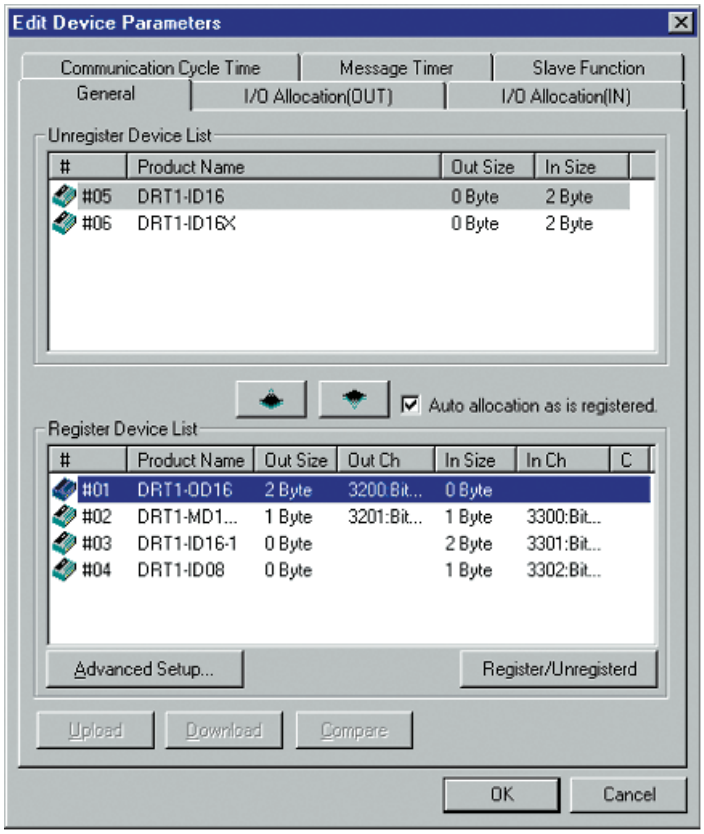
Ist für den Slave keine EDS-Datei installiert, so beschaffen Sie zunächst die EDS-Datei für das Gerät, und installieren Sie diese.

– Wird ein bei einem anderen Master registriertes Slave-Gerät in der Abfrageliste registriert, wird beim Öffnen des Dialogfelds **Edit Device Parameters** das folgende Warnfenster angezeigt.



Ändern Sie den registrierten Slave in der Abfrageliste.

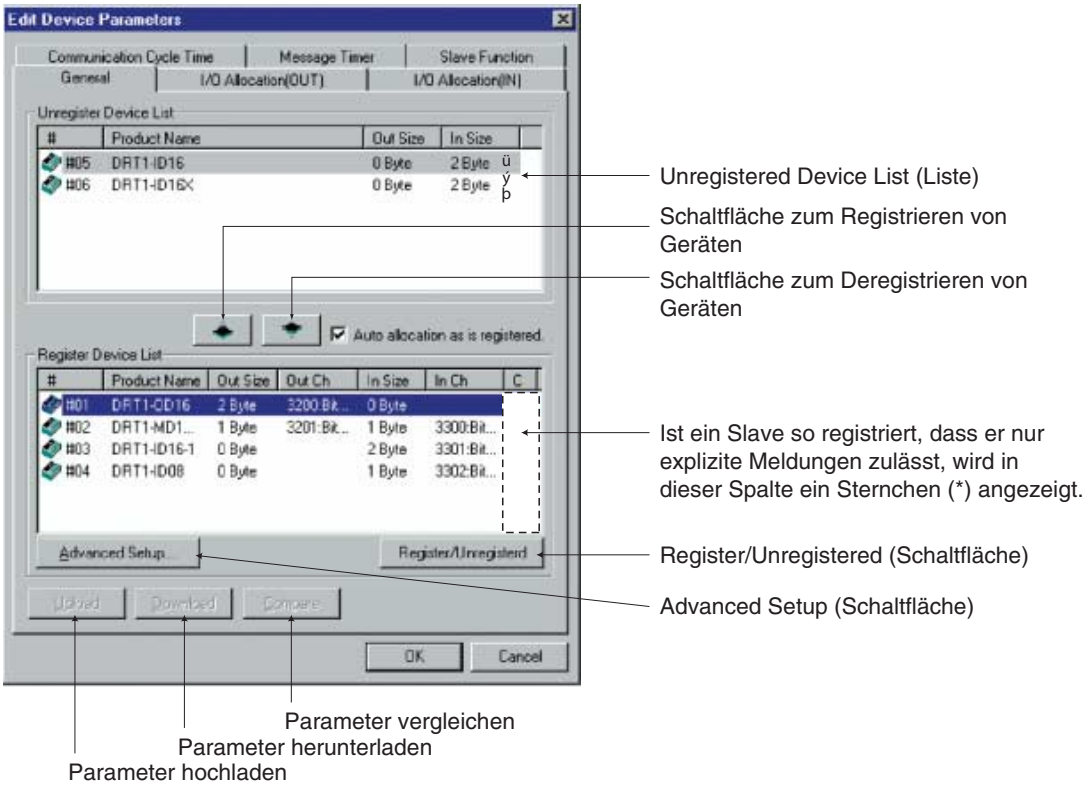
– Um ein Gerät als Master zu betreiben, wählen Sie dieses aus, wählen Sie den Menübefehl ***Device - Properties***, und aktivieren Sie dann im Dialogfeld **Property** des Geräts (CS1W-DRM21(-V1)/CJ1W-DRM21) das Kontrollkästchen **Enable Master Function**.



Das Dialogfeld **Edit Device Parameters** enthält die folgenden sechs Registerkarten:

Registerkartenbezeichnung	**Beschreibung**
General	Registrieren von Geräten in der Abfrageliste und Durchführen von E/A-Zuordnungen mittels automatischer Einstellungen.
I/O Allocation (OUT)	Festlegen der Zuordnung für Ausgabedaten und des zugehörigen Speicherblocks der CPU-Baugruppe im Rahmen der erweiterten Konfiguration.
I/O Allocation (IN)	Festlegen der Zuordnung für Eingangsdaten und des zugehörigen Speicherblocks der CPU-Baugruppe im Rahmen der erweiterten Konfiguration.
Communication Cycle Time	Einstellen der Kommunikationszykluszeit.
Slave Function	Einstellen der Parameter für den Betrieb der Baugruppe als Slave.
Message Timer	Einrichten des Überwachungs-Timers für die Meldungskommunikation, wobei für Kommunikation mit expliziten Meldungen und FINS-Kommunikation derselbe Timer verwendet wird.

Registerkarte „General“



Komponente	Beschreibung
Unregistered Device List	Im Netzwerkkonfigurationsbereich angezeigte, aber noch bei keinem Master registrierte Slave-Geräte.
Registered Device List	Die bei einem Master registrierten Slave-Geräte.
Schaltflächen zum Registrieren und Deregistrieren von Geräten	Mithilfe der Schaltfläche zum Registrieren von Geräten verschieben Sie ein Gerät aus der Liste **Unregistered Device List** (oben) in die Liste **Registered Device List** (unten). Mithilfe der Schaltfläche zum Deregistrieren von Geräten verschieben Sie ein Gerät aus der Liste **Registered Device List** (unten) in die Liste **Unregistered Device List** (oben).
Auto allocation as is registered	Ist dieses Kontrollkästchen aktiviert, werden beim Registrieren von Slaves bei einem Master die ungenutzten Worte in der Reihenfolge der Registrierung zugeordnet.
Register/Unregistered (Schaltfläche)	Mit dieser Schaltfläche können Sie die E/A-Zuordnung (Zuordnung ungenutzter Worte ohne nicht zugeordnete Worte) des ausgewählten Slaves aufheben und neu zuordnen.
Advanced Setup (Schaltfläche)	Einstellen der Verbindungseinstellungen und Anzeigen oder Überprüfen der Geräteinformationen.
Upload (Schaltfläche)	Hochladen der Geräteparameter aus den tatsächlich mit dem Netzwerk verbundenen Geräten.
Download (Schaltfläche)	Herunterladen der Geräteparameter in die mit dem Netzwerk verbundenen Geräte.
Verify (Schaltfläche)	Verifizieren der Geräteparameter der mit dem Netzwerk verbundenen Geräte, d. h. Vergleich der tatsächlichen Geräteparameter mit den im Netzwerkkonfigurator eingestellten Geräteparametern.

Slave-Registrierung und automatische Zuordnung des E/A-Bereichs

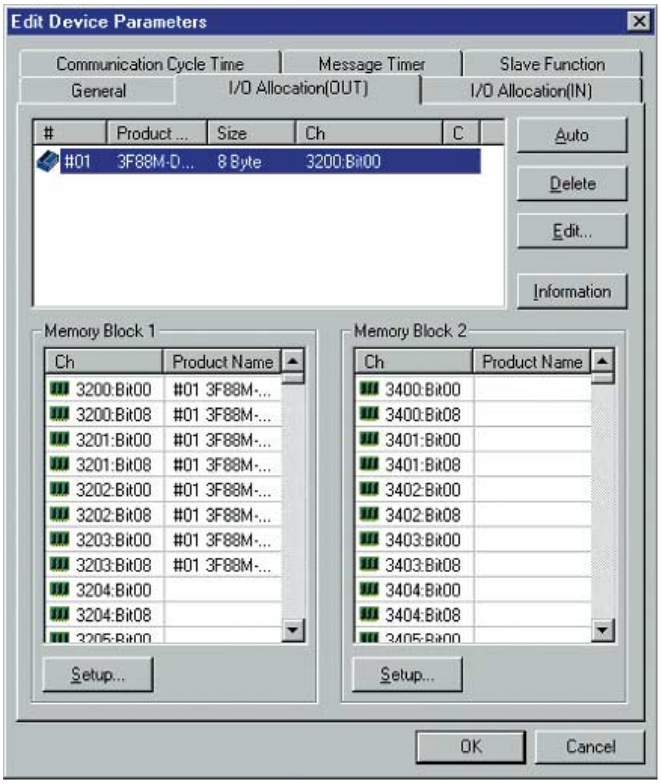
Wird bei aktivierter Master-Funktion ein Slave registriert, werden diesem automatisch Wörter aus dem für die E/A-Zuordnung vorgesehenen Speicherblock zugeordnet.

Die Zuordnung erfolgt für Eingangs- wie für Ausgangsbereiche sequenziell in der Reihenfolge der Registrierung, beginnend beim Anfang von Speicherblock 1. Wurde Speicherblock 1 vollständig zugeordnet, setzt die Zuordnung mit Speicherblock 2 fort. Legen Sie die Bereiche und Größen der für die Zuordnung vorgesehenen Speicherblöcke vorab vor dem Registrieren von Slaves fest.

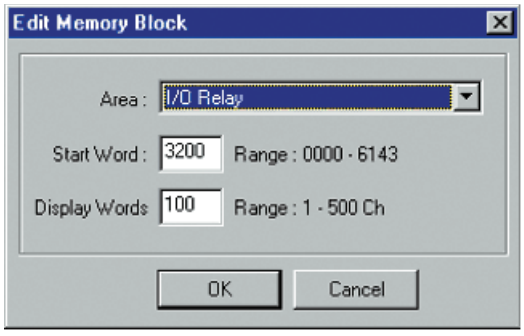
Hinweis: Die automatisch zugeordneten Bereiche können später noch geändert werden.

Festlegen der Speicherblöcke für die Zuordnung

1. Wählen Sie einen Master aus, und wählen Sie in der Menüleiste ***Device - Parameter - Edit***. Nun wird das Dialogfeld **Edit Device Parameter** angezeigt.
2. Klicken Sie auf die Registerkarte **I/O Allocation (OUT)**.



3. Klicken Sie im Bereich **Memory Block 1** auf **Setup…**.
4. Legen Sie die Parameter *Area*, *Start Word* und *Display Words* (die Anzahl der Worte im Speicherblock) für Speicherblock 1 fest.



5. Legen Sie die Parameter für Speicherblock 2 auf die gleiche Weise fest.
6. Klicken Sie auf die Registerkarte **I/O Allocation (IN)**, und legen Sie die Speicherblöcke auf die gleiche Weise wie auf der Registerkarte **I/O Allocation (OUT)** fest.

Hinweis:
- Setzen Sie den Parameter **Area** für nicht verwendete Blöcke auf *Not Use*.
- Der Parameter **Display Words** bestimmt die Anzahl der im Netzwerkkonfigurator angezeigten Worte eines Blocks. Dieser Wert wird nicht in die Baugruppe heruntergeladen. Beträgt die Größe des zugeordneten Bereichs eines Speicherblocks beim Hochladen 100 Worte oder weniger, wird der Parameter **Display Words** auf 100 eingestellt.

Festlegen der automatischen Zuordnung beim Registrieren

- Ist das Kontrollkästchen für die automatische Zuordnung (*Auto-allocation as is registered*) aktiviert, werden die Worte für die E/A beim Registrieren von Slaves bei einem Master in diesem Dialogfeld automatisch in der Reihenfolge der Registrierung zugeordnet. Diese Option ist nur in diesem Dialogfeld **Edit Device Parameters** wirksam.

  Bei der automatischen Zuordnung erfolgt die Zuordnung von Worten beginnend mit den unbenutzten Worten in Block 1 des entsprechenden E/A-Speicherblocks in der Reihenfolge der Registrierung (d. h. in der Reihenfolge, in der die Slaves gezogen und abgelegt werden).
- Das Löschen oder Ändern der Zuordnung für einzelne Slaves (Zuordnung ungenutzter Worte) kann jederzeit erfolgen. Klicken Sie dazu auf die Schaltfläche **Auto Register/Unregistered**.

B-3 E/A-Zuordnung mithilfe des Parameter-Assistenten (einfache E/A-Zuordnung)

- Die E/A im SPS-Speicher kann den Slaves auf einfache und interaktive Weise zugeordnet werden.
- Die E/A-Zuordnung geht folgendermaßen vonstatten: In der Reihenfolge der Knotenadressen, einfache E/A-Zuordnung beginnend bei Block 1 in Blöcken zu je 100 Worten.

Die Zuordnung erfolgt in der Reihenfolge der Slave-Knotenadressen beginnend bei Block 1 (die Zuordnung der Worte von Block 2 beginnt erst, wenn Block 1 vollständig zugeordnet wurde) in Blöcken zu je 100 Worten.

Hinweis: Nach der E/A-Zuordnung mithilfe dieses Assistenten können die Knotenadressen und die E/A-Zuordnung wie weiter hinten in diesem Abschnitt unter *Manuelle E/A-Zuordnung* beschrieben die Knotenadressen und die E/A-Zuordnung geändert werden.

Der Parameter-Assistent legt die Anfangsadresse jedes einzelnen Blocks (die Blockgröße beträgt jeweils 100 Worte), die Zuordnungsmethode (wortweise Zuordnung oder Minimierung der Anzahl der unbenutzten Worte) fest.

Hinweis:
- Die Zuordnung von Bereichen von mehr als 100 Worten je Block ist nur im Rahmen der manuellen Zuordnung möglich.
- Gehen Sie wie im Folgenden beschrieben vor, um die E/A-Zuordnung von Slave-Geräten eines Master-Geräts mithilfe des Parameter-Assistenten durchzuführen.

1. Wählen Sie das Master-Gerät aus, an dem das Slave-Gerät registriert werden soll.
2. Wählen Sie den Menübefehl **Device - Parameter - Wizard**.
3. Klicken Sie auf **Yes**.

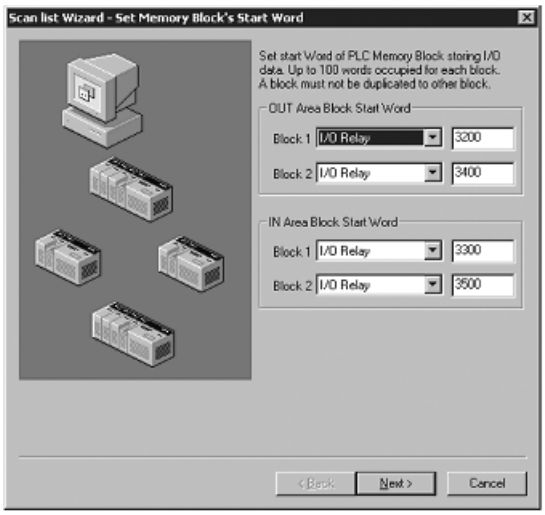
   Wird der Parameter-Assistent für die Einrichtung verwendet, werden alle aktuellen Einstellungen initialisiert. Ein Bestätigungsdialogfeld wird angezeigt (siehe nachstehende Abbildung).

4. Einstellen des Startworts für jeden einzelnen Block

   Nun wird das Fenster **Scan List Wizard-Setting Memory Block's Start Word** angezeigt (siehe nachstehende Abbildung).

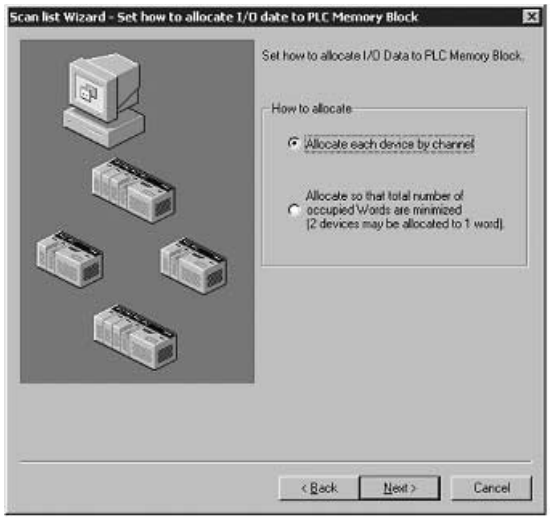
   Stellen Sie die zu verwendenden Speicherbereiche und die zugehörigen Startworte ein, und klicken Sie auf **Next**. Die Zuordnung startet automatisch beginnend bei Block 1. Wurde Block 1 vollständig zugeordnet, setzt die Zuordnung mit Block 2 fort. Die Zuordnung in den einzelnen Blöcken beginnt bei dem eingestellten Startwort. Je Block können maximal 100 Worte (fix) zugeordnet werden.

Hinweis: Sollten sich Blöcke überlappen oder die Einstellung der Startworte dazu führen, dass der Speicherbereich überschritten wird, können Sie nicht zum nächsten Schritt übergehen.

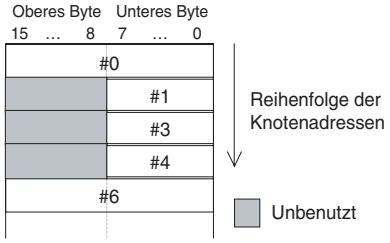
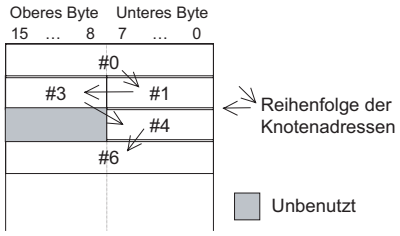


5. Einstellen der E/A-Zuordnungen für die dezentrale E/A

   Nun wird das Fenster **Scan List Wizard-Set how to allocate I/O data to PLC Memory Block** angezeigt, in dem die E/A-Zuordnungsmethode für Geräte festgelegt wird (siehe nachstehende Abbildung). Wählen Sie die gewünschte Zuordnungsmethode aus, und klicken Sie auf **Next**.



Die E/A-Zuordnung für Geräte kann auf zweierlei Weise erfolgen:

Allocate each device by channel	Jedem Slave wird stets das untere Byte (die unteren acht Bits) des Worts zugeordnet. Auf diese Weise wird jedem Slave ein Wort zugeordnet, selbst wenn die Zuordnung für mehrere 1-Byte-E/A-Slaves in Folge durchgeführt wird. Beispiel: 
Allocate so that the total number of allocated words is minimized (two devices may be allocated to one word)	Erfolgt eine Zuordnung für 1-Byte-E/A-Slaves, so erfolgt diese in der Reihenfolge unteres Byte/oberes Byte (untere 8 Bits/obere 8 Bits), um möglichst wenige unbenutzte Bereiche zu erzeugen. Beispiel: 

Im Folgenden finden Sie ein Beispiel für die Zuordnung von Worten.
Diesem Beispiel liegen Slaves der folgenden Datengröße zu Grunde:

#00	1 Byte
#01	2 Bytes
#02	1 Byte
#03	4 Bytes
#04	1 Byte
#05	1 Byte

Zuordnung Slave für Slave (Allocate each device by channel)

	Oberes Byte (15 – 8)	Unteres Byte (7 – 0)
+0		#00
+1	#01	
+2		#02
+3	#03	
+4	#03	
+5		#04
+6		#05

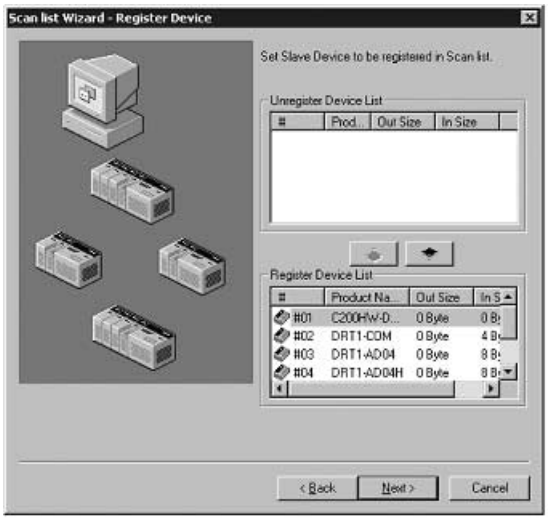
Zuordnung mit Minimierung der Anzahl der unbenutzten Bereiche (Allocate so that the total number of allocated words is minimized (two devices may be allocated to one word))

	Oberes Byte (15 – 8)	Unteres Byte (7 – 0)
+0	#02	#00
+1	#01	
+2	#03	
+3	#03	
+4	#05	#04

6. Registrieren und Deregistrieren von Slaves

   Nun wird das Fenster **Scan List Wizard-Register Device** angezeigt

   Die nachstehende Abbildung zeigt ein Beispiel für dieses Fenster. Wählen Sie die beim Master-Gerät zu registrierenden Slave-Geräte aus, und klicken Sie auf **Next**.

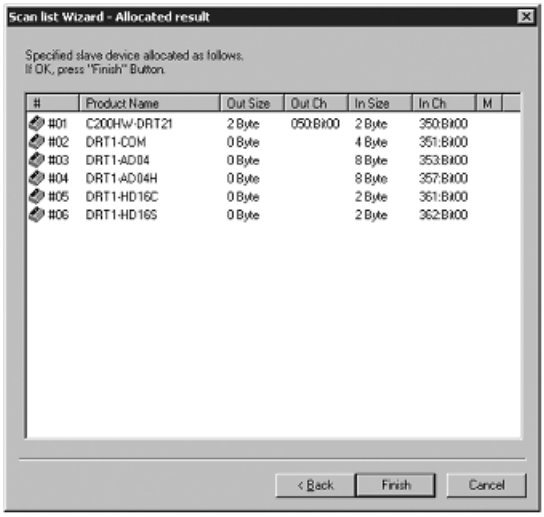


   Im Netzwerk vorhandene Geräte werden in der Liste **Registered Device List** als bereits registriert angezeigt. Wenn es Geräte gibt, die nicht registriert sein sollen, so klicken Sie auf die Schaltfläche , um diese zu deregistrieren. Sind keine Geräte registriert, können Sie nicht zum nächsten Schritt übergehen.

7. Anzeigen des Ergebnis der E/A-Zuordnung für die dezentrale E/A

   Nach Durchführung der Registrierung mit der jeweiligen Methode wird das Fenster **Scan List Wizard - Allocation Result** angezeigt (siehe nachstehendes Beispiel). Sind die angezeigten Details korrekt, so klicken Sie auf **Finish**. Dies beendet den Parameter-Assistenten. Um zu den vorherigen Einstellungs-Fenstern zurückzukehren, klicken Sie auf **Back**.

   Die eingestellten E/A-Zuordnungen werden als Geräteparameter eingestellt.



8. Herunterladen von Parametern in ein Master-Gerät

   Ist der Netzwerkkonfigurator mit dem Netzwerk verbunden, wird das folgende Dialogfeld angezeigt:

   Wenn Sie auf **Yes** klicken, um die Parameter in ein Master-Gerät herunter zu laden, startet die Kommunikation mit der dezentralen E/A mit den neuen Einstellungen.

Hinweis: Mithilfe des Parameter-Assistenten eingerichtete Geräteparameter können bei Bedarf geändert werden.

B-4 Manuelle E/A-Zuweisung

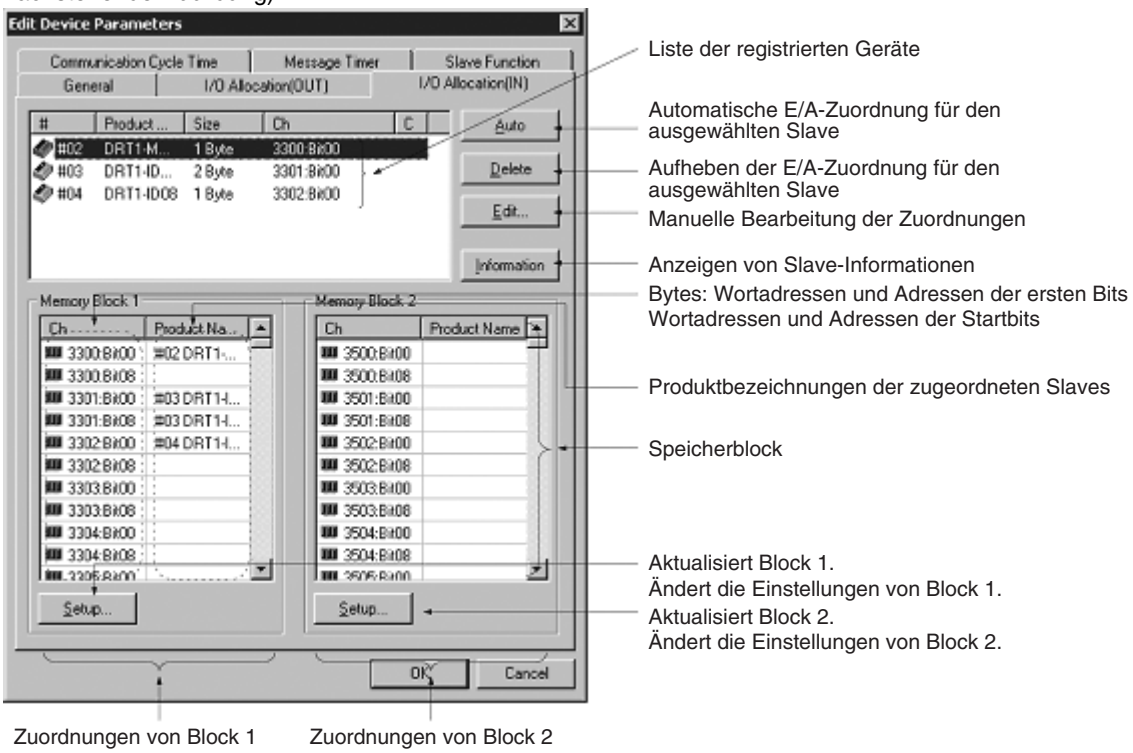
Die Speicherzuordnung für die Slave-E/A kann auch manuell erfolgen.

Registerkarte „I/O Allocation“

Auf der Registerkarte **I/O Allocation** erfolgen die folgenden Einträge:

1. Zuordnung des E/A-Speichers in der CPU-Baugruppe für die E/A-Speicherblöcke 1 und 2
2. Zuordnung der Worte der einzelnen Speicherblöcke zu den Slave-Geräten

Die manuelle Zuordnung erfolgt auf den Registerkarten **I/O Allocation (OUT)** bzw. **I/O Allocation (IN)** (siehe nachstehende Abbildung).



Komponente der Registerkarte		Beschreibung
Liste der registrierten Geräte		Anzeige der Geräte aus der Liste **Register Device List** auf der Registerkarte **General** mit gültigen Eingangs- oder Ausgangsdaten.
Auto (Schaltfläche)		Weist den in der Liste der registrierten Geräte ausgewählten Slaves beginnend mit dem ersten unbenutzten Wort unbenutzte Worte zu.
Delete (Schaltfläche)		Gibt die den in der Liste der registrierten Geräte ausgewählten Slaves zugeordneten Worte frei.
Edit (Schaltfläche)		Manuelle Bearbeitung der Zuordnungen.
Information (Schaltfläche)		Zeigt die Slave-Informationen (zugeordnete Worte und E/A-Kommentare) an.
Memory Block 1 und Memory Block 2		Zeigt den Zuordnungsstatus der Slaves (Spalte **Product Name**) in den Speicherblöcken 1 und 2 an.
	Ch	Beginn der Zuordnung. Hinter der Wortadresse wird die Adresse des ersten Bits angezeigt.
	Product Name	Bezeichnung des Geräts, dem der Speicher zugeordnet wurde.
Setup (Schaltfläche)		Legt die Startadresse und die Größe (Anzahl der Worte) der Speicherblöcke 1 und 2 fest.

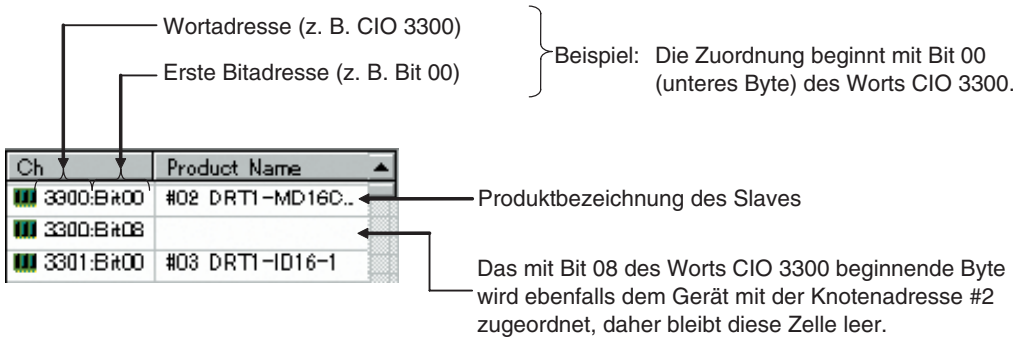
Zusatzinformationen: Zuordnungsstatus der Blöcke 1 und 2

In den Zuordnungszustandlisten der Speicherblöcke werden die Produktbezeichnungen der Geräte, denen Speicher des jeweiligen Blocks zugeordnet wurde, und das erste zugeordnete Wort der CPU-Baugruppe angezeigt.

Die Spalte **Ch** gibt das erste zugeordnete Bit an. Hierbei wird die Wortadresse angegeben, gefolgt von der Adresse des ersten Bits.

Example: „3300: Bit 00“ gibt an, dass das erste zugeordnete Bit das Bit 00 des Worts CIO 3300 ist (die Zuordnung beginnt also mit dem unteren Byte).

Example: „3300: Bit 08“ gibt an, dass das erste zugeordnete Bit das Bit 08 des Worts CIO 3300 ist (die Zuordnung beginnt also mit dem oberen Byte).



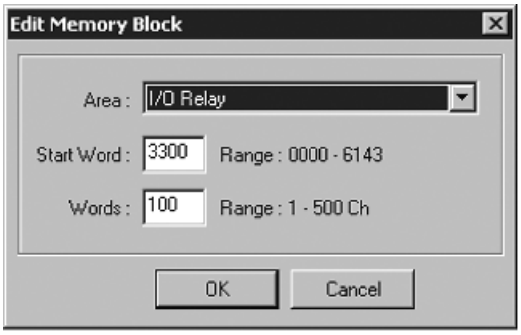
Wird einer der Speicherblöcke nicht benutzt, werden für diesen auch keine Zuordnungsinformationen angezeigt.

Ändern des Startworts des E/A-Blocks

Schaltfläche „Setup“ auf den Registerkarten „I/O Allocation“ (*Device - Parameter - Edit*)

Gehen Sie wie im Folgenden beschrieben vor, um die Zuordnungsbereiche für die E/A-Blöcke im E/A-Speicher der CDU-Baugruppe zu ändern.

1. Klicken Sie auf die Schaltfläche **Setup** des zu ändernden Blocks.
2. Nun wird das folgende Dialogfeld angezeigt:



3. Nehmen Sie die erforderlichen Änderungen an den Einstellungen der Parameter *Area*, *Start Word* und *Words* vor.
   Stellen Sie den Parameter *Words* auf die Anzahl der im Netzwerkkonfigurator angezeigten Worte ein. Für einen Block können maximal 500 Worte zugeordnet werden.
   Die nachstehende Tabelle führt die möglichen Bereiche für diese Einstellungen auf:

SPS-Modell	Speicherbereich	Bereich
CS-Serie CJ-Serie	CIO-Bereich	0000 bis 6143
	DM-Bereich	D0000 bis D8191
	Arbeitsbereich	W000 bis W511
	Haltebereich	H000 bis H511
	Erweiterter Datenspeicherbereich (EM)	E00000 bis E32767

   Beim erweiterten Datenspeicherbereich (EM) können die Speicherbänke 0 bis 12 verwendet werden.

Hinweis:
- Der Parameter **Words** gibt die Anzahl der im Netzwerkkonfigurator angezeigten Worte an. Dieser Wert wird nicht in den Master heruntergeladen.
- Beträgt die Größe des zugeordneten Bereichs eines Speicherblocks beim Hochladen 100 Worte oder weniger, wird der Parameter **Words** auf 100 eingestellt.

4. Klicken Sie auf **OK**, um die geänderten Einstellungen des Speicherblocks zu übernehmen.
   War den Geräten bereits Speicher zugeordnet worden, wird dieser Speicher nun im neuen Speicherblock erneut zugeordnet. Wird der für die Zuordnung zur Verfügung stehende Bereich jedoch überschritten, wird die Zuordnung für die entsprechenden Geräte gelöscht. In diesem Fall muss die Speicherzuordnung wiederholt werden.

E/A-Zuweisungsmethode

Registerkarten „I/O Allocation“ (*Device Parameter Edit*)

Die E/A-Zuordnung kann auf dreierlei Weise erfolgen:

1. Manuelle Zuordnung mithilfe des Dialogfelds „Edit I/O Allocate“

   Wählen Sie ein Slave-Gerät aus der Liste der registrierten Geräte aus, und klicken Sie auf **Edit**. Führen Sie mithilfe des Dialogfelds **Edit I/O Allocate** die manuelle Speicherzuordnung für die einzelnen Slaves durch.
2. Zuordnung im Rahmen einer Drag&Drop-Operation

   Ziehen Sie ein Gerät aus der Liste der registrierten Geräte, und legen Sie es an der entsprechenden Wort-Position im gewünschten Speicherblock ab.
3. Automatische Zuordnung

   Wählen Sie ein Gerät aus der Liste der registrierten Geräte aus, und klicken Sie auf **Auto**. Auf diese Weise wird eine automatische Zuordnung unbenutzter Worte durchgeführt. (Für Geräte, für die unter Verwendung der Schaltfläche **Advanced Setup** auf der Registerkarte **General** eine anwenderdefinierte Einstellung vorgenommen wurde, kann jedoch keine automatische Zuordnung erfolgen.)

Hinweis: Bei Geräten, für die auf der Registerkarte **General** mehrere Verbindungen eingerichtet wurden, wird die E/A-Datengröße in der Spalte **Size** der Liste der registrierten Geräte ähnlich wie im Folgenden dargestellt angezeigt.

Um die E/A zur Linken mittels einer Drag&Drop-Operation zuzuordnen, verwenden Sie zum Ziehen die linke Maustaste. Um die E/A zur Rechten mittels einer Drag&Drop-Operation zuzuordnen, verwenden Sie zum Ziehen die rechte Maustaste. Besteht nur eine Verbindung, so verwenden Sie die linke Maustaste.

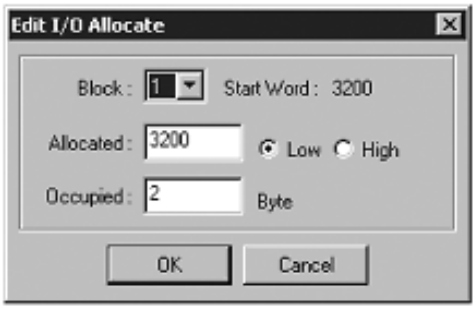
Manuelle Zuordnung mithilfe des Dialogfelds „Edit I/O Allocate“

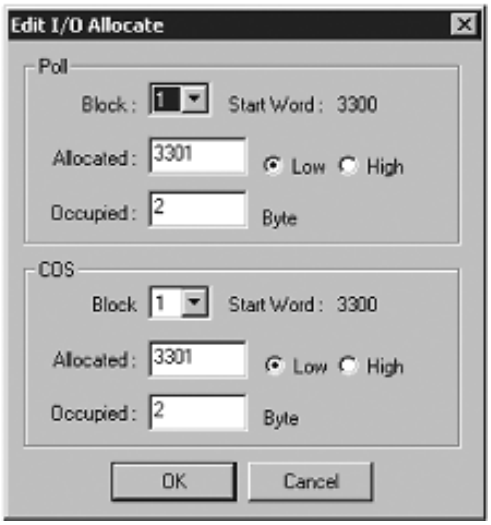
Schaltfläche „Edit“ auf der Registerkarte „I/O Allocation“

Gehen Sie wie folgt vor, um mithilfe des Dialogfelds **Edit I/O Allocate** eine manuelle Zuordnung durchzuführen.

1. Wählen Sie das Gerät aus, dessen E/A-Zuordnung sie bearbeiten möchten.
2. Klicken Sie auf **Edit**.
3. Nun wird das Dialogfeld **Edit I/O Allocate** angezeigt (siehe nachfolgende Beispiele).

   Stellen Sie den gewünschten Block (1 oder 2), das erste zugeordnete Wort, das Startbyte (unteres Byte: *Low*, oberes Byte: *High*) und die Anzahl der zugeordneten Bytes (*occupied*) ein.





Die Definition der Verbindungen erfolgt auf der Registerkarte (Schaltfläche)

Legen Sie das zuzuordnende Startwort und die Anzahl der zuzuordnenden Bytes fest.

Zusätzlich zur Wort-Zuordnung können Sie auch die Byte-Zuordnung (oberes oder unteres Byte) festlegen. Werden zwei oder mehr Bytes zugeordnet, muss die Byte-Zuordnung auf *Low* eingestellt werden.

Zuordnung eines unteren Bytes zu einem Gerät

	Oberes Byte	Unteres Byte
	15 8	7 0
+0CH		#00
+1CH		
+2CH		

Zuordnung eines oberen Bytes zu einem Gerät

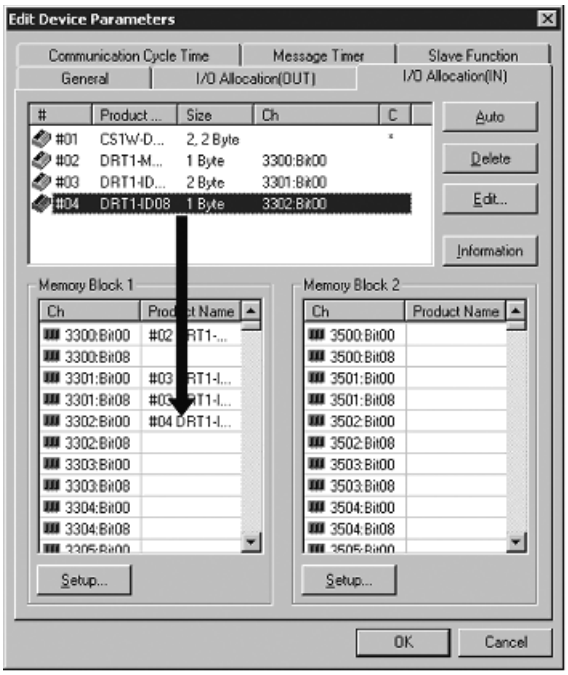
	Oberes Byte	Unteres Byte
	15 8	7 0
+0CH	#00	
+1CH		
+2CH		

4. Klicken Sie auf **OK**, um die E/A-Zuordnung durchzuführen.

Zuordnung im Rahmen einer Drag&Drop-Operation

Drag&Drop-Operation auf einer der Registerkarten „I/O Allocation“

1. Blättern Sie in der Speicherblockliste zu dem Wort, ab dem Sie dem Slave Speicher zuordnen möchten.
2. Wählen Sie den Slave aus der Liste der registrierten Geräte im oberen Bereich aus.
3. Ziehen Sie den Slave zu dem Startbyte, das Sie dem Slave zuordnen möchten.



- Inhalt der Speicherblockliste

  Die Speicherblockliste im unteren Bereich des Fensters zeigt in der Spalte *Ch* den zugeordneten Speicher (d. h. die Wortadresse und Byteadresse) und in der Spalte *Product Name* die Produktbezeichnung des Slaves, dem dieser Speicher zugeordnet ist.
- Inhalt der Liste der registrierten Geräte

  Die Liste der registrierten Geräte im oberen Bereich des Fensters zeigt in der Spalte # die Knotennummer, in der Spalte *Product Name* die Produktbezeichnung des Slaves, in der Spalte *Size* die Anzahl der zugeordneten Bytes und, sofern der Speicher bereits zugeordnet wurde, in der Spalte *Ch* das Startbyte (d. h. die Wortadresse und die Startbitadresse).

Um die Zuordnung für einen Slave zu ändern oder zu löschen, wählen Sie den Slave aus der Liste der registrierten Geräte aus, und klicken Sie auf **Delete**.

Hinweis: Um einem Slave automatisch das nächste unbenutzte Wort zuzuordnen, wählen Sie den Slave aus der Liste der registrierten Geräte aus, und klicken Sie auf **Auto**.

Automatische Zuordnung

Schaltflächen „Auto“ und „Delete“ auf der Registerkarte „I/O Allocation“

- Um dem ausgewählten Slave automatisch das nächste unbenutzte Wort zuzuordnen, klicken Sie auf **Auto**.
- Um die E/A-Zuordnung für den ausgewählten Slave aufzuheben, klicken Sie auf **Delete**.

Ist jedoch die automatische Zuordnung festgelegt, kann die später beschriebene erweiterte Konfiguration nicht verwendet werden.

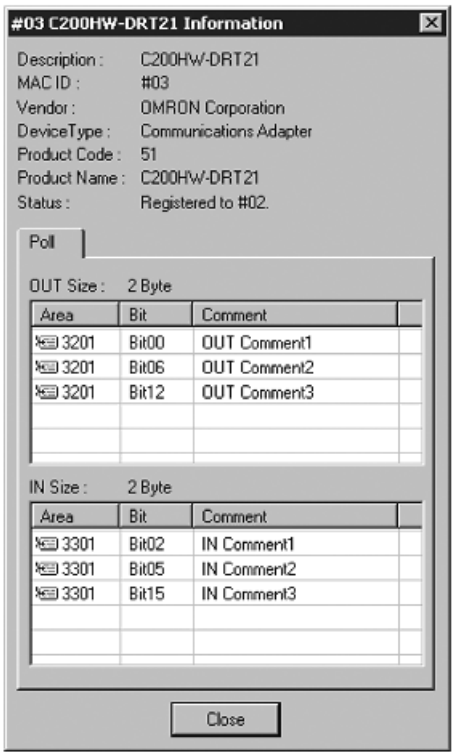
Anzeigen von Slave-Informationen

Schaltfläche „Information“ auf der Registerkarte „I/O Allocation“

Auf der Registerkarte „I/O Allocation“ können bestimmte Informationen zu registrierten Slave-Geräten (z. B. E/A-Kommentare) abgerufen werden. (Zum Einrichten von E/A-Kommentaren für die E/A-Daten von Slave-Geräten wählen Sie den Menübefehl *Device Edit I/O Comment*.)

Gehen Sie wie folgt vor, um Informationen zu einem Slave-Gerät anzuzeigen.

1. Markieren Sie das Gerät, dessen Informationen Sie anzeigen möchten.
2. Klicken Sie auf **Information**.
3. Nun wird das folgende Fenster angezeigt:



Wenn Sie ein registriertes Gerät auswählen, während das Informations-Fenster angezeigt wird, werden die Slave-Informationen in diesem Fenster auf die Informationen des neu ausgewählten Geräts aktualisiert.

B-5 Erweiterte Einstellungen: Verbindung, Kommunikationszykluszeit, Slave-Funktion, Einstellungen usw.

Dieser Abschnitt beschreibt die Verbindungseinstellungen, die Anzeige mit den Geräteinformationen und den Kontrollkästchen für die Auswahl der durchzuführenden Überprüfungen, die Kommunikationszykluszeiteinstellung, die Message Timer-Einstellungen und die Slave-Funktions-Einstellungen.

Erweiterte Konfiguration

Schaltfläche „Advanced Setup“ nach der Auswahl eines Slaves auf der Registerkarte „General“ (*Device - Parameter - Edit*)

Für die Kommunikation mit dezentralen E/A-Geräten können erweiterte Einstellungen (einschließlich Anzeige der Geräteinformationen und der Kontrollkästchen für die Auswahl der durchzuführenden Überprüfungen) und Verbindungseinstellungen vorgenommen werden.

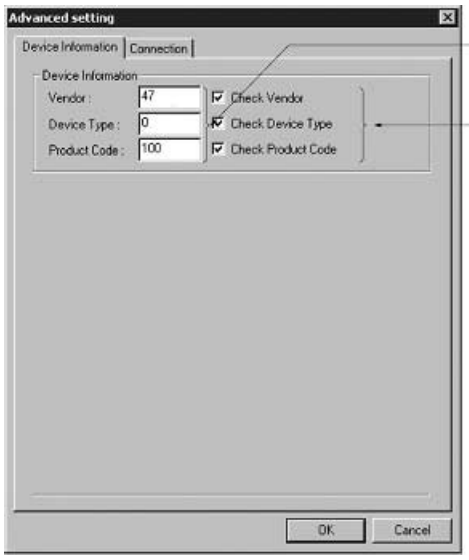
Geräteinformationen und Kontrollkästchen für die Auswahl der durchzuführenden Überprüfungen

- Registerkarte „Device Information“

Die Registerkarte „Device Information“ bietet Geräteinformationen und Kontrollkästchen für die Auswahl der durchzuführenden Überprüfungen. Zum Aufrufen dieser Registerkarte gehen Sie wie folgt vor:

1. Wählen Sie ein Slave-Gerät aus der Liste der registrierten Geräte aus.
2. Klicken Sie auf **Advanced Setup**.
3. Nun wird das folgende Fenster angezeigt.

   Registerkarte „Device Information“



Hier werden die Geräteinformationen des ausgewählten Slave-Geräts angezeigt.

Sind diese Kontrollkästchen aktiviert, werden die Geräteinformationen bei der Kommunikation mit der dezentralen E/A mit den entsprechenden Daten in der Abfrageliste verglichen. Wenn diese Daten nicht übereinstimmen, wird ein Verifizierungsfehler ausgelöst.

Auf dieser Registerkarte werden die Geräteinformationen (Hersteller, Gerätetyp, Produktcode) des aktuell ausgewählten Slave-Geräts angezeigt.

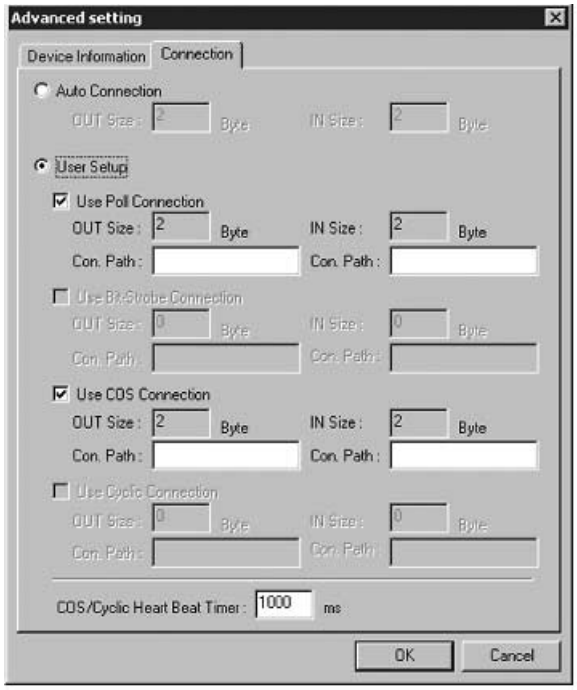
Mithilfe der Kontrollkästchen können Sie festlegen, dass die Geräteinformationen bei jeder Kommunikation mit der dezentralen E/A (d. h. sobald eine Verbindung geöffnet wird) überprüft und beim Feststellen von Inkonsistenzen ein Fehler ausgelöst wird.

Verbindungseinstellungen

- Registerkarte „Connection“

Für jeden Slave können Sie maximal zwei Verbindungen zur Verwendung für die Kommunikation mit der dezentralen E/A festlegen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie das Slave-Gerät aus der Liste der registrierten Geräte aus.
2. Klicken Sie auf **Advanced Setup**.
3. Nun wird das folgende Fenster angezeigt.
   Klicken Sie auf die Registerkarte **Connection**.



Die Standardeinstellung ist *Auto Connection*.

Gehen Sie folgendermaßen vor, um eine Verbindung einrichten:

1. Aktivieren Sie das Optionsfeld *User Setup*.
   Nun können Sie die Einstellungen für die Verbindungen vornehmen.
2. Wählen Sie die zu verwendenden Verbindungen aus.
   Sie können maximal zwei Verbindungen einrichten.

Hinweis: *COS* und *Cyclic* können nicht gleichzeitig eingestellt werden.

3. Legen Sie – sofern erforderlich – den Verbindungspfad fest.
4. Stellen Sie – sofern erforderlich – den Parameter *COS/Cyclic Heartbeat Timer* ein.
5. Klicken Sie auf **OK**.
   In der Spalte *C* rechts in der Liste der registrierten Geräte wird nun ein Sternchen angezeigt.

Wird die Verbindung für ein Gerät, für das bereits eine E/A-Zuordnung durchgeführt wurde, geändert, wird die aktuelle E/A-Zuordnung gelöscht. In diesem Fall muss die Speicherzuordnung wiederholt werden.

WICHTIG:
- COS und Cyclic können nicht gleichzeitig eingestellt werden.
- Werden gleichzeitig eine Poll-Verbindung und eine COS-Verbindung oder eine Poll-Verbindung und eine zyklische Verbindung verwendet, müssen die Ausgangseinstellungen für beide Verbindungen übereinstimmen.

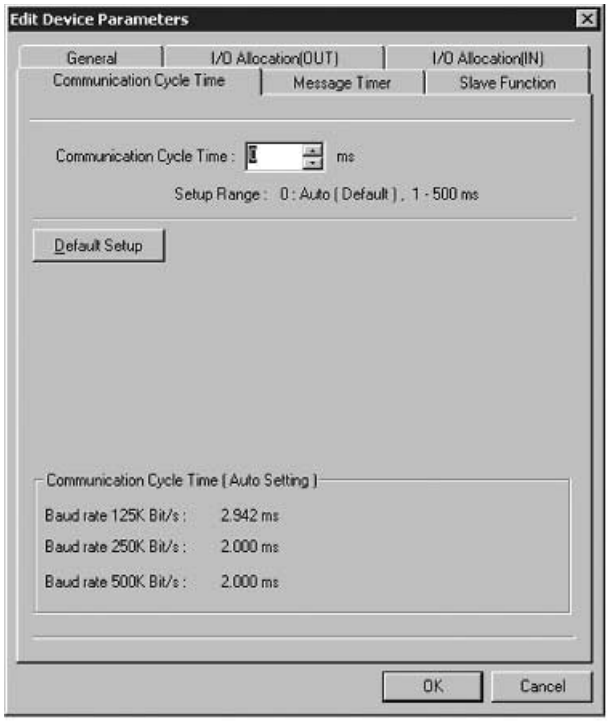
Hinweis: Wurde für ein Gerät auf die geschilderte Weise eine Verbindung eingerichtet, kann die automatische Zuordnung für dieses Gerät nicht mehr verwendet werden. Um die automatische Zuordnung wieder verwenden zu können, müssen Sie das Gerät deregistrieren und erneut registrieren.

Kommunikationszykluszeit

Registerkarte „Communications Cycle Time“ (*Device - Parameter - Edit*)

Die Registerkarte **Communications Cycle Time** ermöglicht das Einstellen der Kommunikationszykluszeit und zeigt zugleich die auf den Informationen zu den aktuell registrierten Geräten basierenden berechneten Kommunikationszykluszeiten an.

Klicken Sie auf die Registerkarte **Communications Cycle Time**, um das folgende Fenster anzuzeigen.



Die Kommunikationszykluszeit kann auf einen Wert zwischen 1 und 500 ms eingestellt werden. Um die Kommunikationszykluszeit automatisch einzustellen, klicken Sie auf **Default Setup**, oder stellen Sie den Wert 0 ms ein.

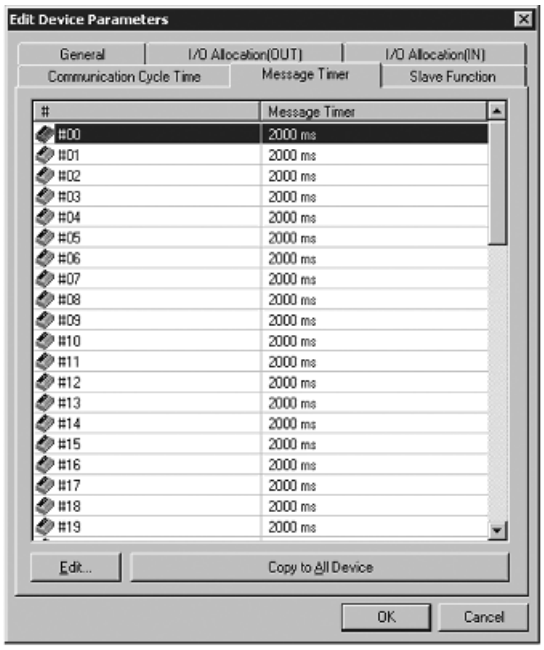
Die automatische Berechnung der Kommunikationszykluszeit erfolgt für jede Baudrate separat, basierend auf den Informationen zu den aktuell registrierten Geräten.

Hinweis: Die Kommunikationszykluszeit bezeichnet das Intervall, mit dem sich die dezentrale E/A-Kommunikation mit ein und demselben Slave wiederholt. Durch Einstellung der Kommunikationszykluszeit können durch die konkreten Betriebsbedingungen verursachte Fluktuationen der Kommunikationszykluszeit verhindert werden. Durch Einstellung einer längeren Kommunikationszykluszeit kann verhindert werden, dass bei einem Slave mit einer langsameren Verarbeitungsgeschwindigkeit irrtümlich ein Fehler festgestellt wird.

Nimmt die tatsächliche E/A-Kommunikation mit den dezentralen Slaves weniger Zeit als die eingestellte Kommunikationszykluszeit in Anspruch, wartet der Master mit dem Einleiten des nächsten E/A-Kommunikationszyklus, bis die Kommunikationszykluszeit verstrichen ist. Nimmt die tatsächliche E/A-Kommunikation mit den dezentralen Slaves mehr Zeit als die eingestellte Kommunikationszykluszeit in Anspruch, findet die E/A-Kommunikation unabhängig von der Einstellung der Kommunikationszykluszeit in der erforderlichen Zeit statt.

Message Timer-Einstellungen

Registerkarte „Message Timer“ (*Device - Parameter - Edit*)



Die Standardeinstellung für den Message Timer beträgt zwei Sekunden (2.000 ms). Sie kann in Schritten von 1 ms auf einen Wert zwischen 500 und 30.000 ms eingestellt werden.

Zum Ändern dieses Werts gehen Sie wie folgt vor:

1. Doppelklicken Sie auf eine Knotenadresse (#), oder wählen Sie eine Knotenadresse aus, und klicken Sie auf **Edit**. Nun wird das folgende Dialogfeld angezeigt:

2. Geben Sie einen Wert ein, und klicken Sie auf **OK**.

Hinweis: Um für alle Geräte denselben Wert einzustellen, wählen Sie die Knotenadresse eines Geräts aus, das bereits auf den gewünschten Wert eingestellt ist, und klicken Sie auf *Copy to All Device*.

Hinweis:
- Der Message Timer überwacht das Auftreten von Zeitüberschreitungen in der Meldungskommunikation, wobei für Kommunikation mit expliziten Meldungen und FINS-Kommunikation derselbe Timer verwendet wird. Er kann für jedes einzelne Gerät, das Kommunikation durchführt (Meldungs-Ziel), individuell gesetzt werden.
- Hat das Ziel-Kommunikationsgerät (d. h. das Ziel der Nachricht) eine zu lange Antwortzeit, muss die Einstellung für den Message Timer erhöht werden. (Erfolgt eine FINS-Kommunikation über mehrere Netzwerkebenen hinweg, führt dies zu einer Verlängerung der Antwortzeiten. Setzen Sie in diesem Fall die Einstellung für den Message Timer auf einen höheren Wert.) Ein hoher Wert für den Message Timer hat jedoch den Nachteil, dass die nächste Nachricht an dasselbe Kommunikationsgerät nicht abgesendet werden kann, solange auf eine Antwort gewartet wird.
- Die DeviceNet-Baugruppe nutzt diesen Timer für die Überwachung auf das Auftreten von Zeitüberschreitungen bei der Kommunikation. Im Gegensatz hierzu verwendet die CDU-Baugruppe die Antwortüberwachungszeit der Befehle CMND, SEND, und RECV für die Überwachung. Es hat daher keinerlei Auswirkungen, ob die Einstellungen für den Message Timer oder die Antwortüberwachungszeit der Befehle CMND, SEND, und RECV länger ist.
- Setzen Sie die Antwortüberwachungszeit der Befehle CMND, SEND, und RECV auf einen Wert, der mindestens so groß ist wie die Einstellung für den Message Timer.

  Treten viele Zeitüberschreitungen auf, so erhöhen Sie beide Einstellungen. Behalten Sie dabei aber das oben angegebene Verhältnis bei.

Einstellungen für die Slave-Funktion

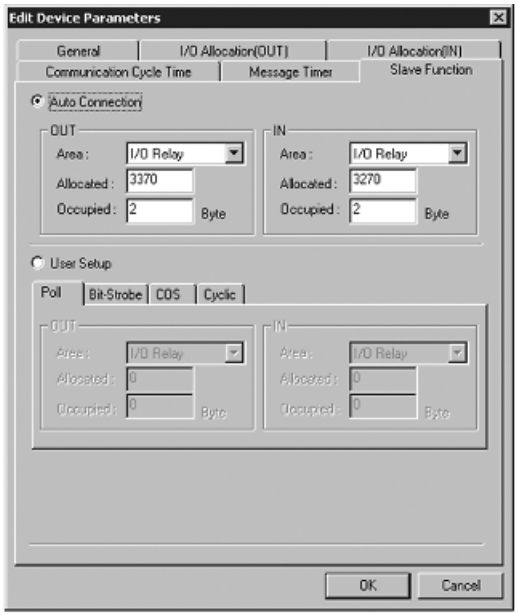
Registerkarte „Slave Function“ (*Device - Parameter - Edit*)

Die Slave-Funktion kann durch eine entsprechende Einstellung auf der Registerkarte **Slave Function** aktiviert werden.

WICHTIG: Zum Aktivieren der Slave-Funktion wählen Sie das Gerät aus, und wählen Sie den Menübefehl ***Device - Property***. Aktivieren Sie das Kontrollkästchen *Enable Slave Function* im Dialogfeld **CS/CJ-series DeviceNet Unit Properties**.

Gehen Sie wie folgt vor, um die Einstellungen für die Slave-Funktion vorzunehmen.

1. Klicken Sie auf die Registerkarte **Slave Function**.
2. Nun wird das folgende Fenster angezeigt.



3. Wählen Sie eine Verbindung aus.

   Die Standardeinstellung ist *Auto Connection*. Zum Einrichten einer Verbindung aktivieren Sie das Optionsfeld *User Setup*.
4. Legen Sie die Bereiche für die dezentrale E/A-Kommunikation fest.

   Legen Sie die Bereiche, die Startworte und die zugeordnete Größe für Eingabe (Slave zu Master) und Ausgabe (Master zu Slave) fest.

   Ist das Optionsfeld *User Setup* aktiviert, müssen alle zu verwendenden Verbindungen eingerichtet werden.

   Sie können maximal zwei Verbindungen einrichten.

WICHTIG:
- COS und Cyclic können nicht gleichzeitig eingestellt werden.
- Werden gleichzeitig eine Poll-Verbindung und eine COS-Verbindung oder eine Poll-Verbindung und eine zyklische Verbindung verwendet, müssen die Ausgabeeinstellungen für beide Verbindungen übereinstimmen.

C EDS-Datei-Verwaltung

Dieser Abschnitt beschreibt die Verwaltung der vom Netzwerkkonfigurator verwendeten EDS-Dateien.

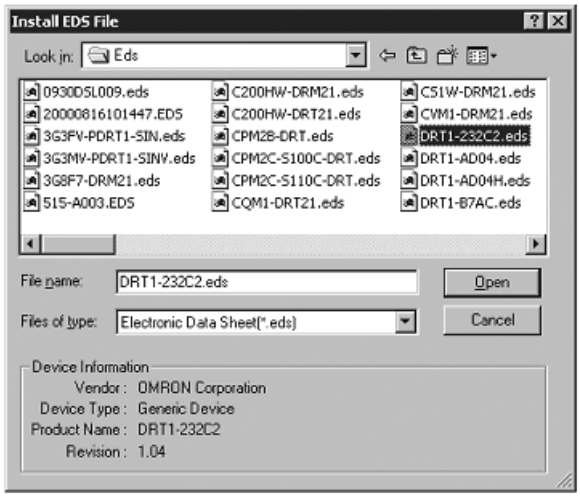
C-1 Installieren von EDS-Dateien

EDS File Install

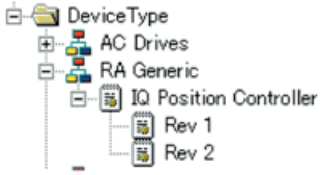
Die Installation einer EDS-Datei ermöglicht dem Netzwerkkonfigurator die Unterstützung eines neuen Gerätetyps.

Zur Installation einer EDS-Datei gehen Sie wie folgt vor:

1. Wählen Sie den Menübefehl ***EDS File - Install***.
   Nun wird das folgende Dialogfeld angezeigt:



2. Wählen Sie die zu installierende EDS-Datei aus. Im unteren Bereich des Dialogfelds werden Informationen zum Gerät angezeigt.
3. Klicken Sie auf **Open**.
   Das durch die Datei beschriebene Gerät wird der Hardwareliste als neue Hardware hinzugefügt.
   Sollte bereits ein identisches Gerät mit gleicher Hardwareversion existieren, wird dieses auf die neueste Version aktualisiert.
   Bei unterschiedlicher Hardwareversion wird das Gerät wie im Folgenden dargestellt der Hardwareliste hinzugefügt.

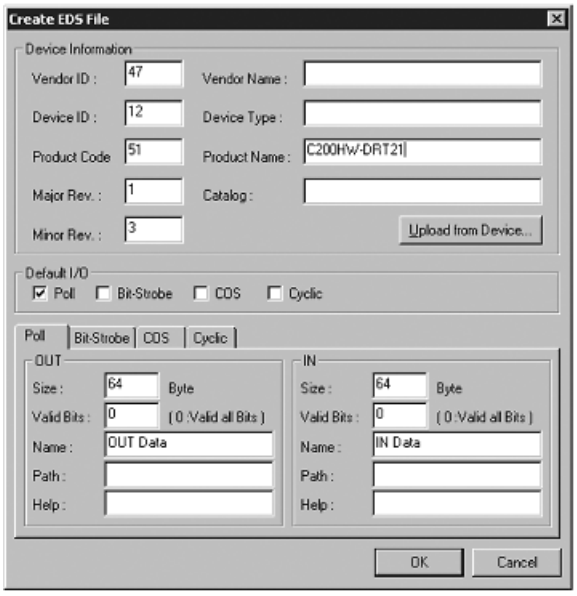


C-2 Erstellen von EDS-Dateien

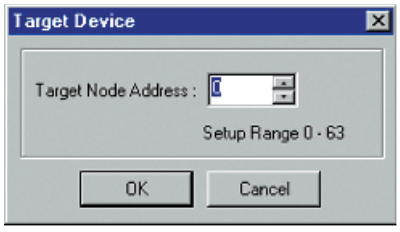
EDS File Create

Für das Erstellen einer Netzwerkkonfiguration mithilfe des Netzwerkkonfigurators sind entsprechende EDS-Dateien absolut unverzichtbar. Zum Erstellen einer EDS-Datei gehen Sie wie folgt vor:

1. Wählen Sie den Menübefehl ***EDS File - Create***.
   Nun wird das folgende Dialogfeld angezeigt:



2. Geben Sie die Geräte- und die E/A-Informationen ein.
   Ist der Netzwerkkonfigurator mit dem Netzwerk verbunden, können die Geräteinformationen aus einem Gerät im Netzwerk abgerufen werden.
3. Klicken Sie dazu auf **Upload from Device**. Nun wird das folgende Dialogfeld angezeigt:



4. Geben Sie die Knotenadresse für das gewünschte Gerät ein, und klicken Sie auf **OK**.
   Legen Sie eine von diesem Gerät unterstützte E/A-Verbindung und E/A-Größe fest. Konsultieren Sie hierzu das Bedienerhandbuch des Geräts.
5. Klicken Sie auf **OK**.
   Das durch die Datei beschriebene Gerät wird wie bei der Installation einer EDS-Datei der Hardwareliste als neue Hardware hinzugefügt.

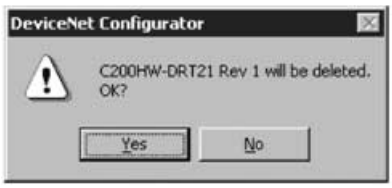
Hinweis: Mithilfe der Netzwerkkonfigurator-Funktion für das Erstellen von EDS-Dateien können keine Geräteparametereinstellungen erstellt werden. Zum Einstellen von Geräteparametern müssen Sie die EDS-Datei vom Gerätehersteller abrufen.

C-3 Löschen von EDS-Dateien

EDS File - Delete

Zum Löschen einer EDS-Datei gehen Sie wie folgt vor:

1. Wählen Sie das Gerät in der Hardwareliste aus.
2. Wählen Sie den Menübefehl ***EDS File - Delete***.
   Nun wird eine Bestätigungsmeldung angezeigt (siehe nachstehende Abbildung).



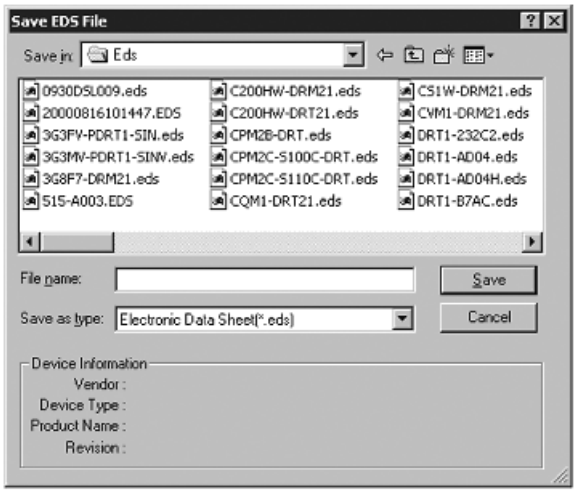
3. Klicken Sie auf **Yes**.
   Die EDS-Datei und das durch diese repräsentierte Gerät werden aus der Hardwareliste gelöscht.

C-4 Speichern von EDS-Dateien

EDS File Save

Zum Speichern einer EDS-Datei gehen Sie wie folgt vor:

1. Wählen Sie das Gerät in der Hardwareliste aus.
2. Wählen Sie den Menübefehl ***EDS File - Save***.
   Nun wird ein Dialogfeld angezeigt, in dem Sie den Ordner und den Dateinamen für die Speicherung der EDS-Datei auswählen bzw. eingeben können (siehe nachstehende Abbildung).



3. Legen Sie den Ordner und den Dateinamen fest, und klicken Sie auf **Save**.
   Die EDS-Datei wird nun unter dem angegebenen Namen gespeichert.

C-5 Suchen nach EDS-Dateien

EDS File - Find

Gehen Sie wie folgt vor, um in der Hardwareliste nach einem Gerät (d. h. einer EDS-Datei) zu suchen.

1. Wählen Sie den Menübefehl ***EDS File - Find***.
   Nun wird das folgende Fenster angezeigt:

2. Geben Sie die Zeichenfolge ein, nach der gesucht werden soll, und klicken Sie auf **Find Next**.
3. Verlief die Suche erfolgreich, wurde also ein entsprechendes Gerät in der Hardwareliste gefunden, springt der Cursor auf dieses Gerät.
4. Zum Beenden der Suche klicken Sie auf **Cancel**.

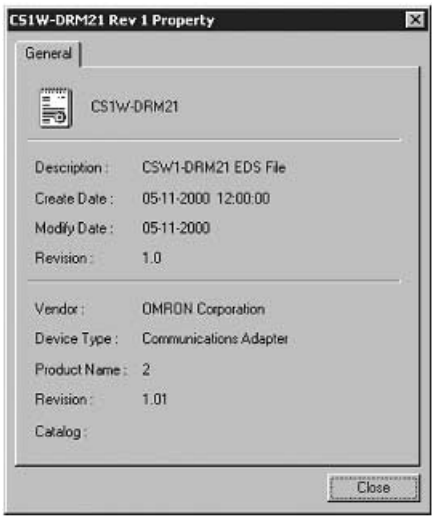
Hinweis:
- Die Suche ist auf die Geräte unterhalb der aktuellen Cursorposition in der Hardwareliste beschränkt.
- Zum Durchsuchen der gesamten Hardwareliste wählen Sie dort den Eintrag ***DeviceNet Hardware*** und führen dann die Suche durch.

C-6 Eigenschaften von EDS-Dateien

EDS File Property

Zum Anzeigen der Eigenschaften einer EDS-Datei gehen Sie wie folgt vor:

1. Wählen Sie das entsprechende Gerät in der Hardwareliste aus.
2. Wählen Sie den Menübefehl ***EDS File Property***.
   Nun wird das folgende Fenster angezeigt:



Dieses gibt u. a. Aufschluss über das Gerät sowie über Datum und Uhrzeit der Erstellung der Datei.

D Verwendung von Universal-Tools zum Einstellen von Geräten

Dieser Abschnitt erläutert das Setzen von Parametern, die nicht in die EDS-Datei geschrieben werden, sowie das Setzen von Knotenadressen und Baudraten über das Netzwerk.

D-1 Setzen von Geräteparametern durch Festlegen von Klasse und Instanz

Tool General Parameter

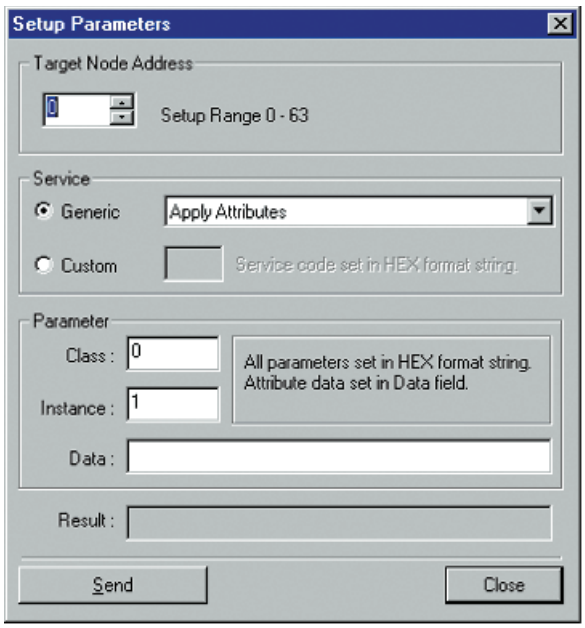
Um das Einstellen von Geräteparametern zu ermöglichen, die nicht in die EDS-Datei geschrieben werden, müssen zunächst die folgenden Codes eingestellt werden.

- Servicecode
- Klasse (Objektklasse), Instanz (Klasseninstanz), Attribut (Instanzenattribut)

Um andere Parameter als diese Codes einzustellen, müssen die Informationen zu den für das Setzen der Attribute erforderlichen Daten vom Gerätehersteller abgerufen werden. Fehlen diese Informationen ganz oder teilweise, können die Parameter nicht eingestellt werden.

Zum Einstellen der Geräteparameter gehen Sie wie folgt vor:

1. Verbinden Sie den Netzwerkkonfigurator mit dem Netzwerk.
2. Wählen Sie den Menübefehl ***Tool - General Parameter*** aus.
   Nun wird das folgende Dialogfeld angezeigt:

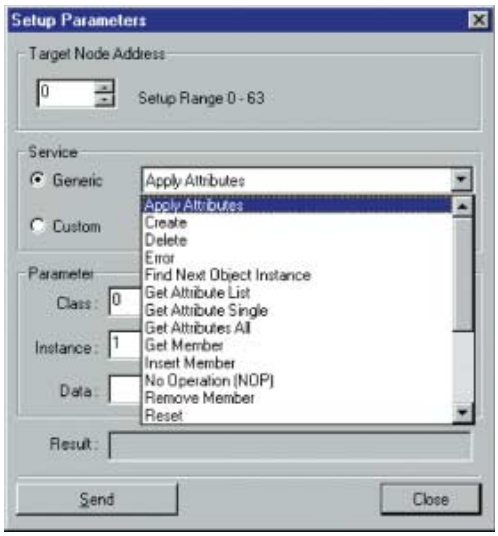
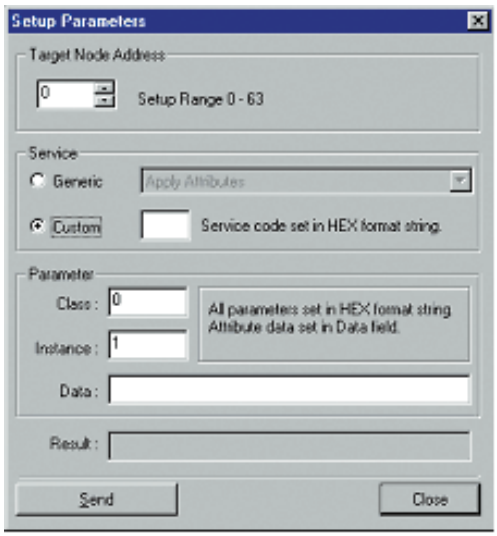


3. Geben Sie im Feld *Target Node Address* die Knotenadresse für das Gerät ein, dessen Parameter eingestellt werden sollen.

4. Legen Sie den Servicecode für das Gerät fest.

   Sie können den Servicecode aus den im DeviceNet definierten gebräuchlichen Servicecodes auswählen oder diesen direkt angeben. Zur Festlegung eines im DeviceNet definierten gebräuchlichen Servicecodes wählen Sie diesen aus dem Listenfeld aus.

   Zur direkten Eingabe eines Servicecodes aktivieren Sie das Optionsfeld *Custom Service* im Bereich *Service* und geben den Servicecode direkt als Hexadezimalzahl ein.

Auswahl eines im DeviceNet definierten gebräuchlichen Servicecodes	**Direkte Angabe des Servicecodes**
	

5. Legen Sie die Klasse und die Instanz der Parameter fest, deren Einstellungen gelesen oder geschrieben werden sollen.
6. Geben Sie basierend auf dem angegebenen Servicecode die benötigten Daten ein.
7. Klicken Sie nach Eingabe aller Daten auf **Send**. Die Antwort des Geräts wird im Feld *Result* angezeigt.
8. Klicken Sie auf **Close**, um das Dialogfeld *Setup Parameters* für die Einstellung der Geräteparameter zu schließen.

   Das Dialogfeld *Setup Parameters* für die Einstellung der Geräteparameter wird nun geschlossen.

Beispiel 1: Lesen von Parametern

1. Aktivieren Sie im Bereich *Service* das Optionsfeld *Generic*, und wählen Sie den Eintrag *Get Attribute Single* aus dem Listenfeld aus.
2. Geben Sie die Klasse und die Instanz des zu lesenden Parameters ein.
3. Geben Sie im Feld *Data* das Attribut des zu lesenden Parameters ein.
4. Klicken Sie auf **Send**. Der ausgelesene Wert wird im Feld *Result* angezeigt.

Beispiel 2: Setzen von Parametern

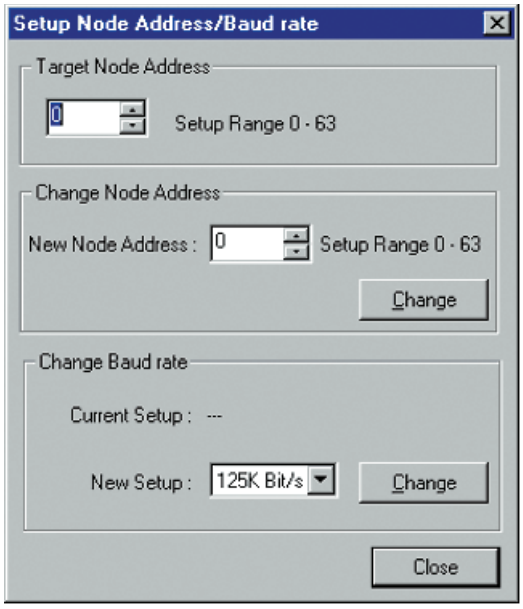
1. Aktivieren Sie im Bereich *Service* das Optionsfeld *Generic*, und wählen Sie den Eintrag *Set Attribute Single* aus dem Listenfeld aus.
2. Geben Sie die Klasse und die Instanz des zu setzenden Parameters ein.
3. Geben Sie im Feld *Data* das Attribut des zu setzenden Parameters ein.
4. Geben Sie im Feld *Data* hinter dem Attribut des zu setzenden Parameters den gewünschten Wert ein.
5. Klicken Sie auf **Send**.

D-2 Einstellen von Knotenadressen und Baudraten über das Netzwerk

Tool - Node Address/Baud Rate Setting

Zum Einstellen der Knotenadresse und Baudrate eines Geräts über das Netzwerk gehen Sie wie folgt vor:

1. Deaktivieren Sie im DeviceNet-Netzwerk alle Geräte außer dem fraglichen Gerät und dem Netzwerkkonfigurator. Bestimmen Sie anhand des Gerätehandbuchs die Knotenadresse des Geräts und die standardmäßig eingestellte Baudrate. Stellen Sie den Netzwerkkonfigurator auf dieselbe Baudrate ein.
2. Verbinden Sie den Netzwerkkonfigurator mit dem Netzwerk.
3. Wählen Sie den Menübefehl ***Tool - Node Address/Baud Rate Setting***.
   Nun wird das folgende Dialogfeld angezeigt:



4. Geben Sie im Feld *Target Node Address* die aktuelle Knotenadresse des fraglichen Geräts ein.
5. Zum Ändern der Knotenadresse geben Sie im Feld *New Node Address* eine neue Knotenadresse ein, und klicken Sie auf **Change**.
   Im fraglichen Gerät ist nun die neue Knotenadresse eingestellt.
6. Zum Ändern der Baudrate wählen Sie im Feld *New Baud Rate* die neue Baudrate aus, und klicken Sie auf **Change**.
   Im fraglichen Gerät ist nun die neue Baudrate eingestellt.

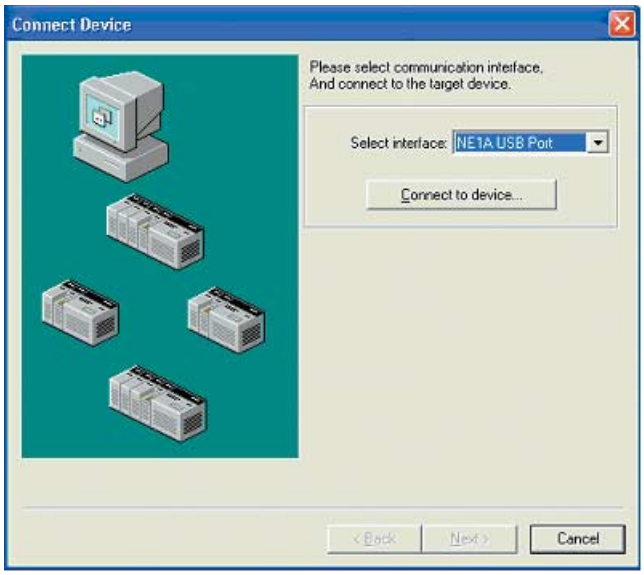
Hinweis: Auf diese Weise können über das Netzwerk nur die Knotenadresse und Baudrate von Geräten geändert werden, die diese Funktion unterstützen.

E Verwendung des Password Recovery Tools

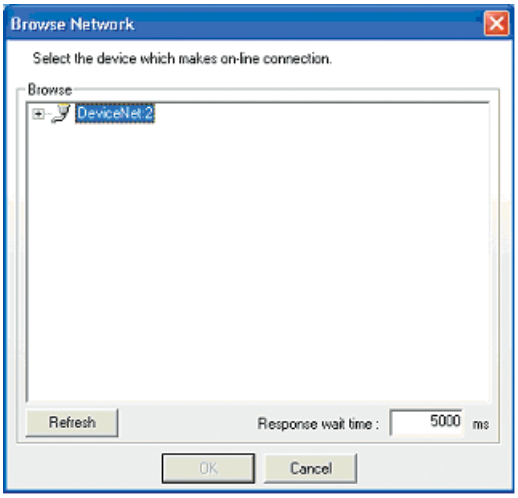
Wenn Sie das für ein Gerät eingestellte Kennwort vergessen haben, können Sie das Kennwort mithilfe des Password Recovery Tool zurücksetzen, so dass das Gerät wieder in einem kennwortlosen Zustand (Standardeinstellung) ist.

Gehen Sie wie folgt vor, um das Geräte-Kennwort zurückzusetzen:

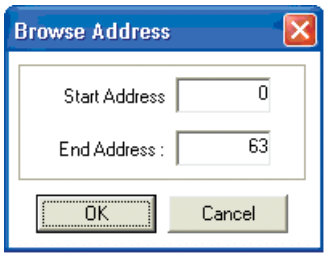
1. Bereiten Sie den Computer für eine Verbindung mit dem DeviceNet über eine USB-Schnittstelle oder eine DeviceNet-Schnittstellenkarte vor.
2. Wählen Sie im Windows-Startmenü ***Programme - OMRON Network Configurator for DeviceNet Safety - Password Recovery Tool*** (Verwendung der Standardnamen für die Programmordner vorausgesetzt). Nun startet das Password Recovery Tool und das folgende Fenster wird angezeigt:



3. Wählen Sie die Schnittstelle für die Verbindung zu dem Netzwerk aus, und klicken Sie auf **Connect to Device**. Klicken Sie auf **Refresh**, wenn das Fenster für die Suche nach dem Zielgerät angezeigt wird.

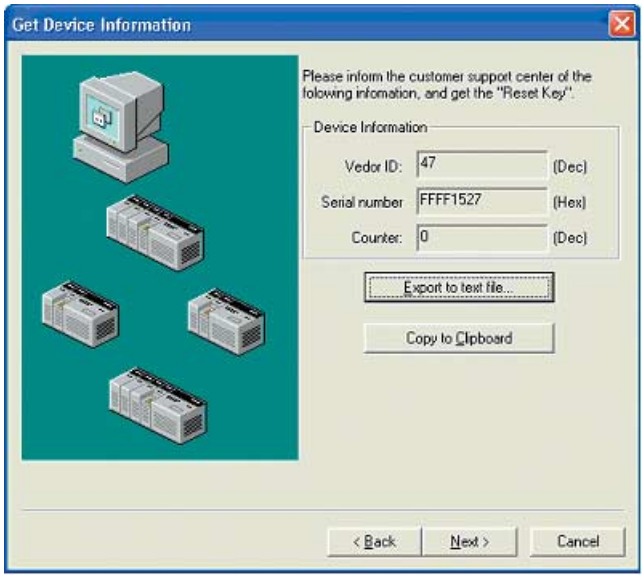


4. Legen Sie den zu durchsuchenden Knotenadressen-Bereich fest, und klicken Sie auf **OK**.

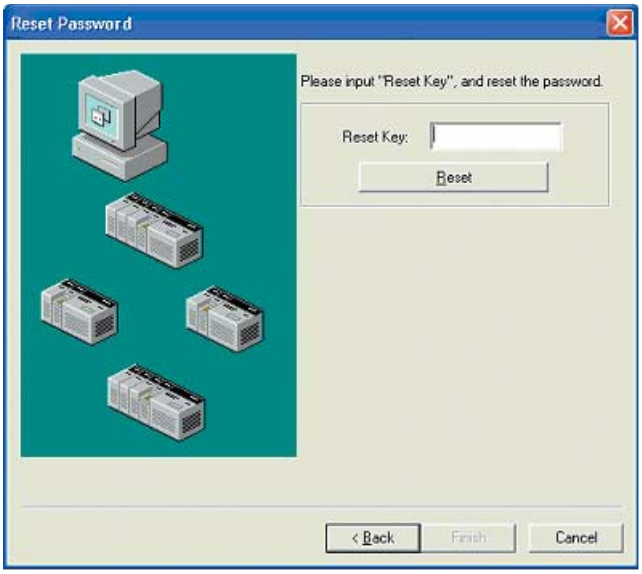


5. Nun werden die im Netzwerk gefundenen Geräte angezeigt. Wählen Sie das Gerät aus, dessen Kennwort Sie zurücksetzen möchten, und klicken Sie auf **OK**.

6. Nun werden die für das Zurücksetzen des Kennworts erforderlichen Informationen angezeigt. Diese Informationen werden von OMRON abgefragt, wenn Sie einen Rücksetzschlüssel für das Gerät anfordern. Drucken Sie die Informationen, indem Sie sie in eine Textdatei ausgeben oder über die Zwischenablage in eine andere Anwendung kopieren.



7. Klicken Sie auf **Next**, um das Dialogfeld **Reset Password** für die Eingabe des Rücksetzschlüssels anzuzeigen. Geben Sie den von OMRON übermittelten Rücksetzschlüssel ein, und klicken Sie auf **Reset**.



8. Nach dem erfolgreichen Zurücksetzen des Kennworts wird das folgende Meldungsfeld angezeigt. Das Gerät befindet sich nun wieder in einem kennwortlosen Zustand (Standardeinstellung). Klicken Sie auf **OK**, um das Meldungsfeld zu schließen. Klicken Sie im Hauptfenster des Password Recovery Tools auf **Finish**, um dieses zu verlassen.

Begriff	Definition
BusOff (Bus aus)	Status, der beim Auftreten einer extrem hohen Kommunikationsfehlerrate eintreten kann. Wenn der interne Fehlerzähler einen bestimmten Grenzwert überschreitet, wird das Vorliegen eines Fehlers erkannt. (Der interne Fehlerzähler wird beim Starten oder Neustarten des Masters gelöscht.)
DeviceNet Safety	Ein Sicherheits-Netzwerk, dass das DeviceNet um ein Sicherheits-Protokoll in Übereinstimmung mit SIL3 gemäß IEC61508 bis Steuerungskategorie 4 entsprechend EN954-1 erweitert.
Diskrepanzzeit	Der zeitliche Abstand zwischen der Änderung des Zustands eines von zwei Eingängen bis zur Änderung des Zustands des anderen Eingangs.
Einkanalmodus	Verwendung jeweils nur eines Eingangs bzw. Ausgangs als Eingang bzw. Ausgang.
EPI	Das Intervall der Sicherheits-Datenkommunikation zwischen dem Sicherheits-Master und dem Sicherheits-Slave.
E/A-Konfiguration	In einem Gerät zu einer Gruppe zusammengefasste Daten, auf die von außerhalb des Geräts zugegriffen werden kann.
Fehlerhaltezeit	Die Zeitdauer, für die ein Fehlerzustand (Steuerungs- und Statusdaten, LED-Anzeigen) gehalten wird.
Konfiguration	Die Einstellungen für ein Gerät und ein Netzwerk.
Multicast-Verbindung	Sicherheits-E/A-Kommunikation in einer 1:n-Konfiguration (n = 1 bis 15).
Open Type (Parameter für die Vorgehensweise beim Herstellen der Verbindung)	Die Vorgehensweise beim Herstellen einer Sicherheitsverbindung. Der entsprechende Parameter in den Einstellungen des Sicherheits-Masters bietet drei mögliche Optionen.
Sicherheits-Controller (Sicherheits-SPS)	Eine für die Sicherheits-Steuerung eingesetzte Steuerung hoher Zuverlässigkeit.
Sicherheitsdaten	Daten hoher Zuverlässigkeit.
Sicherheitskette	Die logische Kette für die Aktualisierung einer Sicherheitsfunktion: Eingangsgerät (Sensor), Steuerungsgerät (einschließlich eines dezentralen E/A-Geräts) und Ausgangsgerät (Betätiger).
Sicherheits-Protokoll	Die für die Einrichtung einer äußerst zuverlässigen Kommunikation hinzugefügte Kommunikationshierarchie.
Sicherheitssignatur	Ein vom Netzwerkkonfigurator an ein Gerät ausgegebenes Zertifikat der Konfigurationsdaten. Das Gerät verifiziert unter Verwendung der Sicherheitssignatur die Korrektheit der Konfigurationsdaten.
Singlecast-Verbindung	Sicherheits-E/A-Kommunikation in einer 1:1-Konfiguration.
Standard	Ein Gerät oder eine Gerätefunktion, bei dem/der keine Sicherheitsmaßnahmen zum Tragen kommen.
Testimpuls	Ein Signal, mit dem festgestellt wird, ob die externe Verdrahtung in Kontakt mit der Versorgungsspannung (+) steht oder ob Kurzschlüsse zwischen Signalleitungen bestehen
TUNID	Die UNID des lokalen Knotens. Üblicherweise wird die TUNID mithilfe des Netzwerkkonfigurators festgelegt.
UNID	Ein Bezeichner, der ein Gerät in allen Netzwerk-Domänen eindeutig identifiziert. Dieser Bezeichner wird aus einer Kombination der Netzwerkadresse und der Knotenadresse gebildet.
Verbindung	Logischer Kommunikationspfad für die Kommunikation zwischen Geräten.
Zweikanal-Äquivalenzmodus	Variante des Zweikanalmodus, bei dem die logischen Zustände der beiden Eingänge bzw. Ausgänge äquivalent sind.
Zweikanalmodus	Verwendung von zwei Eingängen bzw. Ausgängen als redundante Eingänge bzw. Ausgänge
Zweikanal-Komplementärmodus	Variante des Zweikanalmodus, bei dem die logischen Zustände der beiden Eingänge bzw. Ausgänge komplementär sind.

Index

Versionshistorie

Die letzte Zahl der Dokumentennummer in der unteren linken Ecke der Vorder- und Rückseite dieser Anleitung gibt den Überarbeitungsstand an.

Die folgende Tabelle führt die mit den einzelnen Überarbeitungen vorgenommenen Änderungen auf. Die Nummerierung der Seiten bezieht sich auf die vorherige Version.

Versionscode	Datum	Überarbeitung
1	Mai 2005	Ursprungsversion