BALLUFF

BNI CIP-351-000-K015

EtherNet/IP

CIP Safety

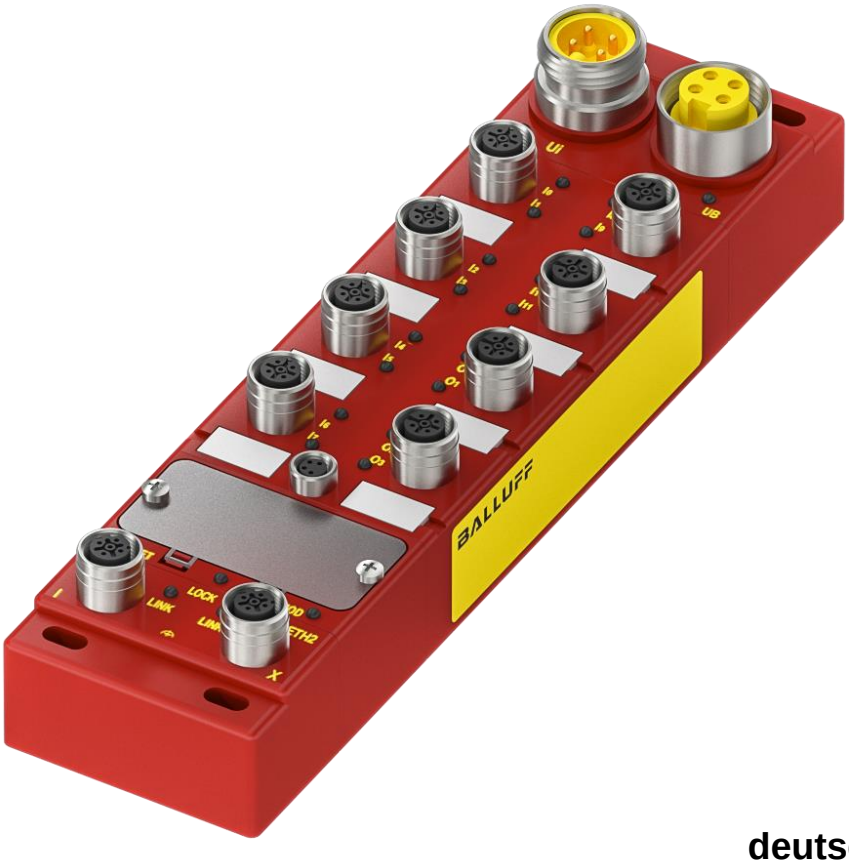
deutsch Betriebsanleitung

english User's Guide

www.balluff.com

EtherNet/IP™ CIP Safety™
Sicheres E/A-Modul
BNI CIP-351-000-K015 (BNI00HN)

Betriebsanleitung



EtherNet/IP™

CIP Safety™

deutsch

www.balluff.com

Originalbetriebsanleitung

Alle Rechte vorbehalten. Im Rahmen der in den Vereinigten Staaten und international gesetzlich zulässigen Grenzen geschützt. Kopien oder Änderungen dieses Dokuments ohne eine vorherige schriftliche Genehmigung durch Balluff sind unzulässig.

Alle hier genannten Produktmarken und -namen dienen ausschließlich zur Identifizierung. Hierbei kann es sich um von den jeweiligen Inhabern registrierte Marken handeln.
Balluff haftet nicht für eventuelle technische oder Druckfehler, das Entfernen hier enthaltenen Texts oder ungewollte bzw. durch den Gebrauch des Materials entstehende Beschädigungen.

1. Über diese Anleitung 6
1.1. Über diese Anleitung 6

2. Allgemeine Sicherheitsanweisungen 10
2.1. Bestimmungsgemäße Verwendung 10
2.2. Verantwortung des Benutzers 10
2.3. Dokumentation 11
2.4. Wartung 12
2.5. Ersatzteile 12
2.6. Versand 12
2.7. Entsorgung 12
2.8. Qualifikationen des Personals 12
2.9. Persönliche Schutzausrüstung 13
2.10. Besondere Gefahren 14
2.11. Beschilderung 15

3. Zu diesem Produkt 16
3.1. Produktbeschreibung 16
3.2. Bestellinformationen 16
3.3. Anwendung 17
3.4. Funktionale Sicherheit - sicherheitsrelevante Parameter 18
3.5. Umgebungs- und Sicherheitsanweisungen des Produkts 19
3.6. Produktmerkmale 21
3.7. Ethernet-Topologien 22

4. Funktionen für die funktionale Sicherheit 23
4.1. Sicherheitszustände 23
4.2. Sicherheitseingänge 24
4.3. Sicherheitsausgänge (BNI CIP-351-000-K015) 29
4.4. E/A-Status 32
4.5. Verhalten bei einem Fehler 33
4.6. Reaktionszeit 35

5. Produkteigenschaften 36
5.1. Hardware-Eigenschaften 36
5.2. Mechanische Eigenschaften 42
5.3. Physische E/A-Anordnung 43
5.4. Sichere E/A-Baugruppen 44
5.5. Sichere E/A-Verbindungen 45
5.6. Zuordnung von sicheren E/A-Daten 47
5.7. Pinbelegung 55
5.8. LED-Zuweisung 56

6. Installation und Beschaltung des Produkts 60
6.1. Spannungsversorgung 60
6.2. Ethernet-Verbindung 61
6.5. Modul-Erdung 64
6.6. E/A-Beschaltung 65

7. Produktbereitstellung 71
7.1. Erste Schritte 71
7.2. IP-Adresseinstellung 71
7.3. EDS-Dateien 79
7.4. Import des Sicheren E/A-Modul – EDS-Datei in Rockwell Bibliothek 81
7.5. Konfigurieren des Sicheren E/A-Moduls - Rockwell RSLogix 5000 90
7.6. Sichere E/A-Baugruppen 93
7.7. Konfigurieren des Sicheren E/A-Moduls in Balluff SNCT 96
7.8. Verbinden und Testen des Sicheren E/A-Moduls in RSLogix 5000 115

8. EtherNet/IP-Verhalten 119
8.1. E/A-Verhalten 119
8.2. IDLE-Verhalten 119
8.3. Doppelte IP-Adresse 119
8.4. EtherNet/IP-Objektklassen 120

9. Produktaustausch 128
9.1. Vor dem Start 128
9.2. Austauschvorgang 129
9.3. Verifizierung 131

10. SNCT-Konfigurationssoftware 132
10.1. Übersicht 132
10.2. Sicherheitsrücksetzung 134
10.3. Konfiguration sperren/entsperren 141
10.4. Speichern der IP-Adresse mit einem DHCP-Server 147
10.5. IP-Adresskonflikt 148
10.6. Diagnose des Ethernet-Ports 149
10.7. Modulinformationen 150
10.8. Kennwort festlegen/zurücksetzen 152
10.9. Zusätzliche Informationen 156
10.10. Firmware herunterladen 158
10.11. Modulkonfiguration drucken 162
10.12. Protokoll (Notfallmodus) 165

11. Produktumfang 166
11.1. Produktumfang 166
11.2. USB-Stick 166
11.3. Speicherschlüssel 167

12. Web-Server-Schnittstelle 168

12.1. Verbinden des Web-Servers 168
12.2. Allgemeine Informationen 169
12.3. Diagnoseinformationen 170

13. Produktsupport 172

14.1. Garantiebedingungen 172
14.2. Produktinformationen 172
14.3. Technischer Support 173

1. Über diese Anleitung

In dieser Betriebsanleitung wird das IP67-zertifizierte, digitale CIP Safety E/A-Modul BNI CIP-351-000-K015 (BNI00HN) von Balluff beschrieben.

1.1. Über diese Anleitung

Allgemeine Sicherheitsanweisungen
Dieses Kapitel enthält einen Überblick über alle wichtigen Sicherheitsaspekte für den optimalen Schutz des Personals sowie für den sicheren und fehlerfreien Betrieb.

Produktübersicht
Dieses Kapitel enthält einen Überblick über die Verwendung des Produkts und seine Haupteigenschaften.

Sicherheitsfunktionen
In diesem Kapitel werden die Eigenschaften der Sicherheitseingänge und der Sicherheitsausgänge des Moduls beschrieben.

Produkteigenschaften
Dieses Kapitel enthält einen Überblick über die Eigenschaften und die technischen Daten des Sicheren E/A-Moduls.

Installation und Beschaltung des Produkts
In diesem Kapitel werden die Beschaltungsmöglichkeiten und die entsprechenden Sicherheitskategorien beschrieben.

Produktbereitstellung
In diesem Kapitel wird anhand eines Beispiels die Vorgehensweise bei der Inbetriebnahme des Sicheren E/A-Moduls mit der RSLogix™ 5000-Software von Rockwell Automation beschrieben.

Produktverhalten
In diesem Kapitel wird das Verhalten des Sicheren E/A-Moduls im Hinblick auf die EtherNet/IP-Kommunikation beschrieben.

Produktaustausch
In diesem Kapitel wird die Strategie bei einem Austausch eines bereits in Betrieb genommenen Sicheren E/A-Moduls beschrieben.

SNCT-Konfigurationssoftware
In diesem Kapitel werden die wichtigen Funktionen der SNCT-Software beschrieben, die für die Inbetriebnahme des Sicheren E/A-Moduls verwendet wird.

Produktumfang
In diesem Kapitel wird der Umfang des Produktpakets beschrieben.

Web-Server-Schnittstelle
In diesem Kapitel werden die Informationen des Sicheren E/A-Moduls beschrieben, die nach der Verbindung des Web-Servers des Moduls verfügbar sind.

Produktsupport

In diesem Kapitel wird beschrieben, wie das Produkt identifiziert und der technische Support kontaktiert wird.

Zielgruppe

Die Anleitung richtet sich an Benutzer mit Hintergrundwissen im Bereich Automatisierung und Netzwerktechnologie, einschließlich Sicherheitsanwendungen, EtherNet/IP™ und CIP Safety™.

Gliederung der Anleitung

Die Anleitung ist in Kapitel unterteilt. Jedes Kapitel enthält eine in sich geschlossene Beschreibung eines bestimmten Themas.

Verfügbarkeit

Die Anleitung ist in elektronischer Form als PDF-Datei (Adobe Acrobat Reader) in englischer Sprache verfügbar. Es muss gewährleistet werden, dass das Produkt von einer Person implementiert wird, die angemessene Kenntnisse der englischen Sprache besitzt.

Symbole und Überschriften

Wichtige Textpassagen werden mit den folgenden Symbolen und Überschriften gekennzeichnet:

Gefahr!

Unmittelbare Gefahr für Leib und Leben von Personal und anderen Personen. Nichtbeachtung führt zum Tod oder zu schweren Verletzungen.

Warnung!

Gefahrensituation für Leib und Leben von Personal und anderen Personen. Nichtbeachtung kann zum Tod oder zu schweren Verletzungen führen.

Achtung!

Weist auf eine potenziell gefährliche Situation hin. Nichtbeachtung kann zu Schäden am Produkt oder an Gegenständen im Umfeld des Produkts führen.

Hinweis!

Ergänzende Informationen und nützliche Tipps.

Haftungsbeschränkung

Alle Daten und Angaben in diesen Anleitungen wurden unter Beachtung der gesetzlichen Standards und Bestimmungen, des aktuellen Stands der Technologie und unseres jahrelangen Wissens- und Erfahrungsschatzes zusammengestellt.

Der Hersteller übernimmt keine Haftung für Schäden, die durch Folgendes verursacht werden:

- Nichtbeachtung der Anleitung
- Nicht bestimmungsgemäße Verwendung
- Einsatz von ungeschultem Personal

Der tatsächliche Lieferumfang kann bei Sonderausführungen, der Inanspruchnahme zusätzlicher Bestelloptionen oder aufgrund neuester technischer Änderungen von den hier beschriebenen Erläuterungen und Darstellungen abweichen.

Der Benutzer trägt die Verantwortung für die Durchführung von Service und die Inbetriebnahme gemäß den Sicherheitsvorschriften der geltenden Normen und allen anderen relevanten staatlichen oder örtlichen Vorschriften betreffend Leiterdimensionierung und Schutz, Erdung, Überstromschutz usw.

Die Person, die die Montage oder Installation ausgeführt hat, haftet für Schäden, die bei der Montage oder beim Anschluss entstehen.

Wir haben den Inhalt dieser Anleitung auf Übereinstimmung mit der beschriebenen Hardware und Software geprüft. Da sich Abweichungen nicht vollständig ausschließen lassen, können wir die vollständige Korrektheit nicht garantieren. Die Angaben in dieser Anleitung werden jedoch regelmäßig überprüft. Notwendige Korrekturen sind in den nachfolgenden Ausgaben enthalten.

Verbesserungsvorschläge sind jederzeit willkommen.

Der Hersteller haftet nicht für Schäden, die durch ein Fehlen oder eine Nichtbeachtung der Betriebsanleitung entstehen. Daher wird dem Betreiber empfohlen, schriftliche Anweisungen von entsprechend qualifizierten Personen anzufordern.

Modifikationen oder funktionelle Änderungen am Produkt sind aus Sicherheitsgründen nicht zulässig. Alle Modifikationen am Produkt, die nicht ausdrücklich vom Hersteller genehmigt wurden, führen zum Verlust jeglicher Haftungsansprüche gegen den Hersteller. Gleiches gilt, wenn nicht zugelassene Teile oder Ausrüstungen verwendet werden.

Copyright

Diese Anleitung muss vertraulich behandelt werden. Sie wird ausschließlich für das Personal bereitgestellt, das dieses Produkt verwendet . Die Weitergabe dieses Dokuments an Dritte ohne schriftliche Genehmigung des Herstellers ist verboten.

Hinweis!

Die Inhalte, Texte, Zeichnungen, Bilder und andere Abbildungen sind urheberrechtlich geschützt und unterliegen anderen Schutzrechten. Die rechtswidrige Verwendung dieser Publikation hat strafrechtliche Folgen.

Verwendung dieser Anleitung

Diese Betriebsanleitung enthält Informationen über die bestimmungsgemäße Verwendung des Sicherheitsmoduls BNI CIP-351-000-K015.

Die Kenntnis von Vorschriften und die technisch einwandfreie Umsetzung der in diesem Handbuch enthaltenen Sicherheitshinweise durch qualifiziertes Personal sind Voraussetzung für die gefahrlose Planung, Projektierung, Programmierung, Installation, Inbetriebnahme und für die Sicherheit bei Betrieb und Instandhaltung der Sicherheitsmodule BNI CIP-351-000-K015.

Bei nicht qualifizierten Eingriffen in die Geräte, bei Abschalten oder Umgehen von Sicherheitsfunktionen oder bei Nichtbeachtung der Anweisungen in dieser Anleitung können schwere Personen-, Sach- oder Umweltschäden eintreten, für die Balluff keine Haftung übernehmen kann.

Die Anleitung enthält Sicherheitsanweisungen, eine Beschreibung der Module und Informationen über den Lebenszyklus.

2. Allgemeine Sicherheitsanweisungen

Dieses Kapitel enthält einen Überblick über alle wichtigen Sicherheitsaspekte für den optimalen Schutz des Personals sowie für den sicheren und fehlerfreien Betrieb.

2.1. Bestimmungsgemäße Verwendung

Die Module wurden ausschließlich für die hier beschriebene bestimmungsgemäße Verwendung konzipiert und konstruiert. Die Module dürfen nur unter Berücksichtigung aller Referenzen und Informationen in dieser Anleitung verwendet werden.

Warnung!

Gefahr durch nicht bestimmungsgemäße Verwendung!

Jede Verwendung des Produkts, die von der bestimmungsgemäßen Verwendung abweicht, kann zu Gefahrensituationen führen.

Darum gilt:

Verwenden Sie das Produkt nur entsprechend seiner Bestimmung.

Verwenden Sie das Produkt nur zusammen mit den empfohlenen Komponenten.

Beachten Sie alle Angaben in dieser Anleitung.

Stellen Sie sicher, dass nur qualifiziertes Personal mit dem Produkt arbeitet.

Stellen Sie während der Konfiguration sicher, dass das Produkt innerhalb seiner Spezifikationen betrieben wird.

Stellen Sie sicher, dass die Spannungsversorgung den angegebenen Spezifikationen entspricht.

Verwenden Sie das Produkt nur in einem technisch angemessenen Zustand.

Verwenden Sie das Produkt nur in Kombination mit zugelassenen Komponenten.

Änderungen und Modifikationen am Produkt

Um Gefahren zu vermeiden und den optimalen Betrieb sicherzustellen, dürfen keine Änderungen oder Modifikationen am Produkt vorgenommen werden, die nicht ausdrücklich vom Hersteller genehmigt wurden.

2.2. Verantwortung des Benutzers

Das Produkt wird in der Fertigungsautomatisierungsumgebung eingesetzt. Der Benutzer des Produkts hat die gesetzliche Pflicht, das sichere Arbeiten zu gewährleisten.

Neben den Sicherheitsanweisungen in dieser Anleitung für die Nutzungsumgebung des Produkts müssen auch die relevanten Bestimmungen für die Unfallvermeidung und den Umweltschutz eingehalten werden.

- Der Benutzer muss die geltenden Arbeitsschutzbestimmungen kennen, um Gefahren zu beurteilen, die bedingt durch die speziellen Bedingungen für das Produkt an der Betriebsstätte entstehen. Diese müssen gemeinsam mit den Arbeitsanweisungen für den Betrieb des Produkts dokumentiert werden.
- Diese Arbeitsanweisungen müssen im direkten Umfeld des Produkts aufbewahrt werden und jederzeit für alle Personen zugänglich sein, die mit dem Produkt arbeiten.
- Halten Sie die Arbeitsanweisungen konsequent ein.
- Das Produkt darf nur in einem technisch einwandfreien und zuverlässigen Zustand betrieben werden.

2.3. Dokumentation

Alle Personen, die mit dem Produkt arbeiten, müssen die Betriebsanweisungen gelesen und verstanden haben, bevor sie die Arbeiten aufnehmen. Die Anleitung muss für alle Mitarbeiter zugänglich sein, die in einem der folgenden Bereiche tätig sind:

- Projektentwicklung
- Installation
- Inbetriebnahme
- Betrieb
- Außerbetriebnahme

Die folgenden Bedingungen müssen erfüllt sein, bevor die in dieser Anleitung beschriebenen Komponenten verwendet oder in Betrieb genommen werden

Warnung!

- Modifikationen am Prozesssteuerungssystem sollten nur durchgeführt werden, wenn das System von der Stromversorgung getrennt ist!
- Installation und Modifikationen sind nur durch ordnungsgemäß geschultes Personal zulässig.
- Die nationalen Richtlinien und Vorschriften des jeweiligen Landes müssen eingehalten werden (Installation, Sicherheit, EMV ...)

Gefahr!

Um Gefahren zu vermeiden und die optimale Performance sicherzustellen, dürfen keine Änderungen, Modifikationen oder Umbauten am Produkt vorgenommen werden, die nicht ausdrücklich vom Hersteller zugelassen wurden.

2.4. Wartung

Das entsprechende Sicherheitsmodul ist wartungsfrei.

2.5. Ersatzteile

Verwenden Sie bitte nur Original-Ersatzteile von Balluff.

Warnung!
Falsche oder defekte Ersatzteile können zu Schäden, Störungen oder einem Ausfall führen und die Sicherheitsfunktion beeinträchtigen.

2.6. Versand

Verwenden Sie für den Versand immer die Originalverpackung.

2.7. Entsorgung

Für die Entsorgung des Gerätes gelten nationale Richtlinien und Vorschriften. Informieren Sie sich bitte bei den lokalen Behörden über die vor Orte geltenden Entsorgungsverfahren.

2.8. Qualifikationen des Personals

Warnung!
Verletzungsgefahr durch ungenügende Qualifikation!
Eine Fehlbedienung kann zu schweren Verletzungen oder Sachschäden führen.

Qualifikation

Das Automatisierungssystem darf nur von geschulten, eingewiesenen und befugten Personen bedient werden. Aktivitäten wie Fehlerbehebung, Wartung, Reinigung und Austausch von Teilen dürfen nur von ausgebildetem oder geschultem Personal durchgeführt werden.

Qualifiziertes Personal
Diese Personen müssen die Betriebsanleitung kennen und entsprechend handeln. Inbetriebnahme und Training darf nur durch qualifizierte Fachkräfte erfolgen.

Bedienpersonal
Das sind Elektrotechniker und Elektriker des Kunden oder von externen Firmen, die vom Hersteller autorisiert sind, die vom Hersteller in den Abläufen für die Installation und Inbetriebnahme geschult wurden und die befugt sind, elektrische Schaltkreise und Geräte in Übereinstimmung mit den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen.

Qualifiziertes Personal wird gemäß den gültigen Standards der Sicherheitstechnik in die Betreuung und Verwendung von Sicherheitseinrichtungen geschult und eingewiesen.

2.9. Persönliche Schutzausrüstung

Während der Arbeit muss persönliche Schutzausrüstung getragen werden, um Gesundheitsrisiken zu minimieren.

- Tragen Sie immer die Schutzausrüstung, die für die jeweilige Aufgabe erforderlich ist.
- Beachten Sie zu Ihrer eigenen Sicherheit alle Schilder und Kennzeichnungen innerhalb Ihres Arbeitsbereichs.

Arbeitskleidung

ist eng anliegende Kleidung mit geringer Zugfestigkeit, engen Ärmeln und ohne hervorstehende Teile. In Abhängigkeit von der Anwendung muss verhindert werden, dass der Träger während der Arbeit ernsthafte Verletzungen erleidet oder Gesundheitsrisiken ausgesetzt wird.

Zur Vermeidung von Verletzungen darf kein Schmuck wie Ringe oder Halsketten getragen werden.

Schutzhelm

zum Schutz vor herunterfallenden oder umherfliegenden Gegenständen.

Sicherheitsschuhe

zum Schutz vor herunterfallenden schweren Gegenständen.

Schutzhandschuhe

zum Schutz der Hände vor Abschürfungen, Einstichen oder Verletzungen sowie vor dem Kontakt mit heißen Gegenständen.

Schutzbrille

zum Schutz der Augen vor umherfliegenden Teilen und Flüssigkeitsspritzern.

2.10. Besondere Gefahren

Im folgenden Abschnitt werden die Restrisiken identifiziert, die sich aus der Gefahrenanalyse ergeben.

Beachten Sie die hier angegebenen Sicherheitswarnungen und die Hinweise in der gesamten Anleitung, um Gesundheitsgefährdungen zu verringern und gefährliche Situationen zu vermeiden.

Elektrischer Strom

Gefahr!

Lebensgefahr durch elektrischen Strom!

Der Kontakt mit stromführenden Teilen führt zu einer unmittelbaren Lebensgefahr. Beschädigte Isolierungen oder Komponenten stellen eine Lebensgefahr dar.

Darum gilt:

Schalten Sie die Stromversorgung unverzüglich aus, wenn die Isolierung beschädigt ist. Arbeiten an der elektrischen Anlage dürfen nur von qualifizierten Fachkräften durchgeführt werden.

Während der Durchführung von Arbeiten muss die elektrische Anlage abgeschaltet und geschützt werden.

Risiko durch Restenergie

Gefahr!

Lebensgefahr durch elektrischen Strom!

Nachdem das Gerät von der Hauptspannungsversorgung getrennt wurde, sollten Teile wie die Stromanschlüsse erst dann berührt werden, wenn sich die Kondensatoren im Gerät entladen haben.

Darum gilt:

Beachten Sie die Entladezeiten der Kondensatoren; berühren Sie stromführende Teile erst nach einer Wartezeit von 1 Minute.

Wenn weitere verbundene Kondensatoren innerhalb der Gesamtverbindung vorhanden sind, kann die Entladung der Gesamtverbindung deutlich länger dauern. In diesem Fall müssen Sie die erforderliche Wartezeit bestimmen oder sogar anhand von Messungen ermitteln, ob das Gerät sicher ist.

Bewegliche Objekte

Warnung!

Verletzungsgefahr durch bewegliche Teile!

Kreisförmig oder geradlinig bewegliche Teile können schwere Verletzungen verursachen.

Darum gilt:

Berühren Sie keine beweglichen Teile im Betrieb. Öffnen Sie nicht die Abdeckung im Betrieb.

Die Höhe der mechanischen Restenergie richtet sich nach der Anwendung.

Angetriebene Komponenten drehen sich auch nach dem Abschalten der Stromversorgung entsprechend länger.

Brandschutz

Gefahr!

Lebensgefahr durch elektrischen Strom!

Es besteht die Gefahr eines Stromschlags, wenn ein leitfähiges Löschmittel verwendet wird.

Verwenden Sie daher das folgende Löschmittel:

- ABC-Pulver / CO2

Verhalten bei Gefahren und Unfällen

Vorbeugende Maßnahmen

- Rechnen Sie jederzeit mit Unfällen oder Bränden!
- Halten Sie Erste-Hilfe-Ausrüstung (Erste-Hilfe-Kasten, Decken usw.) und Feuerlöscher bereit.
- Weisen Sie das Personal in die Abläufe für die Unfallmeldung, die Erste Hilfe und das Rettungswesen ein.

In einem Notfall: korrektes Handeln

- Nehmen Sie das Gerät unverzüglich mit dem Not-Stopp außer Betrieb.
- Leiten Sie Erste-Hilfe-Maßnahmen ein.
- Bringen Sie Personen aus dem Gefahrenbereich.
- Informieren Sie die Verantwortlichen vor Ort.
- Rufen Sie medizinische Hilfe und / oder die Feuerwehr.
- Halten Sie die Zugangswege für Einsatzfahrzeuge frei.

2.11. Beschilderung

Warnung!

Verletzungsgefahr durch unleserliche Symbole

Im Laufe der Zeit können Aufkleber und Symbole an der Ausrüstung verschmutzen oder aus anderen Gründen unleserlich werden.

Darum gilt:

Halten Sie alle Sicherheitswarnungen und Bedienhinweise am Gerät immer in einem lesebaren Zustand.

3. Zu diesem Produkt

3.1. Produktbeschreibung

Das EtherNet/IP™ CIP Safety™-Modul ist eine zuverlässige Lösung für die Einbindung von sicheren Eingangsgeräten (Sicherheitsschalter, Not-Stopps, Lichtvorhänge, Laser-Scanner usw.) und die Ansteuerung von sicheren Ausgangsgeräten (Relais, Muting-Lampen, ausfallsichere Motorstarter usw.) in Kombination mit industriellen Sicherheitssteuerungen in rauen, anspruchsvollen Umgebungen. Das Sichere E/A-Modul ist in einem IP67-geschütztem Gehäuse untergebracht, kann an der Maschine montiert werden und ist für den Einsatz in Bereichen geeignet, in denen Flüssigkeiten, Staub oder Vibrationen vorhanden sind.

Das EtherNet/IP™ CIP Safety™-Modul wird vorrangig in Anwendungen für Automobilhersteller und Maschinenbauer eingesetzt, die ein direkt an der Maschine angebrachtes Sicheres E/A-Modul suchen, um den Platzbedarf im Schrank zu reduzieren. Dank des IP67-geschützten 60-mm-Gehäuses mit M12-Anschlüssen eignet sich das Sichere E/A-Modul ideal für zahlreiche Sicherheitsanwendungen, einschließlich Fördertechnik, automatisierte Montagemaschinen, Automobilanwendungen und in Roboter Zellen.

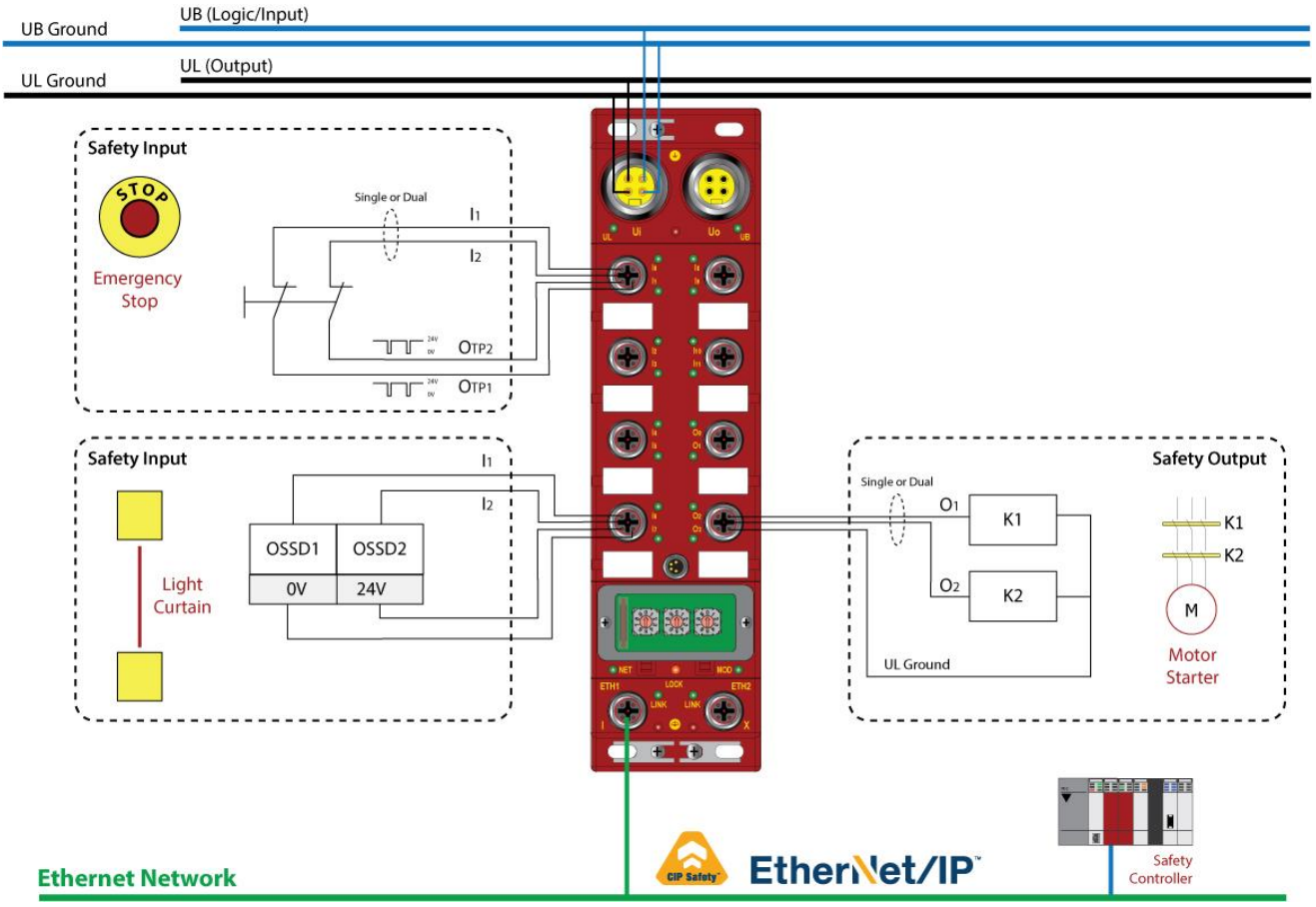
3.2. Bestellinformationen

Produktname	**Bestellcode**
BNI CIP-351-000-K015	BNI00HN

3.3. Anwendung

Die Kombination von EtherNet/IP- und CIP Safety-Protokollen ermöglicht den Austausch von E/A- und Diagnoseinformationen für den Sicherheitsprozess über ein einziges Ethernet-Netzwerk. Die Module müssen so konfiguriert werden, dass sie den Definitionen der Sicherheitsfunktion entsprechen, bis zu SIL 3 gemäß den Anforderungen in IEC 61508 oder CAT 4/ PLe gemäß den Anforderungen in ISO 13849-1 (in diesem Fall sollten die Ein- und Ausgänge für die Verwendung als Dual-Kanal eingerichtet werden).

Das folgende Diagramm zeigt Beispiele für sichere E/A-Beschaltungen.



3.4. Funktionale Sicherheit - sicherheitsrelevante Parameter

In diesem Kapitel werden Parameter beschrieben, die mit der funktionalen Sicherheit im Zusammenhang stehen. Gemäß IEC 61508 bedeutet Sicherheit, dass ein System frei von inakzeptablen Risiken ist. Funktionale Sicherheit ist Teil der Gesamtsicherheit, die die ausfallsichere Reaktion eines Sicherheitssystems gemäß den Eingangsbedingungen garantiert. Hier müssen interne sicherheitsrelevante Gerätefehler erkannt und ein sicherer Zustand hergestellt werden.

Sicherheitsrelevante Parameter sind immer in den entsprechenden Anleitungen der Module zu finden.

Produkt BNI CIP-351-000-K015 (BNI00HN):

Parameter gemäß IEC 61508	Bedeutung
PFH = 4,95 × 10^{-9}/h	**P**robability of **f**ailure per **H**our: Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde
PFDavg = 4,30 × 10^{-4}	**P**robability of **F**ailure on **D**emand **av**era**g**e: Durchschnitt der Wahrscheinlichkeit eines Ausfalls bei niedriger Anforderungsrate
SFF gemäß SIL 3	**S**afe **F**ailure **F**raction: Anteil der Ausfälle, die zu einem sicheren Zustand führen.

Produkt BNI CIP-351-000-K015 (BNI00HN):

Parameter gemäß DIN EN ISO 13849-1	Bedeutung
MTTFd: High	**M**ean **T**ime **T**o **d**angerous **F**ailure (Mittlere Zeit bis zu einem gefahrbringenden Ausfall)
DCavg: High	**D**iagnostic **C**overage **av**era**g**e (Durchschnittliche Diagnoseabdeckung)
Lebensdauer: 20 Jahre	Während der erwarteten Lebensdauer des Geräts von max. 20 Jahren ist kein Proof-Test erforderlich

3.5. Umgebungs- und Sicherheitsanweisungen des Produkts

Zulassungen, Richtlinien, Normen

Das Sichere E/A-Modul wurde in Übereinstimmung mit den folgenden Richtlinien und Normen entwickelt:

Konformität und Zulassung		
CE*	2006/42/EG	Maschinenrichtlinie
	2011/65/UE	RoHS 2-Richtlinie
	2014/30/EU	EMV-Richtlinie für Industrieanwendungen (Klasse B)
UL Listed	UL 508	Zulassung für USA und Kanada
IEC 61508	Ed 2010	Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PE oder E/E/PES)
ISO 13849-1	Ed 2015	Sicherheit von Maschinen
IEC 62061	Ed 2021	Sicherheit von Maschinen: Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme
IEC 61131-2	Ed 2007	Speicherprogrammierbare Steuerungen - Betriebsmittelanforderungen und Prüfungen
ODVA-Konformität	Vol 2 – 1.18	EtherNet/IP™
	Vol 5 – 2.6	CIP Safety™
IEC 60529	Ed 2010	Schutzart IP 67
IEC 61326-3-1	Ed 2017	Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit)

*Die CE-Konformitätserklärung finden Sie auf der Website von Balluff unter: (www.balluff.com).

Das Sichere E/A-Modul wurde speziell für folgende Zwecke entwickelt und produziert:

- Kommunikation und Prozesskontrolle
- allgemeine Steuerungs- und Automatisierungsanwendungen
- industrielle Anwendungen
- Betrieb unter den in den technischen Daten angegebenen Umgebungsbedingungen

Dieses Produkt wurde für den Einsatz in industriellen Bereichen EMV-geprüft. Wenn es in persönlichen oder in Geschäfts- und Handelsumgebungen eingesetzt werden soll, muss es eine EMV-Qualifizierung durchlaufen.

Explosive Umgebungen

Gefahr!
Dieses Gerät ist nicht für Anwendungen in

- explosiven Umgebungen (EX-Zone) zertifiziert

Spannungsversorgung und elektrische Sicherheit

Das Gerät ist für den Betrieb mit 24-VDC-Netzteilen konzipiert, die den PELV-/SELV-Bestimmungen gemäß EN 50178 entsprechen.

Verletzungsgefahr durch elektrischen Strom!

Es dürfen nur Geräte am Modul angeschlossen werden, die eine sichere Trennung vom Netz (z.B. 120V/230V/600V) ermöglichen.

Die Erzeugung der 24 V durch die Netzteile muss den Anforderungen von PELV/SELV gemäß EN 50178 entsprechen.

Schutzart IP67

Das Produkt entspricht bei der Installation der Schutzart IP67. Alle Abdeckungen von nicht genutzten Anschlüssen am Produkt müssen aufgesetzt sein, um die Anforderungen der Schutzart IP67 im Betrieb zu erfüllen.

Gefahr!
Stromschlaggefahr!
Der Kontakt mit stromführenden Teilen führt zu einer unmittelbaren Lebensgefahr.

Gebrauchsdauer

Die erwartete Lebenszeit des Sicheren E/A-Moduls beträgt max. 20 Jahre ohne Notwendigkeit eines Stress-Tests.

Warnung!
Wenn der Benutzer einen Einsatz seiner Sicherheitsanwendung mit den angegebenen Daten für mehr als 20 Jahre kalkuliert, muss das Sichere E/A-Modul außer Betrieb genommen und ersetzt werden. Ein Stress-Test kann nicht vom Benutzer festgelegt werden.

Erdung

Warnung!
Erdungsverbindungen sollten in Übereinstimmung mit dem entsprechenden Kapitel in dieser Anleitung hergestellt werden, um die EMV-Eigenschaften des Produkts zu gewährleisten.

3.6. Produktmerkmale

Zu den Haupteigenschaften des EtherNet/IP CIP Safety I/O-Moduls zählen u.a.:

- Sicherheitseingänge
  - Für den Anschluss von Sicherheitsgeräten, wie z.B. Not-Stopp-Taster, Torschalter und Sicherheitslichtvorhänge.
  - Es wird der Ein- und der Zweikanalmodus unterstützt.
  - Der Zweikanalmodus wertet die Übereinstimmung zwischen zwei Eingangssignalen (Kanälen) aus, was den Einsatz des Moduls für die Sicherheitskategorien 3 und 4 ermöglicht. Die Dauer einer logischen Diskrepanz zwischen zwei Kanälen kann anhand der Diskrepanzzeit-Einstellung überwacht werden.
  - Jedem Sicherheitseingang ist ein eigener Testausgang zugewiesen, um eine Überprüfung auf Kurzschlüsse in der externen Verkabelung vorzunehmen.
  - Es ist eine unabhängig einstellbare EIN- und AUS-Verzögerung pro Kanal verfügbar.
- Testausgänge
  - Es sind separate Testausgänge für die Erkennung von externen Kurzschlüssen eines Sicherheitseingangs verfügbar.
  - Die Geräte, wie z.B. Sicherheitssensoren, können mit Strom (24 V) versorgt werden.
  - Testausgänge können als nicht sichere Standardausgänge konfiguriert werden.
  - 2 Testausgänge können für die Erkennung von Kabeldefekten einer Muting-Lampe verwendet werden.
- Sicherheitsausgänge
  - Max. 1A für Sicherheitsausgänge.
  - Der Zweikanalmodus wertet die Übereinstimmung zwischen zwei Eingangssignalen (Kanälen) aus.
  - Sicherheitsausgänge können impulsgeprüft werden, um Kurzschlüsse in der Feldverdrahtung bis 24 VDC zu erkennen.
- E/A Sicherheits-RPI mit einer Zykluszeit von bis zu 10 ms
- IP67-geschütztes Gehäuse, das bei ordnungsgemäßer Installation Schutz vor dem Eindringen von Staub und Wasser bietet
- Integrierter, nicht verwalteter 2-Port-Ethernet-Switch mit Crossover- und DLR-Funktionalität
- Isolierte Erdung, um die Verwendung von 2 separaten Netzteilen für die Stromversorgung der Modullogik/Eingänge und Ausgänge zu ermöglichen.
- Schutzleiter (für Netzteile)
- Funktionserde (für Ethernet-Anschlüsse)
- Diagnose-LEDs
- Einfache Inbetriebnahme mit dem Balluff Safety Network Configuration Tool (SNCT)
- On-Board-Speicherschlüssel für die Speicherung der Modulkonfiguration und den Austausch in wenigen Minuten ohne Spezialwerkzeuge oder erneute Inbetriebnahme.
- 3 Drehschalter für die Festlegung der IP-Adresse

3.7. Ethernet-Topologien

Das EtherNet/IP CIP Safety I/O-Modul kann mit einem protokollkonformen Scanner als Teil der Steuerungssystemarchitektur verwendet werden. Der integrierte DLR-fähige 2-Port-Ethernet-Switch des Moduls ermöglicht die Nutzung der Netzwerktopologie, die die Anwendungsanforderungen erfüllt. Diese Topologien sind:

- Stern
- Daisy-Chain
- Kombination von Stern und Daisy-Chain
- DLR für Ethernet-Medien-Ring-Redundanz

Hinweis!

Bei der Nutzung der Daisy-Chain-Topologie ist Folgendes zu beachten:

- Wartungsmaßnahmen an einem Modul, das sich nicht physisch am Ende der Daisy-Chain befindet – zum Beispiel Entfernen des Netzwerkkabels oder Ein-/Ausschalten des Moduls – wirken sich auf alle Module aus, die sich abwärts der Kette ausgehend vom gewarteten Modul befinden.
- Der in jedem Modul integrierte Dual-Port-Ethernet-Switch eliminiert die Notwendigkeit von zusätzlichen Ethernet-Switches

4. Funktionen für die funktionale Sicherheit

Das EtherNet/IP CIP Safety I/O-Modul kann mit den richtigen Parametereinstellungen und der richtigen Beschaltung die folgenden Sicherheitsklassen erreichen.

Sicherheitsklassen		
E/A-Konfiguration	**Nach IEC 61508 / IEC 62061**	**Nach ISO 13849-1**
Doppelter E/A-Kanal	SIL 3	PL e / Cat. 4
Einzelner E/A-Kanal	SIL 2	PL d / Cat. 2

4.1. Sicherheitszustände

Die Sicherheitszustände des E/A-Moduls werden wie folgt definiert:

- Sichere Ausgänge werden abgeschaltet (OFF)
- Sichere Eingänge werden im OFF-Zustand im Netzwerk gemeldet

Warnung!
Das Sichere E/A-Modul muss in Systemen verwendet werden, in denen der OFF-Zustand der Sicherheitszustand ist.

4.2. Sicherheitseingänge

Sicherheitseingänge werden verwendet, um den Zustand des Sicherheitseingangsgeräts zu melden.

Ein Sicherheitseingang kann folgendermaßen konfiguriert werden:

- **Nicht verwendet** (Standard) - der Eingang ist deaktiviert und wirkt an keiner Sicherheitsfunktion mit
- **Sicherheit** - der Eingang wirkt an der Sicherheitsfunktion mit, ist jedoch von keinem Testausgang anhängig
- **Sicherheits-Impulstest** - der Eingang wirkt an der Sicherheitsfunktion mit und ist von einem verknüpften Testausgang abhängig, der als “Impulstest” konfiguriert ist
- **Standard** - der Eingang wirkt an keiner Sicherheitsfunktion mit (ermöglicht den Anschluss eines nicht sicheren Eingangsgeräts). Ein **Standard**-Eingang verhält sich aber trotzdem wie ein als **Sicherheit** konfigurierter Eingang.

Verwenden von Sicherheitseingängen auf einem Einzelkanal

Die Eingänge werden als 2 verschiedene Sicherheitseingänge am selben M12-Anschluss konfiguriert.

Der Prozesswert des Eingangs wird auf den physischen Eingangswert des Sicherheitsgeräts gesetzt und der Status auf “1” (gut) gestellt, so lange kein Fehler erkannt wird. Wird ein Fehler erkannt, wird der Prozesswert des Eingangs ausgeschaltet (OFF) und der Status auf “0” (schlecht) gestellt.

Verhalten des BNI CIP-351-000-K015 (BNI00HN) bei Verwendung als sichere Einzeleingänge:

Sicherheitsgerät Physischer Zustand	Fehler erkannt(1)	Sicherer Eingang Prozesswert	Sicherer Eingang Prozessstatus	Sicherer Eingang LED-Status
0 = OFF	Nein	**0** (sicher)	**1**	**OFF**
1 = ON	Nein	**1** (aktiv)	**1**	**GELB**
0 = OFF	Ja	**0** (Fehler) (2)	**0**	**ROT**
1 = ON	Ja	**0** (Fehler)	**0**	**ROT**

Hinweise!

- (1) Wenn der Einzelkanaleingang als “Standard” oder “Sicherheit” konfiguriert ist, können nur interne Hardwarefehler erkannt werden. Der Eingang muss als “Sicherheits-Impulstest” konfiguriert werden, um einen externen Kurzschluss bei ON-Erkennung zu ermöglichen.
- (2) Dieser Zustand ist nur ein Übergangszustand, da er der Fehlerrücksetzungsbedingung entspricht (physischer Wert auf OFF eingestellt). Wenn weiterhin ein physischer Fehler in der Verkabelung vorhanden ist, wird der Fehler beim nächsten ON-Übergang erneut erkannt.

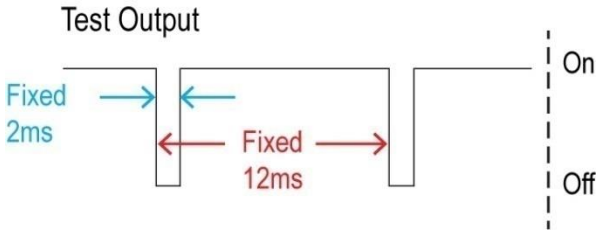
Verwenden eines Testausgangs

Ein Testausgang kann konfiguriert werden als

- **Impulstest** – Wenn der externe Kontakt des Sicherheitsgeräts geschlossen ist, ermöglicht der Testausgangsimpuls die Diagnose von externen Verkabelungsfehlern bei der Spannungsversorgung oder von Kurzschlüssen mit dem anderen Sicherheitseingang am selben M12-Anschluss.

Hinweis!
Charakteristik des Impulstests

- Impulstestlänge: 2 ms
- Impulstestdauer: 12 ms



Hinweis!
Ein Impulstest kann für jeden Sicherheitseingang des M12-Anschlusses konfiguriert werden. Er kann auch beiden Eingängen zugewiesen werden.

- **Spannungsversorgung** – Der Testausgang wird als Spannungsversorgung für die Versorgung des Sicherheitseingangsgeräts mit 24 VDC verwendet.
- **Standard** – Der Testausgang wird als nicht sicherer Digitalausgang verwendet.

Hinweis!
Es ist keine Status-LED mit den Testausgängen verknüpft. Die Werte und der Status des Testausgangs kann trotzdem über Prozessbilder der Eingänge überwacht werden.

- **Muting-Lampe** – Der Testausgang überprüft, ob die Schaltung und die Lampe betriebsbereit sind.

Warnung!
Wenn Testausgänge als **Spannungsversorgung** oder **Muting-Lampe** konfiguriert sind, müssen gegebenenfalls je nach Anwendung und der erwarteten SIL/CAT doppelt isolierte Kabel verwendet werden.

Wenn der Testausgang aktiviert ist, wird der Ausgangsstrom mit der Muting-Lampe geregelt. Unterhalb von 5 mA wird ein Fehler erkannt und der Satus ist 0=OFF. Oberhalb von 25 mA erfolgt ein normaler Betrieb, der Status ist 1=ON.

Im Folgenden finden Sie ein typisches Szenario für die Erkennung eines defekten Kabels der Muting-Lampe:

Prozesswert des Testausgangs	Physischer Zustand der Muting-Lampe	Status der Muting-Lampe
Schritt 1: 1 = ON	Lampe in Ordnung	1
Schritt 2: 1 = ON	Lampe defekt	0
Schritt 3: 0 = OFF	Lampe defekt	0
Schritt 4: 0 = OFF	Lampe ersetzt	1

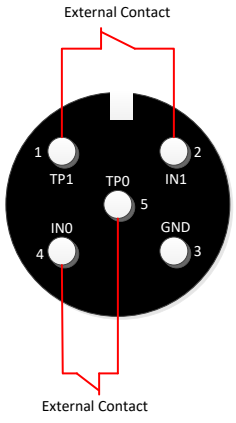
Hinweise!

- Im Multi-Lampen-Modus können nur der *Testausgang 3* und der *Testausgang 7* konfiguriert werden.
- Wenn der Testausgang nicht aktiviert ist, kann kein Fehler wegen eines defekten Kabels erkannt werden. Sobald jedoch ein Defekt erkannt wird (Schritt 2), wird ein Lampenwechsel diagnostiziert, auch wenn der Testausgang deaktiviert ist (Schritt 3)
- Die Kabelbrucherkennung wird in einem Intervall von 3 Sekunden durchgeführt. Es sind zwei aufeinanderfolgende Erkennungen erforderlich, bevor der Status als BAD (SCHLECHT) gemeldet wird. Es kann also bis zu 6 Sekunden dauern, bis der Status der Muting-Lampe auf BAD (SCHLECHT) gesetzt wird.

Typische Beschaltung der Sicherheitseingänge

M12-Pinbelegung und Beschaltung der Sicherheitseingänge mit den verknüpften Impulstestausgängen

- 1: Testausgang 1 (TP1, 24 VDC, Versorgung über UB)
- 2: Sicherer Eingang 1 (IN1)
- 3: Erdungslogik/Eingang (UB GND)
- 4: Sicherer Eingang 0 (IN0)
- 5: Testausgang 0 (TP0, 24 VDC, Versorgung über UB)



Festlegen des Zweikanalmodus und der Diskrepanzzeit

Zur Unterstützung redundanter Kanalsicherheitsgeräte kann die Übereinstimmung zwischen Signalen auf zwei Eingangskanälen überprüft werden. Diese Art der redundanten Beschaltung wird Zweikanalmodus genannt.

Hinweis!

- Die Zweikanalfunktion funktioniert nur bei der Verwendung von 2 Sicherheitseingangssignalen am selben M12-Port des Sicheren E/A-Moduls.
- Es können insgesamt sechs redundante Kanalsicherheitsgeräte mit dem Sicheren E/A-Modul verbunden werden. Ein redundantes Kanalsicherheitsgerät pro M12-Port.

Es muss entweder der Evaluierungsmodus “Äquivalent” oder “Antivalent” des Sicherheitseingangspaars ausgewählt werden. Im Zweikanalmodus überwacht das Sichere E/A-Modul die Zeit, in der eine Diskrepanz zwischen den zwei Kanälen besteht.

Hinweis!

Bei Verwendung der Balluff SNCT-Software

- Die Diskrepanzzeit kann von 10 ms bis 30 s in Schritten von 10 ms konfiguriert werden.
- Der Standardwert für die Diskrepanzzeit ist 10 ms.

Verhalten des BNI CIP-351-000-K015 (BNI00HN) bei Verwendung als äquivalente duale sichere Eingänge:

Physischer Zustand Sicherheitsgerät		**Fehler erkannt(*1)**		**Prozesswert sicherer Eingang**		**Prozessstatus sicherer Eingang**		**LED-Status sicherer Eingang**	
Eingang (Pin 4)	Eingang+1 (Pin2)	Eingang	Eingang +1	Eingang	Eingang +1	Eingang	Eingang +1	Eingang	Eingang +1
0 = OFF	0 = OFF	Nein	Nein	**0** (sicher)	**0** (sicher)	**1**	**1**	**OFF**	**OFF**
0 = OFF	1 = ON	Nein	Nein	**0** (Fehler)	**0** (Fehler)	**0**(a)	**0**(a)	**ROT**(b)	**ROT**(b)
1 = ON	0 = OFF	Nein	Nein	**0** (Fehler)	**0** (Fehler)	**0**(a)	**0**(a)	**ROT**(b)	**ROT**(b)
1 = ON	1 = ON	Nein	Nein	**1** (aktiv)	**1** (aktiv)	**1**	**1**	**GELB**	**GELB**
-	-	Ja	-	**0** (Fehler)	**0** (Fehler)	**0**	**0**	**ROT**	**ROT BLINKEND**
-	-	-	Ja	**0** (Fehler)	**0** (Fehler)	**0**	**0**	**ROT BLINKEND**	**ROT**

(a): Bei “1” bis zum Ablauf der Diskrepanzzeit.

(b): OFF bis zum Ablauf der Diskrepanzzeit.

Verhalten des BNI CIP-351-000-K015 (BNI00HN) bei Verwendung als antivalente duale sichere Eingänge:

Physischer Zustand Sicherheitsgerät		**Fehler erkannt (1)**		**Prozesswert sicherer Eingang**		**Prozessstatus sicherer Eingang**		**LED-Status sicherer Eingang**	
Eingang (Pin 4)	Eingang+1 (Pin2)	Eingang	Eingang +1	Eingang	Eingang +1	Eingang	Eingang +1	Eingang	Eingang +1
0 = OFF	0 = OFF	Nein	Nein	**0** (Fehler)	**1** (Fehler)	**0**(a)	**0**(a)	**ROT**(b)	**ROT**(b)
0 = OFF	1 = ON	Nein	Nein	**0** (sicher)	**1** (sicher)	**1**	**1**	**OFF**	**GELB**
1 = ON	0 = OFF	Nein	Nein	**1** (aktiv)	**0** (aktiv)	**1**	**1**	**GELB**	**OFF**
1 = ON	1 = ON	Nein	Nein	**0** (Fehler)	**1** (Fehler)	**0**(a)	**0**(a)	**ROT**(b)	**ROT**(b)
-	-	Ja	-	**0** (Fehler)	**1** (Fehler)	**0**	**0**	**ROT**	**ROT BLINKEND**
-	-	-	Ja	**0** (Fehler)	**1** (Fehler)	**0**	**0**	**ROT BLINKEND**	**ROT**

(a): Bei “1” bis zum Ablauf der Diskrepanzzeit.

(b): OFF bis zum Ablauf der Diskrepanzzeit.

Hinweise!

- (1) Wenn die Zweikanaleingänge als “Standard” oder “Sicherheit” konfiguriert sind, können nur interne Hardwarefehler und die Diskrepanzzeit zwischen Eingängen erkannt werden. Eingänge müssen als “Sicherheits-Impulstest” konfiguriert werden, um einen externen Kurzschluss bei 1-Erkennung zu ermöglichen.
- Beim Übergang der Eingänge werden während der Diskrepanzzeit Eingänge im sicheren Zustand gemeldet.

Fehlerbehebung für den Sicherheitseingang

Hinweis!

Wenn ein Fehler erkannt wird, bleibt der Prozesswert des Sicherheitseingangs (oder der Sicherheitseingänge) im Sicherheitszustand, bis der folgende Vorgang durchgeführt wird:

1. Beseitigen Sie die Ursache des Fehlers.
2. Setzen Sie den Sicherheitseingang auf seinen Sicherheitszustand.

Eingangsverzögerung

Einschaltverzögerung und Ausschalterzögerung können getrennt für jeden Eingang konfiguriert werden.

Einschaltverzögerung

Die Einschaltverzögerung ist die erforderliche Mindestzeit, nach der ein auf EIN geschalteter physischer Eingang im Netzwerk als “1” gemeldet wird. Wenn beispielsweise die Einschaltverzögerung auf 5 ms eingestellt ist, wird der Eingang im Netzwerk auf Stufe “1” gemeldet, nachdem der Eingang mindestens 5 ms lang auf EIN registriert wurde.

Ausschalterzögerung

Die Ausschaltverzögerung ist die erforderliche Mindestzeit, nach der ein auf OFF geschalteter physischer Eingang im Netzwerk als “0” gemeldet wird. Wenn beispielsweise die Ausschaltverzögerung auf 5 ms eingestellt ist, wird der Eingang im Netzwerk auf Stufe “0” gemeldet, nachdem der Eingang mindestens 5 ms lang auf AUS registriert wurde.

Hinweis!

Bei Verwendung der Balluff SNCT-Software

- Die Parameter für die Einschaltverzögerung und die Ausschalterzögerung können von 0 bis 1000 ms in Schritten von 1 ms konfiguriert werden.
- Der Standardwert für die Einschaltverzögerung und die Ausschalterzögerung ist 0.

Haltezeit für Eingangsfehler

Die Haltezeit (Latch-Zeit) für Eingangsfehler ist ein eindeutiger Parameter, der für alle Eingänge gilt.

Durch das Halten von Eingangsfehlern soll sichergestellt werden, dass intermittierende Fehler, die nur wenige Millisekunden existieren können, lang genug gehalten werden, um von der Steuerung gelesen werden zu können. Die Haltezeit definiert die Mindestdauer, über die ein erkannter Fehler an einem sicheren Eingang im Netzwerk gemeldet werden soll, damit die Steuerung ihn lesen kann.

Hinweis!

Bei Verwendung der Balluff SNCT-Software

- Die Standardparameter für die Haltezeit für Eingangsfehler können von 0 bis 65530 ms in Schritten von 10 ms konfiguriert werden.

- Der Standardwert für die Haltezeit für Eingangsfehler ist 1000 ms.
- Die Haltedauer des Fehlers muss auf dem RPI der Sicherheitsverbindung, der Überwachung der Anwendungssicherheitsaufgabe und anderen anwendungsspezifischen Variablen basieren.

4.3. Sicherheitsausgänge (BNI CIP-351-000-K015)

Stromliefernde Sicherheitsausgänge werden verwendet, um den Zustand der Ausgangsgeräte zu steuern.

Hinweis!
Die sicheren Ausgänge sind:

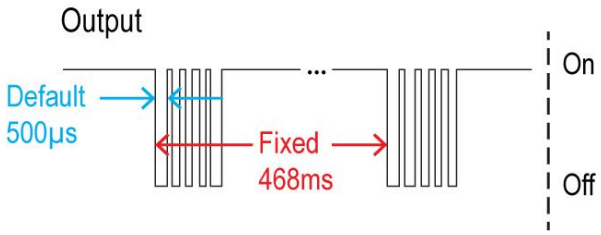
- Bestromung bei max. 1 A
- kurzschlussfest
- Auf Impulstest umschaltbar

Ein Sicherheitsausgang kann folgendermaßen konfiguriert werden:

- **Nicht verwendet** (Standard) - der Ausgang ist deaktiviert und wirkt an keiner Sicherheitsfunktion mit.
- **Sicherheits-Impulstest** - Der Ausgang generiert Impulstests (wenn der Ausgang aktiv ist) zur Überwachung auf einen Kurzschluss zwischen Ausgangspin und Spannungsversorgung (fest eingestellt auf “1”) oder auf einen Kurzschluss mit einem anderen aktiven Ausgang am selben M12-Anschluss.

Hinweise!
Bei Verwendung der Balluff SNCT-Software

- Die Impulstestlänge kann von 300µs bis 10 ms in Schritten von 100 µs konfiguriert werden.
- Der Standardwert für die Impulstestlänge ist 500 µs
- Impulstestdauer: 468 ms



- Neben der Erkennung von externen Kurzschlüssen werden alle Sicherheitsfunktionen, die an der Abschaltung von Ausgängen beteiligt sind, innerhalb der Testdauer ebenfalls diagnostiziert. Es wird also eine Reihe von 4 Impulstests für jeden Sicherheitsausgang durchgeführt.

Hinweis!
Die Impulstests sollten entsprechend der Impedanz des verbundenen Geräts konfiguriert werden. Das Sichere E/A-Modul wurde für die Steuerung einer großen Bandbreite an Geräten mit einer aktiven Entladeschaltung konzipiert. Wenn bei einem Impulstest mit einer Länge von mehr als (oder gleich) 500 µs eine Restspannung vorhanden ist, wird ein Strom von 50 mA über eine Dauer von 300 µs gehalten. Wenn dies jedoch nicht ausreichend ist und der Ausgang bedingt durch die kapazitive Last des verbundenen Equipments in den sicheren Zustand wechselt, kann die Impulslänge erhöht werden (auf bis zu 10 ms).

Hinweise!

- Stromliefernde Sicherheitsausgänge sollten nicht verwendet werden, um ein Gerät oder ein Untersystem mit Strom zu versorgen, bei dem die kapazitive Last im Betrieb schwanken kann.

Warnung!

Achten Sie auf die Reaktionszeit des Ausgangsgeräts, um eine Störung aufgrund des Impulstests zu verhindern.

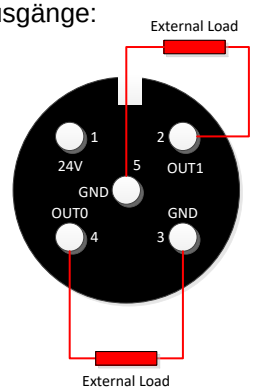
- **Sicherheit Kein Impulstest** - Der Ausgang wird ohne Impulstest verwendet.

Hinweis!

In diesem Modus wird die Diagnose am Ausgang vorgenommen. Wenn ein stromliefernder Ausgang abgeschaltet wird, kann der gemessene Zustand aufgrund der kapazitiven Last des verbundenen Equipments vom erwarteten Zustand abweichen. Das Sichere E/A-Modul wurde für die Steuerung einer großen Bandbreite an Equipment mit einer aktiven Entladeschaltung konzipiert. Wenn ein stromliefernder Ausgang abgeschaltet wird und eine Restspannung vorhanden ist, wird ein Strom von 50 mA über eine Dauer von 2 ms gehalten.

M12-Pinbelegung und Beschaltung der stromliefernden Sicherheitsausgänge:

- 1: 24 VDC (Versorgung über UL)
- 2: Sicherer Ausgang 1 (OUT1)
- 3: Erdungsausgang (UL GND)
- 4: Sicherer Ausgang 0 (OUT0)
- 5: Erdungsausgang (UL GND)



Hinweis!

Der maximal verfügbare Strom an den Pins 1 (24 VDC) der 2 stromliefernden Ausgangsports beträgt 3,5 A.

Verwenden von Sicherheitsausgängen als Einzelkanalausgänge

Ausgänge am selben M12-Anschluss werden als 2 Einzelkanalausgänge konfiguriert.

Nach der Aktivierung durch die Logiksteuerung wird der Ausgang auf EIN geschaltet und der Status auf “1” (gut) gestellt, solange kein Fehler erkannt wird. Wird ein Fehler erkannt, wird der Ausgang zwangsweise in den sicheren Zustand AUS geschaltet und der Status auf “0” (schlecht) gestellt.

Verhalten des BNI CIP-351-000-K015 (BNI00HN) bei Verwendung als sichere Einzelausgänge:

Prozesswert sicherer Ausgang	Fehler erkannt	Physischer Zustand Sicherheitsgerät	Prozessstatus sicherer Ausgang	LED-Status sicherer Ausgang
0	Nein	0 = OFF (sicher)	**1**	**OFF**
1	Nein	1 = ON (aktiv)	**1**	**GELB**
-	Ja (am Ausgang selbst)	0 = OFF (Fehler)	**0**	**ROT**
-	Ja (am Partner)	0 = OFF (Fehler)	**0**	**ROT BLINKEND**

Hinweis!

Wenn an einem Einzelkanalausgang ein Fehler erkannt wird, werden beide Ausgänge am selben M12-Anschluss in einen sicheren Zustand geschaltet.

Hinweis!

- Wenn an einem Sicherheitsausgang kein Impulstest konfiguriert ist, wird nur der zurückgelesene Wert für die Erkennung eines Fehlers verwendet. Es wird also nur ein Kurzschluss gegen 1, wenn der Ausgang zu 0 gesteuert wird, und ein Kurzschluss zu 0, wenn der Ausgang zu 1 gesteuert wird, erkannt.
- Wenn Impulstests aktiviert sind, können interne Fehler sowie Kurzschlüsse gegen 1 erkannt werden.

Verwenden von Sicherheitsausgängen als Zweikanalausgänge

Ausgänge am selben M12-Anschluss können als Ausgangspaar konfiguriert werden.

Nach der Aktivierung der Prozesswerte beider Ausgänge durch die Logiksteuerung werden die Doppelausgänge auf EIN geschaltet und der Status auf “1” (gut) gestellt, solange kein Fehler erkannt wird. Wird ein Hardwarefehler oder eine Diskrepanz der Prozesswerte der Ausgänge erkannt, werden die Ausgänge zwangsweise in den sicheren Zustand AUS geschaltet und der Status auf “0” (schlecht) gestellt.

Verhalten des BNI CIP-351-000-K015 (BNI00HN) bei Verwendung als sichere Doppelausgänge:

Prozesswert sicher Ausgang		Fehler erkannt		Physischer Zustand Sicherheitsgerät		Prozessstatus sicherer Ausgang		LED-Status sicherer Ausgang	
Ausgang	Ausgang +1	Ausgang	Ausgang +1	Ausgang (Pin 4)	Ausgang+1 (Pin2)	Ausgang	Ausgang +1	Ausgang	Ausgang +1
0	**0**	Nein	Nein	0 = OFF (sicher)	0 = OFF (sicher)	**1**	**1**	**OFF**	**OFF**
0	**1**	Nein	Nein	0 = OFF (Fehler)	0 = OFF (Fehler)	**0**	**0**	**ROT**	**ROT**
1	**0**	Nein	Nein	0 = OFF (Fehler)	0 = OFF (Fehler)	**0**	**0**	**ROT**	**ROT**
1	**1**	Nein	Nein	1 = ON (aktiv)	1 = ON (aktiv)	**1**	**1**	**GELB**	**GELB**
-	-	Ja	-	0 = OFF (Fehler)	0 = OFF (Fehler)	**0**	**0**	**ROT**	**ROT BLINKEND**
-	-	-	Ja	0 = OFF (Fehler)	0 = OFF (Fehler)	**0**	**0**	**ROT BLINKEND**	**ROT**

Fehlerbehebung für den Sicherheitsausgang

Hinweis!

Wenn ein Fehler erkannt wird, bleibt der Prozesswert des Sicherheitsausgangs (oder der Sicherheitsausgänge) im Sicherheitszustand, bis der folgende Vorgang durchgeführt wird:

- Beseitigen Sie die Ursache des Fehlers.
- Setzen Sie den Sicherheitsausgang auf seinen Sicherheitszustand.

Haltezeit für Ausgangsfehler

Die Haltezeit (Latch-Zeit) für Ausgangsfehler ist ein eindeutiger Parameter, der für alle Ausgänge gilt.

Durch das Halten von Ausgangsfehlern soll sichergestellt werden, dass intermittierende Fehler, die nur wenige Millisekunden existieren können, lang genug gehalten werden, um von der Steuerung gelesen werden zu können. Die Haltezeit definiert die Mindestdauer, über die ein erkannter Fehler an einem sicheren Ausgang im Netzwerk gemeldet werden soll, damit die Steuerung ihn lesen kann.

Hinweis!

Bei Verwendung der Balluff SNCT-Software

- Die Standardparameter für die Haltezeit für Ausgangsfehler können von 0 bis 65530 ms in Schritten von 10 ms konfiguriert werden.
- Der Standardwert für die Haltezeit für Ausgangsfehler ist 1000 ms.
- Die Haltedauer des Fehlers muss auf dem RPI der Sicherheitsverbindung, der Überwachung der Anwendungssicherheitsaufgabe und anderen anwendungsspezifischen Variablen basieren.

4.4. E/A-Status

Das Sichere E/A-Modul liefert Statusinformationen für die Überwachung der E/A-Schaltung.
Die Statusinformationen können vom EtherNet/IP-Scanner gelesen werden.

Hinweis!

Wenn ein Fehler erkannt wird, ist der Statuswert “0” (schlecht). Im Normalbetrieb ist der Statuswert “1” (gut).

Die einzelnen unten aufgeführten Punkte haben ihren individuellen Status:

- Status Sicherheitseingang
- Status Testausgang
- Status Sicherheitsausgang

4.5. Verhalten bei einem Fehler

Erkannter Fehler	Ausfallsicherer Zustand angewandt für	Methode für die Wiederherstellung	Verfügbarkeit der Feldbus-Kommunikation
Fehler beim Impulstest für Sicherheitseingang (einkanalig)	Fehlerhafter sicherer Eingang	1. Fehler beseitigen 2. Eingang in sicheren Zustand schalten Wartezeit für Halten des Fehlers abgelaufen	Ja
Fehler beim Impulstest für Sicherheitseingang (zweikanalig)	Sicherheits-eingangspaar	1. Fehler beseitigen 2. Eingang in sicheren Zustand schalten Wartezeit für Halten des Fehlers abgelaufen	Ja
Diskrepanz bei Sicherheitseingangspaar (zweikanalig)	Sicherheits-eingangspaar	1. Fehler beseitigen 2. Eingang in sicheren Zustand schalten Wartezeit für Halten des Fehlers abgelaufen	Ja
Fehler beim Impulstest für Sicherheitsausgang oder Fehler bei zurückgelesenem Wert (einkanalig)	Beide Einzelsicherheits-ausgänge am selben Anschluss	1. Fehler beseitigen 2. Ausgänge in sicheren Zustand schalten Wartezeit für Halten des Fehlers abgelaufen	Ja
Fehler beim Impulstest für Sicherheitsausgang oder Fehler bei zurückgelesenem Wert (zweikanalig)	Sicherheits-ausgangspaar	1. Fehler beseitigen 2. Ausgänge in sicheren Zustand schalten Wartezeit für Halten des Fehlers abgelaufen	Ja
Diskrepanzfehler bei Sicherheitsausgang (zweikanalig)	Sicherheits-ausgangspaar	1. Fehler beseitigen 2. Ausgänge in sicheren Zustand schalten Wartezeit für Halten des Fehlers abgelaufen	Ja
Überspannungs-/Unterspannungsfehler bei Eingangsstrom (UB)	Gesamtes Modul (alle Sicherheits-eingänge und -ausgänge)	Spannungsversorgung aus- und wieder einschalten	Ja
Überspannungsfehler bei Ausgangsstrom (UL)	Gesamtes Modul (alle Sicherheits-eingänge und -ausgänge)	Spannungsversorgung aus- und wieder einschalten	Ja

Unterspannungsfehler bei Ausgangsstrom (UL)	Alle Sicherheits-ausgänge	1. Fehler beseitigen 2. Ausgänge in sicheren Zustand schalten	Ja
Überstrom bei Eingangsstrom (UB)	Gesamtes Modul (alle Sicherheits-eingänge und -ausgänge)	Spannungsversorgung aus- und wieder einschalten	Ja
Überstrom bei Ausgangsstrom (UL)	Gesamtes Modul (alle Sicherheits-ausgänge)	Spannungsversorgung aus- und wieder einschalten	Ja
Temperaturfehler	Gesamtes Modul (alle Sicherheits-eingänge und -ausgänge)	Spannungsversorgung aus- und wieder einschalten	NEIN → Kritischer Fehler Alle E/A-LEDs blinken
Interner Hardware-Fehler (CPU, RAM, ADC 3,3V,…)	Gesamtes Modul (alle Sicherheits-eingänge und -ausgänge)	Spannungsversorgung aus- und wieder einschalten	NEIN → Kritischer Fehler Alle E/A-LEDs blinken
CIP Safety Kommunikationsfehler (Eingangsverbindung)	Alle Sicherheits-eingänge	Urheber muss Verbindung neu starten	Ja
CIP Safety Kommunikationsfehler (Ausgangsverbindung)	Alle Sicherheits-ausgänge	Urheber muss Verbindung neu starten	Ja
Rotierender Änderungswert	Gesamtes Modul (alle Sicherheits-eingänge und -ausgänge)	Spannungsversorgung aus- und wieder einschalten	Ja
Externen Schlüssel entfernen	Gesamtes Modul (alle Sicherheits-eingänge und -ausgänge)	Spannungsversorgung aus- und wieder einschalten	Ja

4.6. Reaktionszeit

Berechnen der Reaktionszeit

Für die Berechnung der Reaktionszeit einer Sicherheitsfunktion müssen die schlechtesten Reaktionszeiten aller betreffenden Komponenten zu den Verzögerungen in den Kommunikationspfaden addiert werden. Im Folgenden werden die Reaktionszeiten des Sicheren E/A-Moduls für die Durchführung dieser Berechnungen aufgeführt.

Warnung!
Die Sicherheitsfunktion kann nicht garantiert werden, wenn die folgenden Reaktionszeiten falsch berechnet werden.

1. **Maximale Reaktionszeit eines digitalen Sicherheitseingangs (Einzel- und Zweikanalmodus)**
   Berechnen Sie die maximale Reaktionszeit eines Sicherheitseingangs im fehlerfreien Zustand. Die Reaktionszeit wird zum Zeitpunkt des physischen Ereignisses eines verbundenen Sensors und der Ausgabe des entsprechenden Telegramms im EtherNet/IP-Netzwerk durch das Sichere E/A-Modul berechnet.

   Berechnung der Verzögerungszeiten

Reaktionszeit des verbundenen Sensors/Switches	+ _____	ms
Konfigurierte Eingangsverzögerung + Toleranz von 500 µs	+ _____,5	ms
Interne maximale Verarbeitungszeit des Sicheren E/A-Moduls PT_{IN} max	+ 10,5	ms
	---	
Maximale Reaktionszeit eines digitalen Sicherheitseingangs	**= _____**	**ms**

2. **Maximale Reaktionszeit eines digitalen Sicherheitsausgangs (Einzel- und Zweikanalmodus)**
   Berechnen Sie die maximale Reaktionszeit eines Sicherheitsausgangs im fehlerfreien Zustand. Die Reaktionszeit wird ab dem Moment berechnet, in dem ein Telegramm vom Sicheren E/A-Modul empfangen wird und der Aktor das physische Abschaltereignis verarbeitet.

   Berechnung der Verzögerungszeiten

Interne maximale Verarbeitungszeit des Sicheren E/A-Moduls PT_{OUT} max:	+ 4,5	ms
Konfigurierter Impulstest	+ _____	ms
Abschaltzeit des verbundenen Aktors/Relais	+ _____	ms
Zusätzliche Abschaltverzögerung (physische Signalzeitkommutation)	+ _____	ms
	---	
Maximale Reaktionszeit eines digitalen Sicherheitsausgangs	**= _____**	**ms**

Hinweis!
Die maximale Reaktionszeit eines erkannten Sicherheitsfehlers ist 10 ms (Ausgabe des entsprechenden Telegramms im EtherNet/IP-Netzwerk durch das Sichere E/A-Modul).

5. Produkteigenschaften

5.1. Hardware-Eigenschaften

Typ	**12x Sichere Eingänge + 4x Sichere Ausgänge**
Produktreferenz	BNI CIP-351-000-K015
Sicherheit	
SIL (nach IEC 61508 / IEC 62061)	Bis zu SIL3 (bei Konfiguration in Dual-E/A-Kanal)
CAT (nach ISO 13849-1)	Bis zu Cat. 4 (bei Konfiguration in Dual-E/A-Kanal)
PL (nach ISO 13849-1)	Bis zu PL e (bei Konfiguration in Dual-E/A-Kanal)
PFH	$4{,}95 \times 10^{-9}$/h
PFDavg	$4{,}30 \times 10^{-4}$
DCavg	96,32 %
MTTF	105 Jahre
Lebensdauer	20 Jahre
Strom	
Power IN-Anschluss	Mini-Change (7/8”), 4-poliger Stecker, Edelstahl, geschirmt, Maximal 8 A
Power OUT-Anschluss	Mini-Change (7/8”), 4-polige Buchse, Edelstahl, geschirmt, Maximal 8 A
Modul- & Eingangsstrom (**UB**)	24 VDC, -15% / +20% (geschützt gegen Power Crossing).
Betriebsstrom (**UB**)	< 100 mA
Ausgangsstrom (**UL**)	24 VDC, -15% / +20% (geschützt gegen Power Crossing)
Betriebsstrom (**UL**)	<20 mA (ohne Last)
Sichere Eingänge	
Kanäle	12 Kanäle
Anschluss	M12 Ultra-Lock, 5-polig, Buchse, A-kodiert, Edelstahl, ungeschirmt(*)
Eingangstyp	IEC61131-2 Typ 3
Eingangsspannung	**UB**
Ein-/Ausschaltverzögerung	Konfigurierbar von 0 bis 1000 ms (standardmäßig 0)

Warnung!
Wenn **UB** 2 Sekunden oder länger über 36 V beträgt. Das Sicherheitsmodul wechselt in den Ausfallzustand (alle LEDs blinken rot) und gilt als zerstört. Der interne Überspannungsschutz ist irreversibel beschädigt, wodurch das Modul nicht mehr betrieben werden kann.

Impulstestausgang	
Testratenintervall	max. 12 ms
Impulstestlänge	2 ms
Stromversorgung des Sensors	0,7 A
Max. Kurzschlussstrom	2 A bei 25°C
Sichere Ausgänge	
Ausgangsart	Stromliefernd (PNP)
Kanäle	4 Kanäle, 2-adrig
Ausgangsspannung	**UL**
Anschluss	M12 Ultra-Lock, 5-polig, Buchse, A-kodiert, Edelstahl
Testratenintervall	max. 2 s
Ausgangsnennstrom	1 A pro Kanal
Maximaler Kurzschlussstrom (vorübergehend vor Sicherheitsabschaltung)	6,5 A

Hinweis!
Die Schirmung von E/A-Anschlüssen ist nicht mit der Erdung verbunden. Wenn geschirmte Kabel verwendet werden, muss der Kunde die Kabelschirmung mit der Masse verbinden.

Feldbus	
Ethernet-Anschlüsse	M12, 4-polig, Buchse, D-kodiert, Edelstahl, geschirmt
IP-Einstellung	DHCP basierend auf MAC (unbegrenzte Nutzungsdauer), DHCP basierend auf Name, Statische IP
Protokoll	CIP Safety EtherNet/IP-Adapter gemäß Spezifikation Vol 5 – 2.21 (CIP Safety) und Vol 2 – 1.26 (EtherNet/IP)
Datenzugriff	Implizite Nachrichten für E/A-Datenübertragung
Implizite (E/A) Verbindung	• 1x EO-Verbindung (Exclusive Owner) (sichere Informationen) • 2x IO-Verbindung (Input Only) (zum Austausch von sicheren Prozessdaten mit einem nicht sicheren Scanner) • Bis zu 7 LO-Verbindungen (Listen Only) (zum Austausch von sicheren Prozessdaten mit einem nicht sicheren Scanner)
Explizite (EM) Verbindung	• Bis zu 8 Verbindungen
CIP Safety Verbindung	Typ 1 und Typ 2

Unterstützte CIP-Objekte	• 0x01 – Identitätsobjekt
	• 0x02 – Nachrichten-Router-Objekt
	• 0x04 – Querschnittsobjekt
	  ○ Sicherheitseingangsprofile
	  ▪ 0x20C (T→O)
	  ▪ 0x21C (T→O)
	  ▪ 0x22C (T→O)
	  ▪ 0x243 (T→O)
	  ▪ 0x25C (T→O)
	  ▪ 0x27C (T→O)
	  ○ Sicherheitseingang Herstellerspezifisch
	  ▪ 0x300 (T→O)
	  ○ Sicherheitsausgangsprofile
	  ▪ 0x233 (O→T)
	  ○ Sicherheitsausgang Herstellerspezifisch
	  ▪ 0x301 (O→T)
	  ○ Konfiguration
	  ▪ 0x302 (T→O)
	• 0x06 – Verbindungsmanager-Objekt
	• 0x23 – Diskretes Sicherheits-E/A-Profil
	• 0x37 – Dateiobjekt
	• 0x3B – SDOP-Objekt
	• 0x3D – SDIP-Objekt
	• 0x3F – SDCO-Objekt
	• 0x47 – DLR-Objekt
	• 0x48 – QoS (Quality of Service)
	• 0x80 – SDCI-Objekt
	• 0xF5 – TCP/IP-Schnittstellen-Objekt
	• 0xF6 – Ethernet-Link-Objekt

Integrierter Switch	• Integrierter Switch mit 2x Ports • Geschwindigkeit: 100 Mbps • Auto-Negotiation • Auto-Crossing • Auto-Polarität • 1x Status-LED pro Port • Sturmsicherung gegen Netzwerkschleife (Broadcast-, Multicast- und Unicast-Pakete)

Request Packet Interval (RPI)	Für Sicherheitseingänge (konfigurierbar pro Scanner-Verbindung) → mind. ≥10 ms Für Sicherheitsausgänge (einzelne Scanner-Verbindung) → mind. ≥10 ms
Erkennung von IP-Adresskonflikten	Ja (ACD unterstützt)
DLR	Ja (Beacon Node)
ODVA-Konformität	Ja (CT18EN – CT18ES)

Ethernet-Standardeinstellung:

- IP-Adresse: DHCP
- Subnetzmaske: DHCP
- Gateway: DHCP
- ETH1-Port: Auto-Negotiation + Auto-MDI
- ETH2-Port: Auto-Negotiation + Auto-MDI
- ACD aktiviert

Mechanisch	
Gehäuseabmessungen	235 x 60 x 44 mm
Gehäusewerkstoff	PBT VALOX 420 SEO ROT 7701
Brennbarkeitsklasse	UL 94 V-0
Eckbefestigungsbohrung	4 Montagebohrungen, 5 x10 mm
Erdungsstift	Ja, Edelstahl (erlaubt Kontinuität der Masse, wenn das Modul am Gehäuse der Maschine montiert ist)
Speicherschlüssel	Interner Schlüssel im Fenster
Betriebstemperatur	-25°C … +70°C
Lagertemperatur	-40°C … +90°C
Installationshöhe	max. 2000 m
Vibrationsfestigkeit	Im Betrieb: 7 mm p-p (5-15,7 Hz), 7g (15,7 Hz bis 500 Hz), 3 Achsen
Stockfestigkeit	Im Betrieb: 15 g, 11 ms, 3 Achsen Außer Betrieb: 50 g, 6 ms, 3 Achsen
Luftfeuchtigkeit	10 % bis 95 %, nicht kondensierend
Schutzart	IP67
MTBF	523.750 Stunden / 59,8 Jahre bei 25°C 345.000 Stunden / 39,4 Jahre bei 40°C 136.000 Stunden / 15,5 Jahre bei 70°C

Hinweis!

7/8”-Zubehör (Kabel, Stecker …), das an den Stromanschlüssen des Moduls angeschlossen wird, muss mit einer Schraube mit einem Drehmoment von 2,0 Nm befestigt werden, um die korrekte Abdichtung für die Schutzklasse IP67 sicherzustellen.

M12-Zubehör (Kabel, Stecker …), das an den E/-A- und Netzwerkanschlüssen des Moduls angeschlossen wird, muss mit einer Schraube mit einem Drehmoment von 2,0 Nm befestigt werden, um die korrekte Abdichtung für die Schutzklasse IP67 sicherzustellen.

M8-Zubehör (Kabel, Stecker …), das an den E/-A- und Netzwerkanschlüssen des Moduls angeschlossen wird, muss mit einer Schraube mit einem Drehmoment von 2,0 Nm befestigt werden, um die korrekte Abdichtung für die Schutzklasse IP67 sicherzustellen.

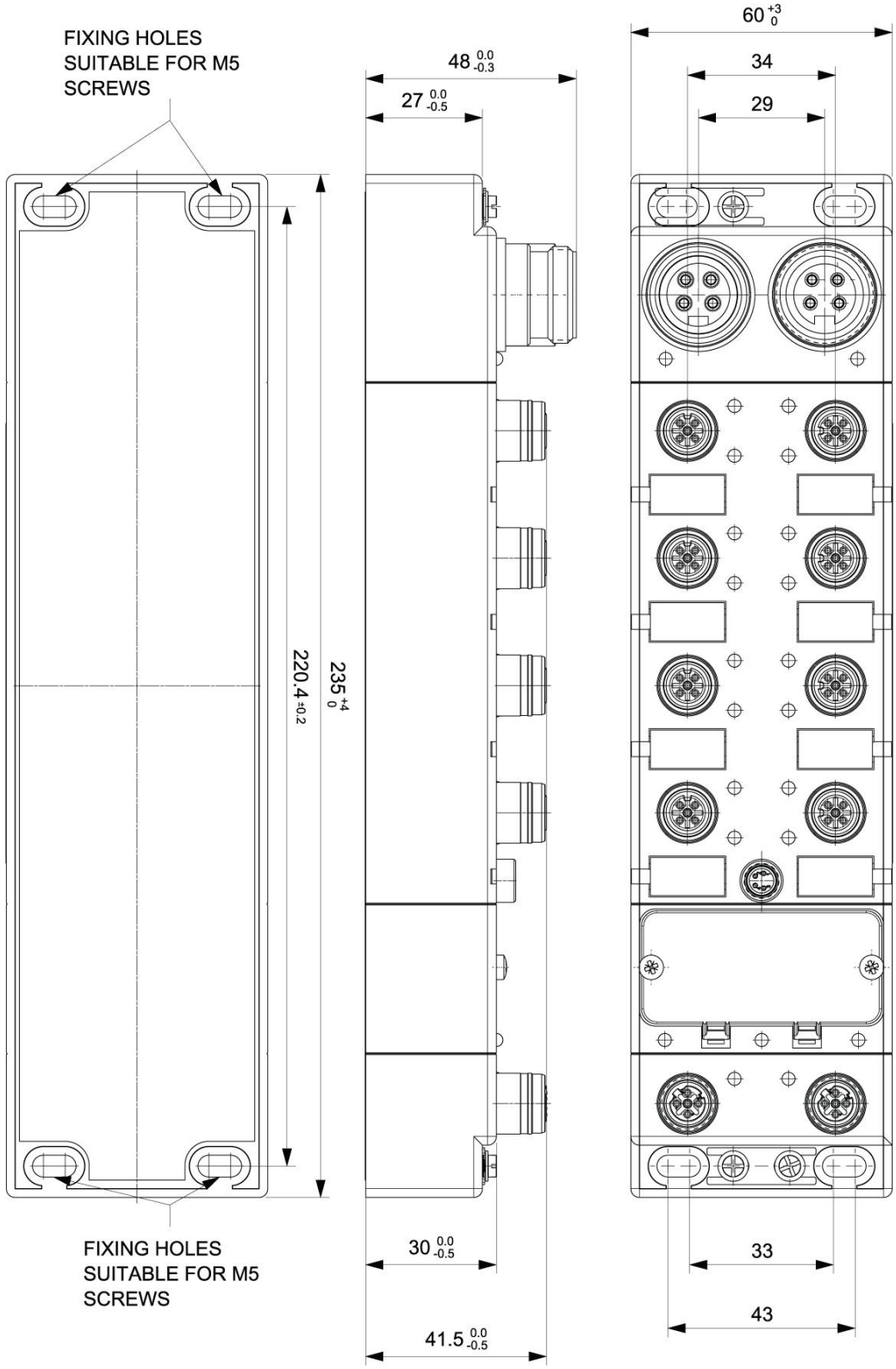
Elektromagnetische Verträglichkeit (EMV)	Standard		Kommentar
Störfestigkeitszone B	EN 61000-6-2		Störfestigkeitsnorm für industrielle Umgebungen
Emissionsnorm für industrielle Umgebungen	EN 61000-6-4 Klasse A (Industrieller Bereich)	EN 61000-4-2	ESD 8 kV Luftentladung 6 kV Kontaktentladung
		EN 61000-4-3	Hochfrequentes elektromagnetisches Feld 80 MHz … 1000 MHz, 20 V/m, 80% AM (1 kHz) 1,4 GHz ... 2,0 GHz, 10 V/m, 80% AM (1 kHz) 2,0 GHz ... 6,0 GHz, 3 V/m, 80% AM (1 kHz)
		EN 61000-4-4	Burst +/- 3 kV 5/50 ns, 5 kHz an Stromanschlüssen +/- 2 kV 5/50 ns, 5 kHz an E/A-Ports +/- 2 kV 5/50 ns, 5 kHz an Kommunikationsanschlüssen
		EN 61000-4-5	Stoßspannungen (Surge) 1 kV Leitung zu Leitung, 2 kV Leitung zu Erde an Stromanschlüssen 2 kV Leitung zu Leitung an E/A-Ports 2 kV Leitung zu Erde an Kommunikationsanschlüssen
		EN 61000-4-6	Leitungsgeführte Störgrößen, induziert durch Funk 150 kHz … 80 MHz, 10V, 80% AM (1 kHz)
		EN 61000-4-16	Prüfung der Störfestigkeit gegen leitungsgeführte, asymmetrische Störgrößen 0 Hz … 150 KHz

Warnung!

Balluff Geräte erfüllen die Anforderungen der EU-Richtlinien und entsprechen (DoC) den geltenden EMV-Normen und können daher problemlos in andere Geräte oder Maschinen integriert werden. Die Erfüllung der EMV-Anforderungen durch das Gesamtsystem liegt jedoch in der Verantwortung des Systemherstellers.

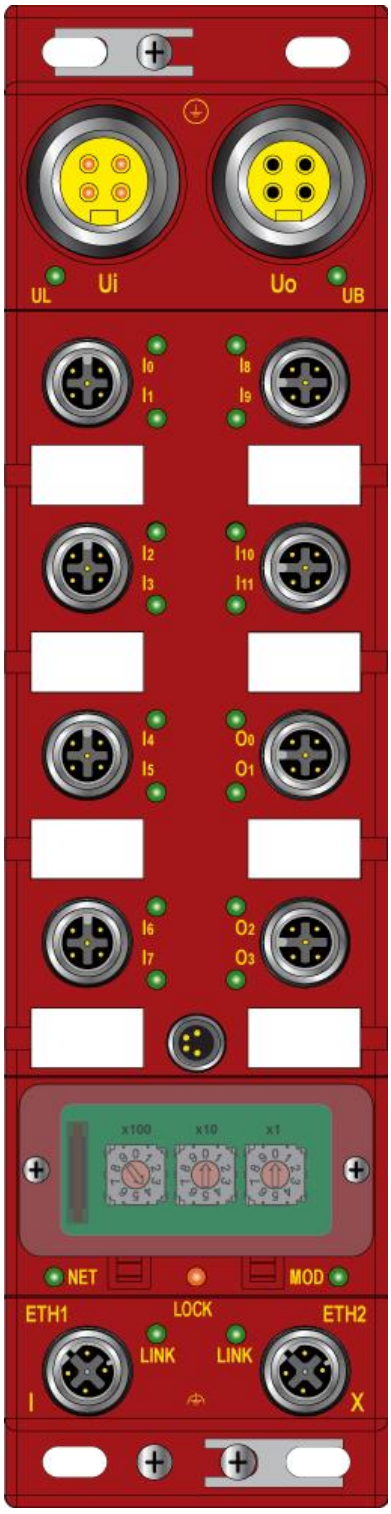
5.2. Mechanische Eigenschaften

Größe und Abmessungen (in mm)



5.3. Physische E/A-Anordnung

BNI CIP-351-000-K015 (BNI00HN)



5.4. Sichere E/A-Baugruppen

Die E/A-Prozessdaten sind über die EtherNet/IP-Baugruppen verfügbar, die auf die erforderlichen Daten angewiesen sind:

- Prozessdaten des Sicherheitseingangs
  - Profil diskreter Sicherheitseingang
    - Baugruppe 524 (20C Hex)
    - Baugruppe 540 (21C Hex)
    - Baugruppe 556 (22C Hex)
    - Baugruppe 579 (243C Hex)
    - Baugruppe 604 (25C Hex)
    - Baugruppe 636 (27C Hex)
  - Herstellerspezifisch
    - Baugruppe 768 (300 Hex):
- Prozessdaten des Sicherheitsausgangs
  - Profil diskreter Sicherheitsausgang
    - Baugruppe 563 (233 Hex)
  - Herstellerspezifisch
    - Baugruppe 769 (301 Hex)
- Konfigurationsdaten
  - Herstellerspezifisch
    - Baugruppe 770 (302 Hex)

5.5. Sichere E/A-Verbindungen

Das E/A-Modul unterstützt

- 1x EO-Verbindung (Exclusive Owner) für die Kontrolle der Prozessdaten für den sicheren Eingang/Ausgang.
- 2x IO-Verbindungen (Input Only) zum Lesen der Prozessdaten für den sicheren Eingang/Ausgang mit einem sicheren oder nicht sicheren EtherNet/IP-Scanner.
- Bis zu 7 LO-Verbindungen (Listen Only) (zum Lesen von sicheren Prozessdaten mit einem nicht sicheren EtherNet/IP-Scanner).

Exclusive Owner

Diese Verbindung ist bidirektional: der Urheber (sichere SPS) produziert Daten, die vom sicheren E/A-Zielmodul verarbeitet werden. Das Ziel wiederum produziert Daten, die der Urheber verarbeitet. Diese Verbindungsart wird EO-Verbindung (Exclusive Owner) oder Kontrollverbindung genannt.

Die EO-Verbindung (Exclusive Owner) wird verwendet, um die Prozessdaten des sicheren Eingangs und des sicheren Ausgangs zu kontrollieren. Es kann nur eine I/O EO-Verbindung eine Eingangs-/Ausgangsverbindung sein.

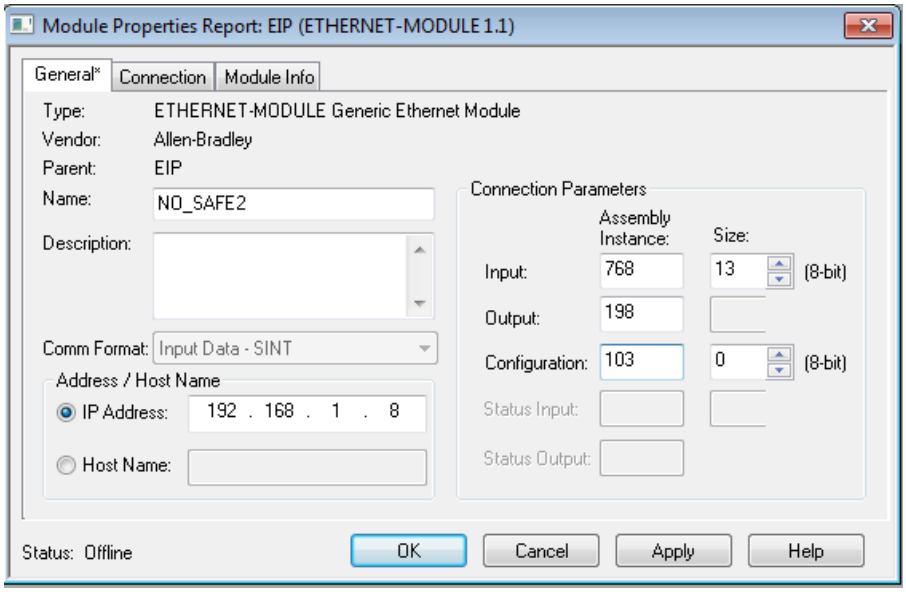
Input Only

Bei dieser Verbindungsart produziert nur das Ziel (Sicheres E/A-Modul) Daten, die vom Urheber (sichere SPS) verarbeitet werden. Der Urheber sendet lediglich ein Heartbeat-Paket, manchmal in einem reduzierten Intervall (seltener als den RPI), mit dem das Sichere E/A-Modul feststellen kann, ob die Verbindung unterbrochen ist. Diese auf den Eingang beschränkte Verbindung kann entweder eine Unicast- oder eine Multicast-Verbindung sein.

Hinweis!

Laden Sie die EDS-Datei vom Sicherheitsmodul hoch, um die Verbindung schnell und einfach zu konfigurieren.

Eingangsbaugruppe	768 (300 Hex), Größe 13 Byte
Ausgangsbaugruppe (Heartbeat)	198 (C6 Hex), Größe 0 Byte
Konfigurationsbaugruppe	103 (67 Hex), Größe 0 Byte



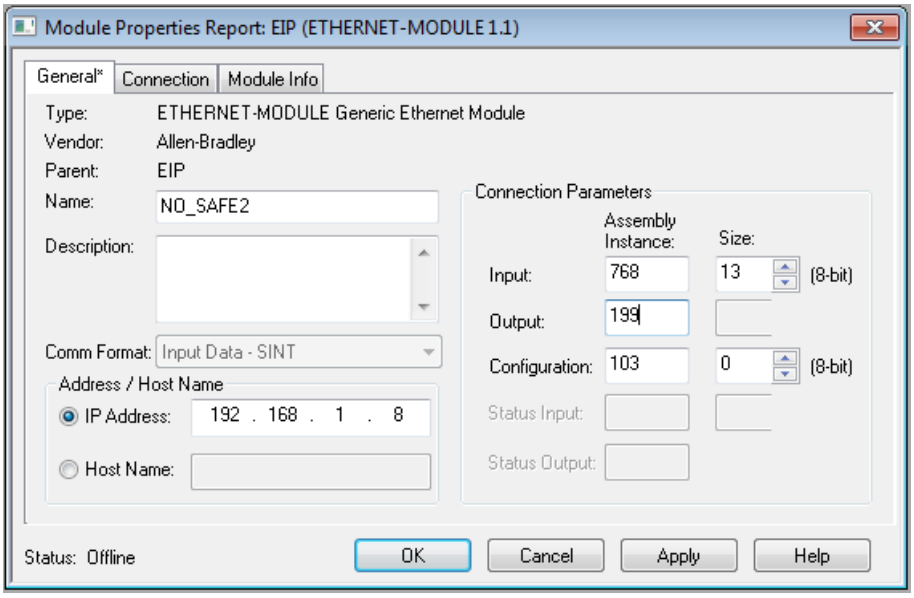
Listen Only

Diese Verbindungsart ist nahezu identisch mit der Input Only-Verbindungsart. Einzige Ausnahme: eine Listen Only-Verbindung kann nur bestehen, wenn eine der anderen E/A-Verbindungsarten (EO) hergestellt wurde. Eine Listen Only-Verbindung kann also nur aufgebaut werden, wenn eine Eingangs-/Ausgangsverbindung oder eine Input Only-Verbindung hergestellt wurde. Umgekehrt gilt: Wenn die letzte Nicht-Listen-Only-Verbindung geschlossen wurde oder abgelaufen ist, wird die Listen Only-Verbindung automatisch ebenfalls geschlossen. Diese Verbindungsart ist die am seltensten verwendete Verbindungsart.

Hinweis!

Laden Sie die EDS-Datei vom Sicherheitsmodul hoch, um die Verbindung schnell und einfach zu konfigurieren.

Eingangsbaugruppe	768 (300 Hex), Größe 13 Byte
Ausgangsbaugruppe (Heartbeat)	199 (C7 Hex), Größe 0 Byte
Konfigurationsbaugruppe	103 (67 Hex), Größe 0 Byte



5.6. Zuordnung von sicheren E/A-Daten

Sichere Eingangsbaugruppen

Profile des diskreten Sicherheitseingangs

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Eingangsdaten (Baugruppe 524 - 20C Hex), Größe: 2 Byte																	
Sicherheits-eingänge	00	n.v.	n.v.	n.v.	n.v.	Sicherer Eingang I11	Sicherer Eingang I10	Sicherer Eingang I9	Sicherer Eingang I8	Sicherer Eingang I7	Sicherer Eingang I6	Sicherer Eingang I5	Sicherer Eingang I4	Sicherer Eingang I3	Sicherer Eingang I2	Sicherer Eingang I1	Sicherer Eingang I0

n.v.: Nicht verwendet
Sicherer Eingang Ix: Prozesswert des Sicherheitseingangs auf Kanal Ix

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Eingangsdaten (Baugruppe 540 – 21C Hex), Größe: 2 Byte																	
Sichere Eingänge + Globaler Status der sicheren Eingänge	00	Komb. Status Sicherer Eingang CIS	n.v.	n.v.	n.v.	Sicherer Eingang I11	Sicherer Eingang I10	Sicherer Eingang I9	Sicherer Eingang I8	Sicherer Eingang I7	Sicherer Eingang I6	Sicherer Eingang I5	Sicherer Eingang I4	Sicherer Eingang I3	Sicherer Eingang I2	Sicherer Eingang I1	Sicherer Eingang I0

n.v.: Nicht verwendet
Sicherer Eingang Ix: Prozesswert des Sicherheitseingangs auf Kanal Ix
Kombinierter Status Sicherer Eingang CIS: Auf “0” setzen, wenn ein Fehler bei einem Sicherheitseingang erkannt wird.

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Eingangsdaten (Baugruppe 556 - 22C Hex), Größe: 3 Byte																	
Sichere Ein-gänge + Status Sicherer Eingang	00	Status Sicherer Eingang I3	Status Sicherer Eingang I2	Status Sicherer Eingang I1	Status Sicherer Eingang I0	Sicherer Eingang I11	Sicherer Eingang I10	Sicherer Eingang I9	Sicherer Eingang I8	Sicherer Eingang I7	Sicherer Eingang I6	Sicherer Eingang I5	Sicherer Eingang I4	Sicherer Eingang I3	Sicherer Eingang I2	Sicherer Eingang I1	Sicherer Eingang I0
	02									Status Sicherer Eingang I11	Status Sicherer Eingang I10	Status Sicherer Eingang I9	Status Sicherer Eingang I8	Status Sicherer Eingang I7	Status Sicherer Eingang I6	Status Sicherer Eingang I5	Status Sicherer Eingang I4

n.v.: Nicht verwendet
Sicherer Eingang Ix: Prozesswert des Sicherheitseingangs auf Kanal Ix
Status Sicherer Eingang Ix: Auf “0” setzen, wenn ein Fehler an Sicherheitseingang Ix erkannt wird

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Eingangsdaten (Baugruppe 579 - 243 Hex), Größe: 1 Byte																	
Status Sicherer Ausgang	00									n.v.	n.v.	n.v.	n.v.	**Status Sicherer Ausgang O3**	**Status Sicherer Ausgang O2**	**Status Sicherer Ausgang O1**	**Status Sicherer Ausgang O0**

n.v.: Nicht verwendet
Status Sicherer Ausgang Ox: Auf “0” setzen, wenn ein Fehler an Sicherheitsausgang Ox erkannt wird

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Eingangsdaten (Baugruppe 604 - 25C Hex), Größe: 2 Byte																	
Sichere Eingänge + Globaler Status der sicheren Eingänge + Globaler Status der sicheren Ausgänge	00	**Komb. Status Sicherer Eingang CIS**	**Komb. Status Sicherer Ausgang COS**	n.v.	n.v.	**Sicherer Eingang I11**	**Sicherer Eingang I10**	**Sicherer Eingang I9**	**Sicherer Eingang I8**	**Sicherer Eingang I7**	**Sicherer Eingang I6**	**Sicherer Eingang I5**	**Sicherer Eingang I4**	**Sicherer Eingang I3**	**Sicherer Eingang I2**	**Sicherer Eingang I1**	**Sicherer Eingang I0**

n.v.: Nicht verwendet
Sicherer Eingang Ix: Prozesswert des Sicherheitseingangs auf Kanal Ix
Kombinierter Status Sicherer Eingang CIS: Auf “0” setzen, wenn ein Fehler bei einem Sicherheitseingang erkannt wird
Kombinierter Status Sicherer Ausgang COS: Auf “0” setzen, wenn ein Fehler bei einem Sicherheitsausgang erkannt wird

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Eingangsdaten (Baugruppe 636 - 27C Hex), Größe: 3 Byte																	
Sichere Eingänge + Globaler Status der sicheren Eingänge	00	**Komb. Status Sicherer Eingang CIS**	n.v.	n.v.	n.v.	**Sicherer Eingang I11**	**Sicherer Eingang I10**	**Sicherer Eingang I9**	**Sicherer Eingang I8**	**Sicherer Eingang I7**	**Sicherer Eingang I6**	**Sicherer Eingang I5**	**Sicherer Eingang I4**	**Sicherer Eingang I3**	**Sicherer Eingang I2**	**Sicherer Eingang I1**	**Sicherer Eingang I0**
Status Sicherer Ausgang	02									n.v.	n.v.	n.v.	n.v.	**Status Sicherer Ausgang O3**	**Status Sicherer Ausgang O2**	**Status Sicherer Ausgang O1**	**Status Sicherer Ausgang O0**

n.v.: Nicht verwendet
Sicherer Eingang Ix: Prozesswert des Sicherheitseingangs auf Kanal Ix
Kombinierter Status Sicherer Eingang CIS: Auf “0” setzen, wenn ein Fehler bei einem Sicherheitseingang erkannt wird
Status Sicherer Ausgang Ox: Auf “0” setzen, wenn ein Fehler an Sicherheitsausgang Ox erkannt wird

Herstellerspezifisch

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Eingangsdaten (Baugruppe 768 - 300 Hex), Größe: 13 Byte																	
Sicherheits-eingänge	00	n.v.	n.v.	n.v.	n.v.	**Sicherer Eingang I11**	**Sicherer Eingang I10**	**Sicherer Eingang I9**	**Sicherer Eingang I8**	**Sicherer Eingang I7**	**Sicherer Eingang I6**	**Sicherer Eingang I5**	**Sicherer Eingang I4**	**Sicherer Eingang I3**	**Sicherer Eingang I2**	**Sicherer Eingang I1**	**Sicherer Eingang I0**
Status Sicherer Eingang	02	n.v.	n.v.	n.v.	n.v.	**Status Sicherer Eingang I11**	**Status Sicherer Eingang I10**	**Status Sicherer Eingang I9**	**Status Sicherer Eingang I8**	**Status Sicherer Eingang I7**	**Status Sicherer Eingang I6**	**Status Sicherer Eingang I5**	**Status Sicherer Eingang I4**	**Status Sicherer Eingang I3**	**Status Sicherer Eingang I2**	**Status Sicherer Eingang I1**	**Status Sicherer Eingang I0**
Wert Testausgang	04	n.v.	n.v.	n.v.	n.v.	**Test-ausgang TO11**	**Test-ausgang TO10**	**Test-ausgang TO9**	**Test-ausgang TO8**	**Test-ausgang TO7**	**Test-ausgang TO6**	**Test-ausgang TO5**	**Test-ausgang TO4**	**Test-ausgang TO3**	**Test-ausgang TO2**	**Test-ausgang TO1**	**Test-ausgang TO0**
Status Testausgang	06	n.v.	n.v.	n.v.	n.v.	**Status Test-ausgang TOS11**	**Status Test-ausgang TOS10**	**Status Test-ausgang TOS9**	**Status Test-ausgang TOS8**	**Status Test-ausgang TOS7**	**Status Test-ausgang TOS6**	**Status Test-ausgang TOS5**	**Status Test-ausgang TOS4**	**Status Test-ausgang TOS3**	**Status Test-ausgang TOS2**	**Status Test-ausgang TOS1**	**Status Test-ausgang TOS0**
Über-wachung Sichere Ausgänge	08	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	**Über-wachung Sicherer Ausgang O3**	**Über-wachung Sicherer Ausgang O2**	**Über-wachung Sicherer Ausgang O1**	**Über-wachung Sicherer Ausgang O0**
Status Sicherer Ausgang	10	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	**Status Sicherer Ausgang O3**	**Status Sicherer Ausgang O2**	**Status Sicherer Ausgang O1**	**Status Sicherer Ausgang O0**
Sonstiges	12									**Fehler Überstrom Eingang UB**	**Fehler Überstrom Ausgang UL**	**Status Muting-Lampe TO7**	**Status Muting-Lampe TO3**	**Komb. Status Sicherer Eingang CIS**	**Komb. Status Sicherer Ausgang COS**	**Fehler Eingangs-strom UB**	**Fehler Ausgangs-strom UL**

n.v.: Nicht verwendet

Sicherer Eingang Ix: Prozesswert des Sicherheitseingangs auf Kanal Ix
Testausgang TOx: Prozesswert Sicherer Ausgang auf Kanal Testausgang TOx
Überwachung Sicherer Ausgang Ox: Prozesswert Sicherer Ausgang auf Kanal Ox für SPS-Überwachung.

Status Sicherer Eingang Ix: Auf “0” setzen, wenn ein Fehler an Sicherheitseingang Ix erkannt wird
Status Testausgang TOSx: Auf “0” setzen, wenn ein Fehler an Testausgang TOx erkannt wird
Status Sicherer Ausgang Ox: Auf “0” setzen, wenn ein Fehler an Sicherheitsausgang Ox erkannt wird

Kombinierter Status Sicherer Eingang CIS: Auf “0” setzen, wenn ein Fehler bei einem Sicherheitseingang erkannt wird
Kombinierter Status Sicherer Ausgang COS: Auf “0” setzen, wenn ein Fehler bei einem Sicherheitsausgang erkannt wird
Status Muting-Lampe TOx: Auf “0” setzen, wenn ein Fehler wegen eines defekten Kabels der Muting-Lamp auf Kanal x erkannt wird

Fehler Ausgangsstrom UL: Diagnose-Bit für Ausgangstromversorgung (UL)

- Auf “1” setzen, wenn UL außerhalb des gültigen Bereichs ist
- Auf “0” setzen, wenn UL innerhalb des gültigen Bereichs ist

Fehler Eingangsstrom UB: Diagnose-Bit für Logik-/Eingangsstromversorgung (UB)

- Auf “1” setzen, wenn UL außerhalb des gültigen Bereichs ist
- Auf “0” setzen, wenn UL innerhalb des gültigen Bereichs ist

Hinweis!

Sichere Eingänge, die als “nicht verwendet” konfiguriert sind, melden einen Prozesswert von 0 und einen Sicherheitsstatus von 1.

Sicherheitsausgänge

Profil diskreter Sicherheitsausgang

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Ausgangsdaten (Baugruppe 563 - 233 Hex), Größe: 1 Byte																	
Sichere Ausgänge	00									n.v.	n.v.	n.v.	n.v.	Sicherer Ausgang O3	Sicherer Ausgang O2	Sicherer Ausgang O1	Sicherer Ausgang O0

n.v.: Nicht verwendet

Sicherer Ausgang Ox: Prozesswert Sicherer Ausgang auf Kanal x

Herstellerspezifisch

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Ausgangsdaten (Baugruppe 769 - 301 Hex), Größe: 4 Byte																	
Sichere Ausgänge	00	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	n.v.	Sicherer Ausgang O3	Sicherer Ausgang O2	Sicherer Ausgang O1	Sicherer Ausgang O0
Testausgänge	02	n.v.	n.v.	n.v.	n.v.	Test-ausgang TO11	Test-ausgang TO10	Test-ausgang TO9	Test-ausgang TO8	Test-ausgang TO7	Test-ausgang TO6	Test-ausgang TO5	Test-ausgang TO4	Test-ausgang TO3	Test-ausgang TO2	Test-ausgang TO1	Test-ausgang TO0

n.v.: Nicht verwendet

Sicherer Ausgang Ox: Prozesssteuerungswert Sicherer Ausgang auf Kanal x

Testausgang TOx: Prozesssteuerungswert Testausgang auf Kanal x

Hinweise!

Die für die sicheren Ausgänge bereitgestellten Werte werden ignoriert, wenn die entsprechenden Ausgänge als “nicht verwendet” konfiguriert sind

Die für die Testausgänge bereitgestellten Werte werden ignoriert, wenn die entsprechenden Testausgänge als “Standardausgang” konfiguriert sind

Konfigurationsdaten

Hinweis!
Die Datengröße kann auf “0” gesetzt werden, wenn der Sichere EtherNet/IP CIP-Scanner keine Konfigurationsdaten beim Herstellen der Verbindung senden muss (Sichere Forward Open-Anfrage), was beispielsweise bei Rockwell Sicherheits-Steuerungen der Fall ist.

Hinweis!
Die Beschreibung der Konfigurationsdaten in der folgenden Tabelle dient nur Informationszwecken. Die Konfigurationsdaten werden direkt von der Balluff SNCT-Software verwaltet und gesendet.

Herstellerspezifisch

	Byte Versatz	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Konfiguration (Baugruppe 770 - 302 Hex), Größe: 123 Byte																	
Version	00	**Nebenversion**								**Hauptversion**							
Testausgangsmodus	02	**Testausgang O_1**								**Testausgang O_0**							
	04	**Testausgang O_3**								**Testausgang O_2**							
	06	**Testausgang O_5**								**Testausgang O_4**							
	08	**Testausgang O_7**								**Testausgang O_6**							
	10	**Testausgang O_9**								**Testausgang O_8**							
	12	**Testausgang O_{11}**								**Testausgang O_{10}**							
Ausgangsfehler Haltezeit	14	**Haltezeit für Ausgangsfehler**															
Ausgangsmodus & Impulstestlänge	16	**Impulstestlänge O_0**								**Ausgangsmodus O_0**							
	18	**Impulstestlänge O_1**								**Ausgangsmodus O_1**							
	20	**Impulstestlänge O_2**								**Ausgangsmodus O_2**							
	22	**Impulstestlänge O_3**								**Ausgangsmodus O_3**							
Sicherer Doppelausgangs-modus	24	**Doppelausgangsmodus O_3 / O_2**								**Doppelausgangsmodus O_0 / O_1**							
Haltezeit für Eingangsfehler	26	**Haltezeit für Eingangsfehler**															
Parameter – Eingang I_0	28	**AUS → EIN Verzögerung Eingang I_0**															
	30	**EIN → AUS Verzögerung Eingang I_0**															
	32	**Test-Quelleingang I_0**								**Eingangsmodus I_0**							
Parameter – Eingang I_1	34	**AUS → EIN Verzögerung Eingang I_1**															

	36	**EIN → AUS Verzögerung Eingang I1**	
	38	**Test-Quelleingang I1**	**Eingangsmodus I1**
Parameter – Eingang I2	40	**AUS → EIN Verzögerung Eingang I2**	
	42	**EIN → AUS Verzögerung Eingang I2**	
	44	**Test-Quelleingang I2**	**Eingangsmodus I2**
Parameter – Eingang I3	46	**AUS → EIN Verzögerung Eingang I3**	
	48	**EIN → AUS Verzögerung Eingang I3**	
	50	**Test-Quelleingang I3**	**Eingangsmodus I3**
Parameter – Eingang I4	52	**AUS → EIN Verzögerung Eingang I4**	
	54	**EIN → AUS Verzögerung Eingang I4**	
	56	**Test-Quelleingang I4**	**Eingangsmodus I4**
Parameter – Eingang I5	58	**AUS → EIN Verzögerung Eingang I5**	
	60	**EIN → AUS Verzögerung Eingang I5**	
	62	**Test-Quelleingang I5**	**Eingangsmodus I5**
Parameter – Eingang I6	64	**AUS → EIN Verzögerung Eingang I6**	
	66	**EIN → AUS Verzögerung Eingang I6**	
	68	**Test-Quelleingang I6**	**Eingangsmodus I6**
Parameter – Eingang I7	70	**AUS → EIN Verzögerung Eingang I7**	
	72	**EIN → AUS Verzögerung Eingang I7**	
	74	**Test-Quelleingang I7**	**Eingangsmodus I7**
Parameter – Eingang I8	76	**AUS → EIN Verzögerung Eingang I8**	
	78	**EIN → AUS Verzögerung Eingang I8**	
	80	**Test-Quelleingang I8**	**Eingangsmodus I8**
Parameter – Eingang I9	82	**AUS → EIN Verzögerung Eingang I9**	
	84	**EIN → AUS Verzögerung Eingang I9**	
	86	**Test-Quelleingang I9**	**Eingangsmodus I9**
Parameter – Eingang I10	88	**AUS → EIN Verzögerung Eingang I10**	
	90	**EIN → AUS Verzögerung Eingang I10**	
	92	**Test-Quelleingang I10**	**Eingangsmodus I10**
Parameter – Eingang I11	94	**AUS → EIN Verzögerung Eingang I11**	
	96	**EIN → AUS Verzögerung Eingang I11**	
	98	**Test-Quelleingang I11**	**Eingangsmodus I11**
Sicherer Dualmodus	100	n.v.	**Sicherer Dual-Eingangsmodus I1 / I0**
Sicherer Dualmodus Diskrepanzzeit	102	**Diskrepanz Betrieb Eingang I1 / I0**	

Sicherer Dualmodus	104	n.v.	**Sicherer Dual-Eingangsmodus I3 / I2**
Sicherer Dualmodus Diskrepanzzeit	106		**Diskrepanz Betrieb Eingang I3 / I2**
Sicherer Dualmodus	108	n.v.	**Sicherer Dual-Eingangsmodus I5 / I4**
Sicherer Dualmodus Diskrepanzzeit	110		**Diskrepanz Betrieb Eingang I5 / I4**
Sicherer Dualmodus	112	n.v.	**Sicherer Dual-Eingangsmodus I7 / I6**
Sicherer Dualmodus Diskrepanzzeit	114		**Diskrepanz Betrieb Eingang I7 / I6**
Sicherer Dualmodus	116	n.v.	**Sicherer Dual-Eingangsmodus I9 / I8**
Sicherer Dualmodus Diskrepanzzeit	118		**Diskrepanz Betrieb Eingang I9 / I8**
Sicherer Dualmodus	120	n.v.	**Sicherer Dual-Eingangsmodus I11 / I10**
Sicherer Dualmodus Diskrepanzzeit	122		**Diskrepanz Betrieb Eingang I11 / I10**

Testausgangsmodus
- 0: Nicht verwendet
- 1: Standard
- 2: Impulstest
- 3: Spannungsversorgung
- 4: Muting-Lampe (nur möglich für Eingang 3 und Eingang 7)

Haltezeit für Ausgangsfehler (in ms)
Ein Wert zwischen 0 und 65530; muss ein Vielfaches von 10 sein.

Ausgangsmodus
- 0: Nicht verwendet
- 1: Sicherheit
- 2: Sicherheits-Impulstest

Länge des Ausgangs-Impulstests (in ms)
Ein Wert zwischen 3 und 100.

Modus Sicherer Doppelausgang Ox/Ox+1
- 0: Einzel
- 1: Dual

Haltezeit für Eingangsfehler (in ms)
Ein Wert zwischen 0 und 65530; muss ein Vielfaches von 10 sein.

Eingang Ix Aus → Ein Verzögerung (in ms)
Ein Wert zwischen 0 und 1000.

Eingang Ix Ein → Aus Verzögerung (in ms)
Ein Wert zwischen 0 und 1000.

Modus Eingang Ix
- 0: Nicht verwendet
- 1: Sicherheits-Impulstest
- 2: Sicherheit
- 3: Standard

Eingang Ix Testquelle (nur der Testausgang am selben Anschluss kann in dieser Liste verwendet werden):

- 0: Nicht verwendet
- 1: Testausgang 0
- 2: Testausgang 1
- 3: Testausgang 2
- 4: Testausgang 3
- 5: Testausgang 4
- 6: Testausgang 5
- 7: Testausgang 6
- 8: Testausgang 7
- 9: Testausgang 8
- 10: Testausgang 9
- 11: Testausgang 10
- 12: Testausgang 11

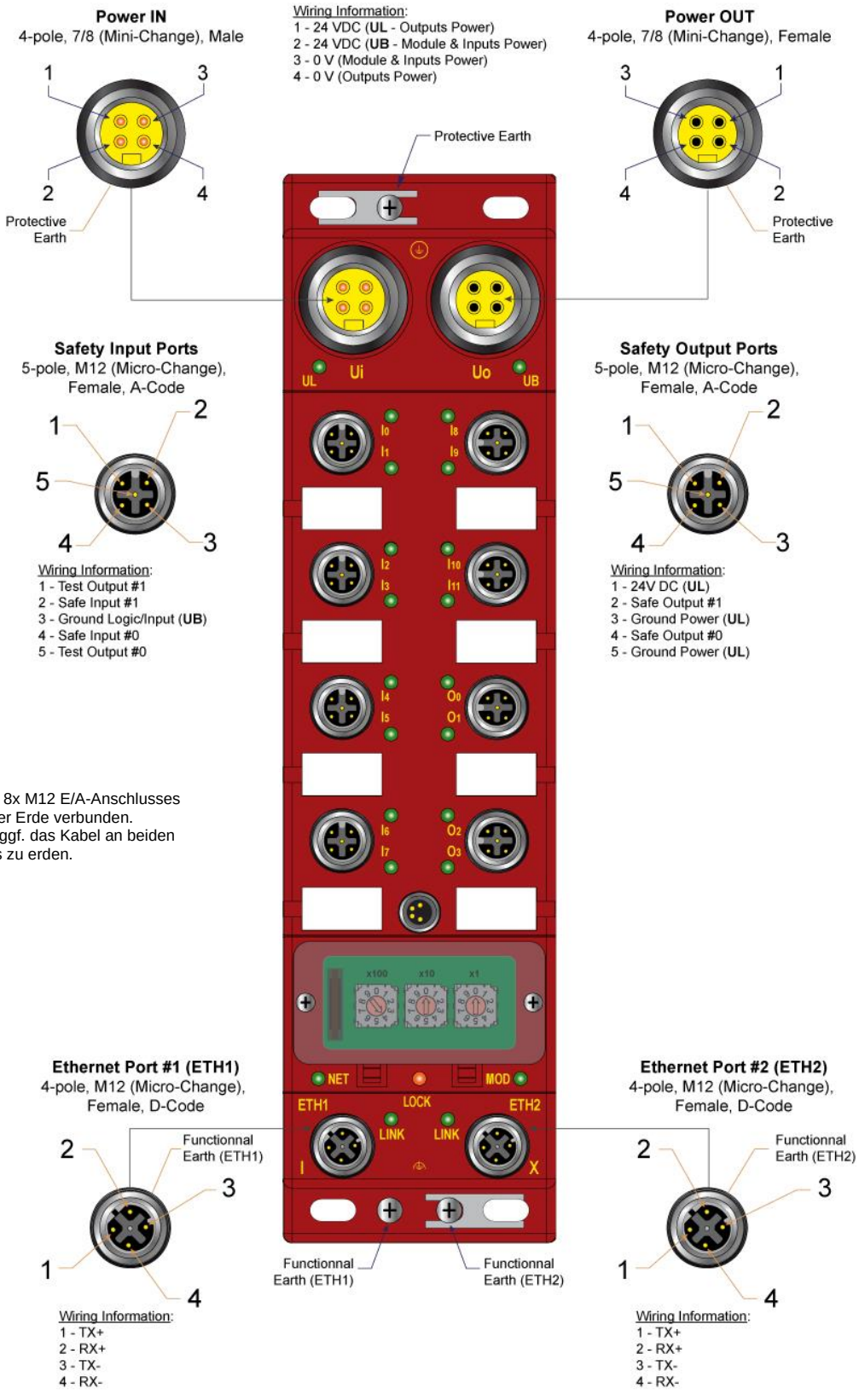
Eingang Ix/Ix+1 Sicherer Dualmodus

- 0: Einzel
- 1: Äquivalent
- 2: Antivalent

Sicherer Dual-Eingang Ix / Ix+1 Diskrepanzzeit (in ms)

Ein Wert zwischen 10 und 30000; muss ein Vielfaches von 10 sein.

5.7. Pinbelegung



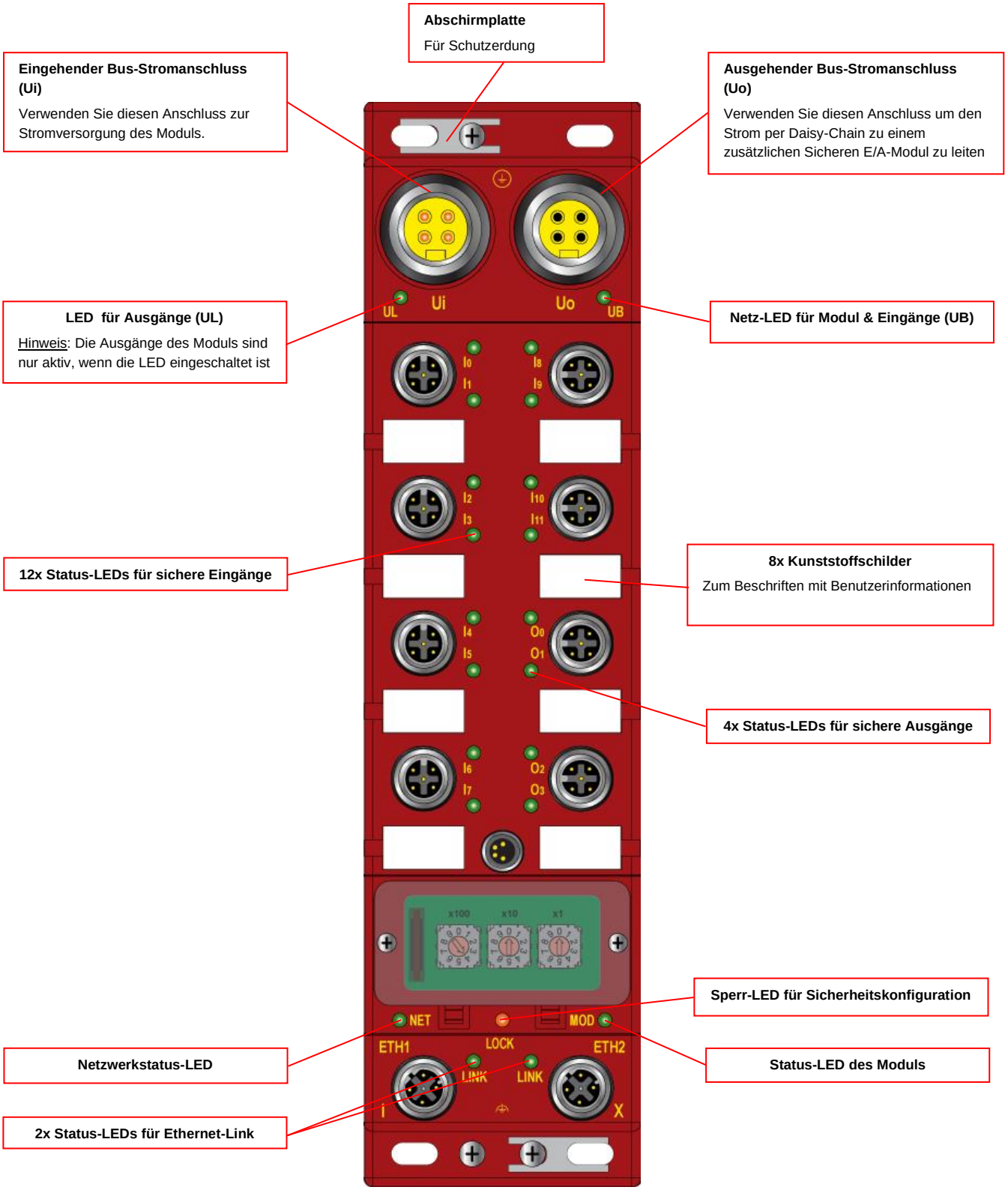
Hinweis!

Die Hülle des 8x M12 E/A-Anschlusses ist nicht mit der Erde verbunden. Spleißen Sie ggf. das Kabel an beiden Enden, um es zu erden.

5.8. LED-Zuweisung

LED-Positionen

Warnung: LEDs sind KEINE verlässlichen Indikatoren und es kann keine Gewähr übernommen werden, dass sie präzise Informationen liefern. Sie sollten NUR für die allgemeine Diagnose während der Inbetriebnahme oder Fehlerbehebung verwendet werden. Versuchen Sie nicht, die LEDs als Betriebsanzeigen zu nutzen.



LED-Zuweisung

Status-LED für Modullogik und Eingangsstrom (UB)

LED-Zustand	Beschreibung
OFF	Modul-Spannungsversorgung nicht angeschlossen
GRÜN	Modul-Spannungsversorgung ist angeschlossen und im gültigen Bereich (24 VDC → -20% bis +25%)
GELB	Modul-Spannungsversorgung wird erkannt, ist aber außerhalb des gültigen Bereichs (24 VDC → -20% bis +25%)

Status-LED Hilfsenergie Modulausgang (UL)

LED-Zustand	Beschreibung
AUS	Modul-Spannungsversorgung nicht angeschlossen
GRÜN	Modul-Spannungsversorgung ist angeschlossen und im gültigen Bereich (24 VDC → -20% bis +25%)
GELB	Modul-Spannungsversorgung wird erkannt, ist aber außerhalb des gültigen Bereichs (24 VDC → -20% bis +25%)

Staus-LEDs für Sicheren Eingang (Ix)

LED-Zustand	Status Sicher-heits-eingang	Beschreibung
OFF	Gut	Eingang ist AUS oder Modul wird konfiguriert.
GELB	Gut	Eingang ist EIN
ROT	Störung	Eine Störung in der Eingangsschaltung wurde erkannt, oder es ist ein Diskrepanzfehler zwischen den beiden Eingängen eines Dual-Eingangspaars aufgetreten.
ROT BLINKEND	Störung	Es wurde ein Fehler in der Eingangsschaltung des Eingangspartners eines Dual-Eingangspaars erkannt, oder es sind nicht behebbare Störungen aufgetreten, die alle Eingänge des Moduls betreffen.

Status-LEDs für Sicheren Ausgang (Ox)

LED-Zustand	Status Sicher-heits-ausgang	Beschreibung
OFF	Gut	Ausgang ist AUS oder Modul wird konfiguriert.
GELB	Gut	Ausgang ist EIN
ROT	Störung	Es wurde eine Störung in der Ausgangsschaltung erkannt, oder die vom Netzwerk empfangenen Werte für die beiden Ausgänge, die als Dual-Ausgangspaar verwendet werden, sind unterschiedlich.
ROT BLINKEND	Störung	Es wurde eine Störung in der anderen Ausgangsschaltung erkannt (unabhängig von der Ausgangskonfiguration: einzeln oder dual), oder es sind nicht behebbare Störungen aufgetreten, die alle Ausgänge des Moduls betreffen.

Status LED für Link- und Netzwerkaktivität (LINK)

LED-Zustand	Negotiation-Geschwindigkeit	Beschreibung
AUS		Kein Netzwerk-Link.
GRÜN BLINKEND	100 Mbps	Link ist aufgebaut und ohne Aktivität.
GRÜN		Link ist aufgebaut und mit Aktivität.
GELB BLINKEND	10 Mbps	Link ist aufgebaut und ohne Aktivität.
GELB		Link ist aufgebaut und mit Aktivität.

Status-LED des Moduls (MOD)

LED-Zustand	Negotiation-Geschwindigkeit	Beschreibung
OFF	Spannungs-versorgung fehlt	Kein Strom am Gerät anliegend.
GRÜN	Betrieb	Das Gerät läuft in einem normalen Zustand.
GRÜN BLINKEND	Leerlauf	Das Gerät ist im Leerlauf oder Standby.
ROT	Kritischer Fehler	Auf dem Gerät ist ein nicht behebbarer Fehler aufgetreten, ggf. Austausch erforderlich.
ROT BLINKEND	Selbsttest	Das Gerät führt einen Selbsttest durch oder muss in Betrieb genommen werden, da die Konfiguration oder TUNID fehlt bzw. unvollständig oder falsch ist.

Netzwerkstatus-LED (NET)

LED-Zustand	Status	Beschreibung
OFF	Kein Strom / Keine IP Adresse	Das Modul ist nicht online. Das Modul wird u.U. nicht mit Strom versorgt, beachten Sie die Status-LED des Moduls (MOD).
GRÜN BLINKEND	Online / Nicht verbunden	Das Modul ist online, hat aber keine Verbindung im festgelegten Zustand (IDLE-Modus).
GRÜN	Link OK / online / verbunden	Das Modul ist online und hat Verbindung im festgelegten Zustand (EXECUTING-Modus).
ROT BLINKEND	Verbindungs-Timeout	Eine oder mehrere E/A-Verbindungen sind in einem Timeout-Zustand.
ROT	Kritischer Link-Fehler	Ausgefallenes Kommunikationsgerät. Das Modul hat einen Fehler erkannt, der die Kommunikation im Netzwerk unmöglich macht.
ROT / GRÜN BLINKEND	Kommunikation gestört	Eine spezifische Kommunikation ist gestört (Gerät verwendet diese Anzeige, um dem Wartungspersonal die Inbetriebnahme der TUNID in einem sicheren Gerät zu ermöglichen).

Status-LED für Konfigurationssperre des Moduls (LOCK)

LED-Zustand	Modus	Beschreibung
OFF	entweder keine Konfiguration oder konfiguriert durch einen CIP Safety Originator	Das Modul ist nicht konfiguriert oder wurde von einem sicheren Urheber konfiguriert (FW Open Typ 1).
GELB	Konfiguration gesperrt	Gültige Konfiguration empfangen und gesperrt.
GELB BLINKEND	Konfiguration nicht gesperrt	Gültige Konfiguration empfangen und nicht gesperrt.
ROT	Modulstörungen	Fehlerhafte Sicherheitskonfiguration

6. Installation und Beschaltung des Produkts

In diesem Kapitel werden die Beschaltungsmöglichkeiten und die entsprechenden Sicherheitskategorien beschrieben.

6.1. Spannungsversorgung

Das sichere E/A-Modul muss mit 2 separaten Netzteilen versorgt werden:

- 1x 24 VDC für Modullogik und Sicherheitseingänge
- 1x 24 VDC für Hilfsenergie für Sicherheitsausgänge

Warnung!

Gemäß den Anforderungen der CE-Richtlinie muss das Modul über eine Quelle mit Sicherheitskleinspannung (SELV) oder mit geschützter Kleinspannung versorgt werden.

Hinweis!

Die 2 Erdungskreise sind getrennt (also voneinander isoliert).

Warnung!

- Der maximale Gesamtstrom für den Logik-/Eingangsstrom (UB) darf nicht höher als 8 A sein.
- Der maximale Gesamtstrom für die Ausgangsstromversorgung (UL) darf nicht höher als 8 A sein.
- Der Strom wird überwacht, um bei einem Überschreiten des Maximalwerts in den ausfallsicheren Zustand wechseln zu können.

Warnung!

Das für Sicherheitsanwendungen zuständige Personal muss kontrollieren, ob der maximale Stromverbrauch niedriger als der Maximalwert in allen unterstützten Temperaturbereichen ist.

Warnung!

Ein Überstromschutz sollte vor dem Sicheren E/A-Modul platziert werden, um eine Zerstörung des Moduls beim Auftreten einer Überstromsituation zu verhindern.

Die Pin-Beschreibung der Stromanschlüsse des Moduls finden Sie hier.

6.2. Ethernet-Verbindung

6.3. Port-Bezeichnung

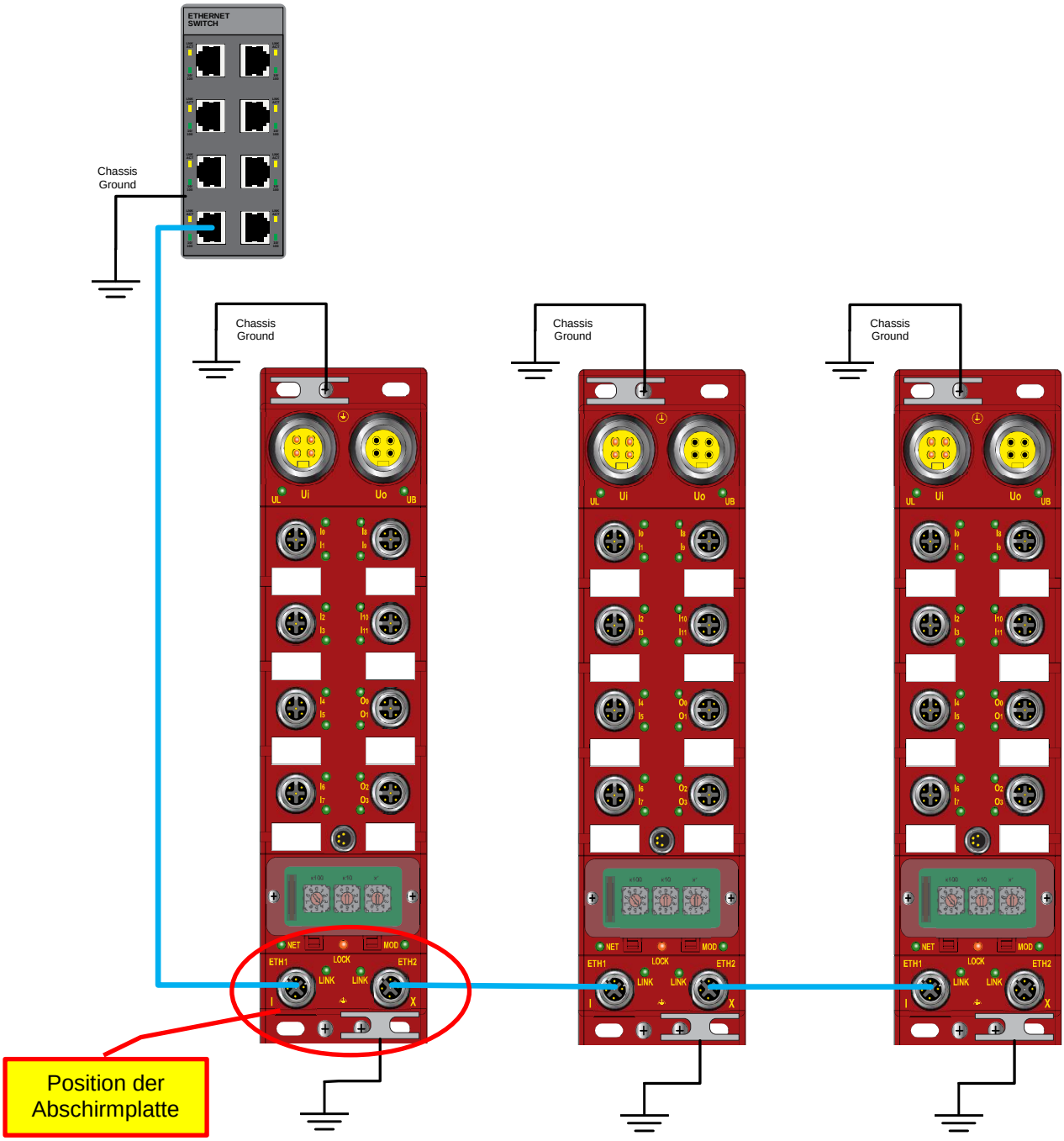
Das Sichere E/A-Modul besitzt einen Ethernet-Switch mit zwei Ports, die mit **ETH1** und **ETH2** beschriftet sind.

6.4. Beschaltung

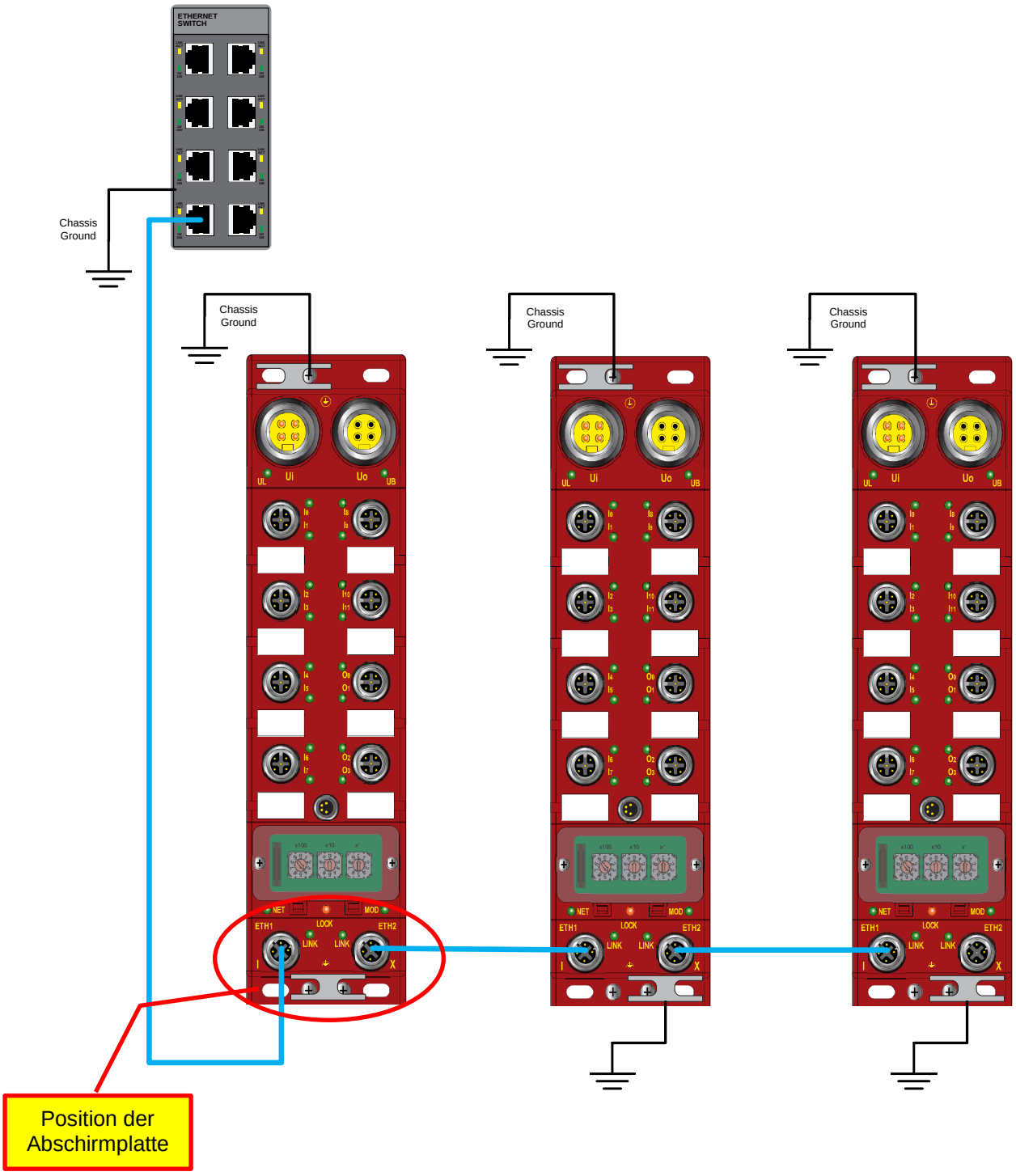
Das Sichere E/A-Modul erfüllt standardmäßig die Anforderungen der ODVA-Empfehlungen:

- Die Abschirmung des linken M12-Anschlusses (ETH1) ist nicht mit der Funktionserde verbunden.
- Die Abschirmung des rechten M12-Anschlusses (ETH2) ist mit der Funktionserde (FE) verbunden.

Diese Konfiguration ermöglicht die folgende Beschaltung:



Eine externe Abschirmplatte ermöglicht die Verbindung zwischen den beiden abgeschirmten Ethernet-Anschlüssen. Dadurch kann die folgende Beschaltung realisiert werden:

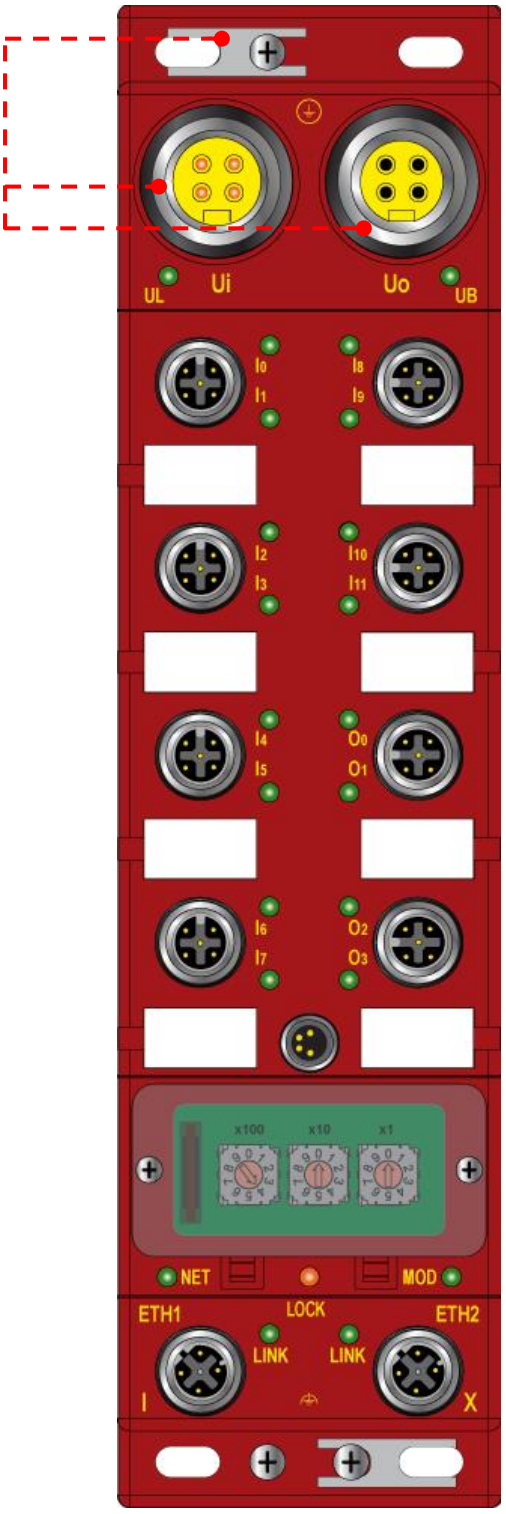


6.5. Modul-Erdung

Achtung!

Für den ordnungsgemäßen Betrieb des Moduls wird empfohlen, dass mindestens eine der Erdungsverbindungen (siehe folgende Abbildung) geerdet ist.

Funktionserde N°0 (FE0)

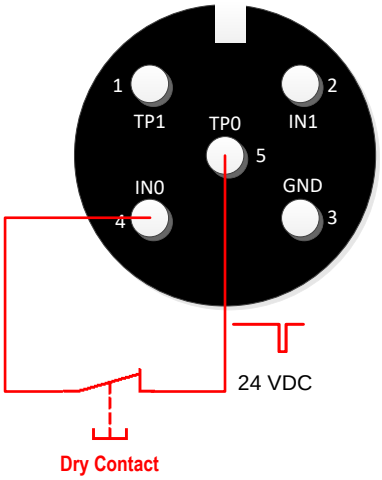
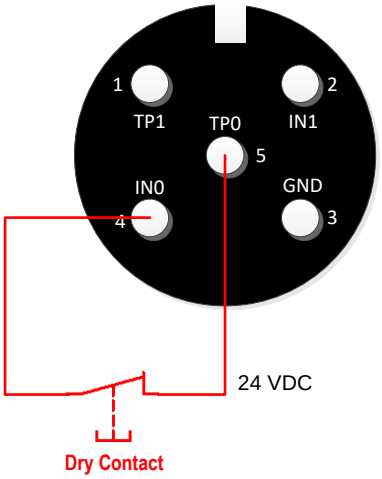


6.6. E/A-Beschaltung

In der folgenden Tabelle werden verschiedene sichere E/A-Beschaltungen mit ihren entsprechenden Sicherheitskategorien aufgeführt:

Beschaltungen für Sicherheitseingänge

Einzelkanal

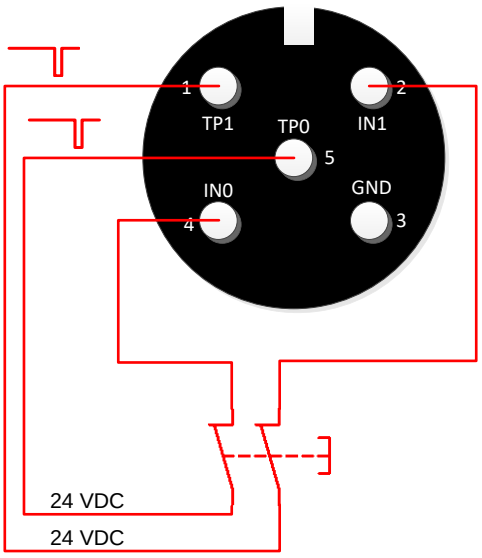
Gerät	Impulstest von Testausgang	Beschaltung des M12-Ports	Sicherheit Kategorie
Drucktaster	Ja TP0 ist als 24-V-Spannungsversorgung mit Impulstest konfiguriert		2
	Nein TP0 ist als 24-V-Spannungsversorgung konfiguriert		1

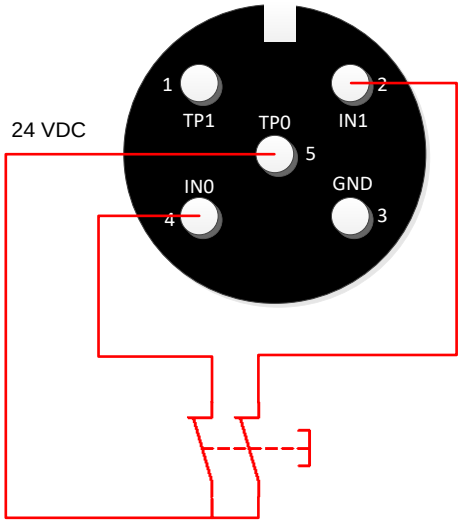
Zweikanal

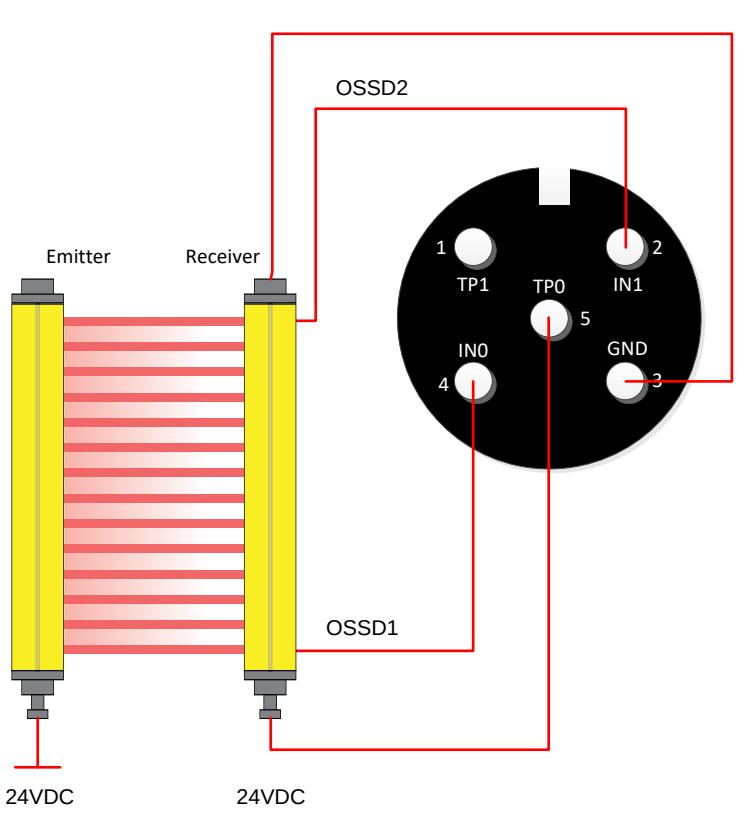
<table>
<tr><th>Gerät</th><th>Impulstest von Testausgang</th><th>Beschaltung des M12-Ports</th><th>Sicherheit Kategorie</th></tr>
<tr><td rowspan="2">Not-Halt

oder

Tür-Überwachung</td><td>Ja

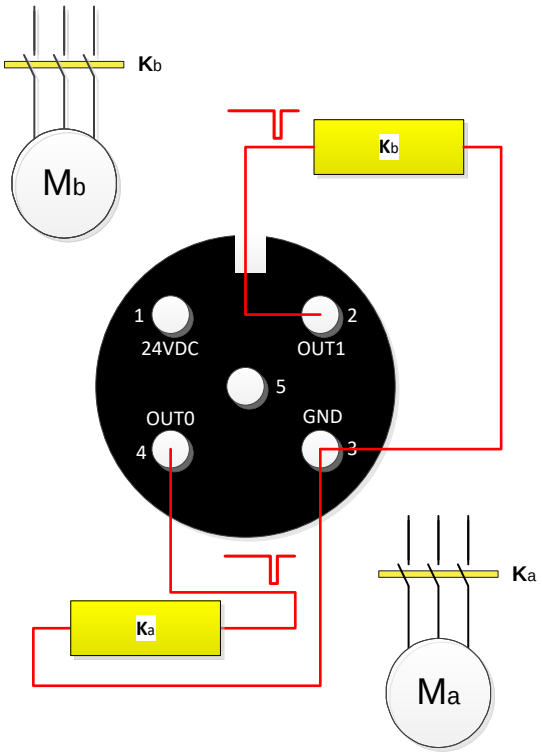
TP0 und TP1 sind als 24-V-Spannungsversorgung mit Impulstest konfiguriert</td><td> 
</td><td>4</td></tr>
<tr><td>Nein

TP0 ist als 24-V-Spannungsversorgung konfiguriert</td><td> 
</td><td>3</td></tr>
</table>

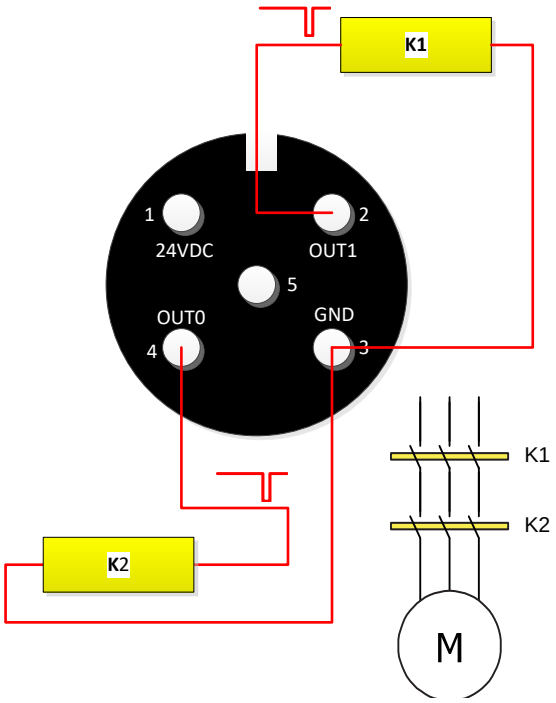
Gerät	Impulstest	Beschaltung des M12-Ports	Sicherheit Kategorie
Lichtvor-hang	Nein TP0 ist als 24-V-Spannungs-versorgung konfiguriert		3 oder 4 in Abhängig-keit vom Licht-vorhang

Beschaltung des Sicherheitsausgangs

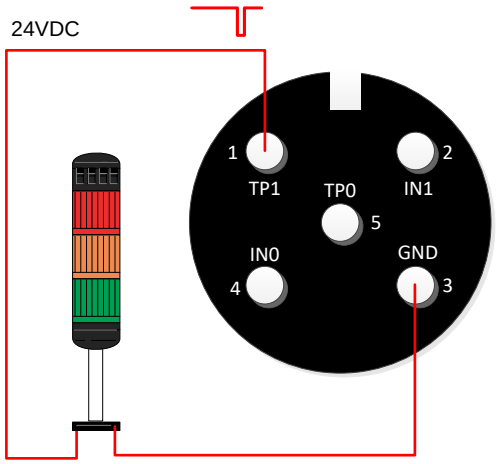
Einzelkanal

Gerät	Impulstest	Beschaltung des M12-Ports	Sicherheit Kategorie
Relais	**Ja** OUT0 und OUT1 sind als Einzelkanal mit Impulstest konfiguriert		3

Zweikanal

Gerät	Impulstest	Beschaltung des M12-Ports	Sicherheit Kategorie
Relais	**Ja** OUT0 und OUT1 sind als Doppelkanal mit Impulstest konfiguriert		4

Beschaltung der Muting-Lampe

Gerät	Impulstest von Testausgang	Beschaltung des M12-Ports	Sicherheit Kategorie
Muting-Lampe	Ja Nur verfügbar, wenn TO_3 oder TO_7 als ein Ausgang der Muting-Lampe konfiguriert ist		ns

Hinweis!
Eine Muting-Lampe ist keine Sicherheitskomponente.

7. Produktbereitstellung

In diesem Kapitel wird anhand eines Beispiels die Vorgehensweise bei der Inbetriebnahme des Sicheren E/A-Moduls mit dem Balluff SNCT-Konfigurationstool und mit der RSLogix™ 5000-Software von Rockwell Automation in der Version 20 beschrieben.

7.1. Erste Schritte

Warnung!
Unkontrollierte Prozesse können zu Verletzungen und Sachschäden führen.

Warnung!
Verwenden Sie nur Komponenten, die der Sicherheitsnorm für die jeweilige erforderliche Sicherheitsstufe entsprechen.

Es wird empfohlen, sich bezüglich der Bewertung des Gesamtsystems an eine Zertifizierungsstelle zu wenden.

Sie müssen die Art der verwendeten Sicherheitskomponenten, einschließlich des Sicheren E/A-Moduls, definieren.
Das ist erforderlich, um die Parameter der gesamten Sicherheitsfunktion berechnen zu können.

Die Sicherheitsfunktion muss das Ergebnis einer Risikobewertung sein.

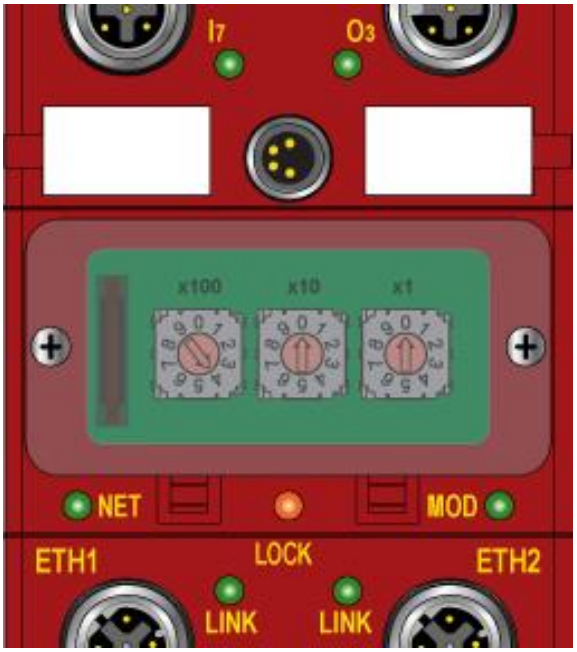
7.2. IP-Adresseinstellung

Das Sichere E/A-Modul wird standardmäßig im DHCP-Modus konfiguriert.

Bei der Einbindung in ein Netzwerk mit einem DHCP-Server wird dem Modul automatisch eine IP-Adresse zugewiesen.

Festlegen der IP-Adresse mit den 3 Drehschaltern

Sie können den DHCP-Vorgang beenden (wenn kein DHCP-Server im Netzwerk vorhanden ist), indem Sie die 3 Drehschalter im Fensterbereich des Moduls auswählen.



Warnung!
Verwenden Sie zum Drehen der Drehschalter einen Kunststoffschraubendreher oder tragen Sie antistatische Ausrüstung.

Positionen und Verhalten der 3 Drehschalter

<table>
<tr><th>Modus</th><th>Drehschalter x100</th><th>Drehschalter x10</th><th>Drehschalter x1</th><th>Beschreibungen</th></tr>
<tr><td>Statische Adresse</td><td>x
[0 bis 2]</td><td>y
[0 bis 9]</td><td>z
[0 bis 9]</td><td>Überschreiben Sie das 4. Byte der IP-Adresse im Flash-Speicher.

IP-Adresse: 192.168.1.xyz
IP-Maske: 255.255.255.0
Gateway: 192.168.1.1 (wenn aber die IP-Adresse
192.168.1.1 lautet, ist die Gateway-Adresse 0.0.0.0).

Hinweis!
Es können Adressen (xyz) im Bereich von 1 bis 254 zugewiesen werden. Ungültige Einstellung (z.B. 000 oder 255 oder 278…) führt zu einem Fall (a,b,c in dieser Tabelle).

Hinweis!
Die IP-Maskenadresse und die Gateway-Adresse sind im Flash-Speicher des Moduls gespeichert.
Zum Ändern dieser Parameter müssen Sie einen expliziten Meldungsbefehl an das Modul senden. Siehe Abschnitt hier.

Hinweis!
In diesem Modus ist es nicht möglich, eine IP-Adresse mit Expliziten CIP-Meldungen (0xF5 TCP/IP-Objekt) zu speichern.</td></tr>
<tr><td>DHCP Modus</td><td>4</td><td>u</td><td>v</td><td>Das Sichere E/A-Modul erhält seine IP-Adresse, seine IP-Maskenadresse und seine Gateway-Adresse entsprechend der DHCP-Methode.

Hinweis!
Für diesen Modus muss ein DHCP-Server-Equipment im Netzwerk aktiv sein, um eine IP-Adresse bereitzustellen.</td></tr>
</table>

				Hinweis! Wenn **u** = **v** = 0 → DHCP basierend auf MAC-Adresse Wenn **uv** = [01 .. 99] → DHCP basierend auf Client-ID
				Hinweis! Modul sendet Anfrage dauerhaft.
				Hinweis! In diesem Modus ist es nicht möglich, eine IP-Adresse mit Expliziten CIP-Meldungen (0xF5 TCP/IP-Objekt) zu speichern.

Firmware-Update	**9**	**9**	**9**	Das Modul wechselt in den Modus für das FPGA- und Firmware-Update. **Hinweis!** Wenden Sie sich für weitere Informationen bitte an den technischen Support von Balluff.

Gespeicherte Adresse (alle anderen Drehschalterpositionen)	**a**	**b**	**c**	Das Sichere E/A-Modul erhält seine IP-Adresse, seine IP-Maskenadresse und seine Gateway-Adresse entsprechend den im Flash-Speicher abgelegten Informationen. **Hinweis!** **a,b,c** bezeichnen Einstellungen, die nicht weiter oben in dieser Tabelle beschrieben werden (z.B. die folgenden Positionen: 000, [255 .. 399], [500 .. 998]). **Hinweis!** In diesem Modus können die TCP/IP-Adressinformationen mit einem EtherNet/IP-Inbetriebnahmetool (mit dem 0xF5 TCP/IP-Objekt) gespeichert werden. **Hinweis!** Wenn das Modul noch nicht in Betrieb genommen wurde, startet das Sichere E/A-Modul im DCHP-Modus, um seine erste IP-Adresse abzurufen.

Hinweis!

Die Drehschalterposition wird NUR beim Start des Sicheren E/A-Moduls gelesen. Wenn die Position geändert wird, muss das Modul aus- und wieder eingeschaltet werden (EIN → AUS → EIN).

Hinweis!

Wenn DHCP zum gespeicherten Modus geändert wird, werden alle IP-Einstellungen (Adresse, Maske, Gateway) so in den Modulen gespeichert, wie sie während der DHCP-Transaktion (vom DHCP-Server vorgegeben) festgelegt wurden.

Warnung!

Nach dem Festlegen der IP-Adresse sollte das Fenster geschlossen und während des Arbeitsablaufs nicht mehr geöffnet werden.

Warnung!

Das Modulfenster muss mit einem Drehmoment von 0,4 Nm verschraubt werden, um die korrekte Abdichtung gemäß der Schutzklasse IP67 zu gewährleisten.

Festlegen der IP-Adresse des Moduls mit Expliziten EtherNet/IP-Meldungen

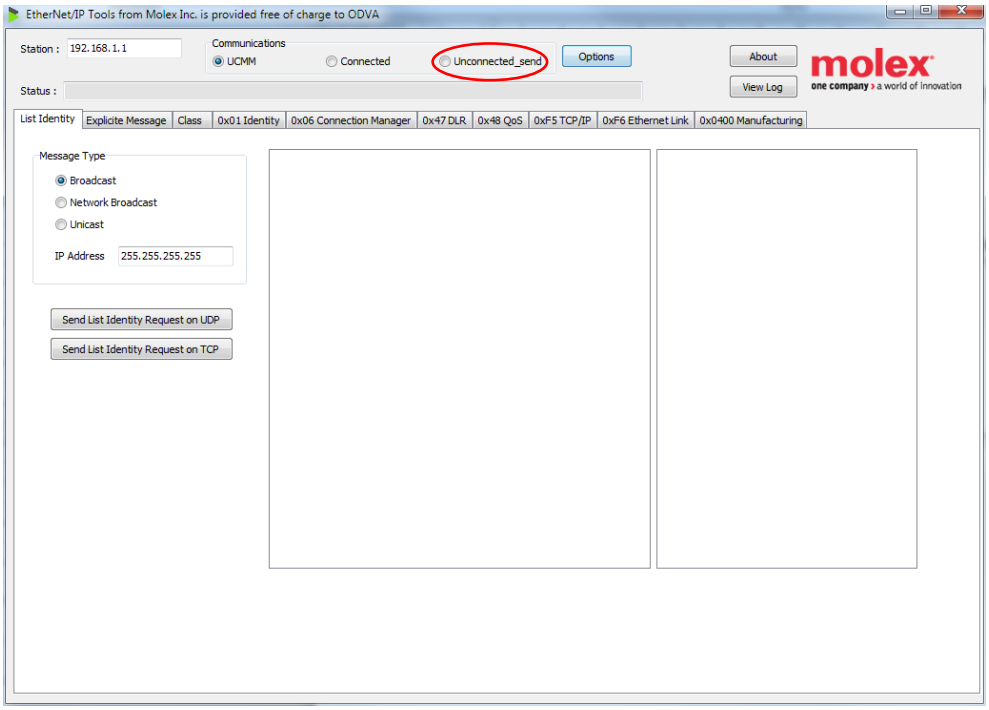
1. *Verwenden der EtherNet/IP-Tools*

   Zum Ändern der IP-Einstellungen des Moduls müssen Sie ein *Ethernet/IP-Softwaretool* verwenden, das *Explizite Meldungsanfragen* verwaltet, um auf CIP-Objekte des Moduls (0xF5 TCP/IP) zuzugreifen und Parameter wie die folgenden festzulegen:
   - Statische oder dynamische IP-Adressierung
   - IP-Adresse
   - Netzwerkmaske
   - usw.

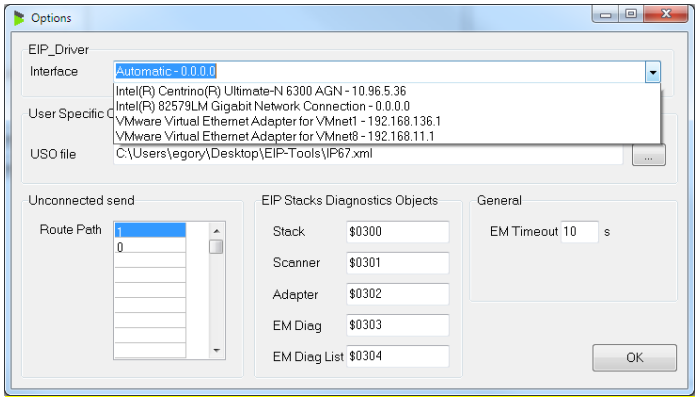
   Ein *EtherNet/IP-Softwaretool* kann hier kostenfrei heruntergeladen werden.

   Es gibt keine Installationsroutine. Kopieren Sie die Dateien einfach in einen neuen Ordner und starten Sie die Datei *EIP_Tools.exe*.

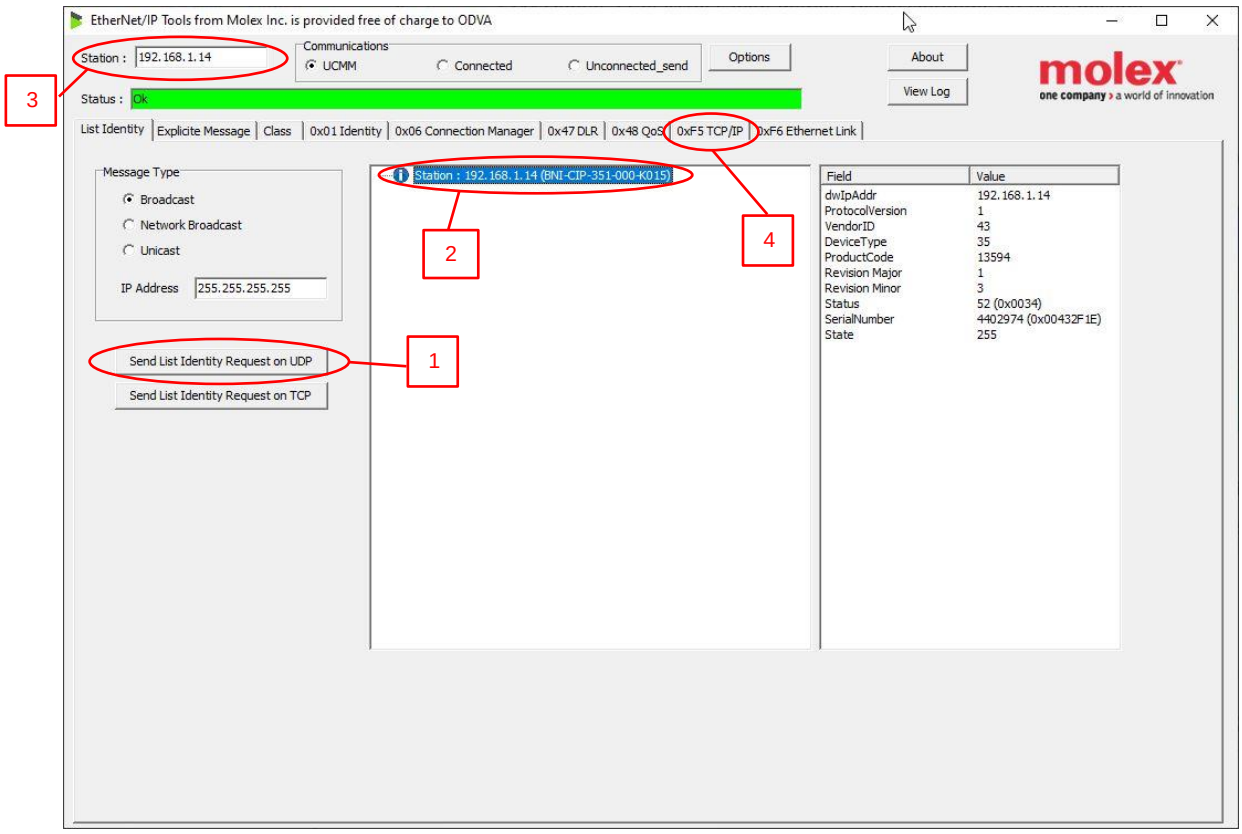
   Klicken Sie auf *Options* (Optionen).



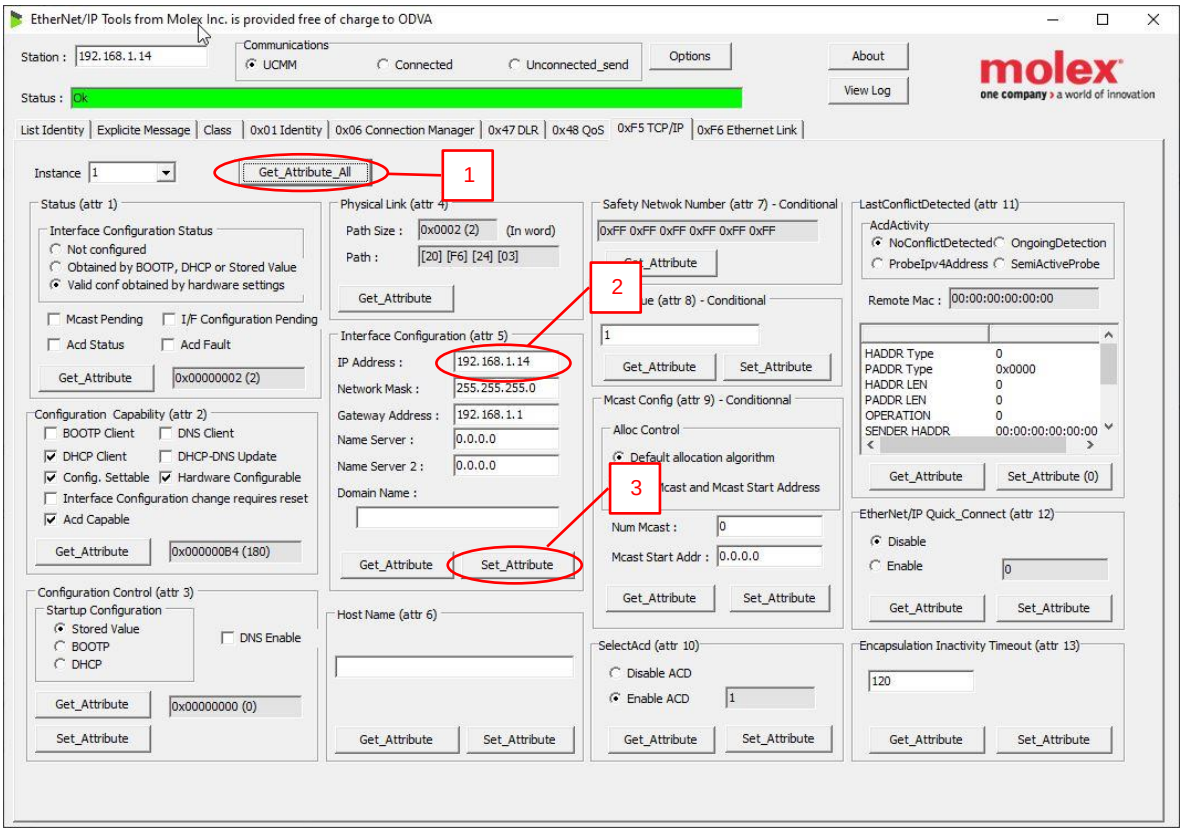
   Wählen Sie die Ethernet-Schnittstelle des Computer-Netzwerks aus und klicken Sie auf OK.



Wählen Sie *Send List Identity Request on UDP* (Listen-Identitätsanfrage auf UDO senden), um alle mit dem Netzwerk verbundenen EtherNet/IP-Geräte zu erkennen. Klicken Sie dann auf ein EtherNet/IP-Gerät in der Stationsliste, um es auszuwählen. Für das ausgewählte Gerät sollte im Bereich *Station:* <IP> die IP-Adresse festgelegt sein.



Klicken Sie auf das Register *0xF5 TCP/IP* und dann auf *Get_Attribute_All* (Attribut Alle abrufen). Die Geräteparameter werden angezeigt.



Wenn Sie beispielsweise den Parameter *IP Address* (IP-Adresse) ändern möchten, geben Sie die neue IP ein und klicken dann auf die Schaltfläche *Set_Attribute* (Attribut festlegen), um den Befehl zu senden.

Hinweis!

Das Modul ist jetzt mit einer neuen IP-Adresse konfiguriert, die im Flash-Speicher abgelegt wird.

Stellen Sie die 3 Drehschalter im Fenster des Moduls auf die Position **000**.

Starten Sie das Modul neu, um die neue IP-Adresse zu übernehmen.

7.3. EDS-Dateien

Die EDS-Dateien sind einfache Textdateien, mit denen Netzwerk-Konfigurationstools Produkte erkennen und einfach in einem Netzwerk in Betrieb nehmen können.

EDS-Dateiliste gemäß der entsprechenden Version des EtherNet/IP CIP Safety I/O-Moduls:

Bestellcode	Typencode	EDS-Dateiname	Produktcode
BNI00HN	BNI CIP-351-000-K015	002B0023351A0103.eds	13594 0x351A

Vom USB-Stick

Die ESD-Dateien des Sicheren E/A-Moduls befinden sich auf dem mit dem Produkt mitgelieferten USB-Stick im Ordner *EDS files*.

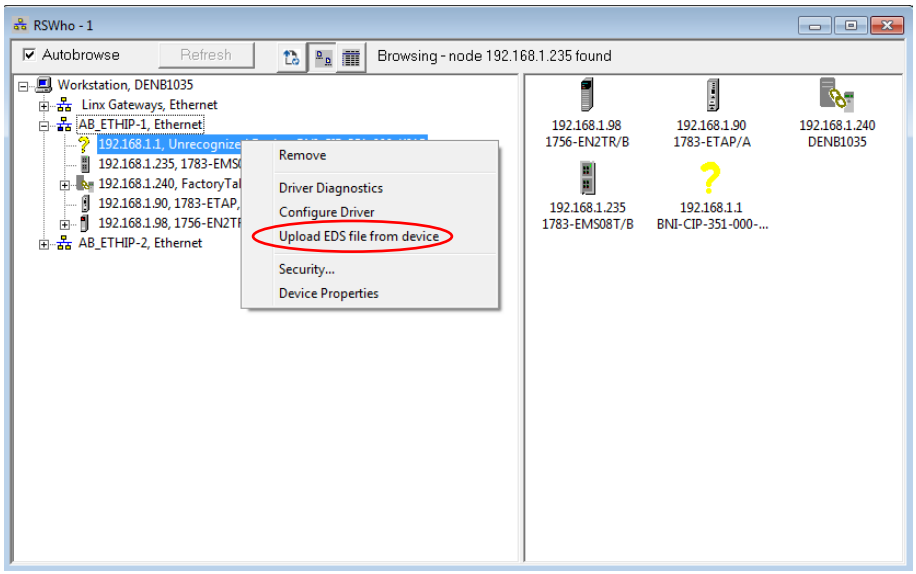
Von der Balluff Website

Die EDS-Dateien und die Produktdokumentation können von der Balluff Website heruntergeladen werden.

https://www.balluff.com

EDS vom Modul hochladen

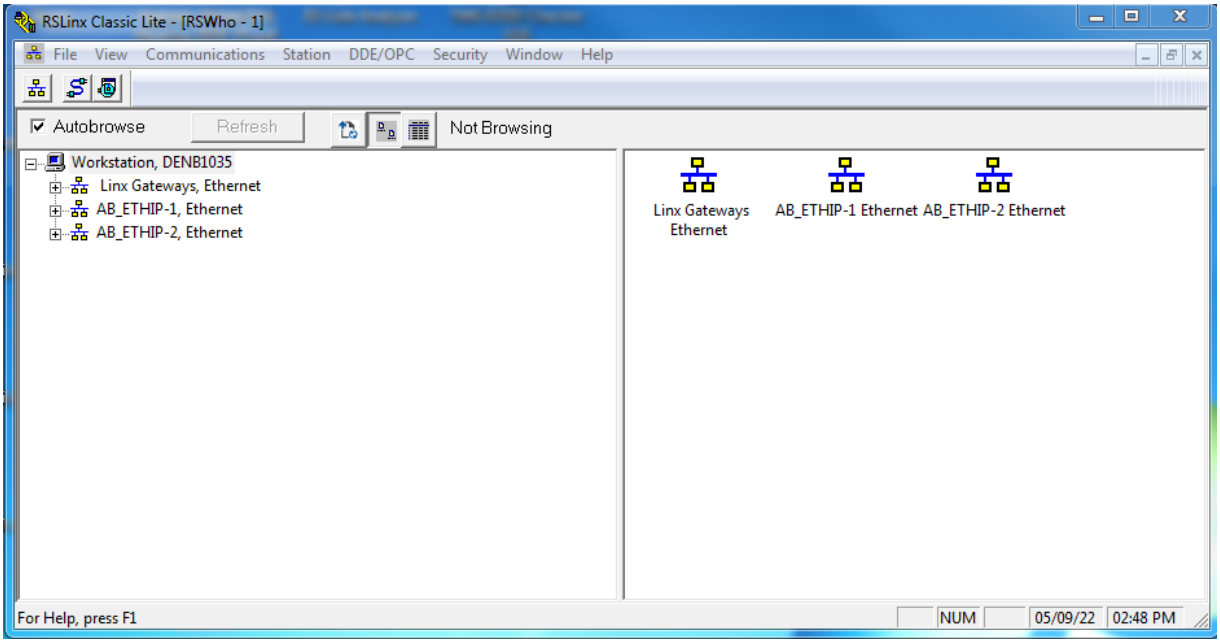
Die EDS-Datei kann auch vom Sicheren E/A-Modul hochgeladen werden. Mit einem Tool wie der Rockwell RSLinx-Software kann der Dienst *Upload EDS from device* (EDS vom Gerät hochladen) aufgerufen werden.



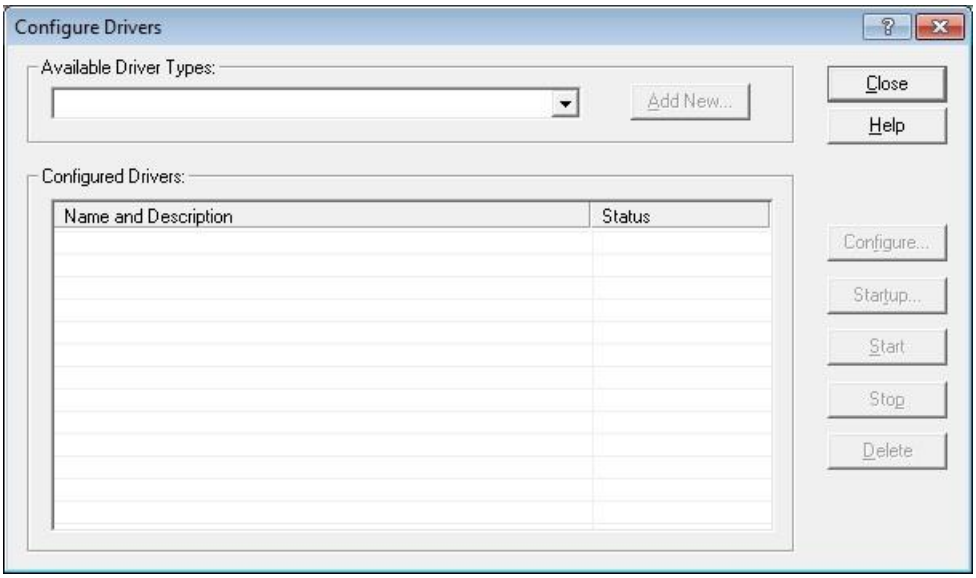
7.4. Import des Sicheren E/A-Modul – EDS-Datei in Rockwell Bibliothek

Der erste Schritt für die Inbetriebnahme ist der Import der EDS-Datei Sicheres E/A-Modul – Sicherheit in die Rockwell-Hardwarebibliothek mit der Software RSLinx™ von Rockwell Automation.

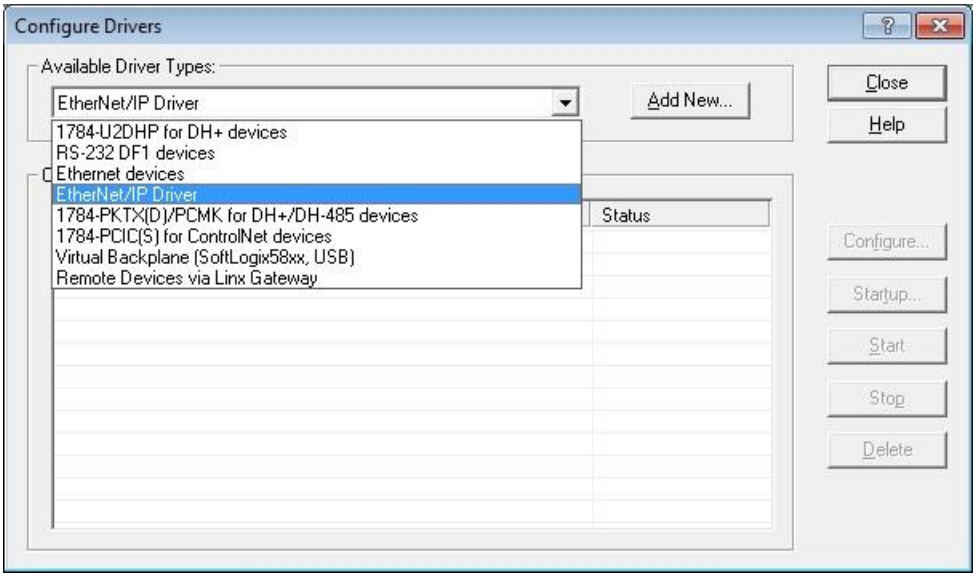
Starten Sie die RSLinx-Software von Rockwell.



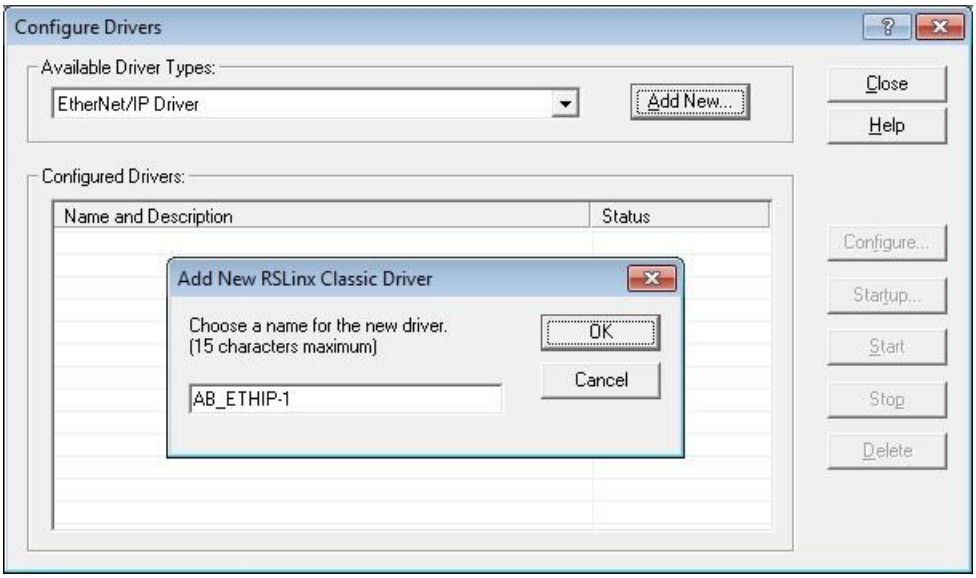
Wählen Sie das Menü *Communications*/*Configure Drivers*… (Kommunikation/Treiber konfigurieren...).



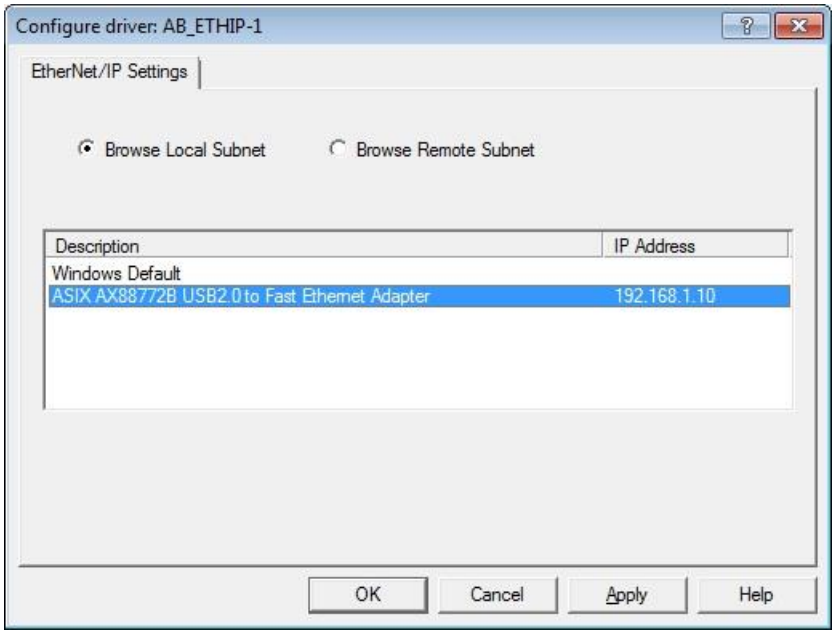
Wählen Sie *EtherNet/IP Driver* (EtherNet/IP-Treiber).



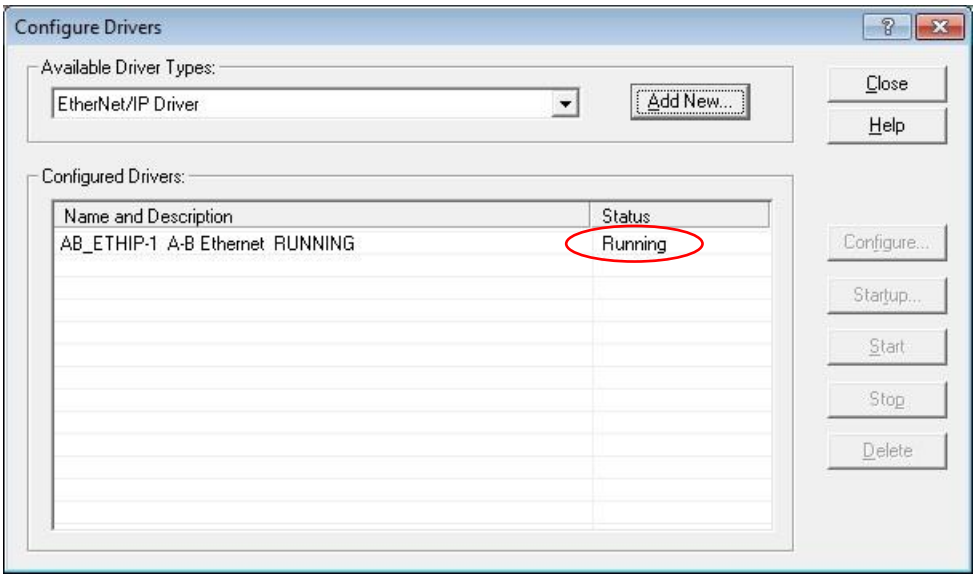
Legen Sie einen Namen für den Treiber fest.



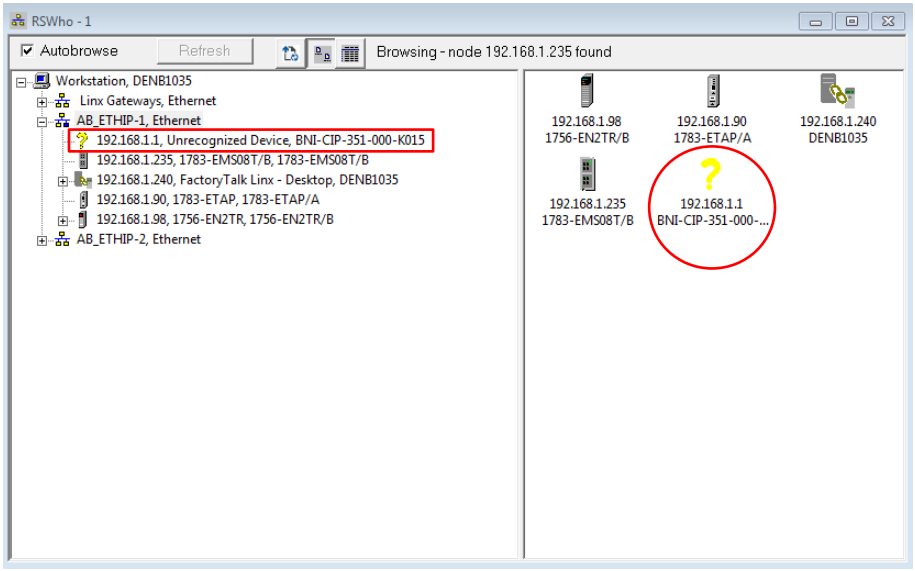
Wenn im Computer mehrere Netzwerkschnittstellen vorhanden sind, wählen Sie die Schnittstelle aus, die mit dem Sicheren E/A-Modul kommunizieren soll.



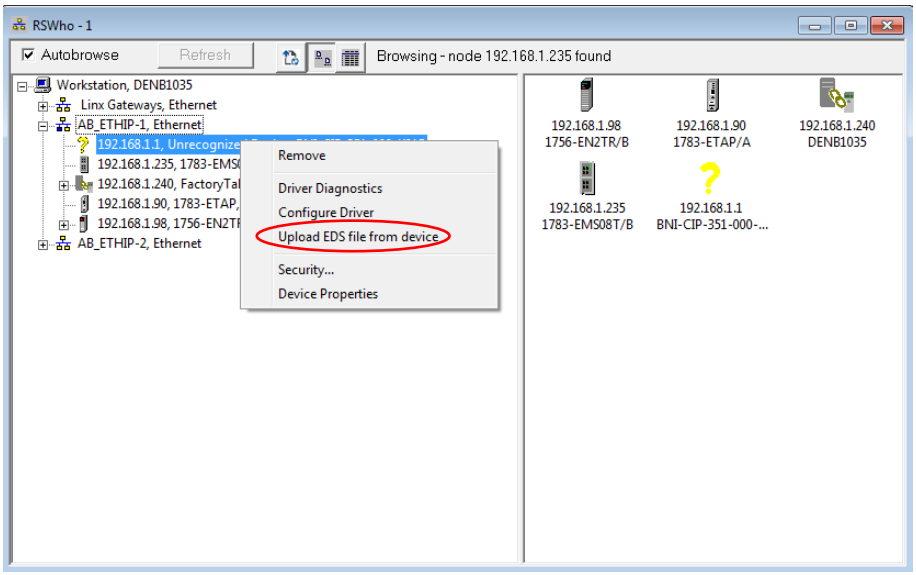
Überprüfen Sie, ob der Treiber ausgeführt wird.



RSLinx durchsucht jetzt das Netzwerk, um die EtherNet/IP-Geräte zu erkennen. In dieser Phase wird das Sichere E/A-Modul zwar erkannt, aber lediglich als Symbol mit einem Fragezeichen dargestellt, da seine EDS-Datei noch nicht importiert wurde.

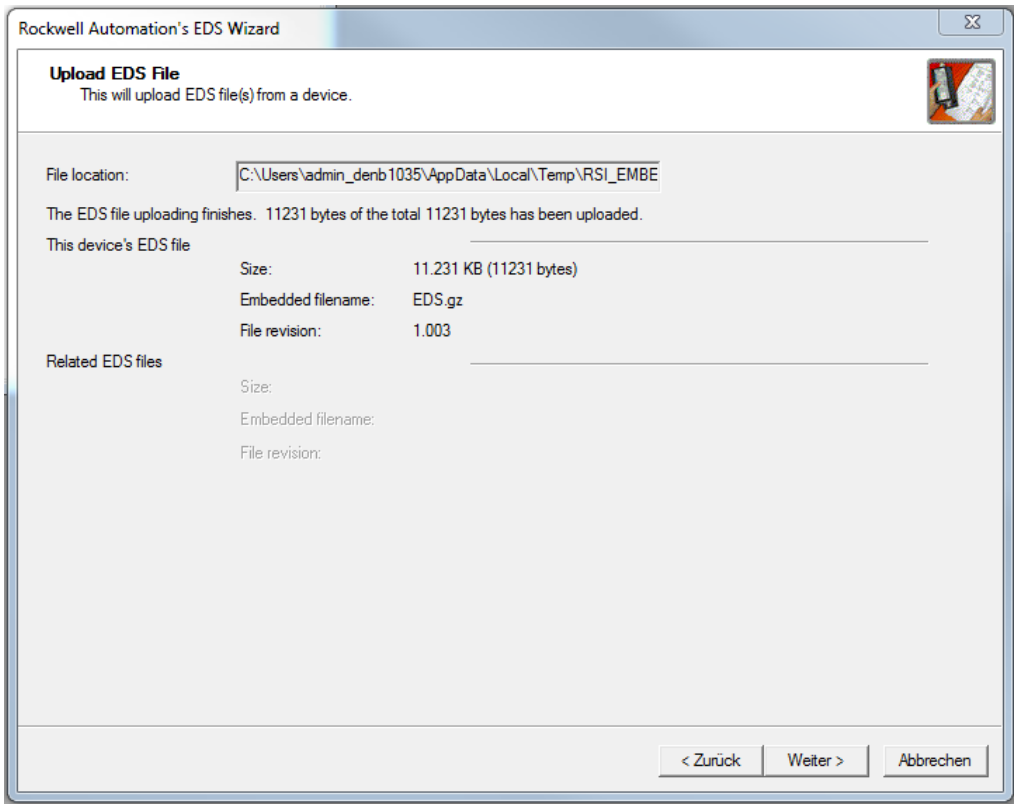


Wählen Sie das Sichere E/A-Modul aus, klicken Sie mit der rechten Maustaste und wählen Sie *Upload EDS file from device* (EDS-Datei vom Gerät hochladen).

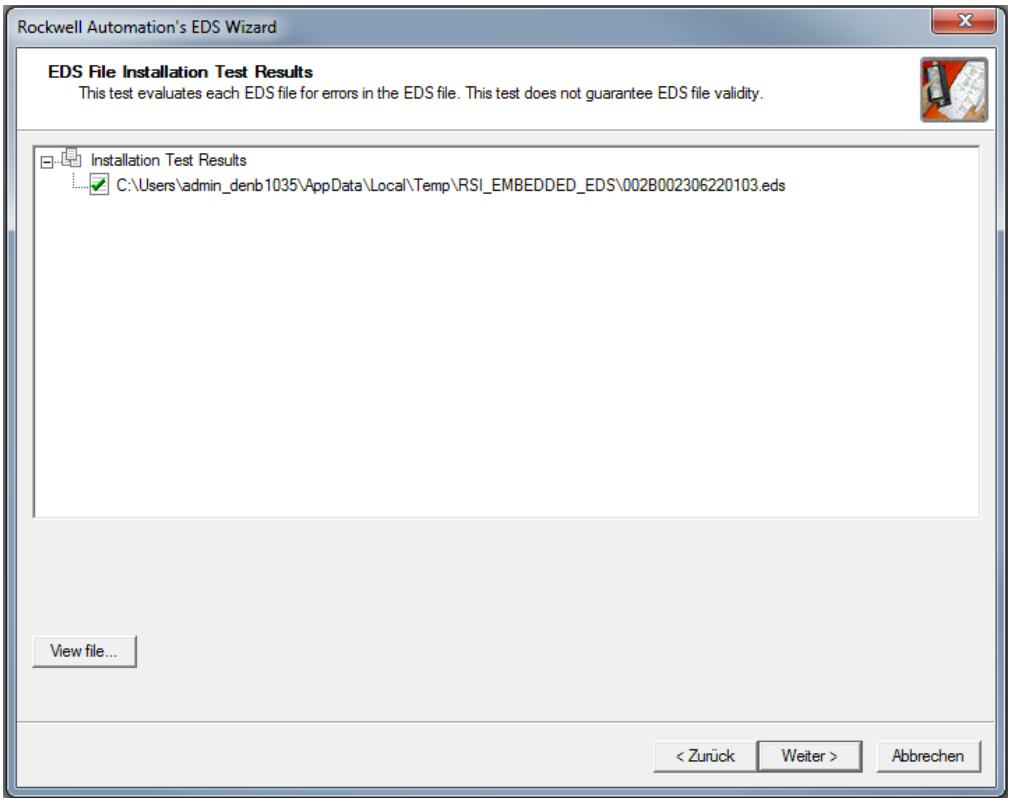


Es wird ein neues Tool gestartet. Wählen Sie die Schaltfläche *Next* (Weiter).

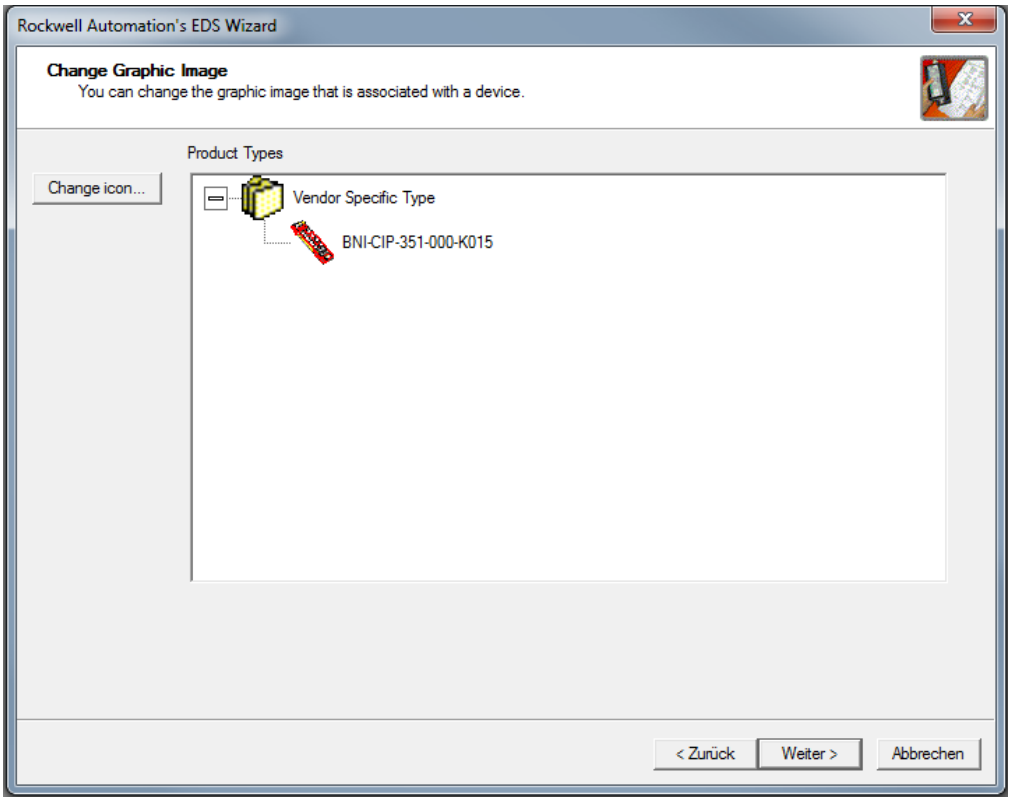
Der EDS Wizard überprüft die Revision der EDS-Datei im Gerät.



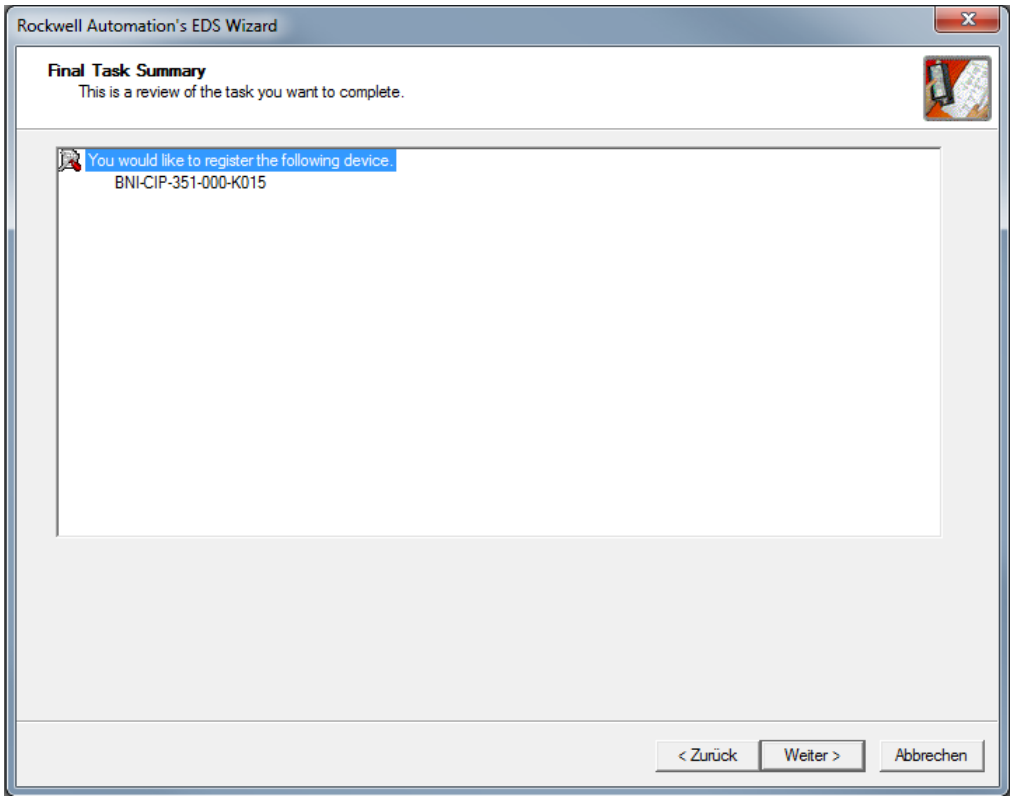
Der EDS Wizard überprüft die Integrität der EDS-Datei.



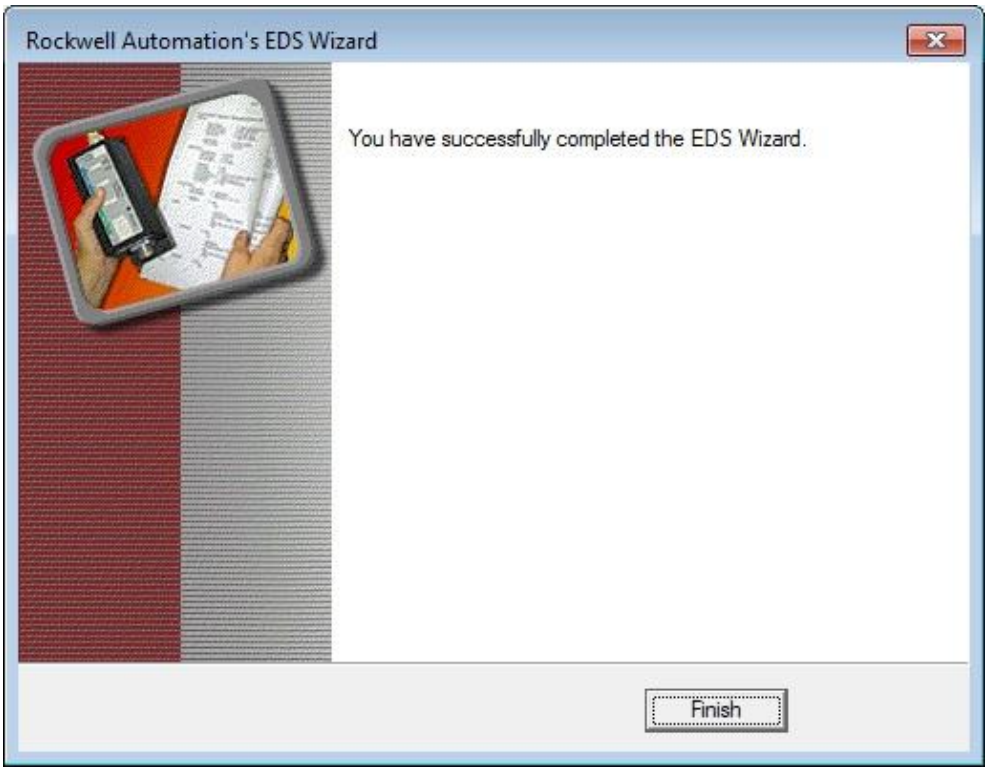
Der EDS Wizard überprüft die Integrität der Symboldatei.



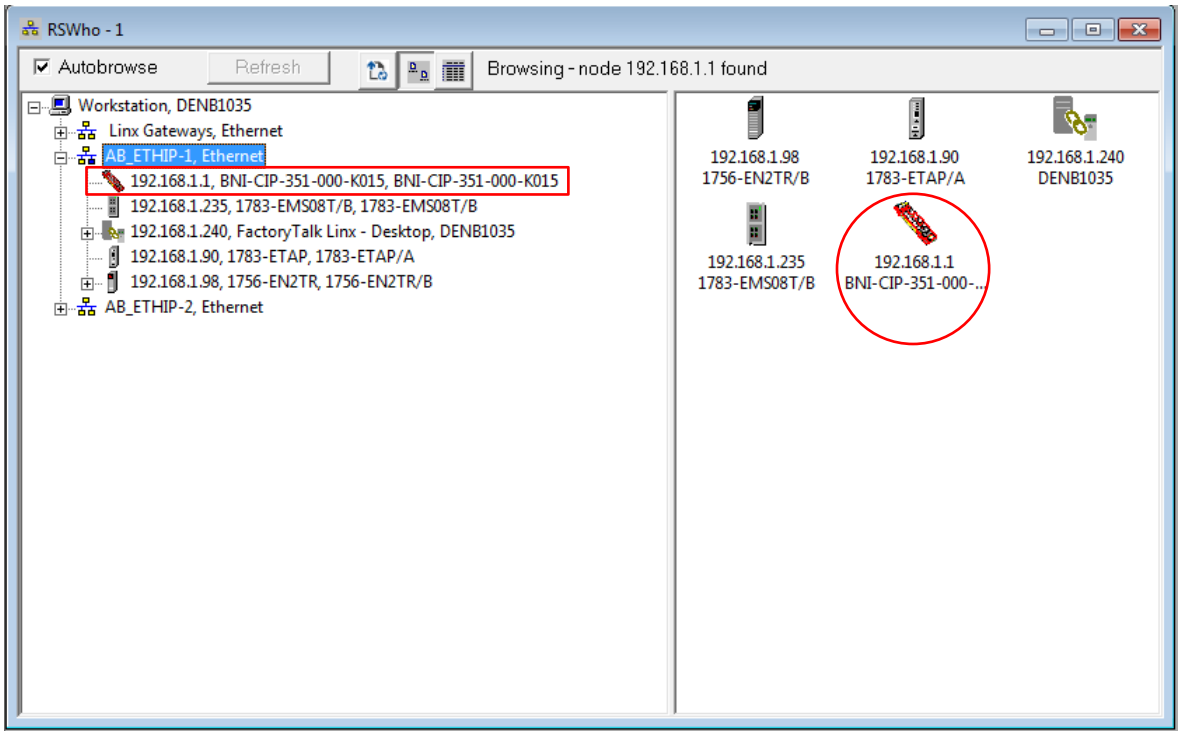
Der EDS Wizard importiert die EDS-Datei und das Symbol in die Rockwell-Hardwarebibliothek.



Der EDS Wizard hat die Dateien erfolgreich importiert.



RSLinx hat die EDS-Datei ordnungsgemäß registriert und zeigt jetzt das korrekte Symbol des Sicheren E/A-Moduls an.

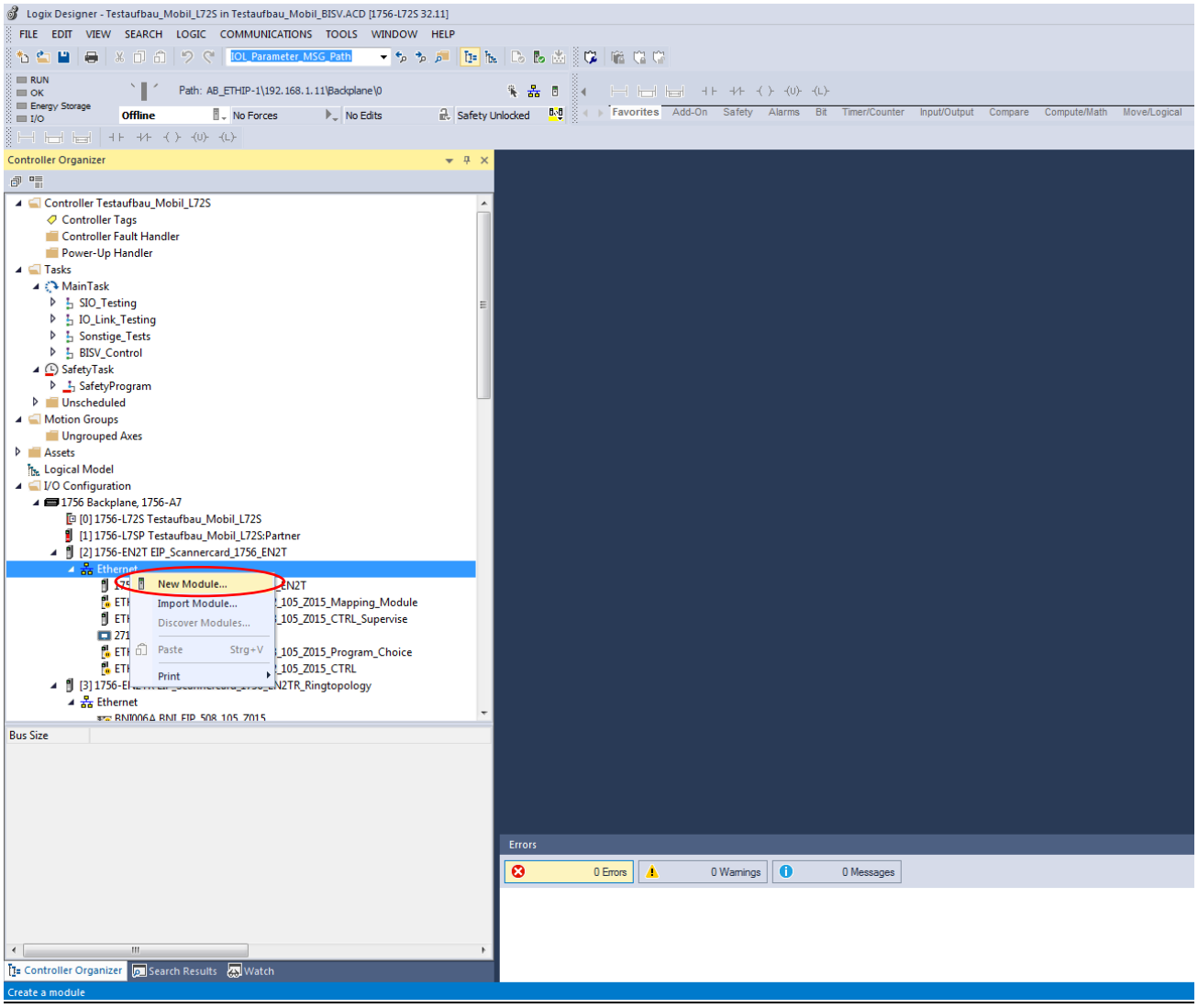


7.5. Konfigurieren des Sicheren E/A-Moduls - Rockwell RSLogix 5000

Starten Sie die RSLogix5000-Software.

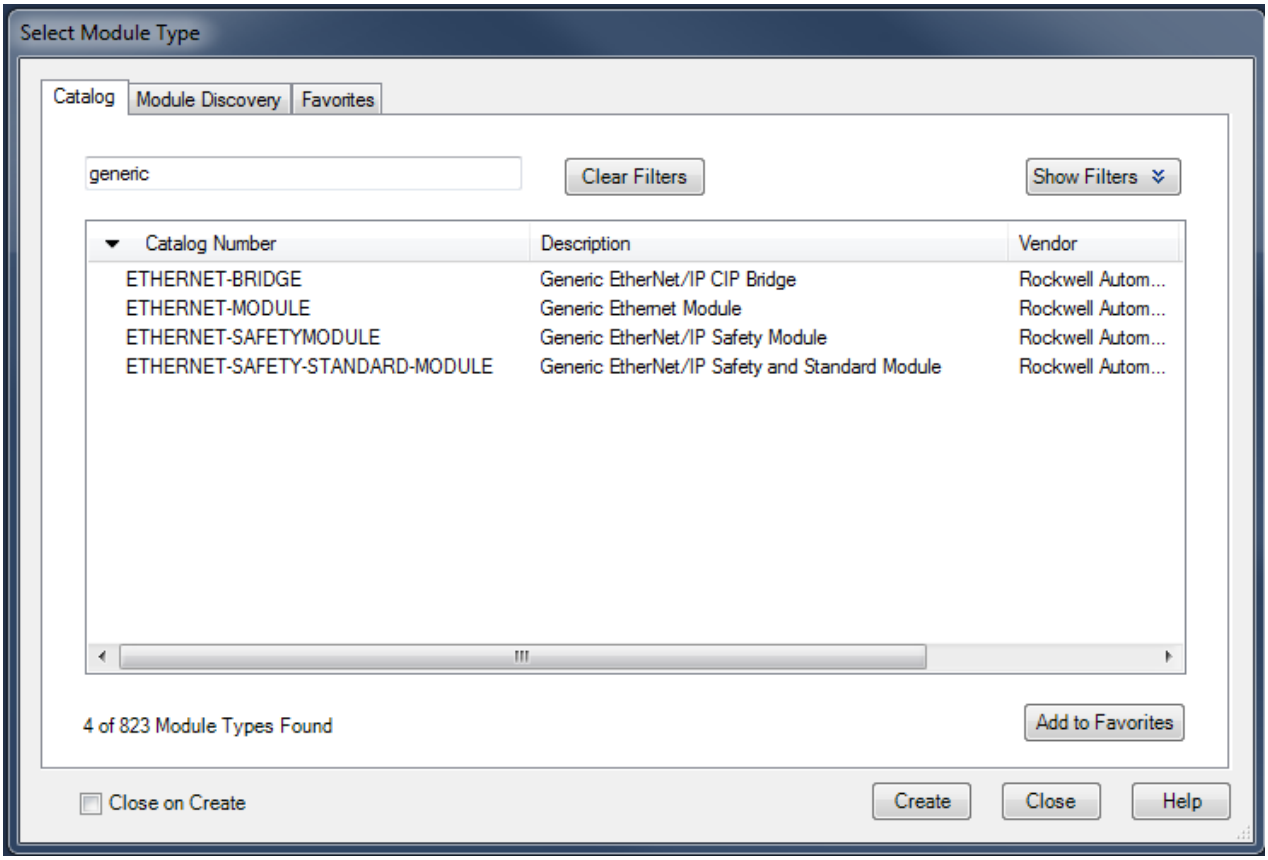
Wählen Sie den Knoten *Ethernet* des EtherNet/IP-Connectivity-Kanals.

Klicken Sie mit der rechten Maustaste und wählen Sie *New Module…* (Neues Modul...).

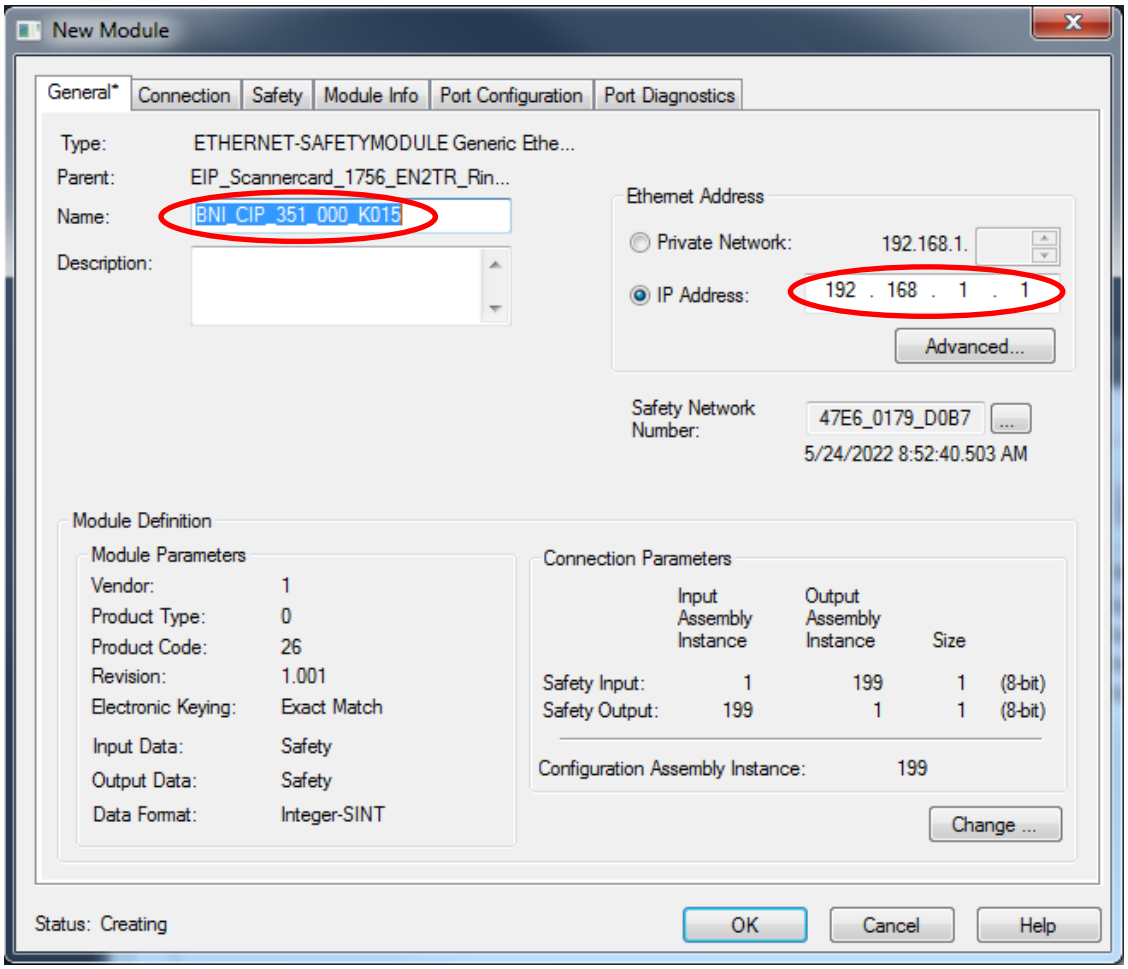


Suchen Sie im Katalog nach *Generic EtherNet/IP Safety Module* (Generisches EtherNet/IP-Sicherheitsmodul) und wählen Sie den Eintrag aus.

Wählen Sie das Modul aus, klicken Sie mit der rechten Maustaste und wählen Sie *Create* (Erstellen).



Vergeben Sie einen Namen und legen Sie die IP-Adresse des Moduls fest, das von RSLinx erkannt wurde.



Die RSLogix-Software erstellt automatisch eine Sicherheitsnetzwerknummer (SNN). Die Sicherheitsnetzwerknummer ist eine eindeutige Kennung in Form einer 48-Bit-Nummer, mit der die Annahme von fehlgeleiteten Verbindungsanfragen verhindert wird. Damit wird sichergestellt, dass jedes Modul im Sicherheitsnetzwerk eindeutig identifiziert werden kann.

Warnung!
Sicherheitsteuerungen, die eine Funktion für die “automatische” SNN-Einstellung besitzen, sollten diese Funktion nur dann verwenden, wenn das Sicherheitssystem keine kritische Rolle spielt.

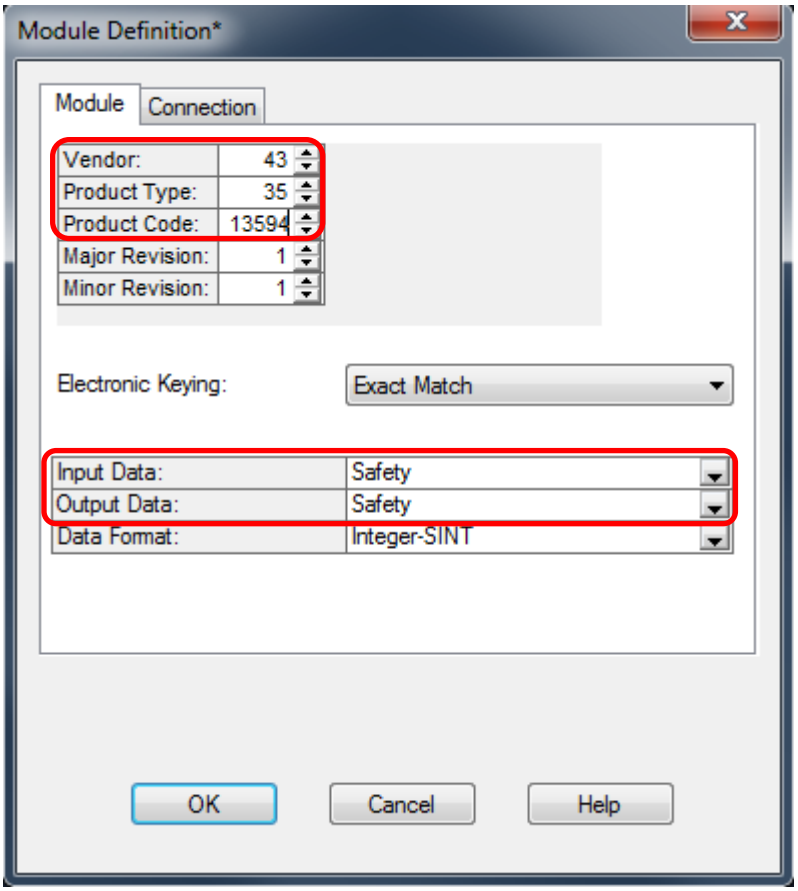
Wählen Sie im Bereich *Connection Parameters* (Verbindungsparameter) die Option *Change* (Ändern).

Ändern Sie im Modulregister die folgenden Parameter:

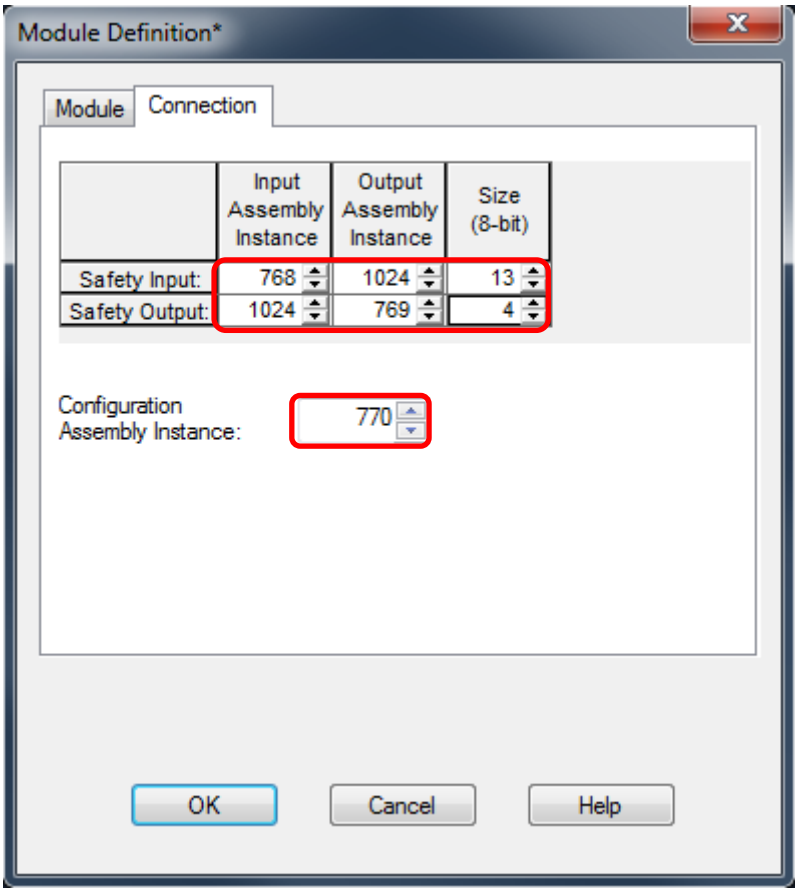
- Vendor (Hersteller): **43** (Balluff)
- Product Type (Produkttyp): **35**
- Product Code (Produktcode): **13594**

7.6. Sichere E/A-Baugruppen

Die Eingangsdaten und die Ausgangsdaten sollten auf *Safety* (Sicherheit) eingestellt sein.



Ändern Sie die Einstellungen für die Verbindungsbaugruppe.

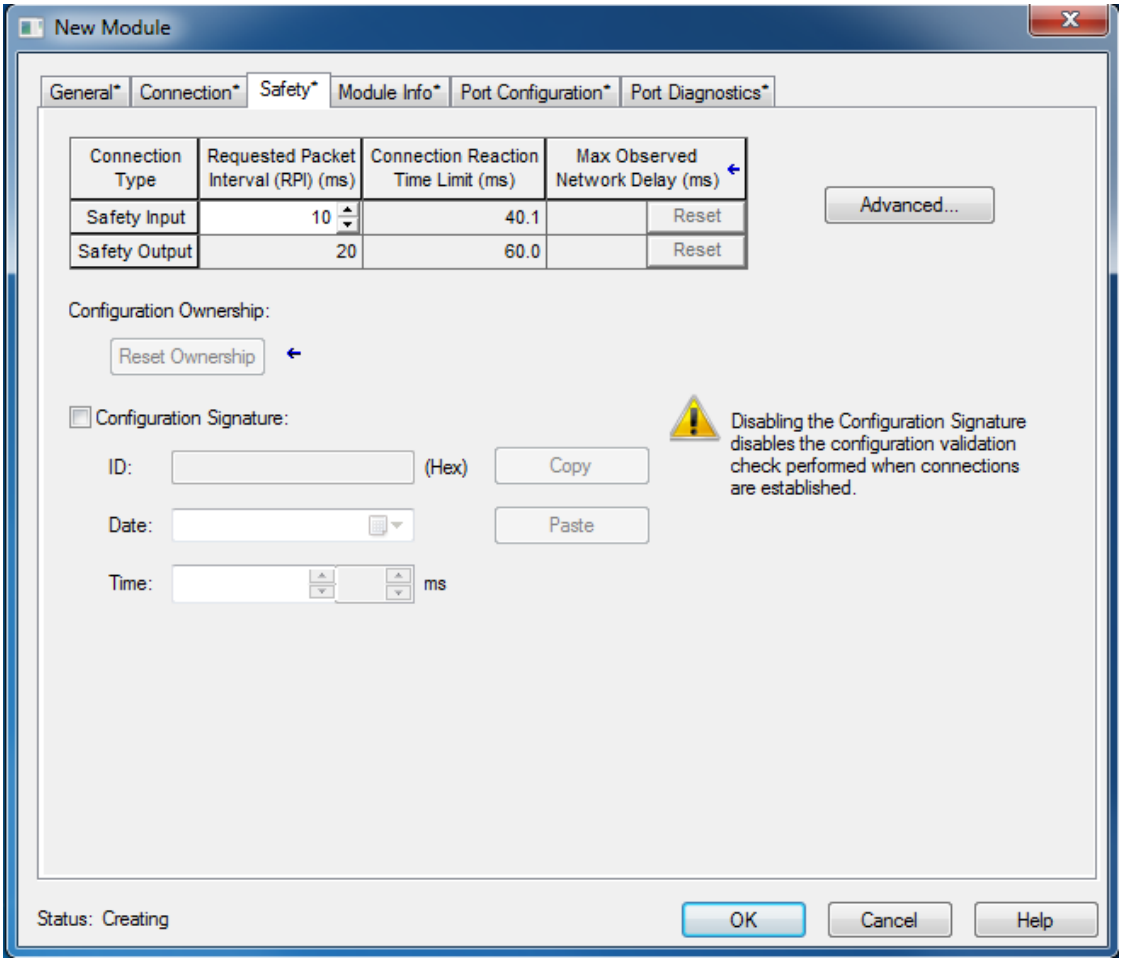


In diesem Beispiel verbinden wir die herstellerspezifischen Baugruppen Sicherheitseingang und Sicherheitsausgänge.

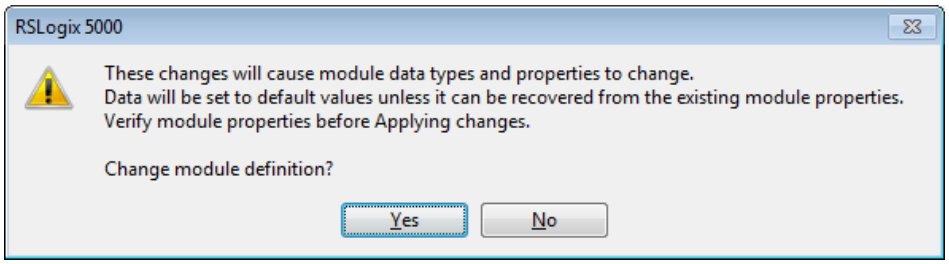
Hinweis!
Das Sichere E/A-Modul unterstützt verschiedene Arten von sicheren E/A-Verbindungen entsprechend der Anzahl und des Typs der Prozessdaten, auf die die Anwendung zugreifen muss.

Eine Liste der sicheren E/A-Verbindungen finden Sie unter Zuordnung von E/A-Daten.

Deaktivieren Sie das Kontrollkästchen *Configuration Signature* (Konfigurationssignatur), um die Änderung zu übernehmen.



Wählen Sie *Yes* (Ja), um die neuen Parameter zu übernehmen.



7.7. Konfigurieren des Sicheren E/A-Moduls in Balluff SNCT

Das Balluff Safety Network Configuration Tool (SNCT) ist eine kostenlose Software, die auf dem im Produktpaket enthaltenen USB-Stick gespeichert ist oder von der Balluff Website heruntergeladen werden kann.

https://www.balluff.com

Warnung!

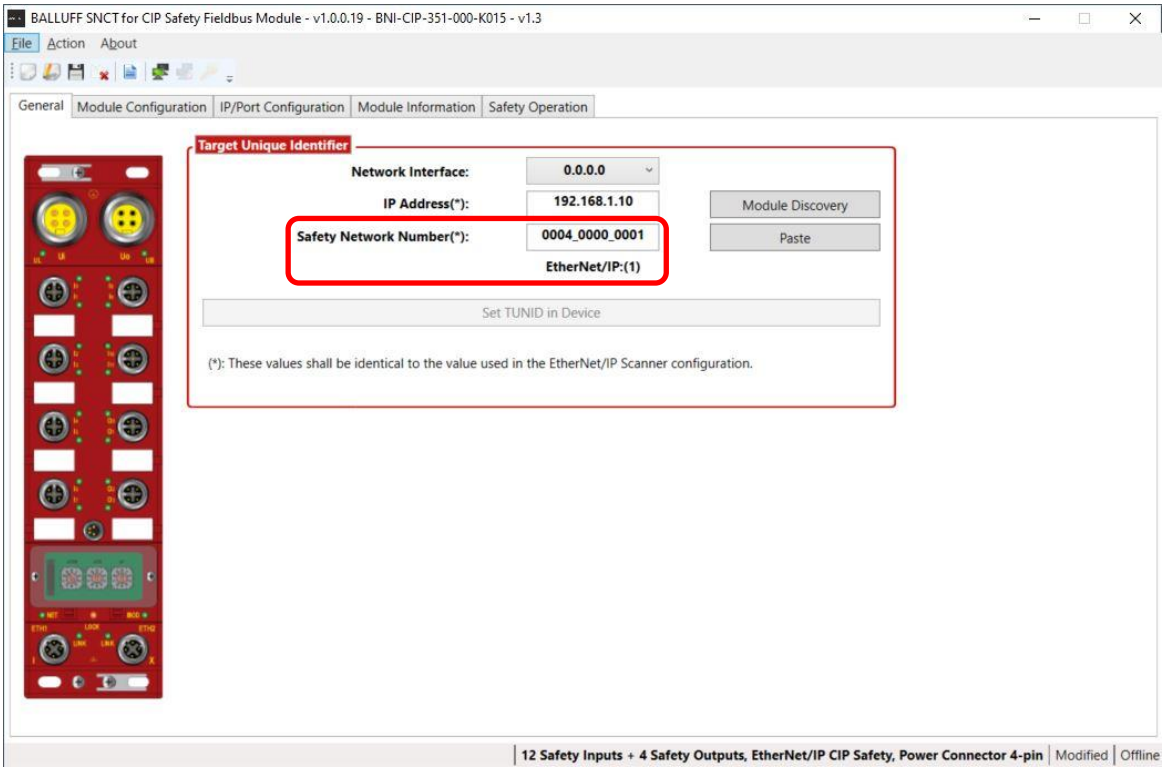
Um Software auf der Balluff Website suchen und herunterladen zu können, müssen Sie der Verwendung von Cookies im Internet Explorer zustimmen.

Starten Sie die Balluff SNCT-Software.

Wählen Sie File/New (Datei/Neu).

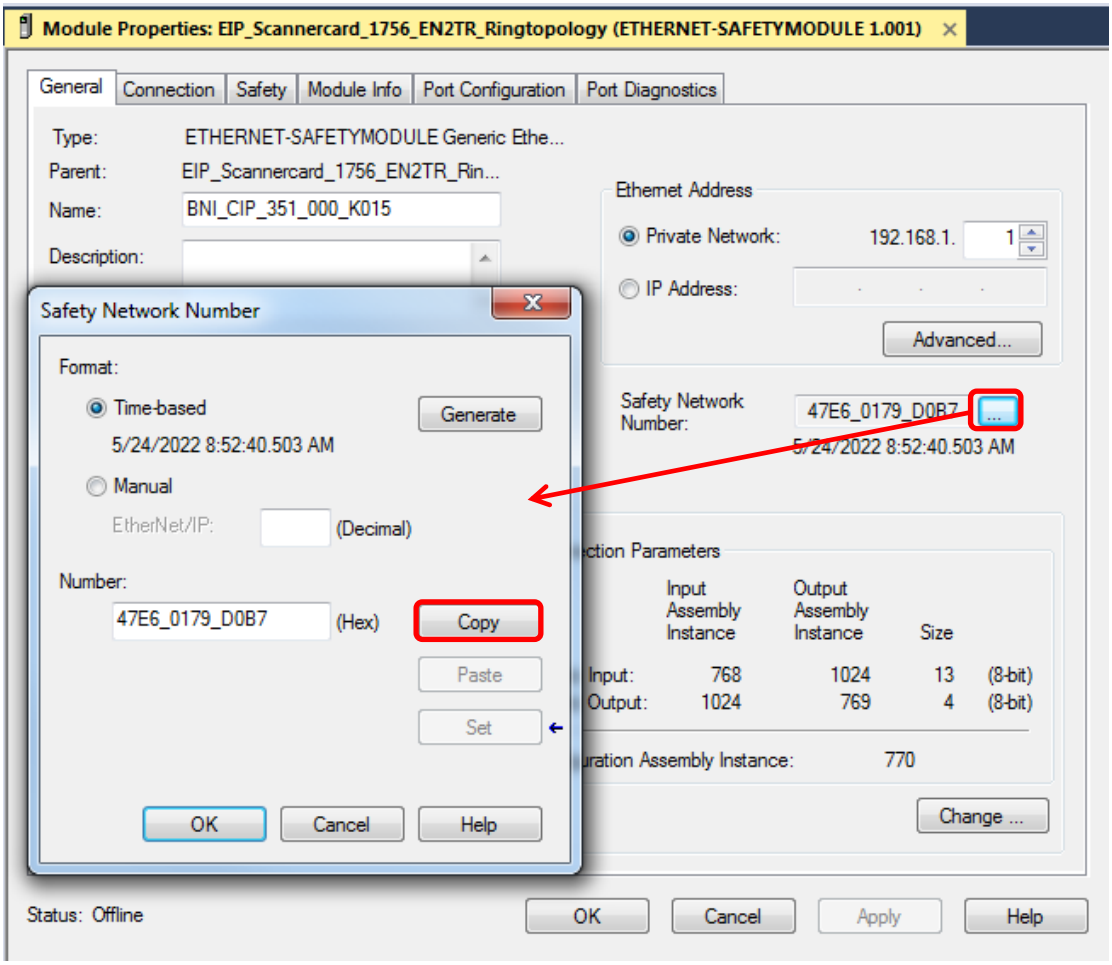
Wählen Sie das Sichere E/A-Modul und seine Version aus.

Im nächsten Schritt muss die Sicherheitsnetzwerknummer eingerichtet werden.

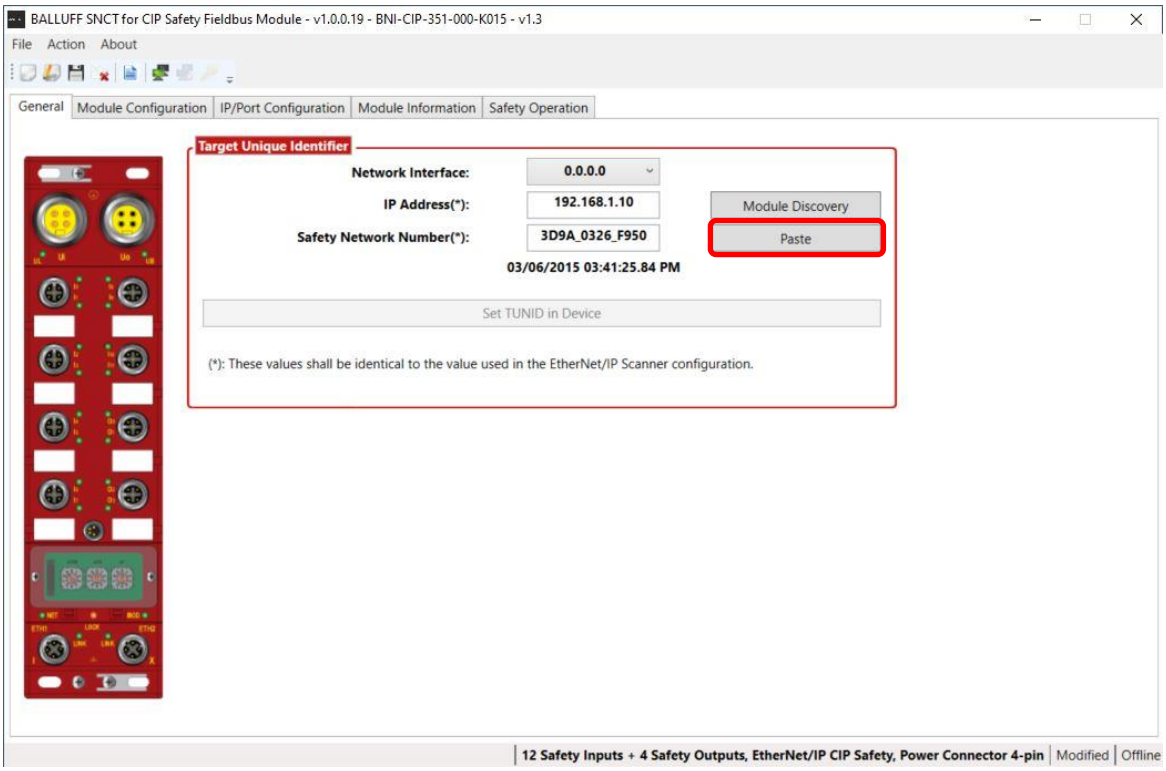


Gehen Sie in der RSLogix 5000-Software zum Eigenschaftsdialogfeld für das Sichere E/A-Modul.

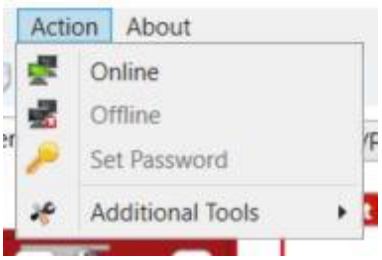
Wählen Sie die Schaltfläche für die Parameter der Sicherheitsnetzwerknummer.



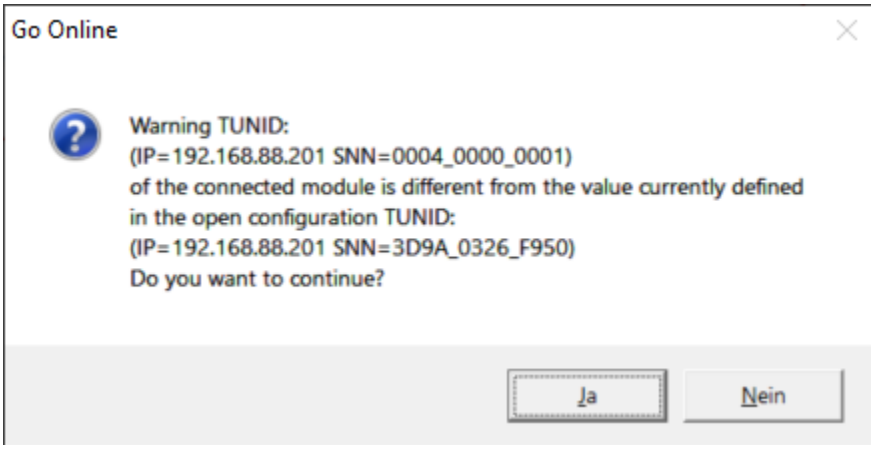
Kopieren Sie die SNN in die Zwischenablage und fügen Sie sie in der SNCT-Software ein.



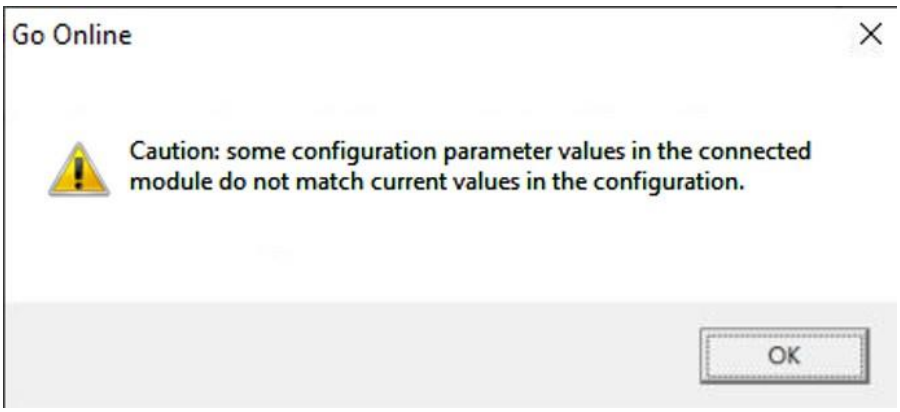
Verbinden Sie das Modul, indem Sie im Menü *Action* (Aktion) den Eintrag *Online* wählen.



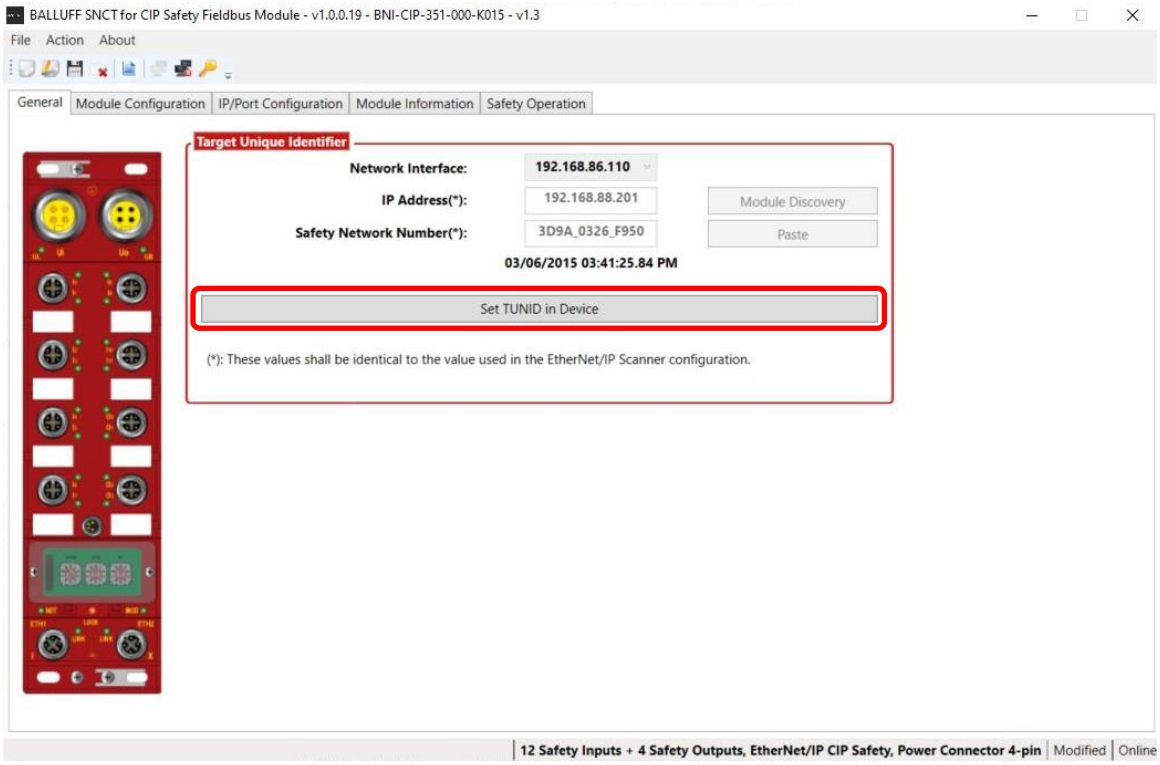
Wenn die TUNID von der im Modul konfigurierten TUNID abweicht, wird die folgende Meldung angezeigt:



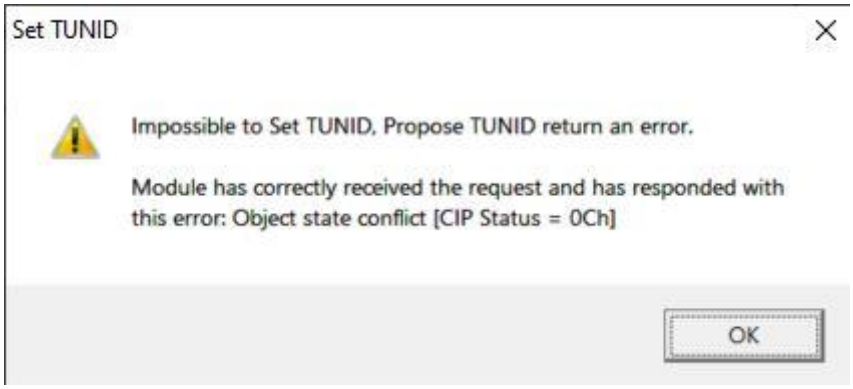
Wenn einige vorhandenen Parameter bereits im Modul festgelegt wurden, wird die folgende Meldung angezeigt:



Klicken Sie auf die Schaltfläche *Set TUNID in Device* (TUNID im Gerät festlegen).

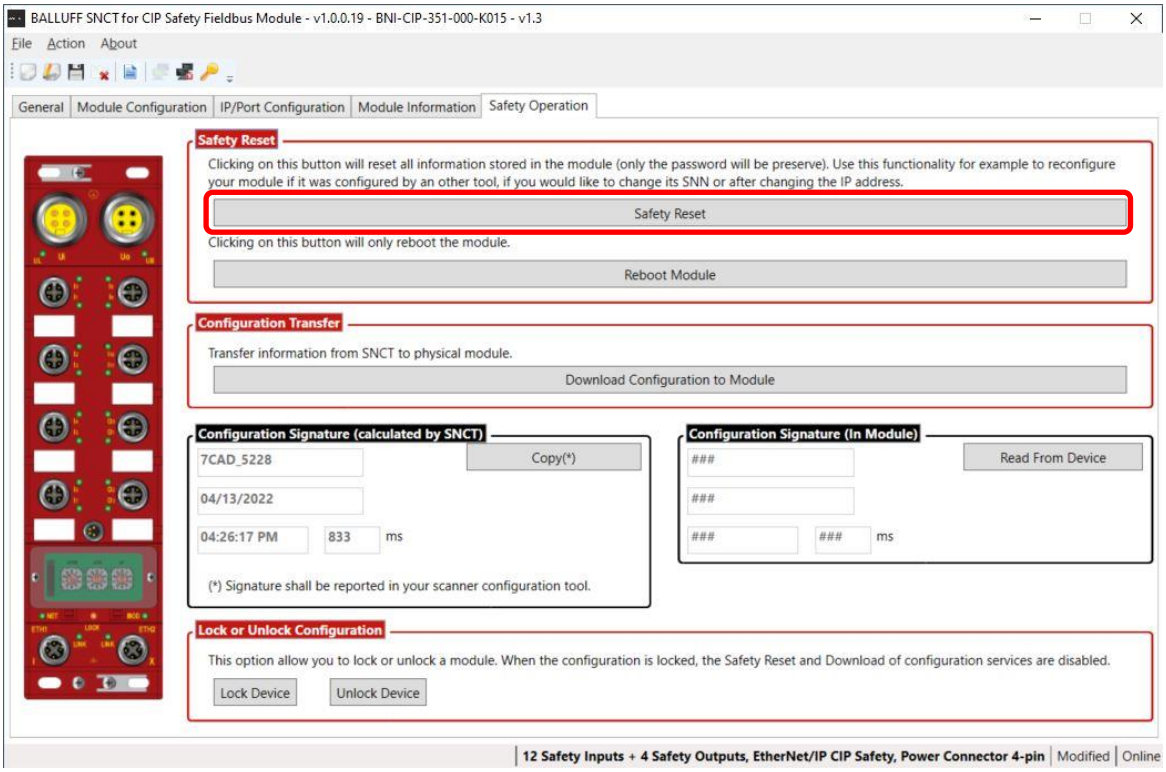


Hinweis!
Wenn die folgende Meldung angezeigt wird, ist im Modul bereits eine TUNID konfiguriert.

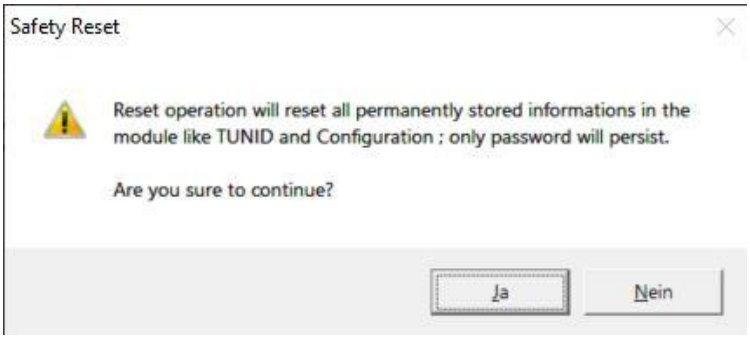


Führen Sie eine Sicherheitsrücksetzung durch, bevor Sie die TUNID festlegen.

Gehen Sie zum Register Safety Operation (Sicherheitsbetrieb) und klicken Sie auf die Schaltfläche *Safety Reset* (Sicherheitsrücksetzung).



Wählen Sie Yes (Ja), um die TUNID und die Konfiguration des Moduls zurückzusetzen.



Das Modul wurde erfolgreich zurückgesetzt.

Hinweis!

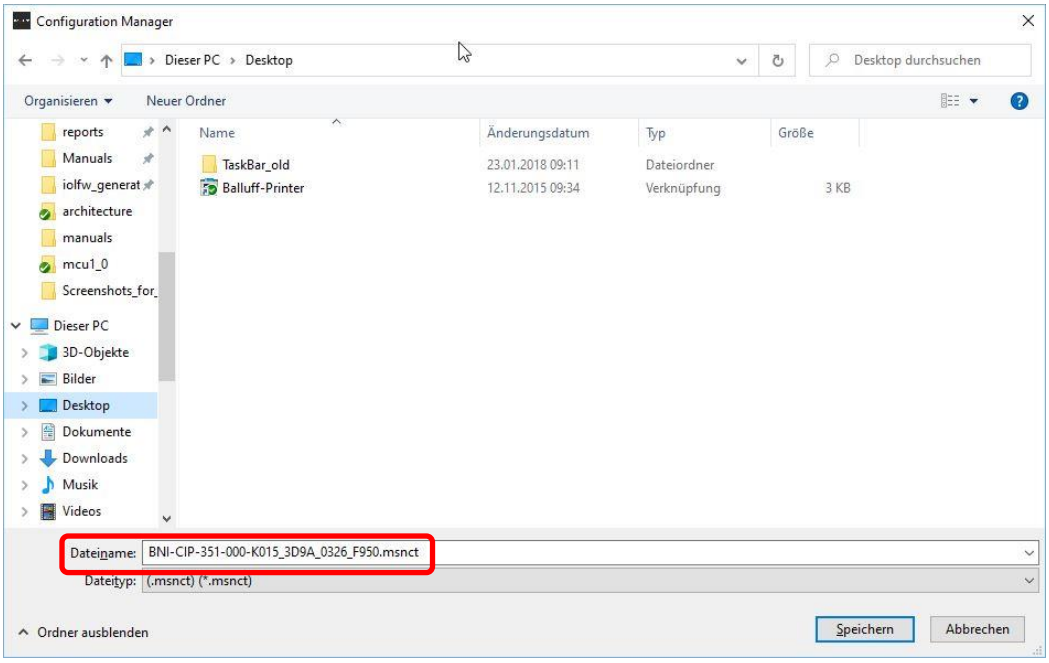
Achten Sie beim Festlegen der TUNID darauf, dass keine E/A-Verbindungen des EtherNet/IP-Scanners offen sind, da die Festlegung der TUNID in dem Fall fehlschlägt.

Die TUNID wurde erfolgreich festgelegt. Im nächsten Schritt muss das Modul konfiguriert werden.

Hinweis!
Da die TUNID nun konfiguriert ist, kann die Modulkonfiguration gespeichert werden.

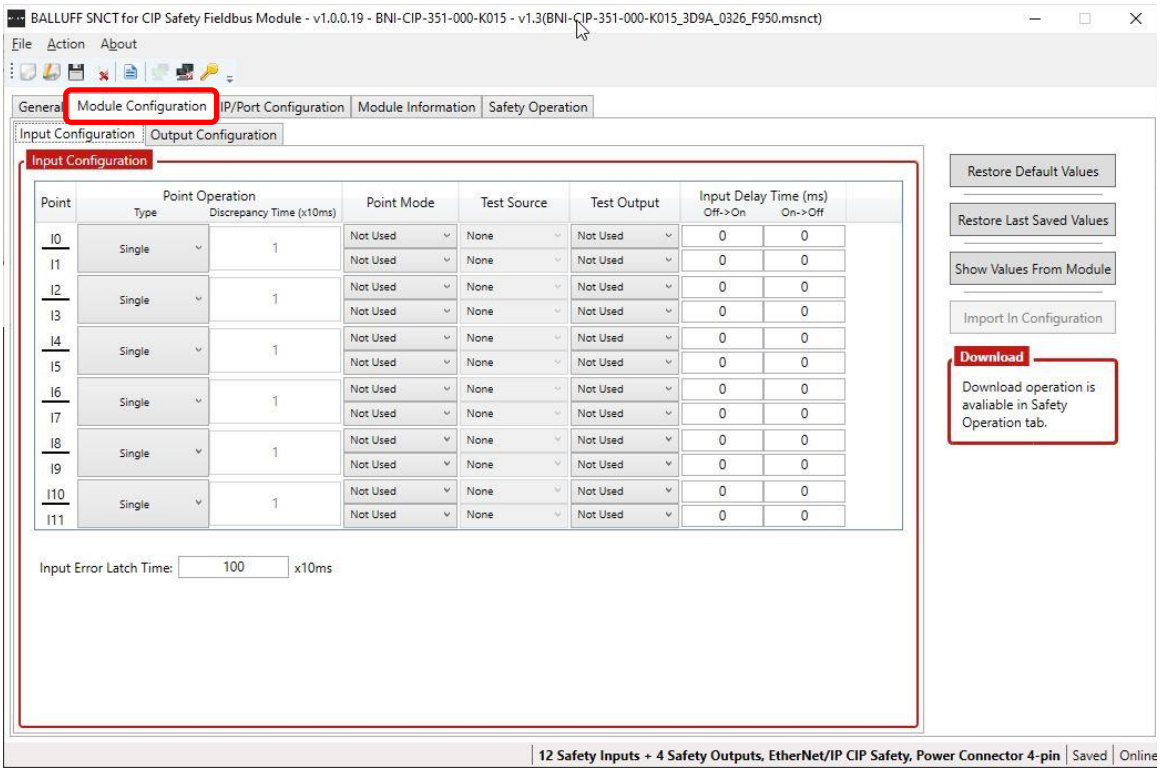
Wählen Sie File / Save (Datei / Speichern).

Der Standard-Dateiname ist eine Kombination aus der Produktnummer des Sicheren E/A-Moduls und der im Modul konfigurierten TUNID. Der Dateiname kann bei Bedarf geändert werden.



Wählen Sie das Register *Module Configuration* (Modulkonfiguration), um die Parameter für die Sicherheitseingänge und die Sicherheitsausgänge festzulegen.

Konfiguration der Sicherheitseingänge



Punkt-Betriebsart

Typ	Bemerkungen
Einzel	Sicherheitseingänge werden getrennt behandelt.
Äquivalent	Sicherheitseingänge werden als Äquivalenter Doppelkanal behandelt. Die Evaluierung erfolgt nach der Diskrepanzzeit.
Antivalent	Sicherheitseingänge werden als Antivalenter Doppelkanal behandelt. Die Evaluierung erfolgt nach der Diskrepanzzeit.

Punkt-Modus

Modus	Bemerkungen
Nicht verwendet	Der Eingang ist deaktiviert.
Sicherheit	Der Eingang ist aktiviert und es ist kein externer Impulstest erforderlich. Das wird in der Regel verwendet, wenn das Eingangsgerät seinen eigenen Impulstest generiert, wie z.B. ein Lichtvorhang.
Sicherheits-Impulstest	Der Eingang ist aktiviert und ein Impulstest muss als 24 V verwendet werden. Der Impulstest wird über die Option *Test Source* (Testquelle) konfiguriert.

Standard	Der Eingang ist aktiviert, wirkt aber an keiner Sicherheitsfunktion mit. Das wird in der Regel für die Verbindung eines nicht sicheren Eingangsgeräts verwendet.

Testquelle

Wählen Sie die entsprechende Testquelle für den Sicherheitseingang aus.

Hinweis!

Die Testquelle kann nur ausgewählt werden, wenn ein Punkt-Modus für den Sicherheitsimpulstest festgelegt wurde.

Hinweis!

Als Testquelle kann nur einer der zugewiesenen M12-Anschlüsse verwendet werden.

Testausgang

Modus	Bemerkungen
Nicht verwendet	Der Testausgang ist deaktiviert.
Standard	Der Pin des Testausgangs ist so konfiguriert, dass er sich als nicht sicheres Ausgangssignal verhält. Das Signal wird über die SPS im Prozessausgangsbild des Moduls kontrolliert.
Impulstest	Der Testausgang ist für die Generierung von 24 VDC bei einem Impulstest konfiguriert.
Spannungsversorgung	Der Testausgang ist für die Bereitstellung einer 24-VDC-Spannungsversorgung konfiguriert. Nach dem Einschalten des Moduls wird der Testausgang dauerhaft mit Spannung (24 VDC) versorgt.
Muting-Lampe	Der Testausgang wird als Muting-Lampe verwendet. Der Testausgang kann eine unterbrochene Kabelverbindung erkennen (Überprüfung erfolgt alle 3s; nach 2 aufeinanderfolgenden fehlgeschlagenen Tests wird ein Fehler gemeldet).

Hinweis!

Die Auswahl der Muting-Lampe ist nur für Eingang 3 und Eingang 7 verfügbar.

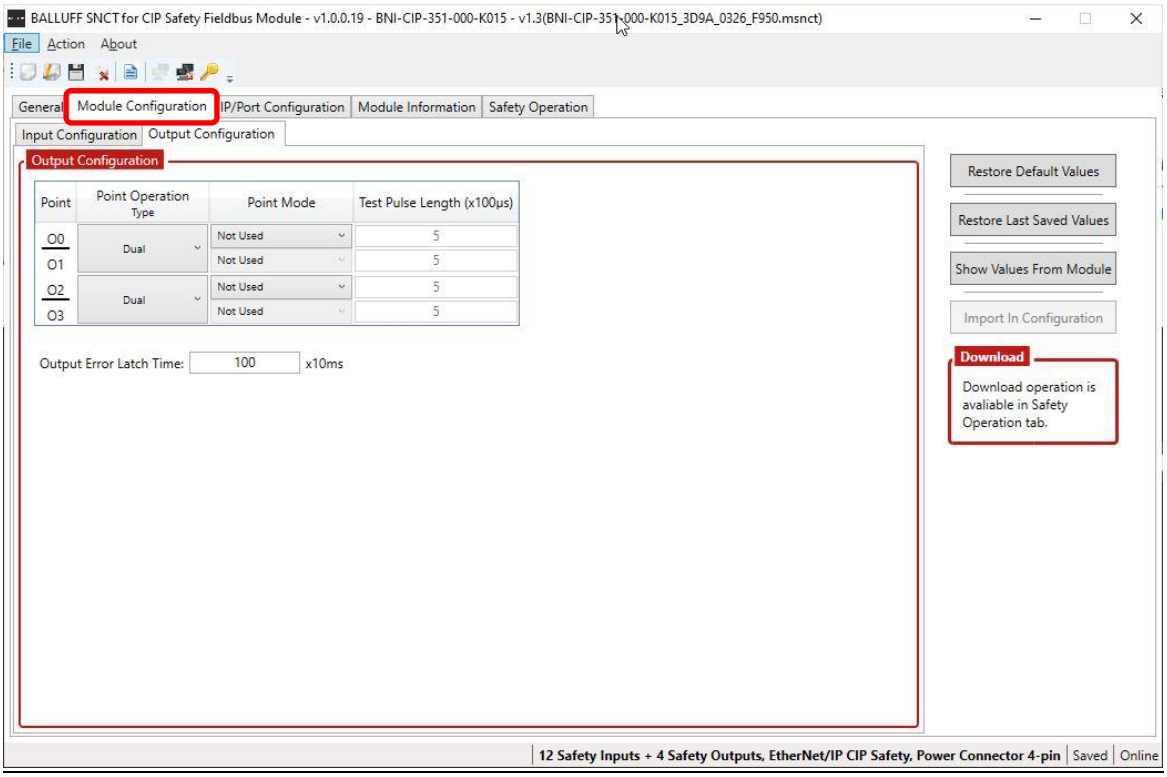
Eingangsverzögerung

Definieren Sie die Filterzeit für den Übergang des Sicherheitseingangs. Siehe Eingangsverzögerung für weitere Informationen.

Haltezeit für Eingangsfehler

Definieren Sie die Dauer, in der das Modul einen Fehler hält, damit er von der Sicherheitssteuerung erkannt werden kann. Siehe Haltezeit für Eingangsfehler für weitere Informationen.

Konfiguration der Sicheren Ausgänge



Punkt-Betriebsart

Modus	Bemerkungen
Einzel	Die Sicherheitsausgänge werden getrennt behandelt.
Zweikanal	Die Sicherheitseingänge werden als Doppelkanal behandelt.

Punkt-Modus

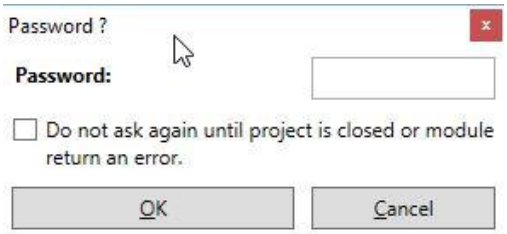
Modus	Bemerkungen
Nicht verwendet	Der Ausgang ist deaktiviert.
Sicherheit Kein Impulstest	Der Ausgabe ist aktiviert und es wird KEIN Impulstest generiert.
Sicherheits-Impulstest	Der Ausgabe ist aktiviert und es wird ein Impulstest generiert.

Impulstestlänge

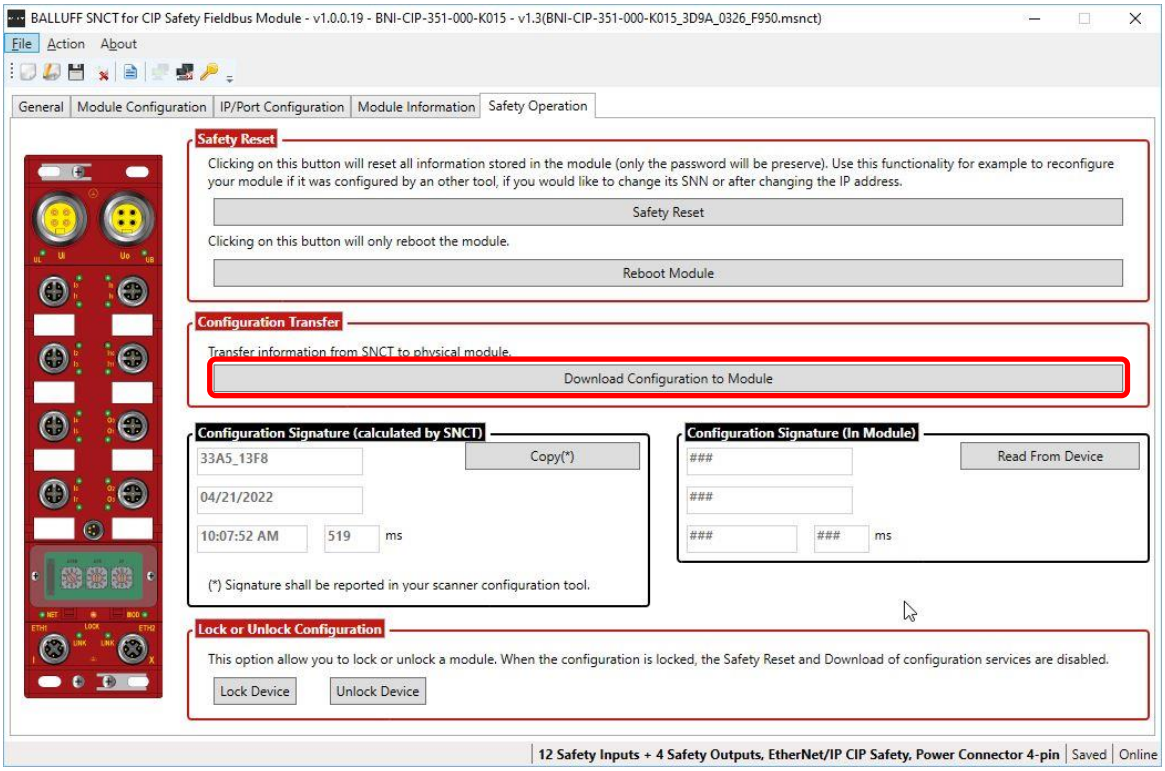
Definieren Sie die Impulstestlänge des entsprechenden Ausgangs. Siehe Ausgangs-Impulstest für weitere Informationen.

Wenn die sichere E/A-Einstellung abgeschlossen ist, muss im nächsten Schritt die Konfiguration im Modul heruntergeladen werden.

Hinweis!
Wenn Sie ein Kennwort für den Schutz der Modulkonfiguration festgelegt haben, fordert SNCT Sie auf, das Kennwort für den nächsten Sicherheitsbetrieb einzugeben.

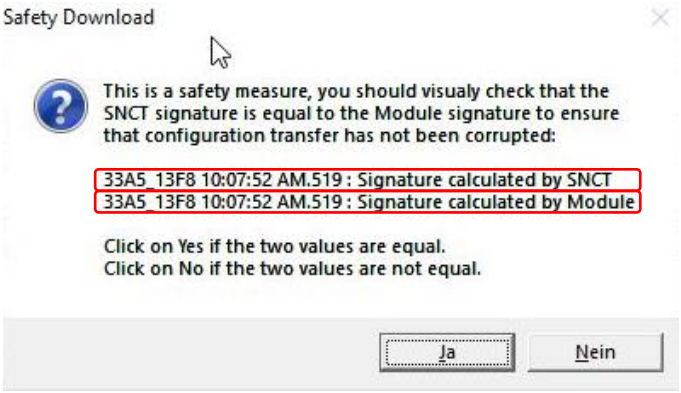


Gehen Sie zum Register *Safety Operation* (Sicherheitsbetrieb) und klicken Sie auf *Download Configuration to Device* (Konfiguration auf Gerät herunterladen).



Warnung!
Die Validierung der Konfigurationssignatur ist ein wichtiger Schritt bei der Inbetriebnahme des Moduls.

Es ist Aufgabe des Sicherheitsexperten sicherzustellen, dass die zum Modul gesendete Konfigurationsdatei ordnungsgemäß übertragen wird, indem er die von der SNCT-Software und vom Sicheren E/A-Modul berechnete Signatur verifiziert.

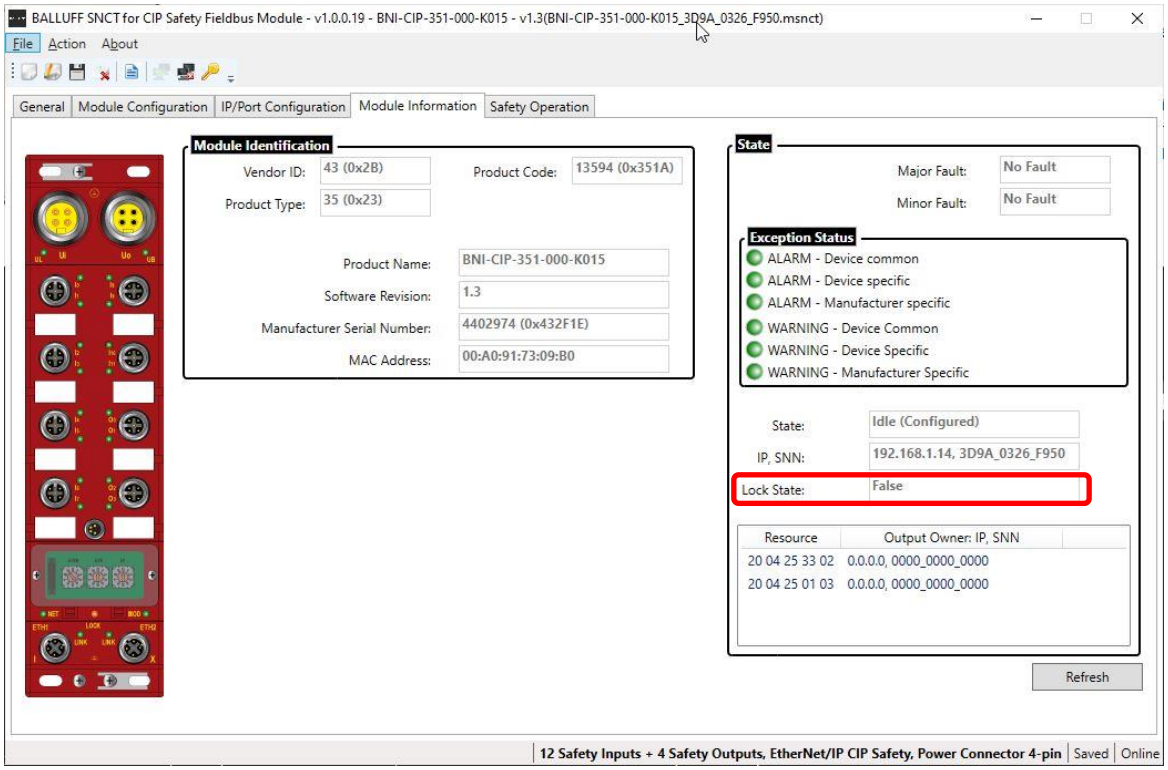


Wenn die Signaturen übereinstimmen, klicken Sie auf die Schaltfläche *Yes* (Ja). Andernfalls klicken Sie auf *No* (Nein), um den Vorgang abzubrechen.

Warnung!
Alle Vorgänge müssen von einem Sicherheitsexperten durchgeführt werden. Für die Durchführung der Vorgänge wird das Modulkennwort benötigt.

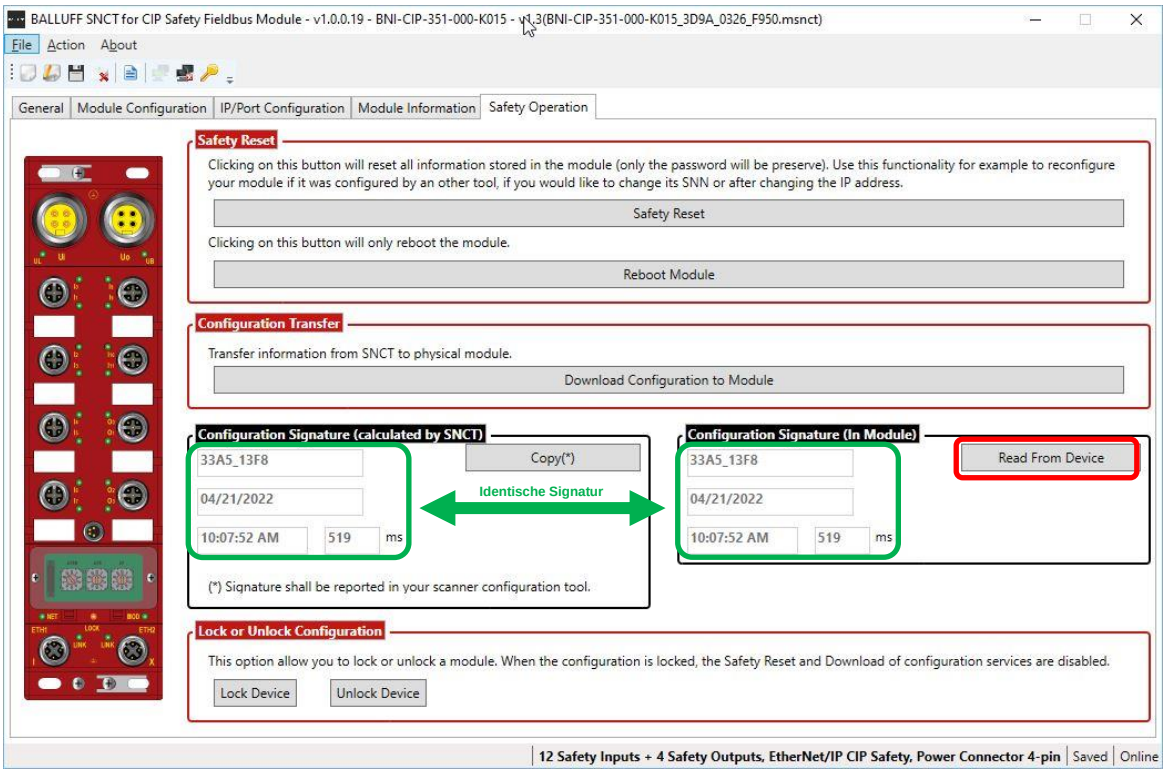
Hinweis!
Stellen Sie vor dem Download der Datei sicher, dass die Modulkonfiguration nicht gesperrt ist. Dieser Status kann entweder anhand der gelben “Sperr”-LED am Modul

oder über das Register Module Information (Modulinformationen) ermittelt werden.

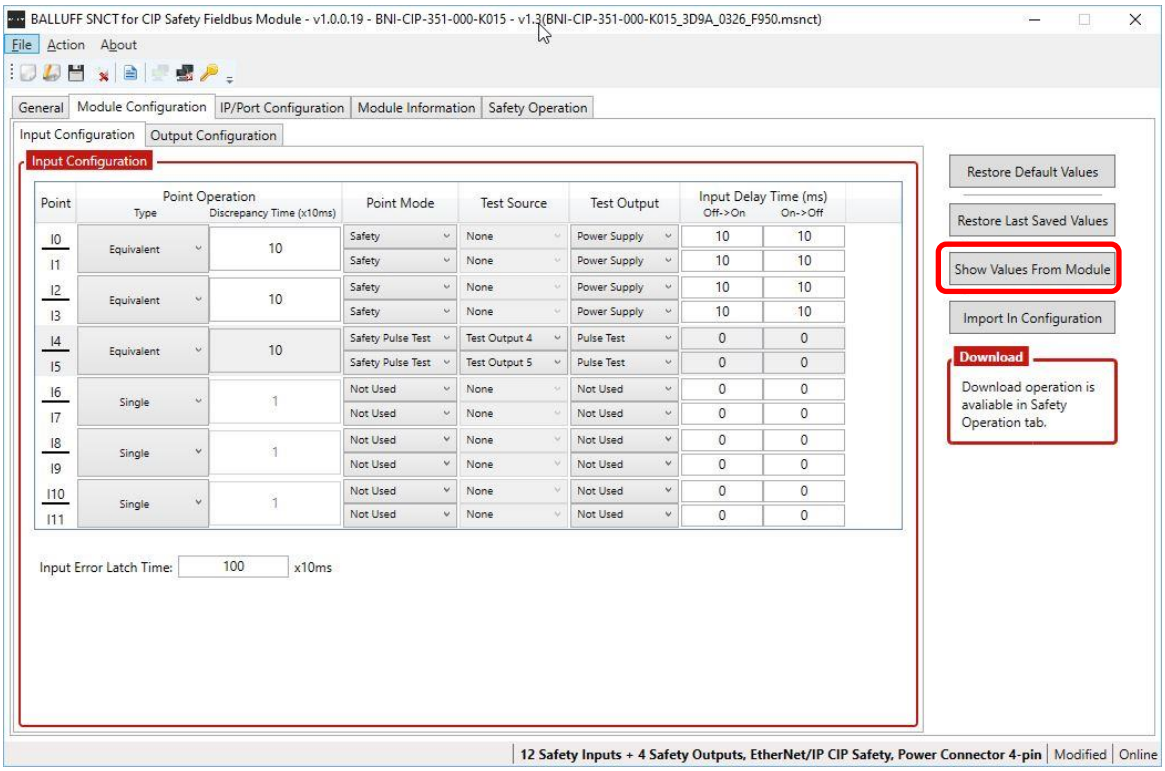


Verifizierung der übertragenen Modulkonfiguration

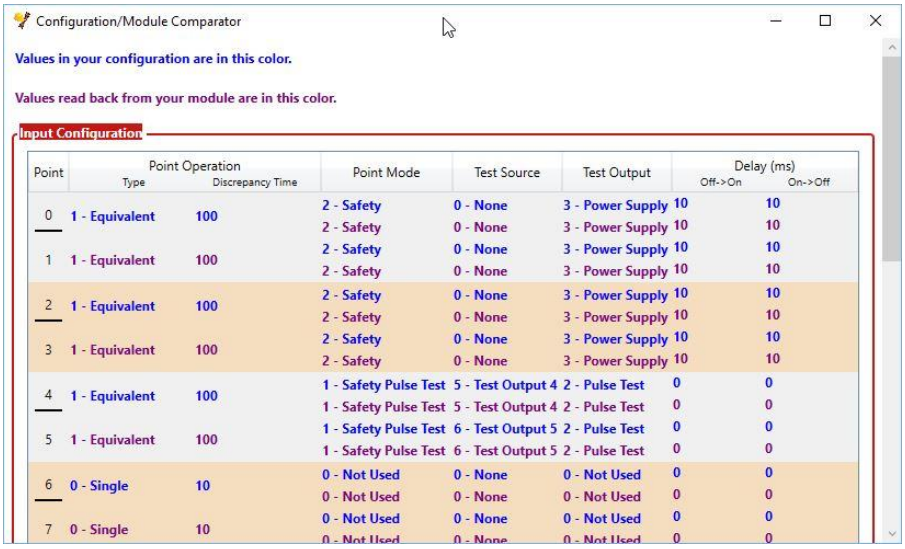
Das Modul ist jetzt konfiguriert. Sie können die Konfigurationssignatur verifizieren, indem Sie auf die Schaltfläche
Read from device (Aus dem Gerät lesen) klicken, um zu überprüfen, ob die SNCT-Konfiguration und die Gerätekonfiguration identisch sind.



Im Rahmen des Sicherheitsprozesses muss visuell überprüft werden, ob die Parameter des Sicherheitseingangs und des Sicherheitsausgangs übereinstimmen. Gehen Sie zum Register *Module Configuration* (Modulkonfiguration) und klicken Sie auf *Show Values from Module* (Werte aus Modul anzeigen).



In einem Fenster werden die einzelnen E/A-Parameter nacheinander aufgelistet.



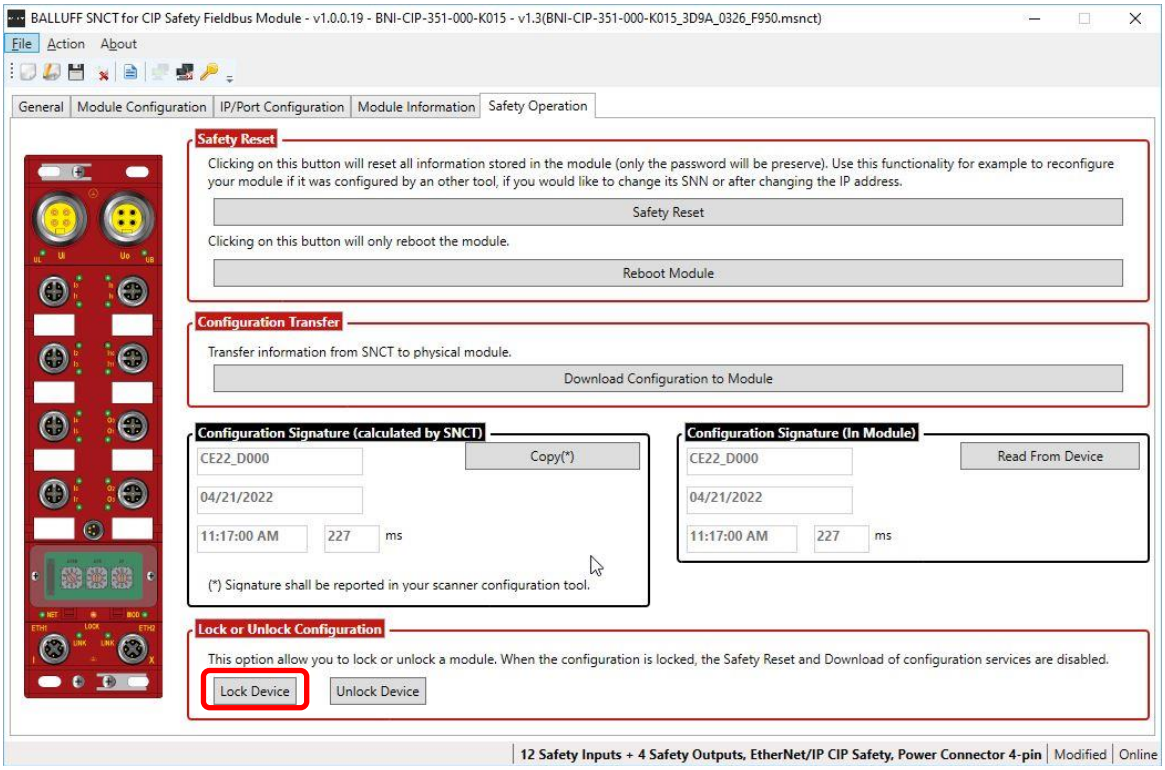
Hinweis!

Gefundene Unterschiede werden absichtlich nicht hervorgehoben, da die Überprüfung von einer Sicherheitsexpertenstelle und nicht durch die SNCT-Software durchgeführt werden muss.

Warnung!

Im Rahmen des Sicherheitsprozesses muss ein Testsystem von jedem konfigurierten sicheren Eingang und sicheren Ausgang realisiert werden. Die Tests müssen von einem Sicherheitsexperten durchgeführt und dokumentiert werden.

Sperren Sie die Konfiguration, um sie vor einer Änderung durch Benutzer zu schützen.

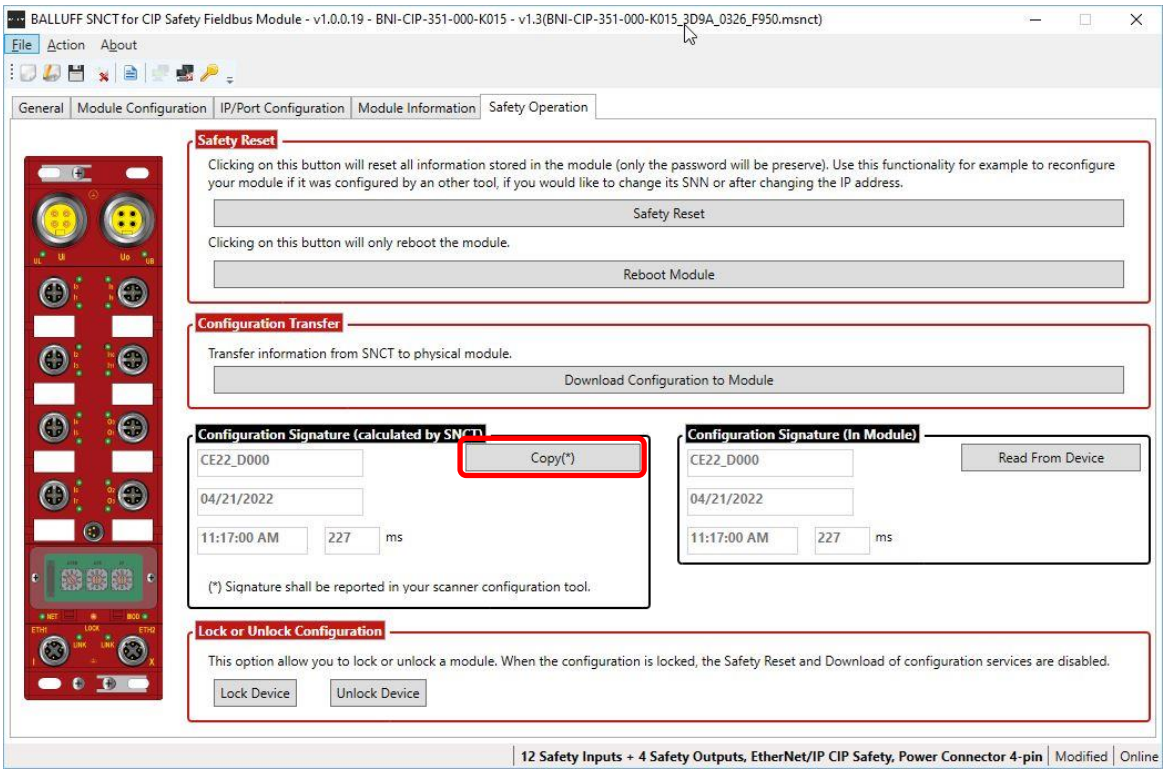


Das Modul ist jetzt gesperrt.

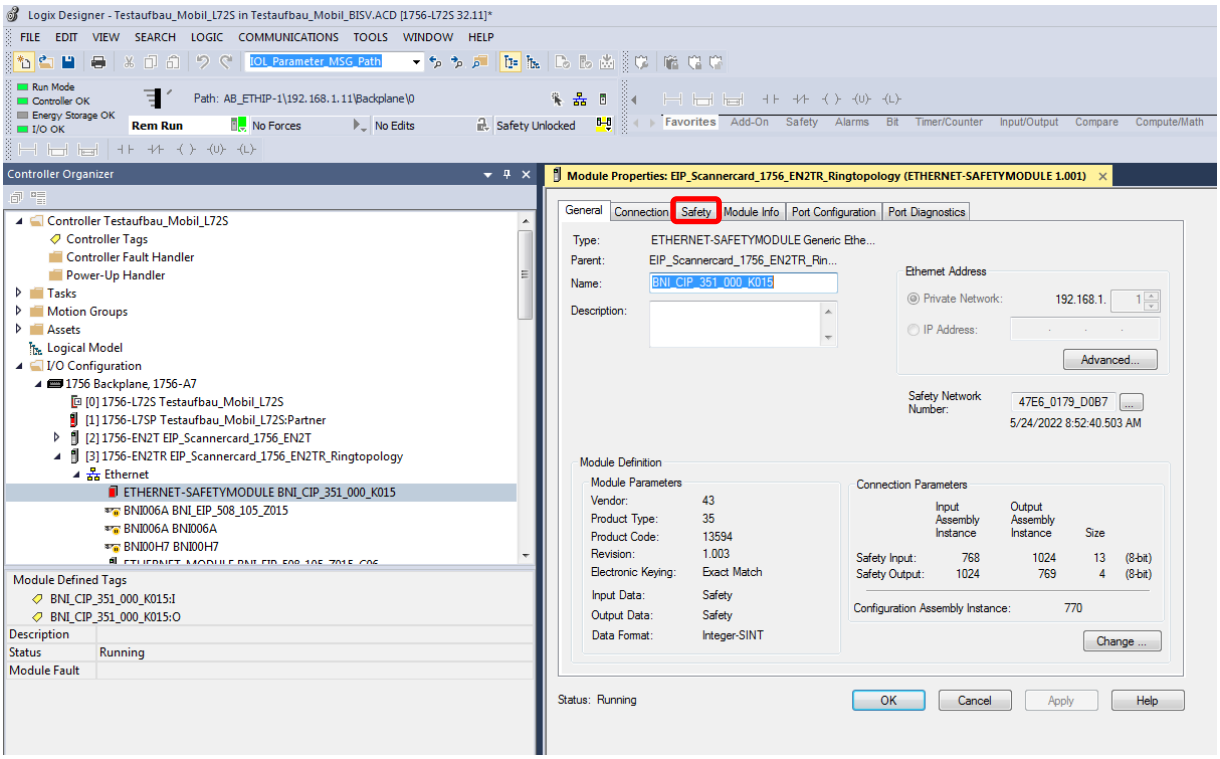
7.8. Verbinden und Testen des Sicheren E/A-Moduls in RSLogix 5000

Importieren der Modulsignatur in Logix5000

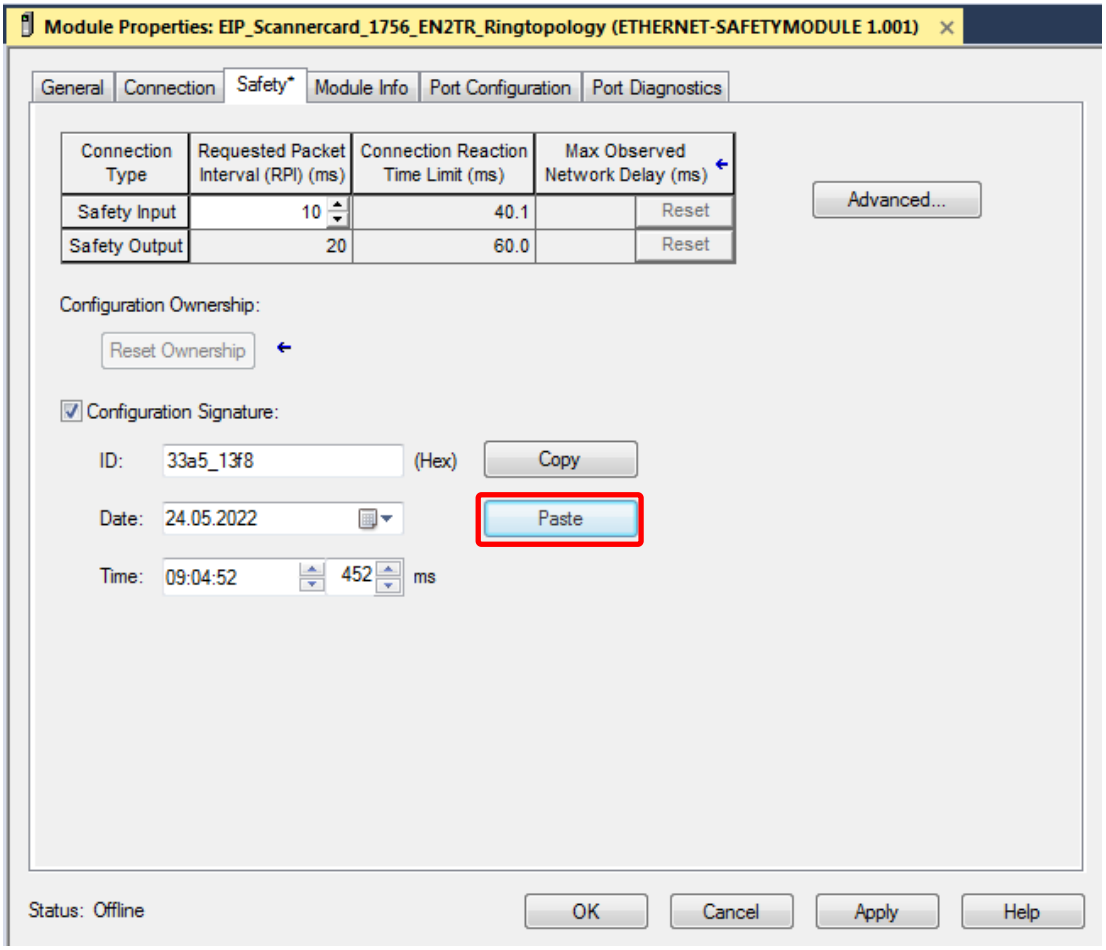
Gehen Sie zu *Safety Operation* (Sicherheitsbetrieb) und wählen Sie *Copy* (Kopieren).



Öffnen Sie in RSLogix das Eigenschaftsfenster des Sicheren E/A-Moduls und wählen Sie das Register *Safety* (Sicherheit).



Klicken Sie auf die Schaltfläche *Paste* (Einfügen).

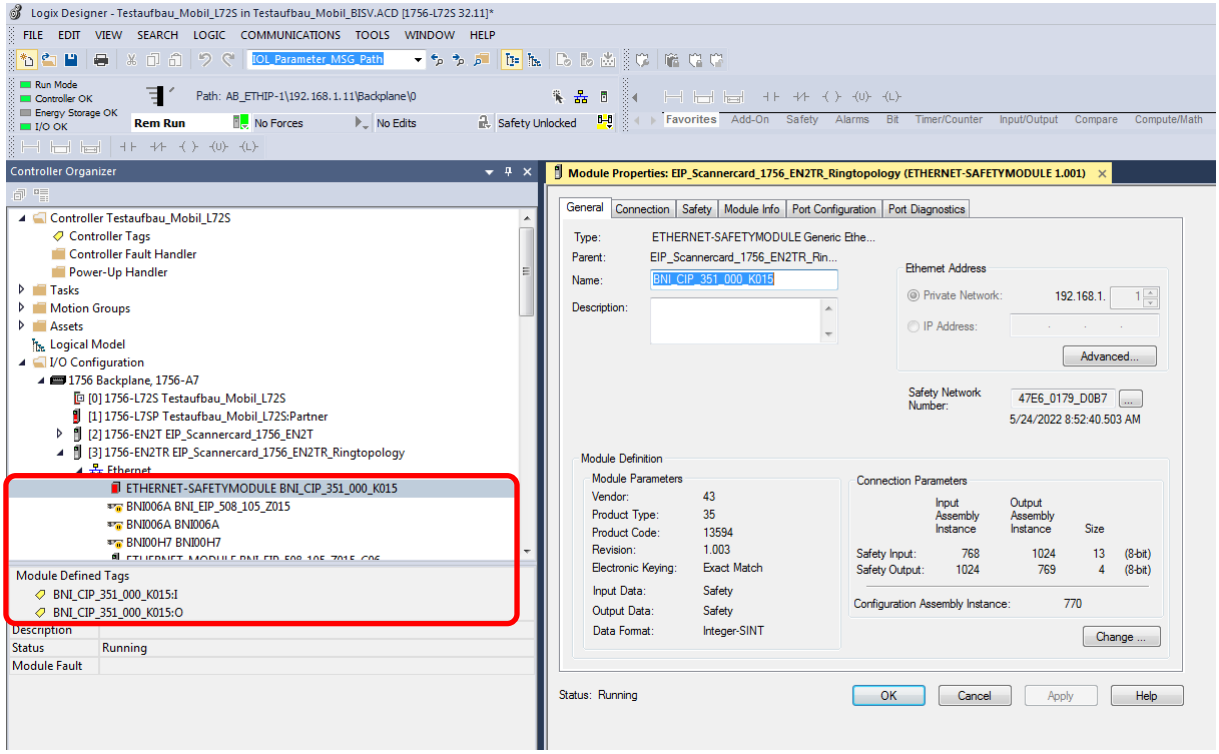


Um die Konfiguration abzuschließen, passen Sie das RPI für die Sicherheitseingangsverbindung auf den erforderlichen Wert an.

Warnung!
Das Mindest-RPI für das Sichere E/A-Modul ist 10 ms.

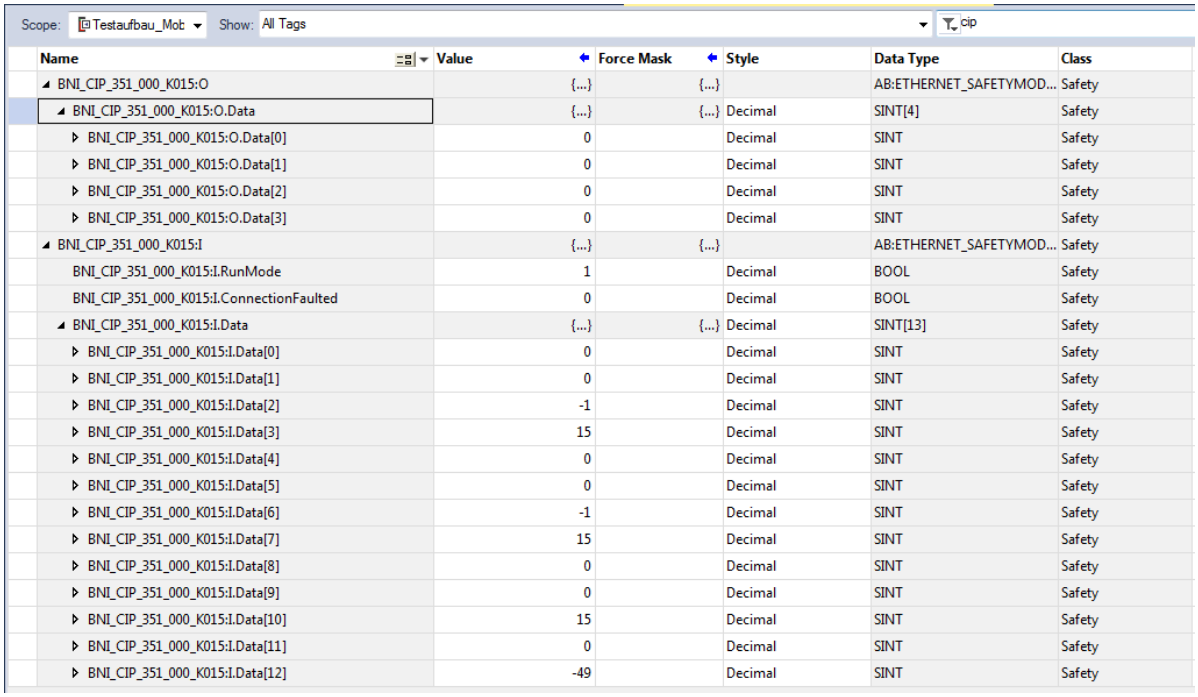
Warnung!
Wenn die Option Configuration Signature (Konfigurationssignatur) nicht aktiviert ist, muss autorisiertes Personal sicherstellen, dass die Konfiguration der Steuerung und des Sicheren E/A-Moduls korrekt ist.

Gehen Sie online und laden Sie das Projekt herunter. Schalten Sie die Sicherheitssteuerung in den Run-Modus.



Die Verbindung des Sicheren E/A-Moduls ist hergestellt und aktiv.

Sie können jetzt auf die Sicherheitsprozessdaten zugreifen und beginnen, die Sicherheitskontrollanwendung zu schreiben.



Name	Value	Force Mask	Style	Data Type	Class
BNI_CIP_351_000_K015:O	{...}	{...}		AB:ETHERNET_SAFETYMOD...	Safety
BNI_CIP_351_000_K015:O.Data	{...}	{...}	Decimal	SINT[4]	Safety
BNI_CIP_351_000_K015:O.Data[0]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:O.Data[1]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:O.Data[2]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:O.Data[3]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I	{...}	{...}		AB:ETHERNET_SAFETYMOD...	Safety
BNI_CIP_351_000_K015:I.RunMode	1		Decimal	BOOL	Safety
BNI_CIP_351_000_K015:I.ConnectionFaulted	0		Decimal	BOOL	Safety
BNI_CIP_351_000_K015:I.Data	{...}	{...}	Decimal	SINT[13]	Safety
BNI_CIP_351_000_K015:I.Data[0]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[1]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[2]	-1		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[3]	15		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[4]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[5]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[6]	-1		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[7]	15		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[8]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[9]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[10]	15		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[11]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[12]	-49		Decimal	SINT	Safety

8. EtherNet/IP-Verhalten

In diesem Kapitel wird das Verhalten des Sicheren E/A-Moduls im Hinblick auf die EtherNet/IP-Kommunikation beschrieben.

8.1. E/A-Verhalten

Wenn das Sichere E/A-Modul läuft (Scanner-Verbindung aktiv) und das Modul einen Abbruch der Verbindung zum Scanner feststellt, setzt das Modul die Prozessdaten des Sicherheitsausgangs automatisch auf “0”.

Die Erkennung eines Abbruchs der Verbindung zum Scanner wird basierend auf dem Timeout (Multiplikator x RPI) berechnet, der in der vom Scanner gesendeten E/A-Verbindung (Sichere Forward Open-Anfrage) definiert ist.

8.2. IDLE-Verhalten

Ein EtherNet/IP-Scanner kann die Prozessdaten des Sicherheitsausgangs im IDLE-Modus produzieren (im Normalfall erfolgt dieser Vorgang im Programmiermodus). In diesem Fall hält der Controller seine E/A-Verbindungen offen, informiert aber die Geräte darüber, dass die Ausgangsprozessdaten nicht verarbeitet werden dürfen.

Wenn das Sichere E/A-Modul Sicherheitsausgangsdaten im IDLE-Modus empfangen hat:

- setzt das Modul alle seine Sicherheitsausgangsdaten auf 0
- produziert das Modul seine Sicherheitseingangsdaten zum Scanner

8.3. Doppelte IP-Adresse

Das Sichere E/A-Modul führt eine Überprüfung auf doppelte IP-Adressen nach der ACD-Methode (Erkennung von IPv4-Adresskonflikten) durch, die von ODVA und RFC 5227 definiert wird.

Mit dieser Funktion soll sichergestellt werden, dass die IP-Adresse nicht von einem anderen Gerät im Netzwerk verwendet wird. Dieser Mechanismus wird beim Start des Moduls, während des Betriebs des Moduls (wenn ein neues Gerät ins Netzwerk eingebunden wird, das versucht, dieselbe IP-Adresse zu verwenden) oder nach dem Software-Reset (CIP-Objekt 0x01, Instanz 1 Service 5) ausgeführt.

Wenn das Modul ein anderes Gerät mit derselben IP-Adresse erkennt, geschieht Folgendes:

- Das Modul verteidigt seine IP-Adresse.
- Wenn der Konflikt bestätigt wird
  - Das Modul gibt seine IP-Adresse frei.
  - Die Diagnose-LEDs des Moduls NET, LOCK und MOD blinken **ROT**

8.4. EtherNet/IP-Objektklassen

Identität (0x01)

Dieses Objekt ermöglicht das Lesen der Identität des Moduls.

Klassenattribute

ID	Beschreibung	Get	Set	Limits
01h	Revision	●	○	1
02h	Max. Instanz	●	○	1
03h	Anzahl der Instanzen	●	○	1

● Unterstützt ○ Nicht unterstützt

Klassenservices

ID	Service	Param.-optionen
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instanzattribute

ID	Beschreibung	Get	Set	Limits
01h	Hersteller-ID	●	○	8
02h	Gerätetyp	●	○	12
03h	Produktcode	●	○	Je nach Produkt
04h	Revision	●	○	Je nach Revision
05h	Status	●	○	
06h	Seriennummer	●	○	
07h	Produktname	●	○	Je nach Produkt

● Unterstützt ○ Nicht unterstützt

Instanzservices

ID	Service	Param.-optionen
01h	Get_Attributes_All	
05h	Reset	
0Eh	Get_Attribute_Single	

Nachrichten-Router (0x02)

Klassenattribute

ID	Beschreibung	Get	Set	Limits
1	Revision	○	○	
4	Optionale Attribut-Liste	○	○	
5	Optionale Service-Liste	○	○	
6	Max. ID von Klassenattributen	○	○	
7	Max. ID von Instanzattributen	○	○	

● Unterstützt ○ Nicht unterstützt

Klassenservices

Service		Param.-optionen
Get_Attributes_All	○	
Get_Attribute_Single	○	

● Unterstützt ○ Nicht unterstützt

Instanzattribute

ID	Beschreibung	Get	Set	Limits
1	Objektliste	○	○	
2	Max. unterstützte Verbindungen	○	○	
3	Anzahl von aktiven Verbindungen	○	○	
4	Liste der aktiven Verbindungen	○	○	

● Unterstützt ○ Nicht unterstützt

Instanzservices

Service		Param.-optionen
Get_Attributes_All	○	
Get_Attribute_Single	○	

● Unterstützt ○ Nicht unterstützt

Baugruppe (0x04)

Dieses Objekt ermöglicht den Zugriff auf E/A-Prozessdaten.

Klassenattribute

ID	Beschreibung	Get	Set	Limits
01h	Revision	●	○	2
02h	Max. Instanz	●	○	199
03h	Anzahl der Instanzen	●	○	4

● Unterstützt ○ Nicht unterstützt

Klassenservices

Service		Param.-optionen
Get_Attribute_Single	●	

● Unterstützt ○ Nicht unterstützt

Instanzattribute

ID	Beschreibung	Get	Set	Limits
03h	Daten	●	●	Der Set-Befehl ist nicht möglich, wenn eine exklusive Besitzerverbindung offen ist

● Unterstützt ○ Nicht unterstützt

Instanzservices

ID	Service	Param.-optionen
0Eh	Get_Attribute_Single	
10h	Set_Attribute_Single	

Verbindungsmanager (0x06)

Klassenattribute

ID	Beschreibung	Get	Set	Limits
01h	Revision	●	○	1
02h	Max. Instanz	●	○	1
03h	Anzahl der Instanzen	●	○	1

● Unterstützt ○ Nicht unterstützt

Klassenservices

ID	Service	Param.-optionen
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instanzattribute

ID	Beschreibung	Get	Set	Limits
01h	Offene Anfragen	●	○	
02h	Offene Formatablehnungen	●	○	
03h	Offene Ressourcen-Ablehnungen	●	○	
04h	Offene Sonstige Ablehnungen	●	○	
05h	Geschlossene Anfragen	●	○	
06h	Geschlossene Formatanfragen	●	○	
07h	Geschlossene Sonstige Anfragen	●	○	
08h	Verbindungs-Timeouts	●	○	

● Unterstützt ○ Nicht unterstützt

Instanzservices

ID	Service	Param.-optionen
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	
4Eh	Forward_Close	
54h	Forward_Open	

5Bh	Large_Forward_Open	Nur Klasse 3

TCP/IP-Schnittstelle (0xF5)

Klassenattribute

ID	Beschreibung	Get	Set	Limits
01h	Revision	●	○	2
02h	Max. Instanz	●	○	1
03h	Anzahl der Instanzen	●	○	1

● Unterstützt ○ Nicht unterstützt

Klassenservices

ID	Service	Param.-optionen
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instanzattribute

ID	Beschreibung	Get	Set	Limits
1	Status	●	○	
2	Konfigurationsfähigkeit	●	○	
3	Konfigurationskontrolle	●	●	
4	Physischer Link	●	○	
5	Interface Configuration	●	●	
6	Host-Name	●	●	
7	Sicherheitsnetzwerknummer	●	●	
8	TTL-Wert	○	○	
9	Mcast-Konfig	○	○	
10	Auswahl ACD	●	●	
11	LetzterKonfliktErkannt	●	●	
12	EtherNet/IP-Schnellverbindung	●	●	

● Unterstützt ○ Nicht unterstützt

Instanzservices

ID	Service	Param.-optionen
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	
10h	Set_Attribute_Single	

Ethernet-Link (0xF6)

Klassenattribute

ID	Beschreibung	Get	Set	Limits
01h	Revision	●	○	3
02h	Max. Instanz	●	○	3
03h	Anzahl der Instanzen	●	○	3

● Unterstützt ○ Nicht unterstützt

Klassenservices

ID	Service	Param.-optionen
0Eh	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instanzattribute

ID	Beschreibung	Get	Set	Limits
01h	Schnittstellen-geschwindigkeit	●	○	
02h	Schnittstellen-Flags	●	○	
03h	Physische Adresse	●	○	
04h	Schnittstellenzähler	●	○	
05h	Medienzähler	●	○	
06h	Schnittstellenkontrolle	●	●	
07h	Schnittstellentyp	○	○	
08h	Schnittstellenzustand	○	○	
09h	Admin-Zustand	○	●	
10h	Schnittstellen-kennzeichnung	●	○	

● Unterstützt ○ Nicht unterstützt

Instanzservices

ID	Service	Param.-optionen
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	
10h	Set_Attribute_Single	
4Ch	Get_and_Clear	

DLR (0x47)

Klassenattribute

ID	Beschreibung	Get	Set	Limits
01h	Revision	●	○	3
02h	Max. Instanz	●	○	1

● Unterstützt ○ Nicht unterstützt

Klassenservices

ID	Service	Param.-optionen
0Eh	Get_Attribute_Single	

Instanzattribute

ID	Beschreibung	Get	Set	Limits
01h	Netzwerktopologie	●	○	0 steht für “Linear” 1 steht für “Ring”
02h	Netzwerkstatus	●	○	0 steht für “Normal” 1 steht für “Ring-Fehler” 2 steht für “Unerwartete Schleife erkannt” 3 steht für “Partieller Netzwerkfehler” (nicht erwartet)
10h	Aktive Supervisor-Adresse	●	○	IP- und/oder MAC-Adresse des aktiven Ring-Supervisors
12h	Fähigkeitsflags	●	○	Wert 0x02 Beacon-basierter Ring-Knoten

● Unterstützt ○ Nicht unterstützt

Instanzservices

ID	Service	Param.-optionen
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	

QoS (0x48)

Klassenattribute

ID	Beschreibung	Get	Set	Limits
01h	Revision	●	○	1
02h	Max. Instanz	●	○	1
03h	Anzahl der Instanzen	●	○	1

● Unterstützt ○ Nicht unterstützt

Klassenservices

ID	Service	Param.-optionen
0Eh	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instanzattribute

ID	Beschreibung	Get	Set	Limits
04h	DSCP Dringend	●	●	
05h	DSCP Geplant	●	●	
06h	DSCP Hoch	●	●	
07h	DSCP Niedrig	●	●	
08h	DSCP Explizit	●	●	

● Unterstützt ○ Nicht unterstützt

Instanzservices

ID	Service	Param.-optionen
0Eh	Get_Attribute_Single	
10h	Set_Attribute_Single	

9. Produktaustausch

In diesem Kapitel wird die Strategie bei einem Austausch eines bereits in Betrieb genommenen Sicheren E/A-Moduls beschrieben.

9.1. Vor dem Start

In diesem Kapitel wird erläutert, wie ein defektes Produkt in einer vorhandenen Anwendung ersetzt wird, ohne dass dabei eine vollständige Inbetriebnahme eines neuen Moduls durchgeführt werden muss, indem das defekte Modul verwendet wird.

Hinweis!

Wenn das neue Modul nicht den Speicherschlüssel des defekten Moduls verwendet. Siehe Abschnitt Produktbereitstellung für Informationen zur standardmäßigen Inbetriebnahme mit dem SNCT-Konfigurationstool.

Wichtig!

Wenn der Speicherschlüssel für den Produktaustausch verwendet werden soll, muss der Endbenutzer mit zusätzlichen Maßnahmen während der Austauschverifizierung sicherstellen, dass die SIL3-Integrität gewährleistet ist.

Wenn diese Maßnahmen angewandt werden können, kann der Speicherschlüsselaustausch nicht vorgenommen werden. Siehe Abschnitt Produktbereitstellung für Informationen zur standardmäßigen Inbetriebnahme mit dem SNCT-Konfigurationstool.

Dieser automatische Produktaustauschvorgang ist möglich, da der Speicherschlüssel am Modul angeschlossen ist. Verwenden Sie den internen Schlüssel im Fenster (siehe Abschnitt Speicherschlüssel für weitere Informationen). Auf dem Speicherschlüssel sind alle Modulinformationen gespeichert. Ohne den Schlüssel kann das Sichere E/A-Modul nicht betrieben werden.

Überprüfen Sie vor dem Austausch eines defekten Produkts Folgendes:

- Das System (Maschine, Anwendung...) ist angehalten und in einem sicheren Zustand.

Hinweis!

Während des Austauschs des Moduls muss die Spannungsversorgung ausgeschaltet werden. Dadurch können in Abhängigkeit von der Systemarchitektur (z.B. Daisy-Chain-/Spannungsversorgungstopologie) Störungen bei anderen Geräten verursacht werden.

- Das neue Sichere E/A-Modul muss strikt dem defekten Produkt entsprechen (identische Teilenummer, gleiche Produktversion → die entsprechenden Angaben finden Sie auf den rückseitigen und seitlichen Etiketten am Produkt), andernfalls **ist eine neue Inbetriebnahme erforderlich**.

- Das neue Sichere E/A-Modul darf keine Konfiguration besitzen (d.h. Werkseinstellungen). Wenn Sie sich nicht sicher sind, können Sie eine Sicherheitsrücksetzung ausführen, um die Modulkonfiguration zu löschen.

- Lokalisieren und identifizieren Sie unbedingt alle Kabel / Kabelsätze, die mit dem Modul verbunden sind, um einen fehlerhaften Anschluss zu vermeiden.

- Sie haben die erforderlichen Fähigkeiten, um diesen Austausch vorzunehmen.

9.2. Austauschvorgang

Führen Sie diese Schritte durch, um ein Modul erfolgreich auszutauschen:

1. Trennen Sie die 7/8''-Spannungsversorgungskabel.

Gefahr!

Lebensgefahr durch elektrischen Strom!

Nachdem das Gerät von der Hauptspannungsversorgung getrennt wurde, sollten Teile wie die Stromanschlüsse erst dann berührt werden, wenn sich die Kondensatoren im Gerät entladen haben.

Darum gilt:

Beachten Sie die Entladezeiten der Kondensatoren; berühren Sie stromführende Teile erst nach einer Wartezeit von 30 Sekunden.

Wenn weitere verbundene Kondensatoren innerhalb der Gesamtverbindung vorhanden sind, kann die Entladung der Gesamtverbindung deutlich länger dauern. In diesem Fall müssen Sie die erforderliche Wartezeit bestimmen oder sogar anhand von Messungen ermitteln, ob das Gerät sicher ist.

2. Trennen Sie die Ethernet-Kabel.
3. Trennen Sie die Kabel, die mit den sicheren E/A-Geräten verbunden sind.
4. Ergreifen Sie Maßnahmen zur Vermeidung einer elektrostatischen Entladung im Modul oder in seinem Zubehör.
5. Entfernen Sie das Sichere E/A-Modul von der Systemhalterung.
6. Beachten Sie die Position der metallischen Erdungsplatte der Ethernet-Anschlüsse.
7. Beachten Sie die Position 3 Drehschalter.
8. Entfernen Sie den Speicherschlüssel, öffnen Sie das Modulfenster und trennen Sie den Schlüssel mit einem geeigneten Werkzeug. Berühren Sie nicht die freiliegenden Teile der Leiterplatte.
9. Bewahren Sie das defekte Modul an einem geeigneten Ort auf (z.B. Recycling-Stelle).

Der erste Teil des Vorgangs ist abgeschlossen. Das defekte Modul ist entfernt und wird durch ein neues Modul ersetzt.

10. Packen Sie das neue Modul aus.
11. Entfernen Sie den Speicherschlüssel und setzen Sie den Schlüssel des defekten Moduls ein, öffnen Sie das Modulfenster und trennen Sie den vorhandenen Schlüssel mit einem geeigneten Werkzeug. Installieren Sie den alten Schlüssel unter Beachtung der Einbaurichtung und schließen Sie das Fenster.
12. Konfigurieren Sie die 3 Drehschalter; öffnen Sie das Modulfenster und drehen Sie die einzelnen Drehschalter in die Positionen, die im Schritt 7 vermerkt wurden.
13. Platzieren Sie die metallische Erdungsplatte der Ethernet-Anschlüsse in der Position, die im Schritt 6 vermerkt wurde.
14. Ersetzen Sie das Modul auf seiner Halterung.
15. Schließen Sie die Kabel wieder an den sicheren E/A-Geräten an.

16. Schließen Sie die Ethernet-Kabel wieder an.
17. Schließen Sie das 7/8''-Spannungsversorgungskabel wieder an.
18. Vergewissern Sie sich, dass alle nicht verwendeten Anschlüsse (7/8 '', M12, M8) am Modul mit einem Stopfen verschlossen sind.

9.3. Verifizierung

Das neue Sichere E/A-Modul wird gestartet. Es können verschiedene Situationen eintreten:

1. Alle E/A-Diagnose-LEDs blinken rot. Dieser Zustand gibt an, dass das neue Modul die im Speicherschlüssel gespeicherte Konfiguration nicht akzeptiert.
    a. Wiederholen Sie den Vorgang mit einem anderen Modul.

    b. Führen Sie eine Sicherheitsrücksetzung des neuen Moduls mit dem Original-Speicherschlüssel durch und führen Sie den Vorgang erneut durch.

2. Nach der Selbsttest-Sequenz beim Boot-Vorgang startet das Modul, wird aber nicht wieder mit dem Netzwerk-Controller verbunden.
    a. Überprüfen Sie, ob die Kabel (Strom, Netzwerk) ordnungsgemäß angeschlossen sind, indem Sie den Status der Diagnose-LEDs am Modul ablesen.

    b. Testen Sie die Kommunikation mit dem Modul mit Hilfe eines Netzwerktools:
        i. Senden eines PING-Befehls aus einem DOS-Fenster
        ii. Verwenden Sie die Ethernet/IP-Tool-Software (kostenlos hier erhältlich), um das Modul zu erkennen.
        iii. Starten Sie einen Web-Browser, um den Web-Server des Moduls zu verbinden.

3. Nach der Selbsttest-Sequenz beim Boot-Vorgang wird das Modul wieder mit dem Netzwerk-Controller verbunden (MOD- und NET-LEDs leuchten oder blinken grün). **Der Austausch wurde erfolgreich durchgeführt**.

Hinweis!

Wenn der Austausch nicht erfolgreich ist, stellen Sie sicher, dass das neue Modul keine Konfiguration hat. Wenn Sie sich nicht sicher sind, können Sie eine Sicherheitsrücksetzung ausführen, um die Modulkonfiguration zu löschen.

Wichtig!

Beim Austausch eines Sicherheitsgeräts ist es erforderlich, dass eine Sicherheitsexpertenstelle die korrekte Platzierung und den ordnungsgemäßen Betrieb des neuen Geräts im System überprüft.

10. SNCT-Konfigurationssoftware

In diesem Kapitel werden die wichtigen Funktionen der SNCT-Konfigurationssoftware beschrieben, die für die Inbetriebnahme des Sicheren E/A-Moduls verwendet wird.

10.1. Übersicht

Das Balluff *Safety Network Configuration Tool* (auch SNCT genannt) ist ein Windows-Softwaretool für die Sicherheitskonfiguration und Inbetriebnahme des Sicheren E/A-Moduls.

Warnung!
Balluff SNCT ist ein T3-Softwaretool gemäß der Definition von IEC61508. Aus diesem Grund muss der Benutzer alle entsprechenden Maßnahmen gemäß dem Standard für diesen Typ von Softwaretools ergreifen.

Hinweis!
Vor der Verwendung des SNCT-Tools muss die IP-Adresse des Sicheren E/A-Moduls bereits eingerichtet sein.

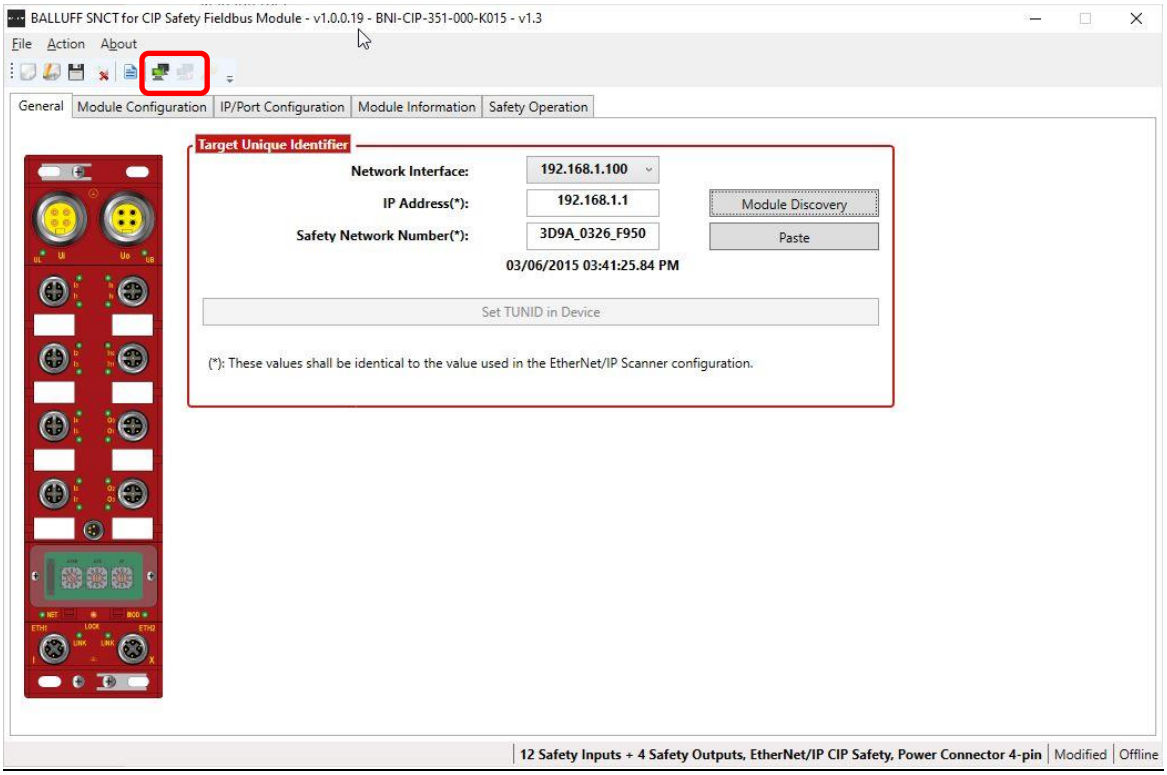
Hinweis!
Die SNCT-Software ist mit Windows 32-Bit- und 64-Bit-Betriebssystemen unter Windows XP und Windows 7 kompatibel.

Die Standard- und Sicherheitsfunktionen von SNCT umfassen:

- Erstellen, Öffnen und Speichern von Modulkonfigurationen
- Vorschau und Druck einer Modulkonfiguration
- Automatische Modulerkennung
- Festlegen von Parametern für Sicherheitseingänge und Sicherheitsausgänge
- Festlegen von TCP/IP-Parametern
- Konfiguration und Diagnose von Ethernet-Ports
- Modul-Identifizierung und Statusinformationen
- Sicherheitsmaßnahmen
  - Festlegen der Sicherheitsnetzwerknummer (SNN)
  - Sicherheitsrücksetzung
  - Modulrücksetzung
  - Übertragung der Sicherheitskonfiguration
  - Sperren und Entsperren der Modulkonfiguration
- Festlegen / Zurücksetzen von Kennwörtern für eine Konfiguration
- Erweiterte Funktionen
  - Notfallmodus (erlaubt das Lesen von Informationen vom Speicherschlüssel)
  - Firmware-Download

Die meisten Funktionen werden ausgeführt, wenn die SNCT-Software mit dem Sicheren E/A-Modul verbunden ist.

Um online/offline zu gehen, wählen Sie das Menü *Action* (Aktion) oder klicken Sie auf das folgende Symbol:



10.2. Sicherheitsrücksetzung

Die Sicherheitsrücksetzung ist ein Befehl für das zurücksetzen der benutzerspezifischen Einstellungen zwischen dem EtherNet/IP-Scanner und einem Sicheren E/A-Modul, wenn einer der unten angegebenen Parameter geändert wurde:

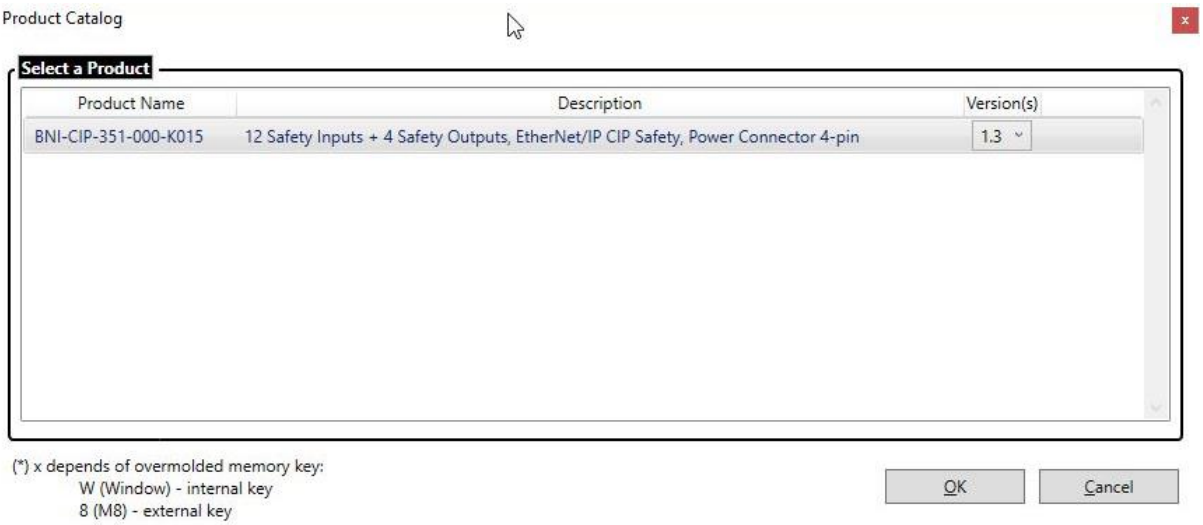
- TCP/IP-Adresse
- Netzwerknummer (SNN)
- Signatur für die Modulkonfiguration

Hinweis!
Der Befehl ist nützlich, wenn ein bereits in Betrieb genommenes Sicheres E/A-Modul auf die standardmäßigen Einstellungen der Werkskonfiguration (also Standard-SNN, keine Konfigurationssignatur und keine gespeicherte IP-Adresse) zurückgesetzt werden muss.

Hinweis!
Die Vorgehensweise basiert auf der Annahme, dass das Modul bereits in Betrieb genommen wurde und dass keine Informationen über das Modul (IP-Adresse, SNN, Sperre, Signatur, Kennwort…) bekannt sind.

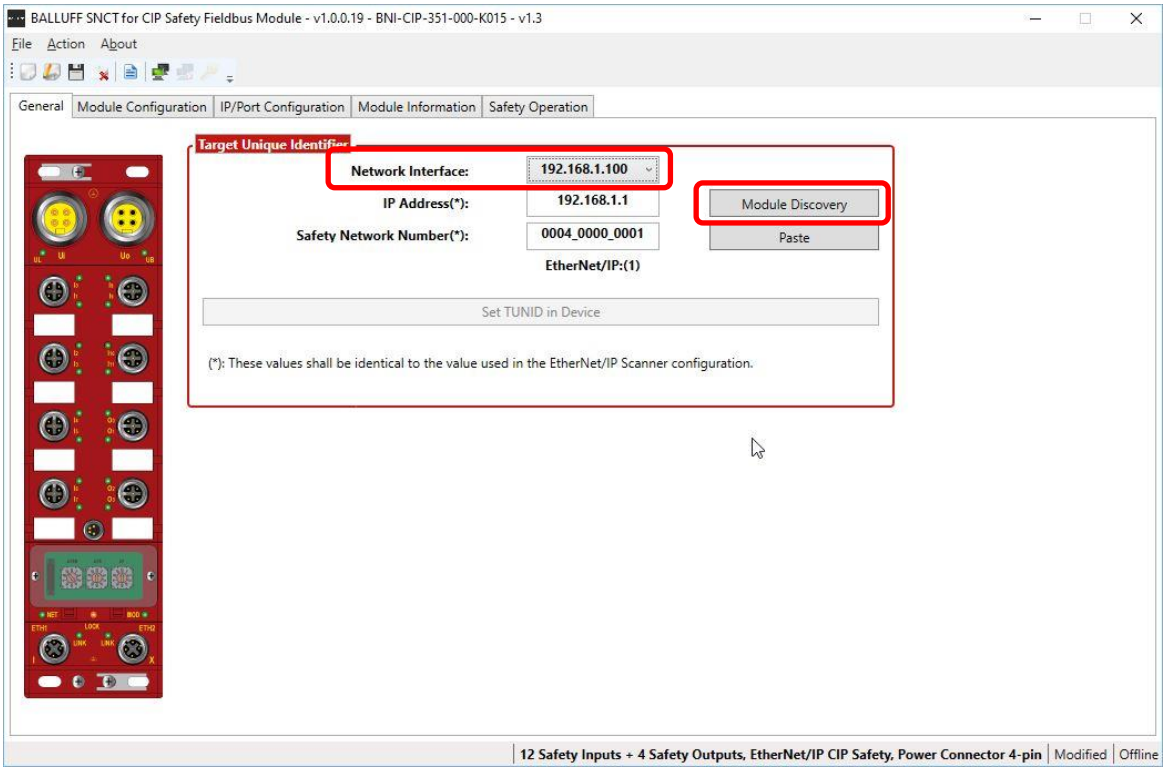
Gehen Sie folgendermaßen vor, um eine Sicherheitsrücksetzung durchzuführen:

1. Setzen Sie die Netzwerkschnittstelle des Computers auf **192.168.1.100**.
2. Öffnen Sie das Fenster des Sicheren E/A-Moduls und stellen Sie die 3 Drehschalter auf die Position **001** (was der statischen IP-Adresse **192.168.0.1** entspricht).
3. Schalten Sie das Modul ein.
4. Starten Sie die SNCT-Software.
5. Erstellen Sie ein neues Projekt (*File/New* (Datei/Neu)).
6. Wählen Sie das korrekte Modell und die korrekte Version des Sicherheitsmoduls aus.

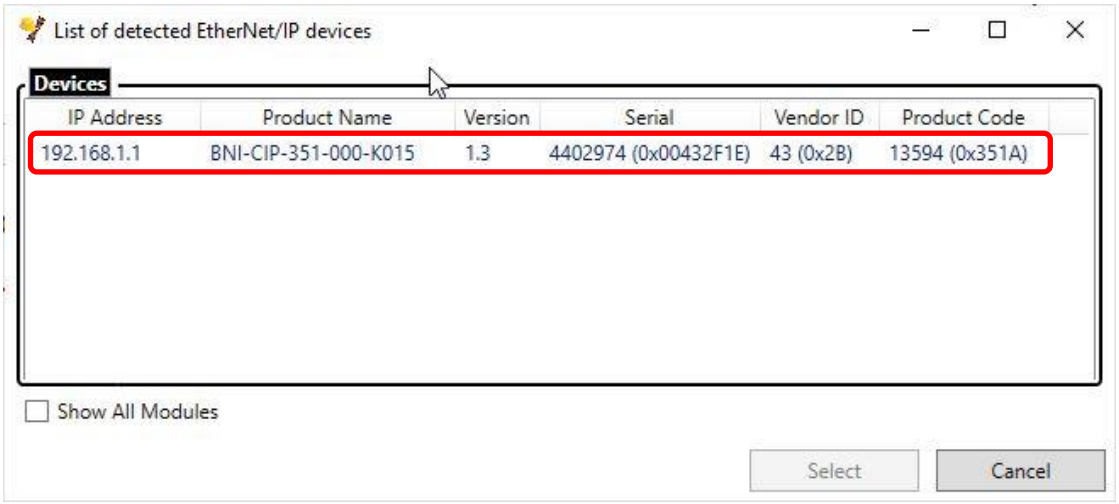


7. Wählen Sie die Netzwerkschnittstelle aus.

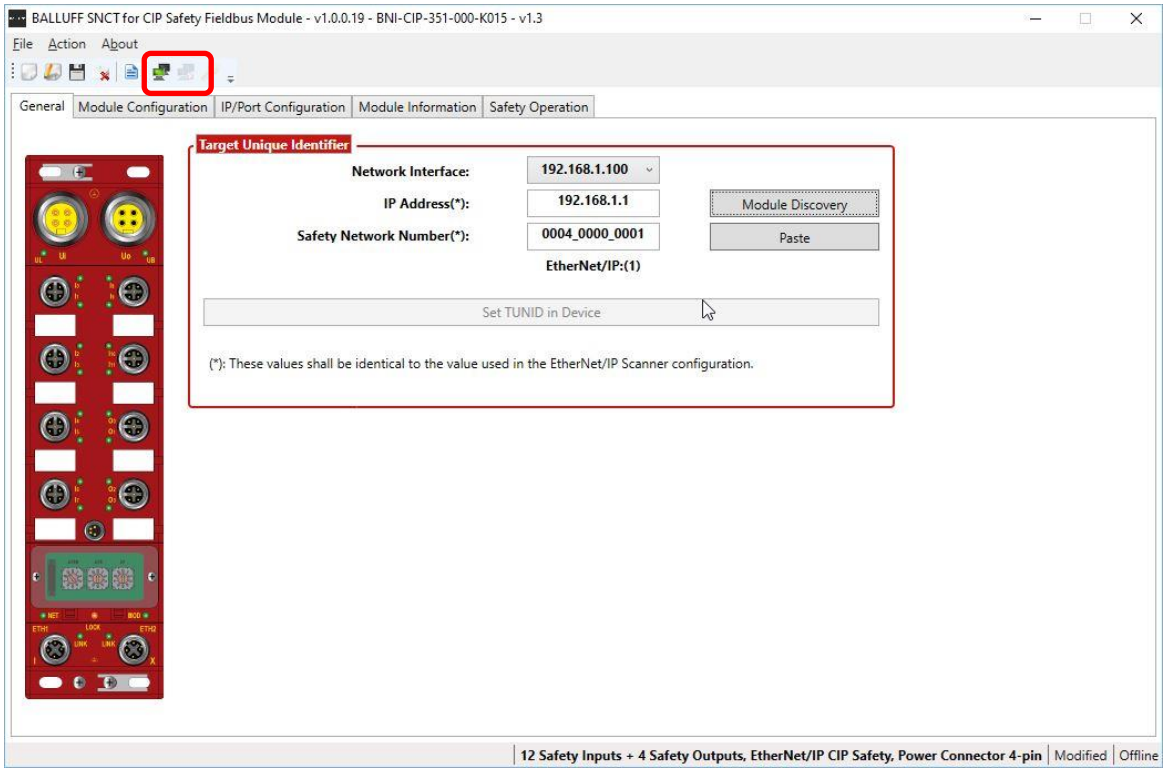
8. Führen Sie eine Modulerkennung durch.



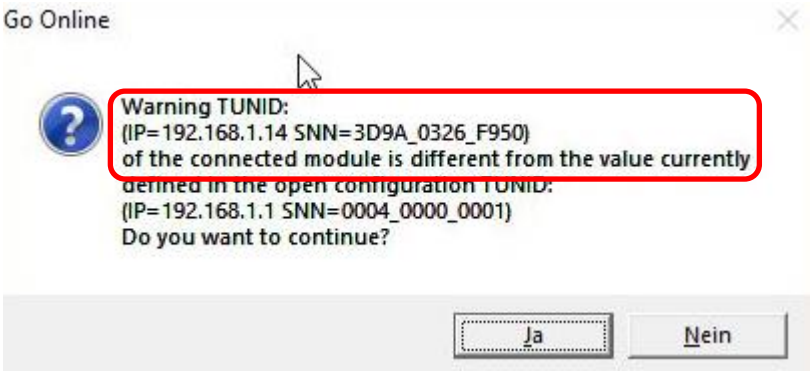
9. Doppelklicken Sie auf das Modul, um es auszuwählen.



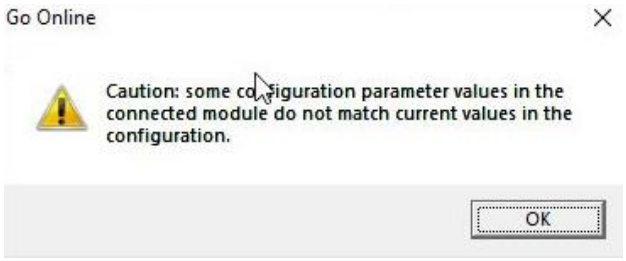
10. Gehen Sie **online**, um das Modul zu verbinden (*Action/Online* (Aktion/Online)).



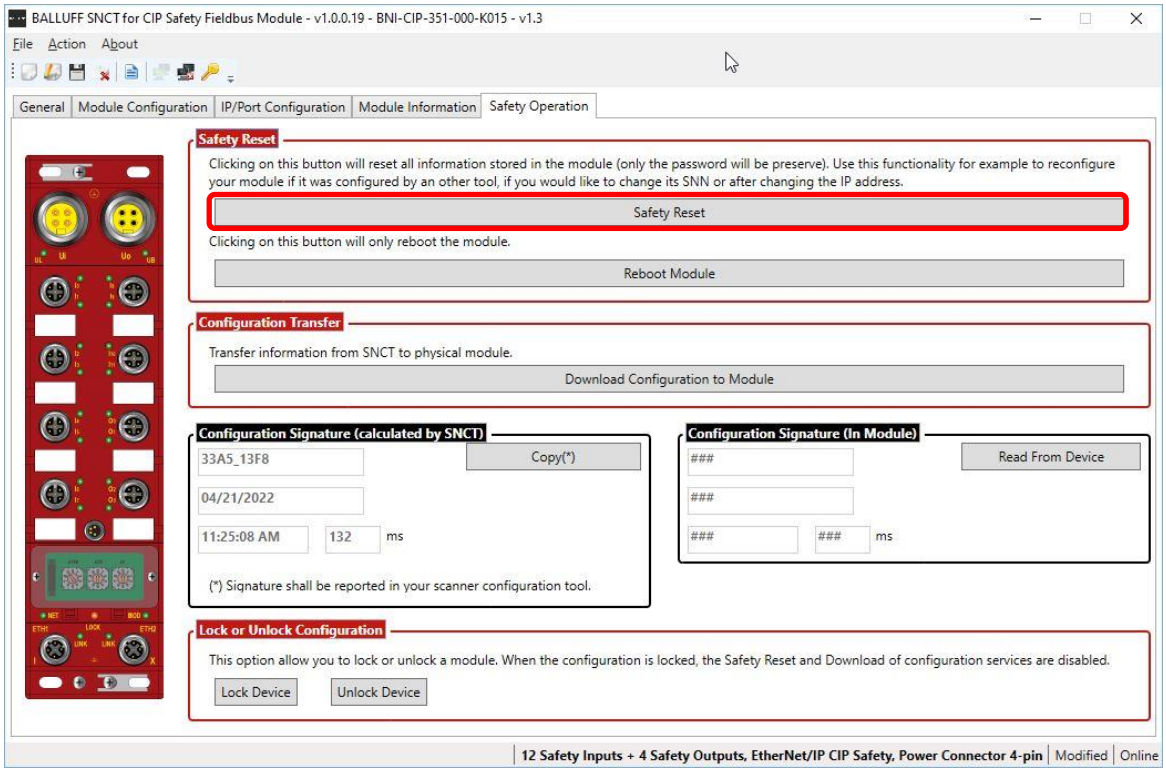
11. Die SNCT-Software erkennt eine Nichtübereinstimmung zwischen der aktuellen TUNID, die im Projekt festgelegt ist (IP / SNN), und der im physischen Modul gespeicherten TUNID.



12. Wählen Sie Yes (Ja) und dann OK.



13. Gehen Sie zum Register *Safety Operation* (Sicherheitsbetrieb).



14. Klicken Sie auf die Schaltfläche *Safety Reset* (Sicherheitsrücksetzung).

15. In einem Benachrichtigungsfeld wird darauf hingewiesen, dass alle permanenten Informationen im Modul zurückgesetzt werden (SNN, IP-Adresse, Signatur). Wählen Sie Yes (Ja).

16. In einem Benachrichtigungsfeld wird darauf hingewiesen, dass die im Projekt konfigurierte TUNID nicht mit der TUNID im physischen Modul übereinstimmt. Wählen Sie Yes (Ja).

17. Die SNCT-Software nimmt jetzt eine Überprüfung vor, um zu ermitteln, ob:
    a. Das Modul gesperrt ist
    b. Das Modul kennwortgeschützt hat

18. Wenn das Modul gesperrt ist, klicken Sie auf die Schaltfläche *Unlock Device* (Gerät entsperren).

19. Wenn das Modul kennwortgeschützt ist, geben Sie das Kennwort ein und wählen Sie dann *OK*. Wenn das Kennwort nicht bekannt ist, gehen Sie zum Abschnitt Kennwort zurücksetzen

20. Die Sicherheitsrücksetzung wurde erfolgreich durchgeführt.

21. Schalten Sie das Modul aus.

22. Gehen Sie *Offline* und schließen (*Exit*) Sie die SNCT-Software.

Hinweis!

Nach einer Sicherheitsrücksetzung ist das Sicherheitsmodul folgendermaßen konfiguriert:

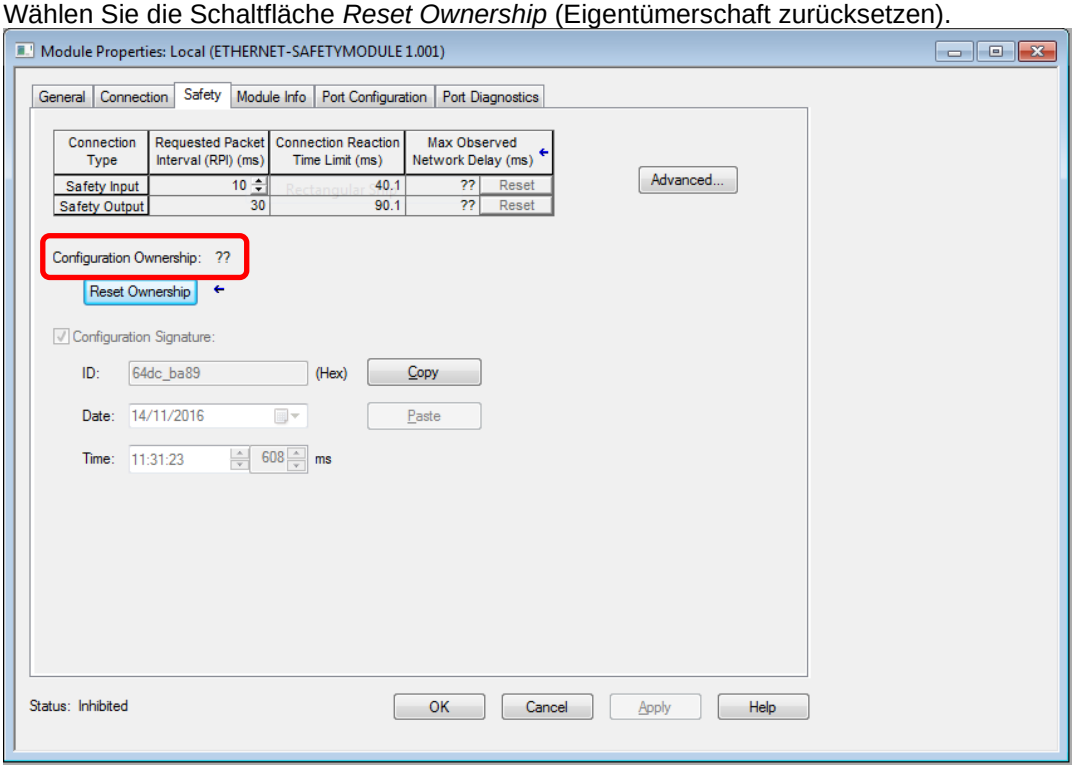
- Zustand: Warten auf TUNID
- Sperrstatus: Falsch
- IP-Adresse: DHCP oder Statisch (gemäß Drehschalter-Position)

Hinweis!

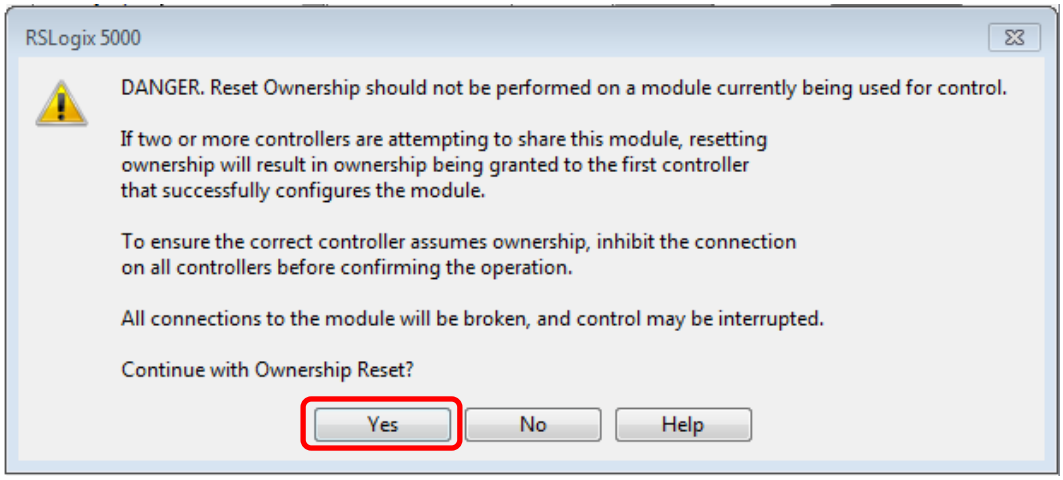
Die Sicherheitsrücksetzung kann auch mit der Rockwell Logix5000 / Studio5000-Software durchgeführt werden.

Rufen Sie das Dialogfeld für die Sicherheitseigenschaften des Moduls auf und wählen Sie das Register *Safety* (Sicherheit).

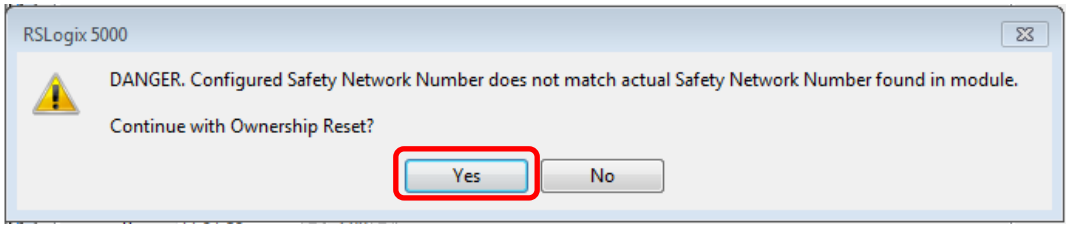
Wählen Sie die Schaltfläche *Reset Ownership* (Eigentümerschaft zurücksetzen).



Wählen Sie Yes (Ja).



Wählen Sie Yes (Ja).



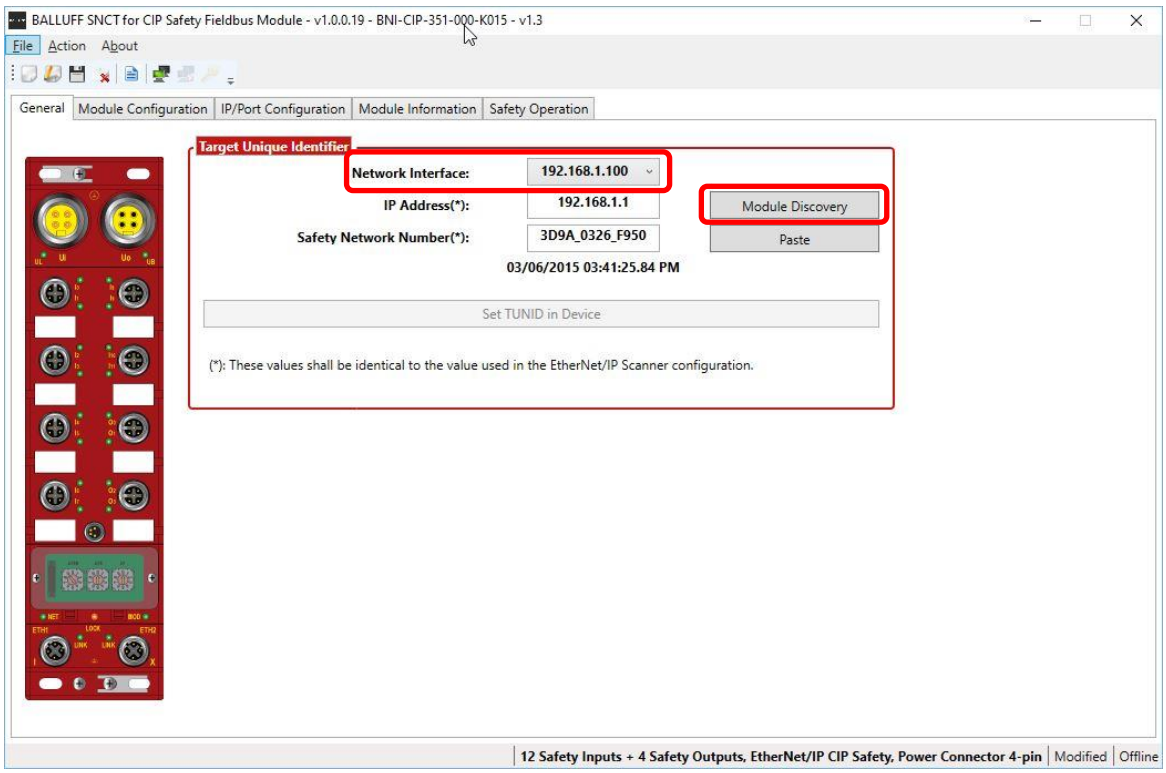
10.3. Konfiguration sperren/entsperren

Die Sperre ist eine Schutzfunktion für das Sichere E/A-Modul, mit der die Änderung der Konfiguration nach der Inbetriebnahme durch eine Sicherheitsexpertenstelle verhindert wird.

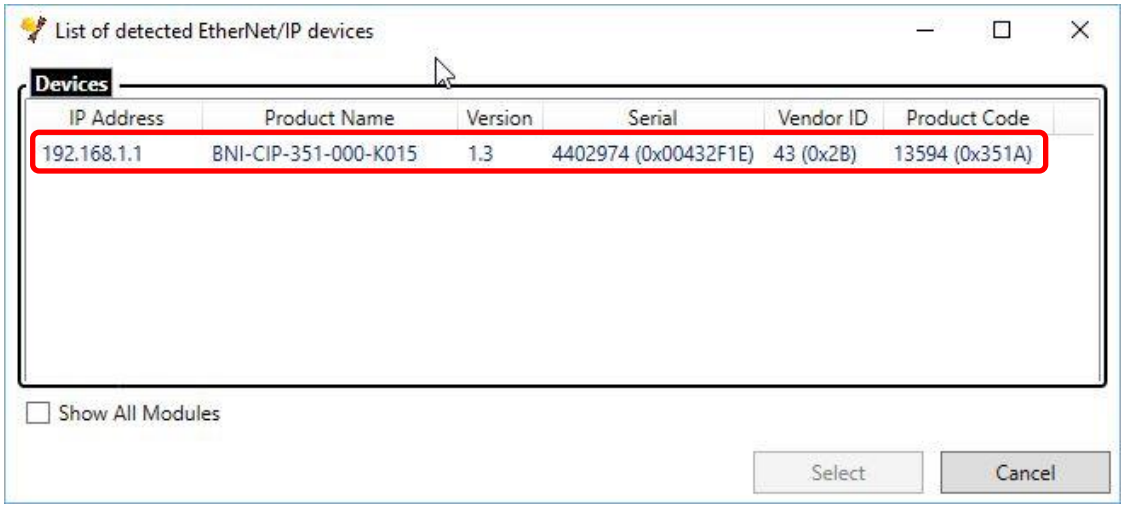
Hinweis!
Wenn das Modul kennwortgeschützt ist, muss zum Sperren und Entsperren das Kennwort eingegeben werden.

Sperren einer Modulkonfiguration

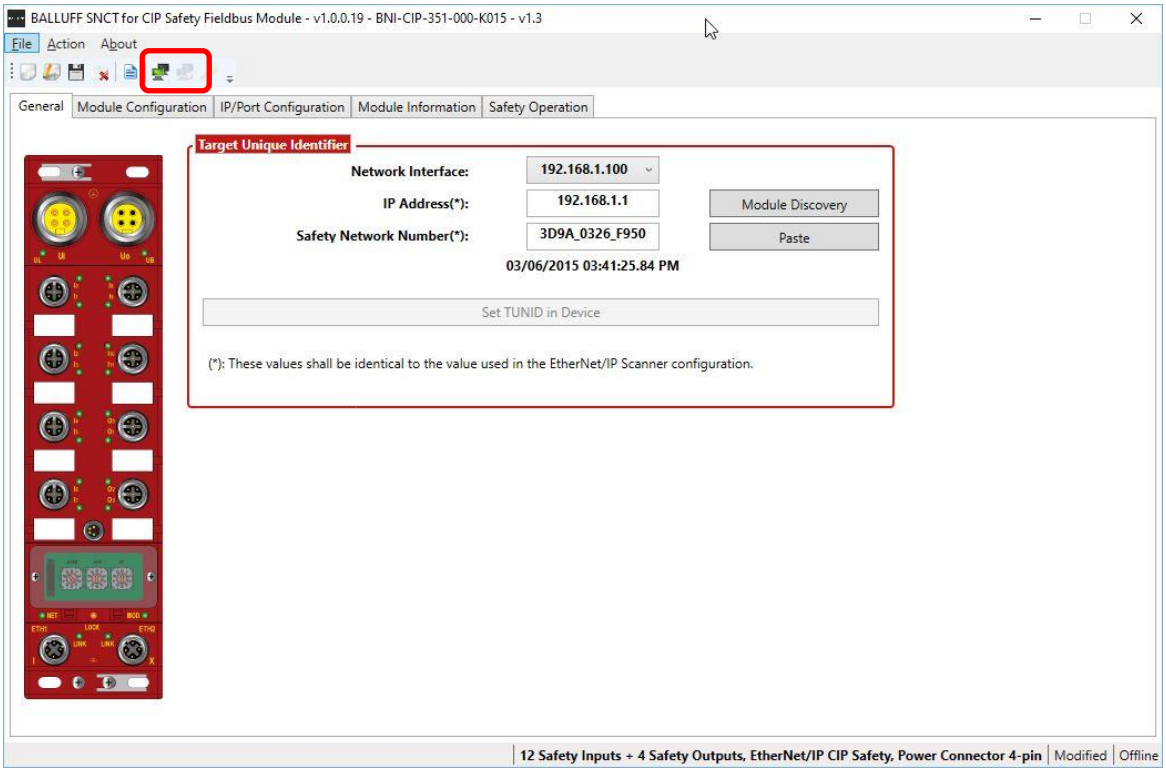
1. Starten Sie die SNCT-Software.
2. Öffnen Sie die Modulkonfiguration (File/Open) (Datei/Öffnen).
3. Wählen Sie die Netzwerkschnittstelle aus.
4. Führen Sie eine Modulerkennung durch.



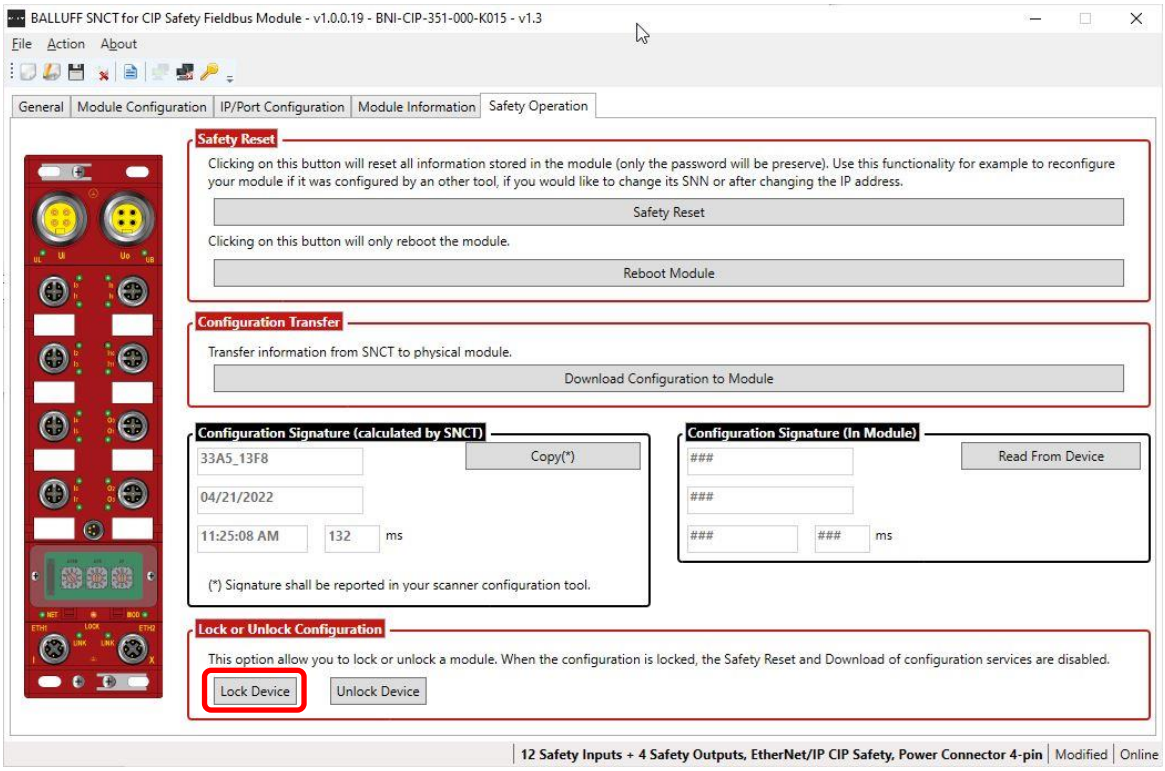
5. Doppelklicken Sie auf das Modul, um es auszuwählen.



6. Gehen Sie *Online*, um das Modul zu verbinden (Action/Online (Aktion/Online)).



7. Gehen Sie zum Register *Safety Operation* (Sicherheitsbetrieb) und wählen Sie die Schaltfläche *Lock Device* (Gerät sperren).

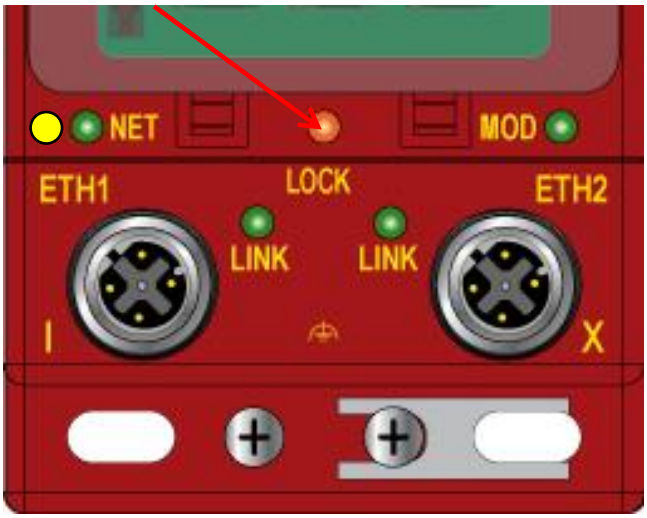


8. Wenn das Modul kennwortgeschützt ist, geben Sie das Kennwort ein und wählen Sie dann OK. Wenn das Kennwort nicht bekannt ist, gehen Sie zum Abschnitt Kennwort zurücksetzen

9. Der Sperrvorgang wurde erfolgreich durchgeführt.

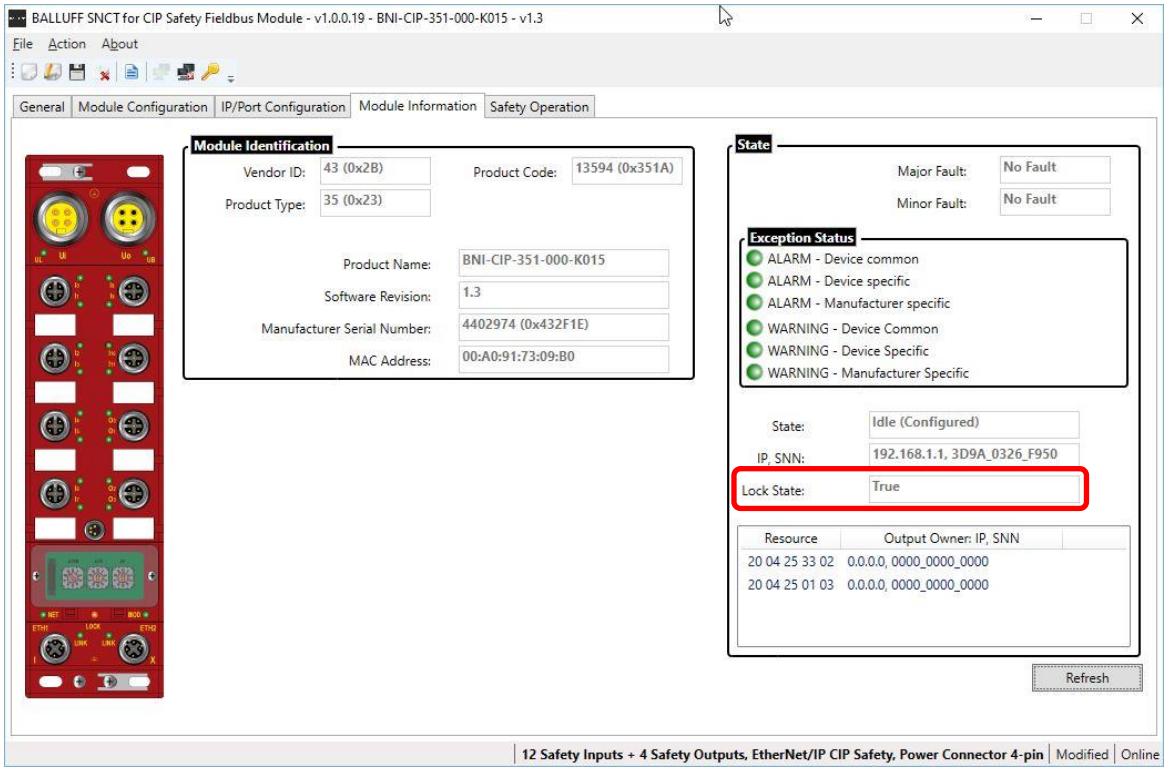
10. Um zu überprüfen, ob die Sperre des Moduls aktiv ist,

    a. vergewissern Sie sich, dass die Sperr-LED (Lock) gelb leuchtet.



oder

    b. Gehen Sie zum Register *Module Information* (Modulinformationen) und klicken Sie auf die Schaltfläche *Refresh* (Aktualisieren), um den Wert für den Sperrzustand anzuzeigen.

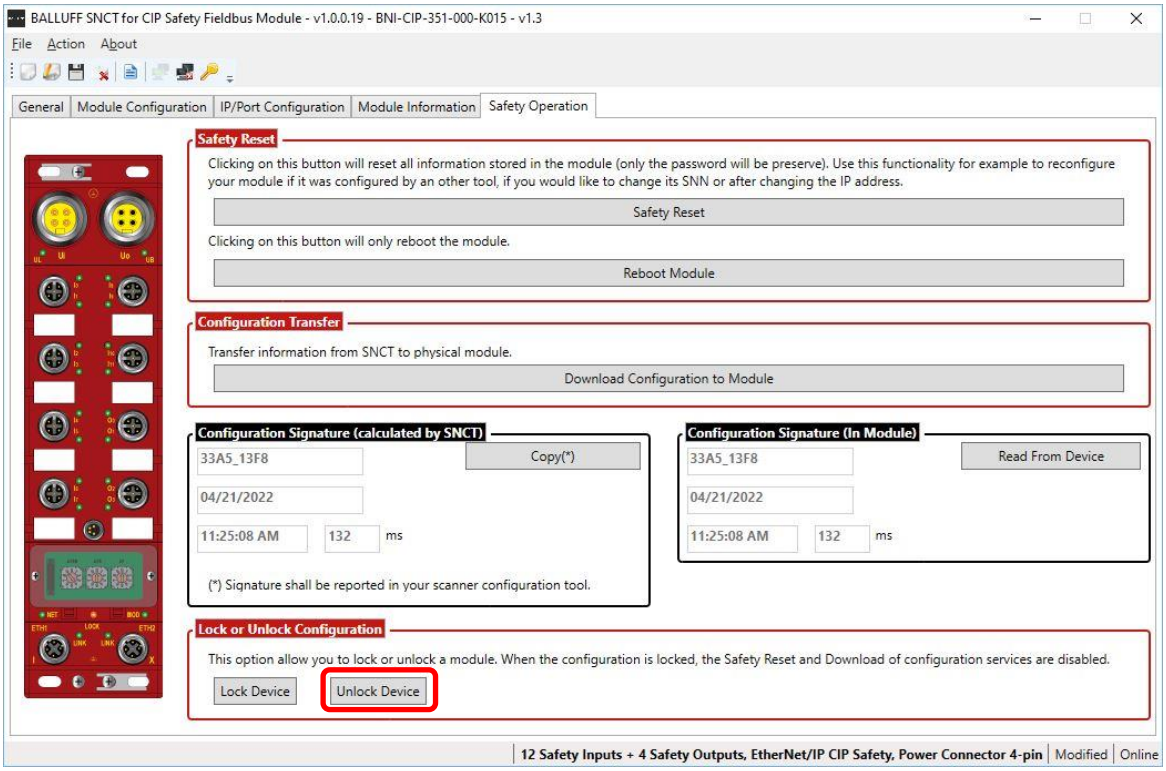


11. Gehen Sie *Offline* und schließen (*Exit*) Sie die SNCT-Software.

Entsperren einer Modulkonfiguration

Die Schritte zum Entsperren einer Modulkonfiguration ähneln den Schritten 1 bis 6 des Sperrvorgangs.

7. Gehen Sie zum Register *Safety Operation* (Sicherheitsbetrieb) und wählen Sie die Schaltfläche *Unlock Device* (Gerät entsperren).

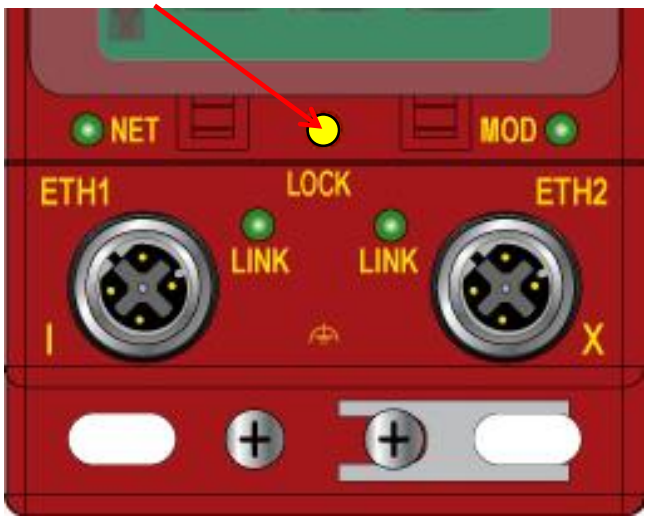


8. Wenn das Modul kennwortgeschützt ist, geben Sie das Kennwort ein und wählen Sie dann OK. Wenn das Kennwort nicht bekannt ist, gehen Sie zum Abschnitt Kennwort zurücksetzen

9. Der Entsperrvorgang wurde erfolgreich durchgeführt.

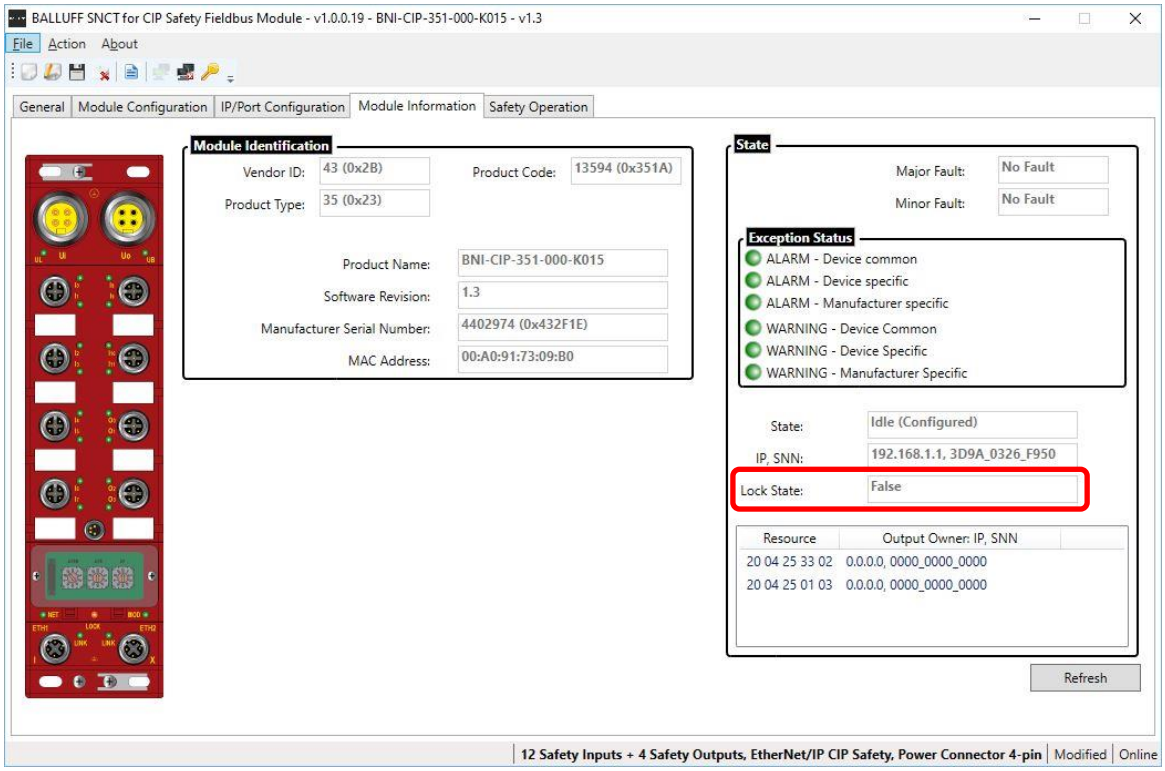
10. Um zu überprüfen, ob das Modul entsperrt ist,

    a. vergewissern Sie sich, dass die Sperr-LED (Lock) gelb blinkt.



    oder

    b. Gehen Sie zum Register Module Information (Modulinformationen) und klicken Sie auf die Schaltfläche Refresh (Aktualisieren), um den Wert für den Sperrzustand anzuzeigen.



11. Gehen Sie *Offline* und schließen (*Exit*) Sie die SNCT-Software.

10.4. Speichern der IP-Adresse mit einem DHCP-Server

Um eine IP-Adresse in einem Modul zu speichern, das sich im Auslieferungszustand befindet, starten Sie eine *DHCP-Server*-Anwendung, um die IP-Adresskonfiguration zu verwalten.

Starten Sie das SNCT-Tool. Erstellen oder öffnen Sie ein Projekt. Wählen Sie die Netzwerkschnittstelle aus. Geben Sie die IP-Adresse des Moduls ein oder führen Sie eine Modulerkennung durch und wählen Sie das Modul aus.

1. Gehen Sie *Online*.
2. Gehen Sie zum Register *Module Information* (Modulinformationen) und klicken Sie auf *Refresh* (Aktualisieren). Überprüfen Sie, ob das Modul im Zustand “Waiting for TUNID” (Warten auf TUNID) ist (wenn sich das Modul wirklich im Auslieferungszustand befindet, ist dies der Fall). Wenn das nicht der Fall ist, können Sie die IP des Moduls nicht ändern und müssen eine Sicherheitsrücksetzung durchführen und den Vorgang ab Schritt 1 wiederholen.
3. Gehen Sie zum Register *IP/Port Configuration* (IP/Port-Konfiguration) und klicken Sie auf die Schaltfläche *Refresh* (Aktualisieren).
4. Klicken Sie unter *Configuration Control* (Konfigurationskontrolle) auf die Schaltfläche *Change* (Ändern).
5. Wählen Sie im Feld die Option *Static* (Statisch) und klicken Sie auf OK.
6. Die Änderung wird sofort übernommen, und die Meldung “Modification done with success” (Änderung erfolgreich durchgeführt) wird angezeigt.
7. Klicken Sie auf OK.
8. Klicken Sie unter Interface Configuration (Schnittstellenkonfiguration) auf die Schaltfläche Change (Ändern).
9. Geben Sie die neue IP-Adresse und Netzwerkmaske ein.
10. Die Änderungen werden sofort übernommen.
11. SNCT geht offline und dann automatisch mit der neuen IP-Adresse wieder online.

Hinweis!
Aufgrund der neuen IP-Adresse kann eine Warnung angezeigt werden, die darauf hinweist, dass die Konfigurationsparameter zwischen Konfiguration und Modul voneinander abweichen.

10.5. IP-Adresskonflikt

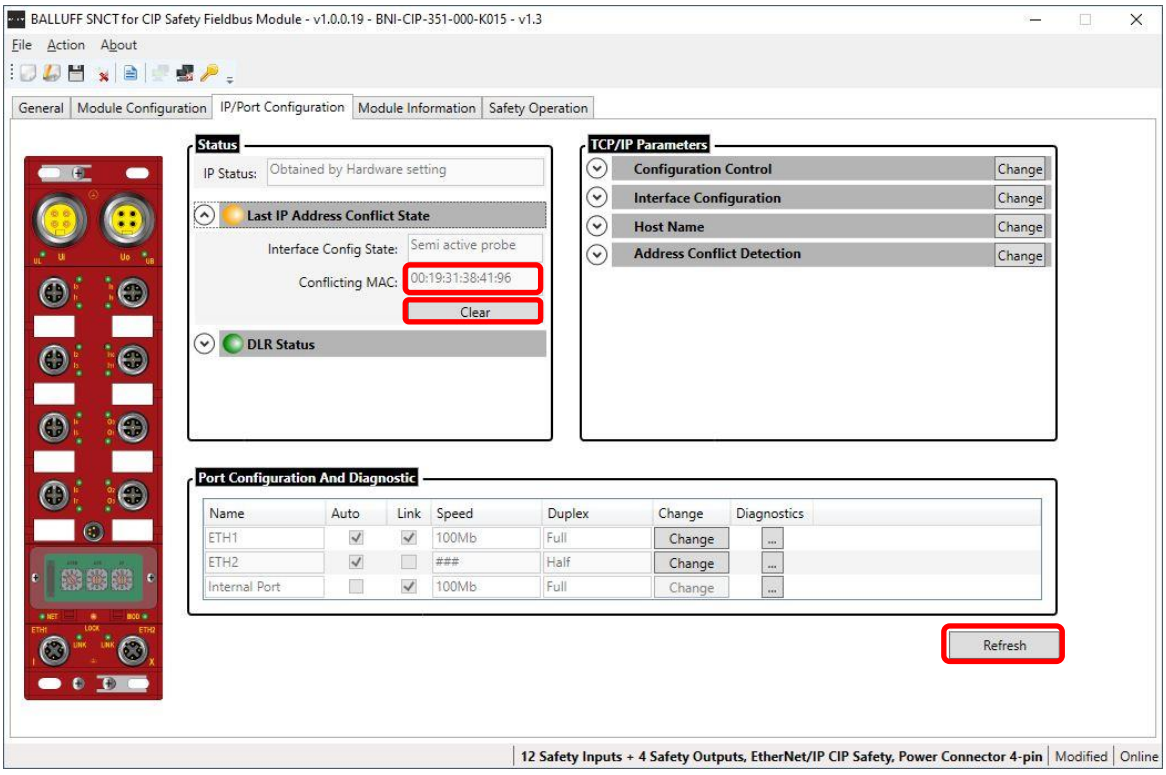
Wenn ein IP-Konflikt zwischen dem Sicheren E/A-Modul und anderen TCP/IP-Geräten im Netzwerk auftritt, kann das Modul dieses Problem erkennen (wenn die ACD-Funktion aktiviert ist). Nach der Erkennung des Problems bricht das Modul selbsttätig die Kommunikation im Netzwerk ab.

Hinweis!
In diesem Fall verhalten sich die LEDs am Modul folgendermaßen:
NET = ROT – **LOCK** = ROT – **MOD** = ROT blinkend.

SNCT kann in dem Fall nicht mehr mit dem Modul kommunizieren, oder es wird eine Warnmeldung angezeigt.

Gehen Sie folgendermaßen vor, um einen IP-Konflikt zu verifizieren:

1. Ändern Sie die Position des Drehschalters, um eine im Netzwerk verfügbare IP-Adresse zu generieren, und starten Sie das Modul neu.
2. Starten Sie SNCT und gehen Sie online (Action/Go Online (Aktion/Online gehen)).
3. Gehen Sie zur Seite IP/Port Configuration (IP/Port-Konfiguration) und klicken Sie auf die Schaltfläche Refresh (Aktualisieren).



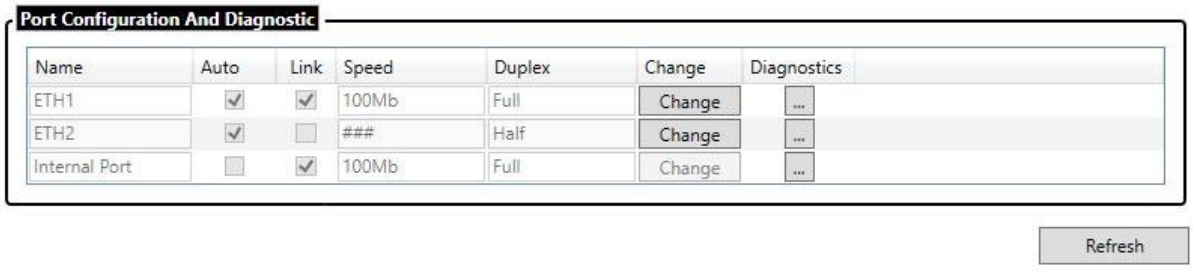
4. Wenn ein IP-Adresskonflikt im Modul besteht, leuchtet die entsprechende LED gelb. Außerdem wird die MAC-Adresse des TCP/IP-Geräts, das den Konflikt verursacht, angezeigt. Klicken Sie auf die Schaltfläche Clear (Löschen), um den Konflikt zu quittieren.

10.6. Diagnose des Ethernet-Ports

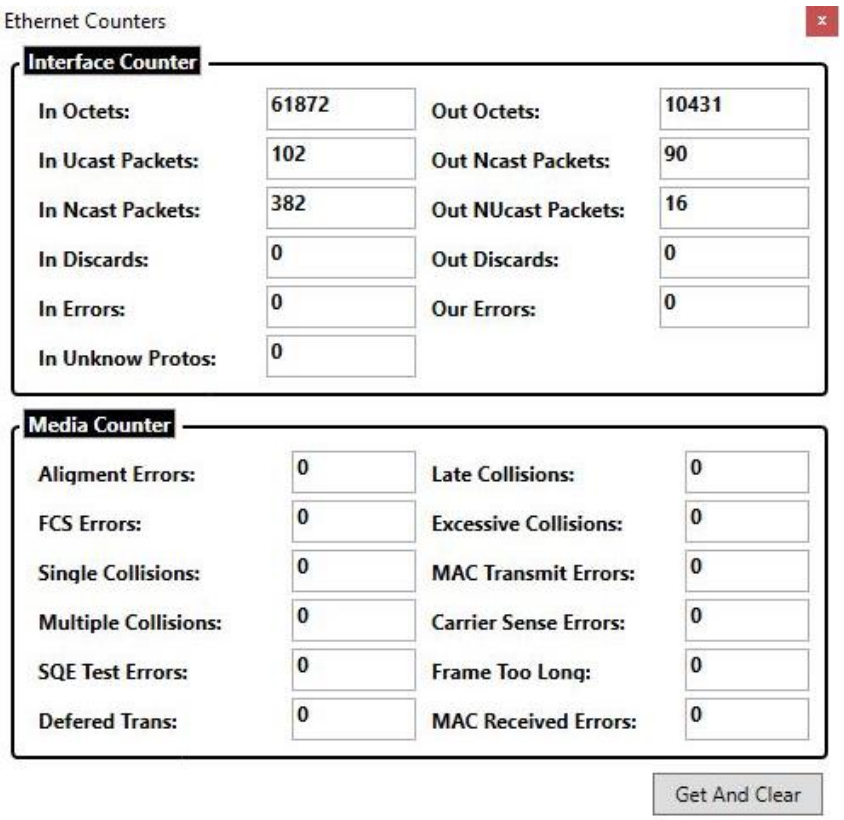
SNCT kann an jedem Ethernet-Port einen Diagnosezähler bereitstellen, um den Traffic zu überwachen.

Gehen Sie folgendermaßen vor, um eine Diagnose des Ethernet-Ports durchzuführen:

1. Starten Sie SNCT und gehen Sie online (Action/Go Online (Aktion/Online gehen)).
2. Gehen Sie zur Seite *IP/Port Configuration* (IP/Port-Konfiguration) und klicken Sie auf die Schaltfläche *Refresh* (Aktualisieren).
3. Klicken Sie auf die Diagnoseschaltfläche "…" für den Port, den Sie analysieren möchten.



4. SNCT zeigt ein Dialogfeld mit dem aktuellen Wert für die Zähler an.



5. Die Zähler können mit einem Klick auf die Schaltfläche *Get and Clear* (Abrufen und löschen) zurückgesetzt werden.

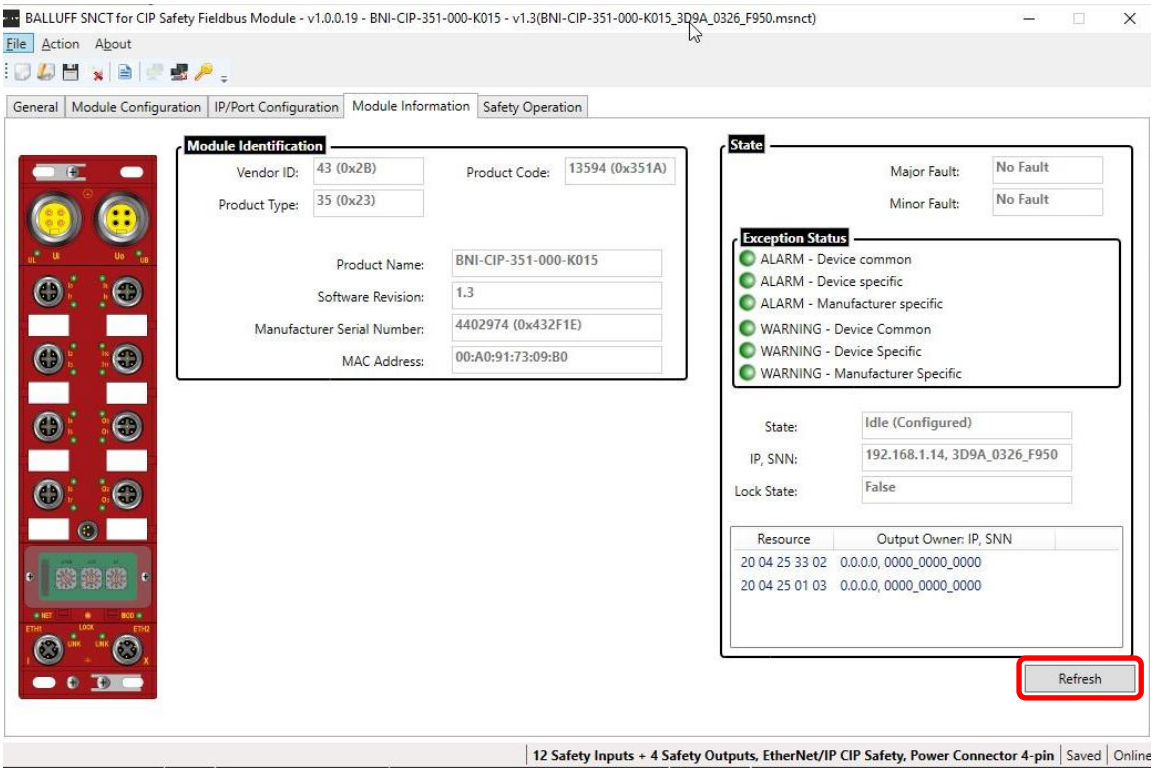
10.7. Modulinformationen

Mit dieser Funktion können Daten über das Sichere E/A-Modul abgerufen werden, um seinen aktuellen Zustand zu überwachen.

Gehen Sie folgendermaßen vor, um die Modulinformationen abzurufen:

Hinweis!
Die Vorgehensweise basiert auf der Annahme, dass sich das Modul in einem unbekannten Zustand befindet, aber eine bekannte IP-Adresse hat. Wenn die IP-Adresse des Moduls nicht bekannt ist, gehen Sie zum Abschnitt Sicherheitsrücksetzung.

1. Starten Sie die SNCT-Software.
2. Erstellen Sie ein neues Projekt und wählen Sie den Modultyp aus.
3. Wählen Sie die Netzwerkschnittstelle aus.
4. Führen Sie eine Modulerkennung durch und wählen Sie das Modul aus.
5. Gehen Sie *Online*, um das Modul zu verbinden (Action/Online (Aktion/Online)).
6. Bei diesem Schritt werden in Abhängigkeit vom Modulzustand zwei Warnungen angezeigt:
   a. Die konfigurierte TUNID weicht von der TUNID im Modul ab (die Angabe einer TUNID ist nicht zwingend erforderlich, um die Modulinformationen abzurufen).
   b. Parameter im Modul weichen von den Parametern in der Konfiguration ab. Das ist normal, da Sie ein neues Projekt erstellt haben.
7. Wählen Sie das Register *Module Information* (Modulinformationen) und klicken Sie auf die Schaltfläche *Refresh* (Aktualisieren).



8. SNCT zeigt die folgenden Informationen an:

   - **Modul-Identifikation** liefert Informationen über das Modul. Sie können die Seriennummer und die IP-Adresse des Moduls abrufen. Die in diesem Bereich angezeigte Softwareversion stellt Angaben zur Produktversion bereit. Ausführlichere Informationen zu den verschiedenen Elementen, aus denen sich das Modul zusammensetzt, werden unter “Action\Additional Tools\Information…” (Aktion\Zusätzliche Tools\Informationen…) bereitgestellt (siehe Abschnitt Zusätzliche Informationen).

   - **Schwerer/leichter Fehler**:
     - Kein Fehler: Es wurde kein Problem erkannt.
     - Behebbarer Fehler: Es wurde ein Fehler der folgenden Art erkannt:
       - Position des Drehschalters geändert,
       - Speicherschlüssel entfernt,
       - Sicherheitsprobleme an einem Eingang oder Ausgang (Kurzschluss…).

     Zusätzliche Informationen über das Problem finden Sie unter Zusätzliche Informationen. Sie müssen das Problem beheben und dann das Modul neu starten, um den Fehler zu beseitigen.

     Nicht behebbarer Fehler: Ein schwerwiegendes Hardwareproblem wurde erkannt. Sie sollten das Modul nicht weiter verwenden und sich an das technische Supportteam von Balluff wenden.

   - **Zustand**: Dieser Wert vermittelt den Zustand des Moduls und hilft bei der Definition der erforderlichen Maßnahmen:
     - Warten auf TUNID: Im Modul ist keine TUNID festgelegt; es muss eine TUNID festgelegt werden, bevor ein anderer Vorgang ausgeführt werden kann.
     - Konfiguration: Das Modul besitzt eine TUNID, aber keine Konfiguration; laden Sie eine Konfiguration herunter.
     - Leerlauf (Konfiguriert): Das Modul ist konfiguriert und betriebsbereit, es ist aber kein EtherNet/IP-Scanner verbunden.
     - Betrieb: Das Modul ist konfiguriert und es ist ein EtherNet/IP-Scanner verbunden.
     - Abbrechen: Das Modul wurde in den Sicherheitszustand versetzt (siehe Schwerer/leichter Fehler weiter oben).

   - **IP/SNN**: Das ist die aktuelle TUNID für das Modul.

   - **Sperrzustand**: Gibt an, ob das Modul gesperrt wurde und damit als konfiguriert und getestet gilt.

   - **“Besitzer des Ausgangs”**: Gibt an, ob ein EtherNet/IP-Scanner Besitzer der Sicherheitsausgangsbaugruppe des Moduls ist.

     Der erste EtherNet/IP-Scanner, der sich mit der Ausgangsbaugruppe verbindet, ist ihr Besitzer. Nur dieser EtherNet/IP-Scanner ist später autorisiert, diese Ausgangsbaugruppe zu verbinden.

     Wenn ein anderer EtherNet/IP-Scanner die Ausgangsbaugruppe verbinden soll, müssen Sie eine Sicherheitsrücksetzung durchführen und das Modul neu konfigurieren.

     In dieser Liste werden die beiden Baugruppenformate aufgeführt:

     20 04 25 33 02: Baugruppe 0x0233 - Sicheres, diskretes Ausgangsprofil

     20 04 25 01 03: Baugruppe 0x0301 - Herstellerspezifisch

9. Gehen Sie *Offline* und schließen (*Exit*) Sie die SNCT-Software.

10.8. Kennwort festlegen/zurücksetzen

Kennwort festlegen

Mit dem Service für die Festlegung des Kennworts kann die Nutzung der folgenden SNCT-Funktionen beschränkt und geschützt werden:

- Sicherheitsrücksetzung
- Modul-Neustart
- Modul-Download
- Sperren/Entsperren der Modulkonfiguration
- (Kennwort festlegen)

Nach dem Festlegen eines Kennworts wird dieses Kennwort immer abgefragt , wenn eine der oben genannten Funktionen verwendet wird.

Das Kennwort wird im Modul (auf dem Speicherschlüssel) gespeichert. Das Kennwort ist also nicht mit dem SNCT-Projekt, sondern mit dem Modul verknüpft. Wenn der Speicherschlüssel in einem neuen Modul weiterverwendet wird, wird für den Zugriff auf die Funktionen dasselbe Kennwort abgefragt.

Warnung!
Stellen Sie sicher, dass Sie das Kennwort nicht vergessen oder verlieren. SNCT bietet zwar eine Funktion für die Rücksetzung des Kennworts. Dieser Vorgang nimmt aber viel Zeit in Anspruch, da in dem Fall der technische Support von Balluff kontaktiert werden muss.

Gehen Sie folgendermaßen vor, um ein Kennwort festzulegen:

1. Starten Sie die SNCT-Software.
2. Öffnen Sie die Modulkonfiguration (File/Open) (Datei/Öffnen).
3. Wählen Sie die Netzwerkschnittstelle aus.
4. Führen Sie eine Modulerkennung durch.
5. Doppelklicken Sie auf das Modul, um es auszuwählen.
6. Gehen Sie *Online*, um das Modul zu verbinden (Action/Online (Aktion/Online)).
7. Wählen Sie *Set Password* (Kennwort festlegen) (Action/Set Password (Aktion/Kennwort festlegen))
8. Im Feld:

   a. Wenn im Modul noch kein Kennwort festgelegt ist, lassen Sie *Current Password* (Aktuelles Kennwort) leer.
   b. Wenn bereits ein Kennwort im Modul festgelegt ist, geben Sie das aktuelle Kennwort unter *Current Password* (Aktuelles Kennwort) ein.

9. Geben Sie das neue Kennwort unter *New Password* (Neues Kennwort) und dann erneut unter *New Password (Confirmation)* (Neues Kennwort (Bestätigung)) ein.
10. Klicken Sie auf OK.
11. SNCT zeigt die Meldung "*Password modified with success*" (Kennwort erfolgreich geändert) an.
12. Gehen Sie *Offline* und schließen (*Exit*) Sie die SNCT-Software.

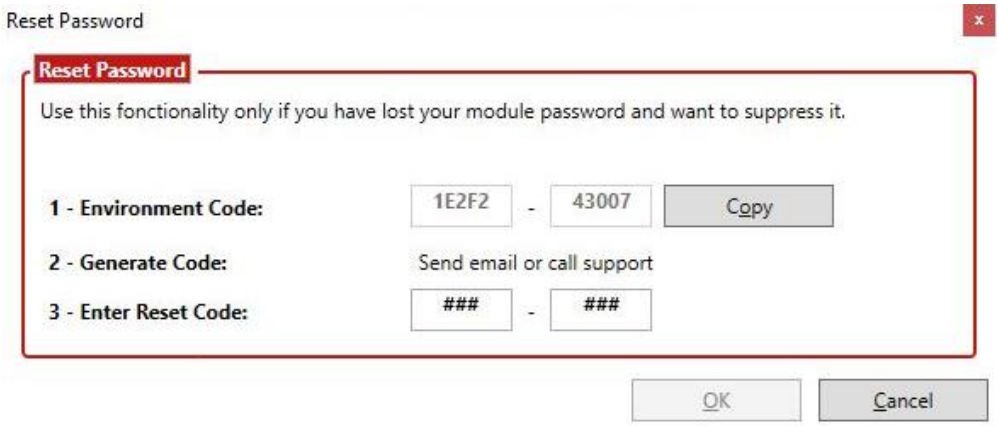
Kennwort zurücksetzen

Wenn das Modulkennwort verloren gegangen ist, wenden Sie sich an den technischen Support von Balluff und fordern Sie einen Wiederherstellungscode an, mit dem Sie das Modulkennwort zurücksetzen können.

Warnung!
Die Sicherheitsexpertenstelle muss sicherstellen, dass nur autorisierte Personen Zugriff auf die Balluff SNCT-Software haben, um den Befehl *Reset Password* (Kennwort zurücksetzen) auszuführen. Balluff nimmt keine Identifizierung der Personen vor, die einen Rücksetzungscode anfordern.

Gehen Sie folgendermaßen vor, um ein Kennwort zurückzusetzen:

1. Starten Sie die SNCT-Software.
2. Öffnen Sie die Modulkonfiguration (File/Open) (Datei/Öffnen).
3. Wählen Sie die Netzwerkschnittstelle aus.
4. Führen Sie eine Modulerkennung durch.
5. Doppelklicken Sie auf das Modul, um es auszuwählen.
6. Gehen Sie *Online*, um das Modul zu verbinden (Action/Online (Aktion/Online)).
7. Wählen Sie Res*et Password* (Kennwort zurücksetzen) (Action / Additional Tools / Reset Password (Aktion / Zusätzliche Tools / Kennwort zurücksetzen))

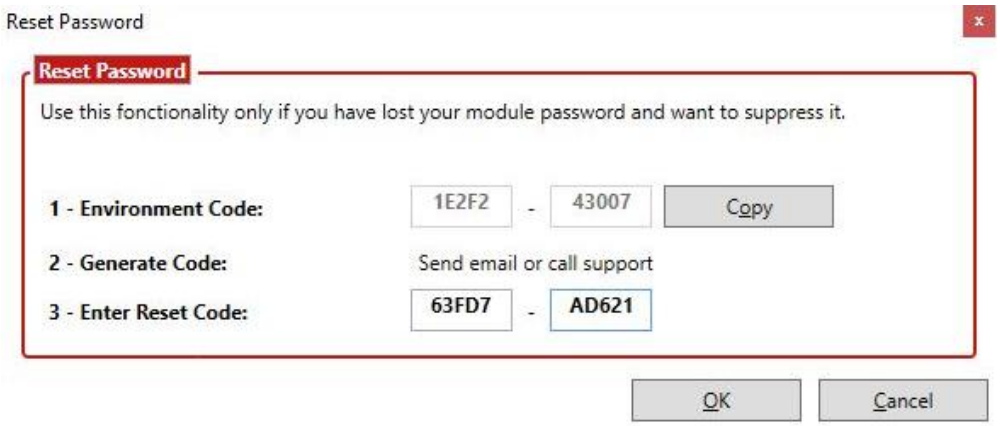


Warnung!
Der Umgebungscode ist für jedes Modul anders. Nach jeder erfolgreichen Kennwortrücksetzung mit *Reset Password* (Kennwort zurücksetzen) wird ein neuer Umgebungscode im Modul generiert. Der Rücksetzungscode kann also nur einmal verwendet werden.

8. Besuchen Sie die Supportseite von Balluff unter https://www.balluff.com/support. Senden Sie eine E-Mail an die angegebene Supportadresse:
   a. Schreiben Sie in die Betreffzeile “CIP Safety I/O Module – Reset Password Request” (Sicheres CIP-E/A-Modul – Anforderung Kennwortrücksetzung).
   b. Kopieren Sie den Umgebungscode (in diesen Beispiel “1E2F2-43007”) und fügen Sie ihn in den Bereich für den Nachrichtentext ein.

9. Das technische Supportteam von Balluff verarbeitet die Anfrage innerhalb der Geschäftszeiten. Innerhalb von ca. 24 h nach dem Eingang der Anfrage wird Ihnen ein Rücksetzungscode zugestellt.

10. Führen Sie nach dem Erhalt der Antwort die Schritte 1 bis 7 erneut durch und ersetzen Sie dabei die Zeichenfolge ### in den Feldern *Enter Reset Code* (Rücksetzungscode eingeben) durch den erhaltenen Wert:



Klicken Sie auf OK.

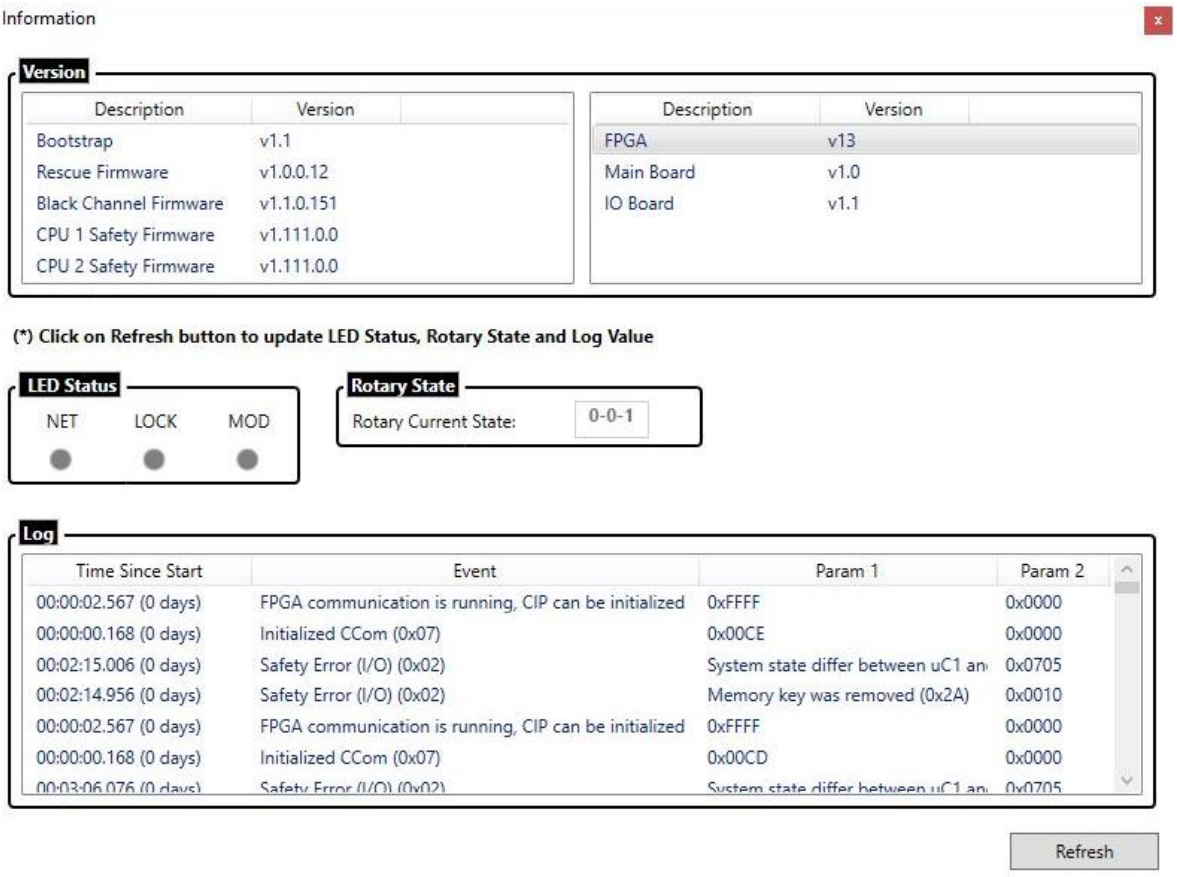
11. Wenn das Kennwort erfolgreich zurückgesetzt wurde, wird die Meldung "*The password has been correctly removed. It is recommended to set a new password in the module.*" (Das Kennwort wurde erfolgreich entfernt. Es wird empfohlen, ein neues Kennwort im Modul festzulegen.).

10.9. Zusätzliche Informationen

Mit den zusätzlichen Modulinformationen erhalten Sie ausführliche Angaben zum Modul.

Gehen Sie folgendermaßen vor, um zusätzliche Informationen abzurufen:

1. Starten Sie die SNCT-Software.
2. Erstellen Sie ein neues Projekt für dasselbe Modell des Moduls.
3. Wählen Sie die Netzwerkschnittstelle aus.
4. Führen Sie eine Modulerkennung durch und wählen Sie das Modul aus.
5. Gehen Sie *Online*, um das Modul zu verbinden (Action/Online (Aktion/Online)).
6. Bei diesem Schritt werden in Abhängigkeit vom Modulzustand zwei Warnungen angezeigt:
   a. Die konfigurierte TUNID weicht von der TUNID im Modul ab (die Angabe einer TUNID ist nicht zwingend erforderlich, um die Modulinformationen abzurufen).
   b. Parameter im Modul weichen von den Parametern in der Konfiguration ab. Das ist normal, da ein neues Projekt erstellt wurde.
7. Klicken Sie auf *Information* im Menü *Action/Additional tools* (Aktion/Zusätzliche Tools).
8. SNCT zeigt die folgenden Informationen an:



- **Version**: Dieser Abschnitt enthält alle Firmware-Versionen der verschiedenen Hardwarekomponenten.

- **LED Status**: Gibt den aktuellen Zustand der LEDs an.

- **Rotary State (Drehschalterzustand)**: Gibt die Positionen der 3 Drehschalter an.

- **Log (Protokoll)**: Dieser Bereich enthält die im Modulspeicher abgelegten Protokollmeldungen. Die erste Meldung ist die jüngste Meldung. Die Meldungen haben einen Zeitstempel; die Zeit basiert auf dem Einschalten des Moduls und wird daher bei jedem Neustart des Moduls wieder auf 0 gesetzt.

  Beim Neustart des Moduls werden 2 Spezialmeldungen generiert. Diese Meldungen dienen nur Informationszwecken:
  - Initialized CCom (0x07) (CCom (0x07) initialisiert) – Param 1 gibt die Anzahl (im Hexadezimalformat) der Starts des Moduls seit seiner Herstellung an.
  - FPGA communication is running, CIP can be initialized (FPGA-Kommunikation aktiv, CIP kann initialisiert werden)

Hinweis!

Diese Seite wird nicht regelmäßig aktualisiert. Klicken Sie auf die Schaltfläche *Refresh* (Aktualisieren), um die Inhalte zu aktualisieren.

10.10. Firmware herunterladen

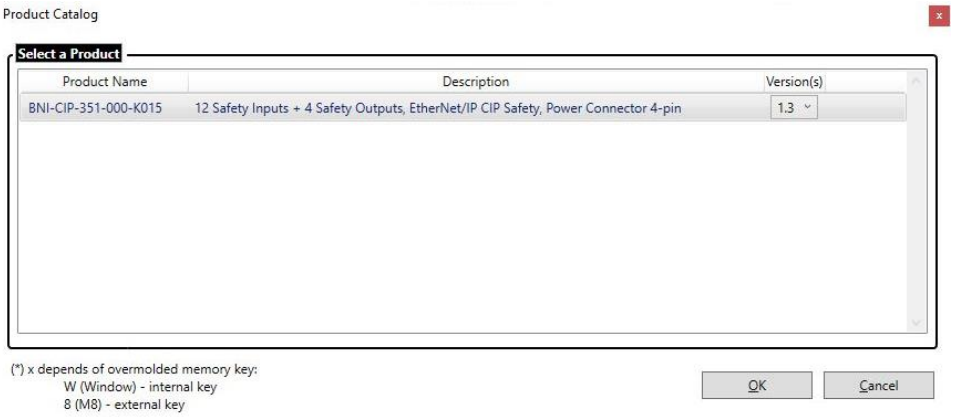
Mit dieser Funktion können Sie die Firmware des E/A-Moduls aktualisieren.

Hinweis!
Bei diesem Vorgang werden die im sicheren E/A-Modul gespeicherten Konfigurationsparameter nicht gelöscht.

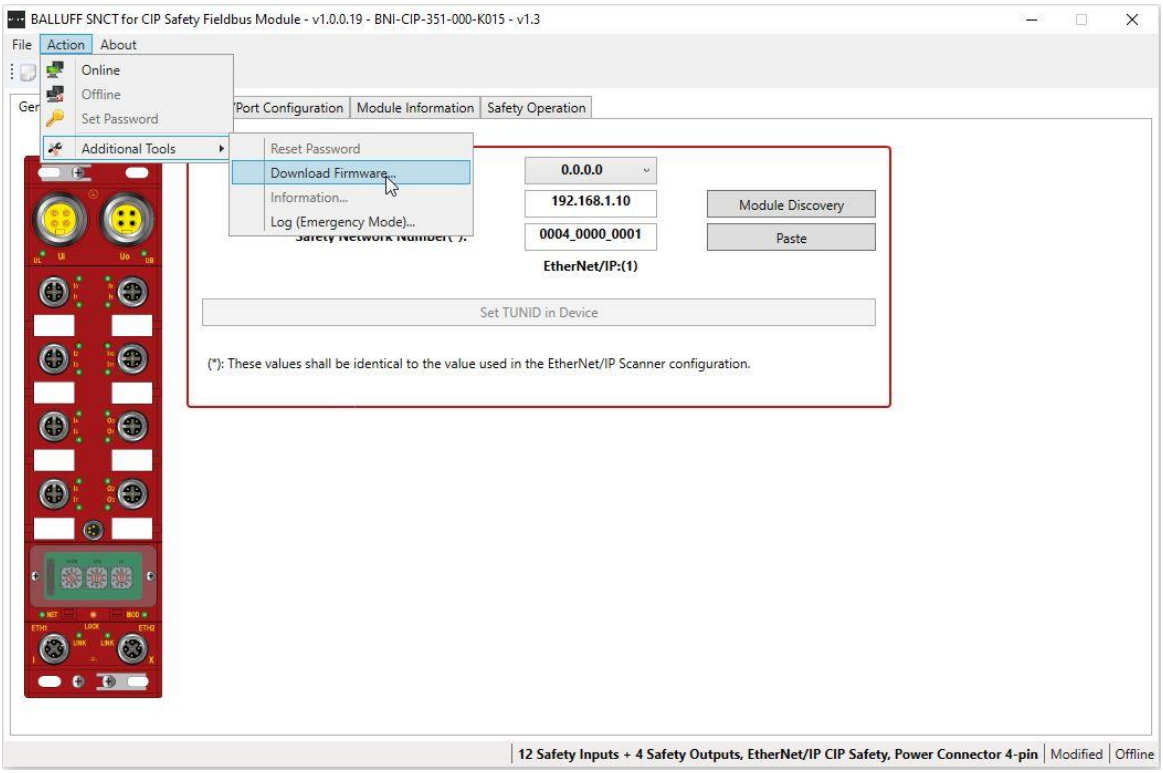
Warnung!
Es wird dringend empfohlen, eine Punkt-zu-Punkt-Ethernet-Verbindung für die Übertragung der Firmware zwischen dem Computer und dem Sicheren E/A-Modul zu verwenden, um Störungen während der Dateiübertragung zu vermeiden.

Gehen Sie folgendermaßen vor, um eine Firmware herunterzuladen:

1. Setzen Sie die Netzwerkschnittstelle des Computers auf **192.168.1.100**.
2. Starten Sie die SNCT-Software.
3. Erstellen Sie ein neues Projekt (File/New (Datei/Neu)).
4. Wählen Sie die Version des Sicheren E/A-Moduls aus.

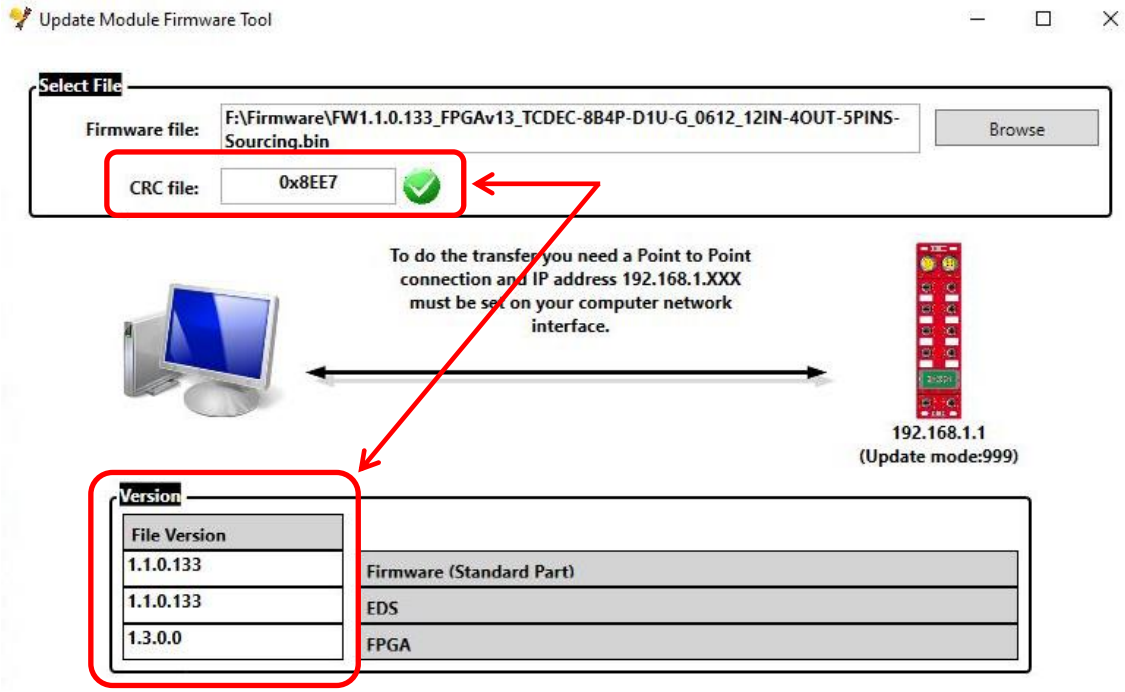


5. Wählen Sie im Menü *Action* (Aktion) den Eintrag , *Additional Tools*/*Download Firmware*… (Zusätzliche Tools/Firmware herunterladen...).

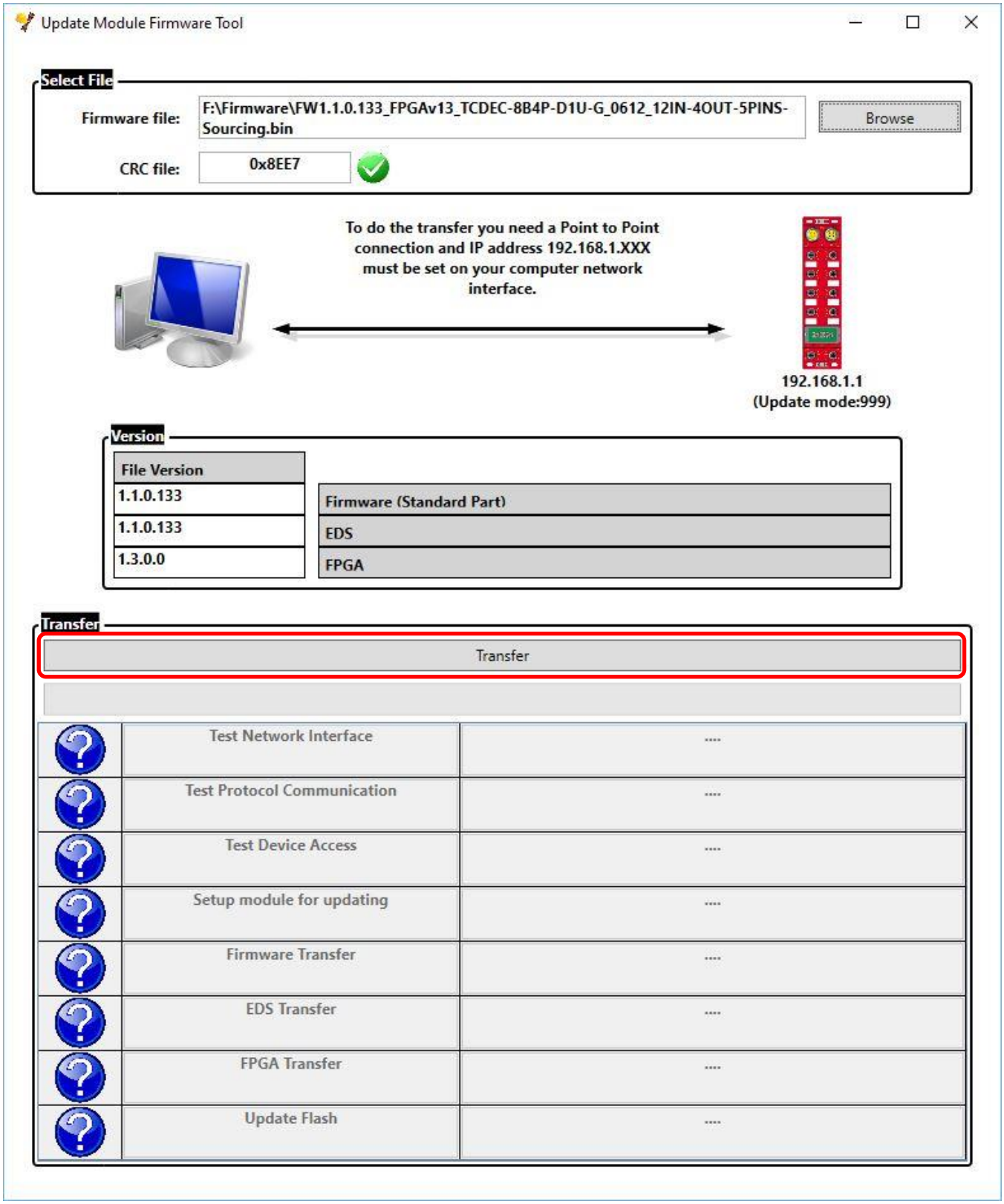


6. Navigieren Sie auf dem Computer zur Firmware des E/A-Moduls, markieren Sie sie und klicken Sie auf *Open* (Öffnen).

7. SNCT überprüft die CRC-Datei der Firmware und zeigt Versionsinformationen an.

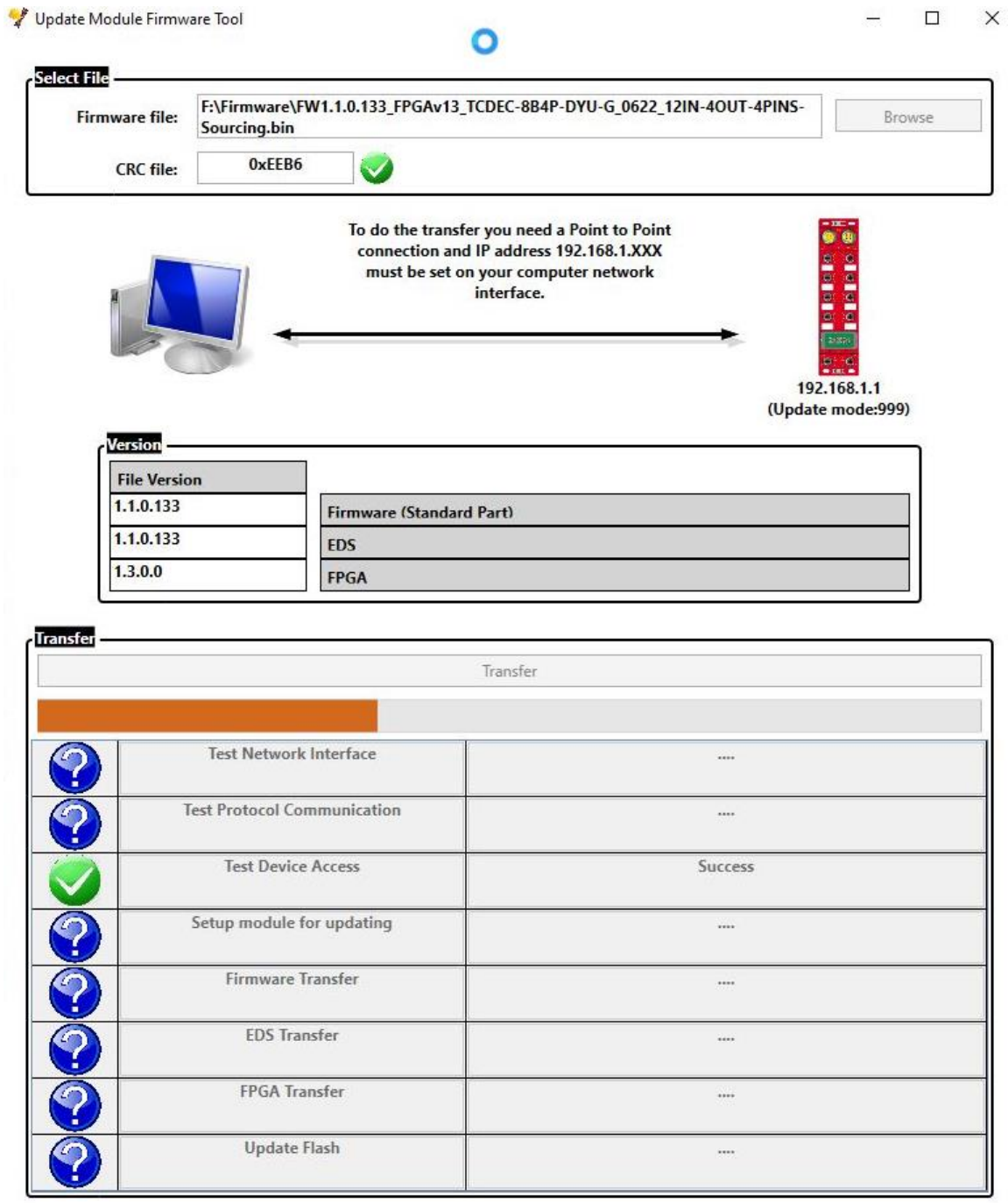


8. Klicken Sie auf die Schaltfläche *Transfer* (Übertragen).



9. Folgen Sie den Anweisungen.

10. SNCT startet den Download und zeigt während der Übertragung, die ca. 30 s dauert, Informationen an.



11. Die Übertragung wurde erfolgreich abgeschlossen. Folgen Sie den Anweisungen, um das Modul neu zu starten.

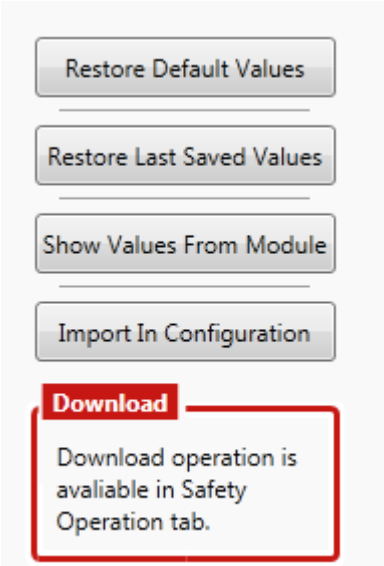
10.11. Modulkonfiguration drucken

Mit dieser Funktion können Sie einen Bericht erstellen und diesen ausdrucken oder speichern. Die Funktion kann auch verwendet werden, um zu überprüfen, ob die Konfiguration ordnungsgemäß im Modul angewandt wurde.

Warnung!

Die Sicherheitsexpertenstelle muss Sicherheitsmaßnahmen durchführen, um sicherzustellen, dass jeder konfigurierter Parameter ordnungsgemäß im Modul angewandt wurde. Mit der Funktion “*Show Value From Module*” (Wert vom Modul anzeigen) können diese Parameter angezeigt werden.

Die Druckfunktionalität (*Print*) kann ebenfalls verwendet werden. In diesen beiden Fällen muss der Sicherheitsexperte nach der Überprüfung, ob die Konfigurationssignatur unter *In SNCT* mit der Signatur unter *In Modul* übereinstimmt, sicherstellen, dass die einzelnen Parameterwerte im Abschnitt “Safety Inputs” (Sichere Eingänge), “Safety Input X and Safety Input Y (Sicherer Eingang X und Sicherer Eingang Y)”, “Safety Outputs” (Sichere Ausgänge), “Safety Output X and Safety Output Y” (Sicherer Ausgang X und Sicherer Ausgang Y) identisch sind.



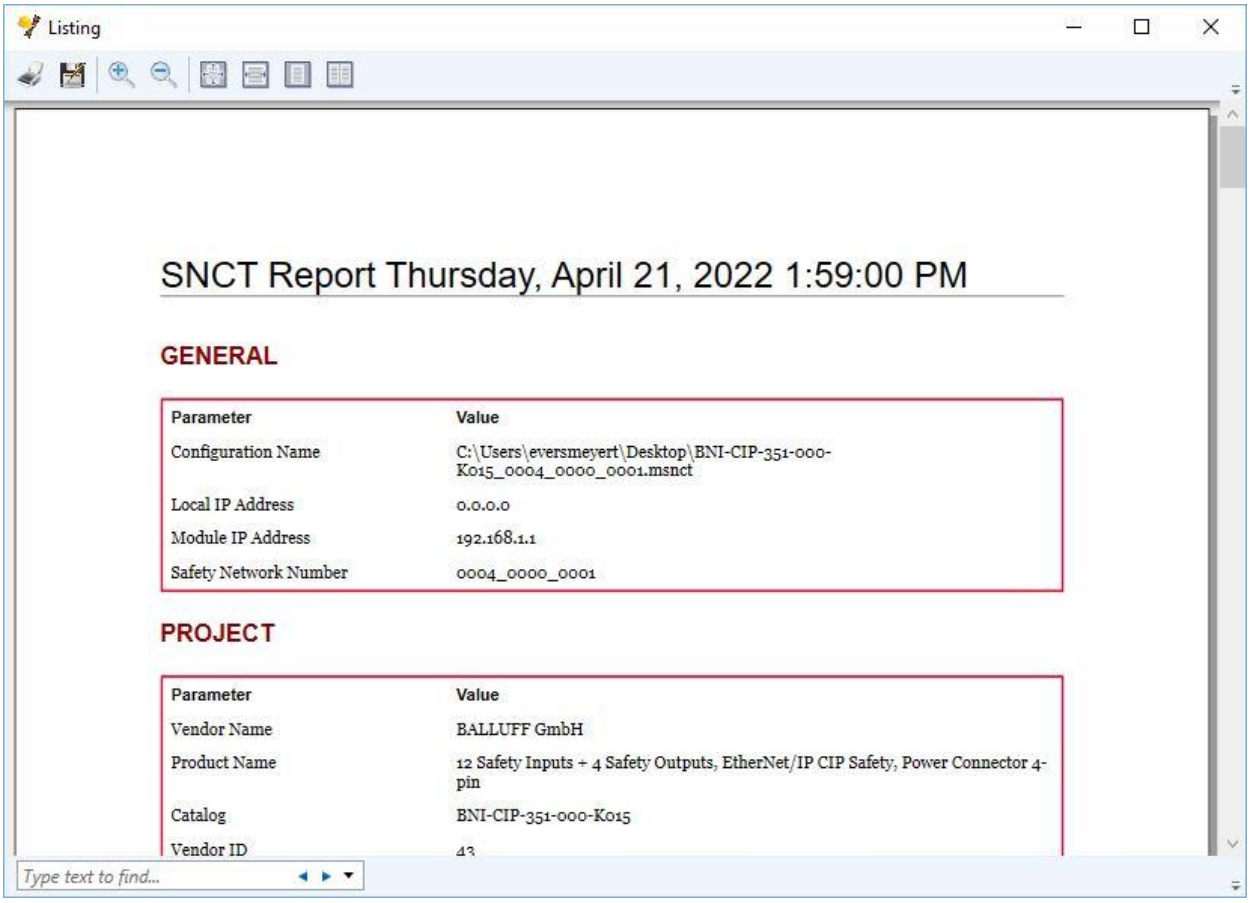
Wenn die Konfigurationssignaturen identisch sind, bei der Überprüfung aber Unterschiede festgestellt werden, wenden Sie sich an das technische Supportteam von Balluff.

Gehen Sie folgendermaßen vor, um eine Aufstellung zu generieren:

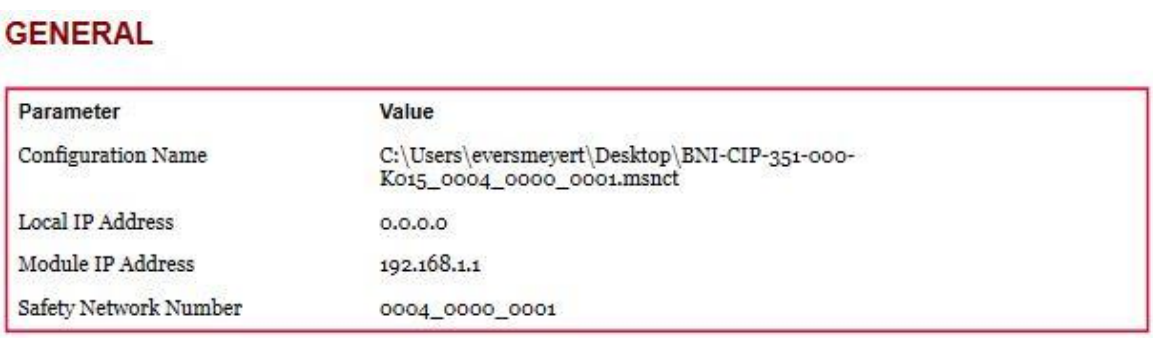
Hinweis!
Dieser Vorgang basiert auf der Hypothese, dass der Benutzer bereits eine gültige Konfiguration zum Modul heruntergeladen und seitdem keine Änderungen am Projekt vorgenommen hat.

1. Starten Sie die SNCT-Software.
2. Öffnen Sie das Projekt.
3. Gehen Sie *Online*, um das Modul zu verbinden (Action/Online (Aktion/Online)). Bei diesem Schritt sollte aufgrund der oben erwähnten Hypothese keine Warnmeldung generiert werden.

4. Generieren Sie die Aufstellung (*File/Print* (Datei/Drucken))



5. Stellen Sie sicher, dass es sich um das korrekte Modul handelt, indem Sie in der Aufstellung die IP und die SNN prüfen.



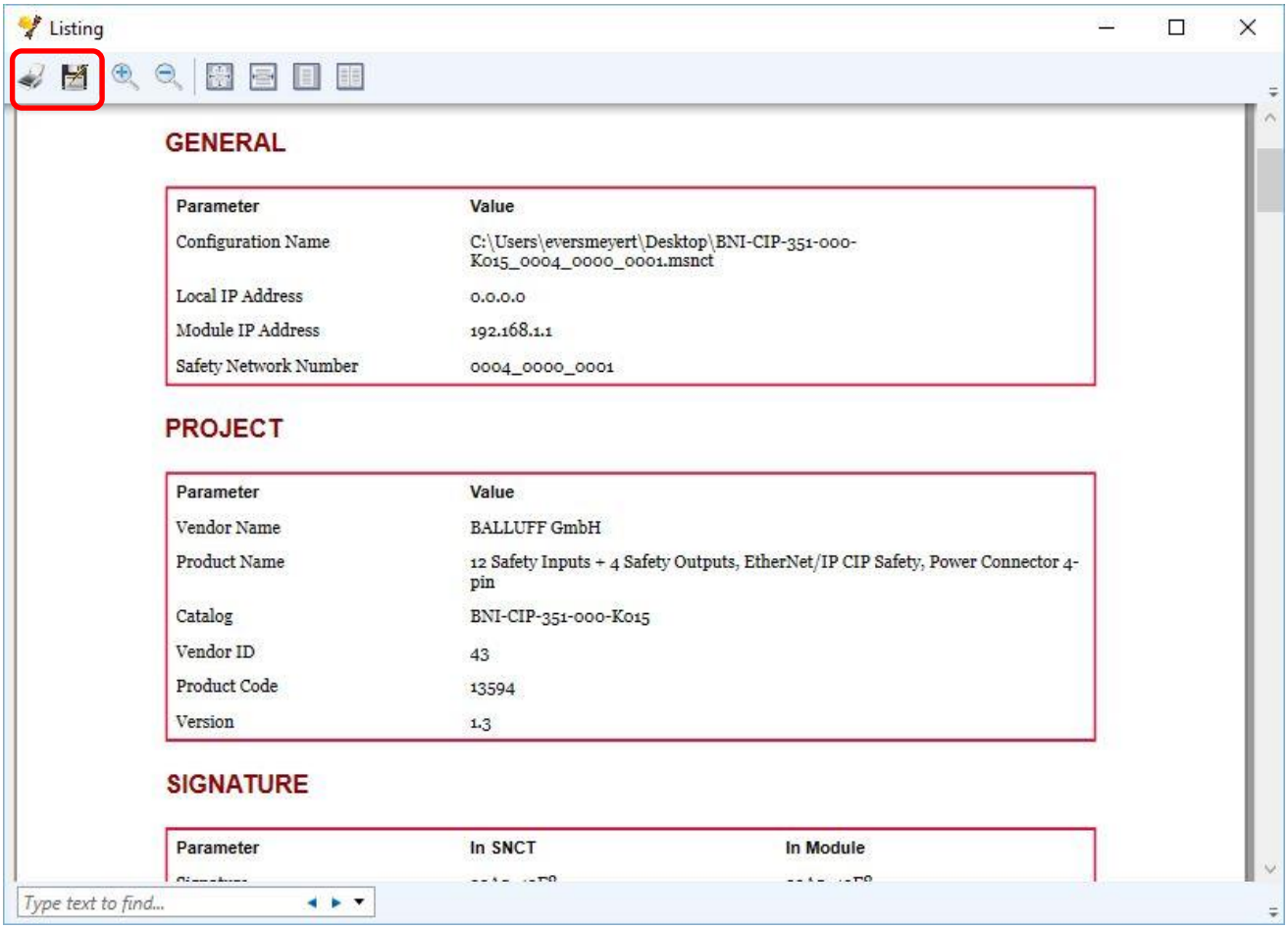
6. Vergleichen Sie die Signaturen (In SNCT / In Modul) in der Aufstellung.

7. Vergleichen Sie die einzelnen Parameter im Abschnitt “Safety Inputs” (Sichere Eingänge), “Safety Input X and Safety Input Y (Sicherer Eingang X und Sicherer Eingang Y)”, “Safety Outputs” (Sichere Ausgänge), “Safety Output X and Safety Output Y” (Sicherer Ausgang X und Sicherer Ausgang Y).

Hinweis!
Die unten gezeigten gerundeten Werte sind die in der Konfigurationsbaugruppe festgelegten Werte. Diese werden im Abschnitt “Zuordnung von sicheren E/A-Daten / Konfigurationsdaten” beschrieben.

Parameter	In SNCT	In Module	Unit
Input Operation Type	0 - Single	0 - Single	
Discrepancy Time	10	10	x10ms
Input Io OffOn Delay	0	0	ms
Input Io OnOff Delay	0	0	ms
Input Io Mode	0 - Not Used	0 - Not Used	

8. Drucken oder speichern Sie die Aufstellung.



9. Gehen Sie offline / schließen Sie die SNCT-Software.

10.12. Protokoll (Notfallmodus)

Das ist eine Expertenfunktion für den Abruf von Protokollinformationen eines Moduls, das nicht mehr funktioniert.

Hinweis!

Diese Funktion darf nur nach Aufforderung des technischen Supportteams von Balluff verwendet werden.

11. Produktumfang

In diesem Kapitel wird der Umfang des Produktpakets beschrieben.

11.1. Produktumfang

Das Produktpaket umfasst:

- Ein IP67-geschütztes E/A-Modul.
  Die Beschaltungsinformationen können dem Etikett an der Rückseite des Moduls entnommen werden.

- Ein Speicherschlüssel.
  Der Schlüssel wird verwendet, um die Modulkonfiguration zu speichern, und ermöglicht einen schnellen Austausch ohne erneute Inbetriebnahme (siehe Kapitel – Produktaustausch).

- Ein USB-Stick.
  Der USB-Stick enthält wichtige Informationen und Software für die Inbetriebnahme des Moduls.

11.2. USB-Stick

Der USB-Stick enthält wichtige Dokumente im elektronischen Format, wie z.B.:

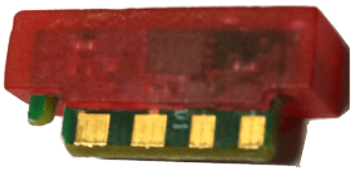
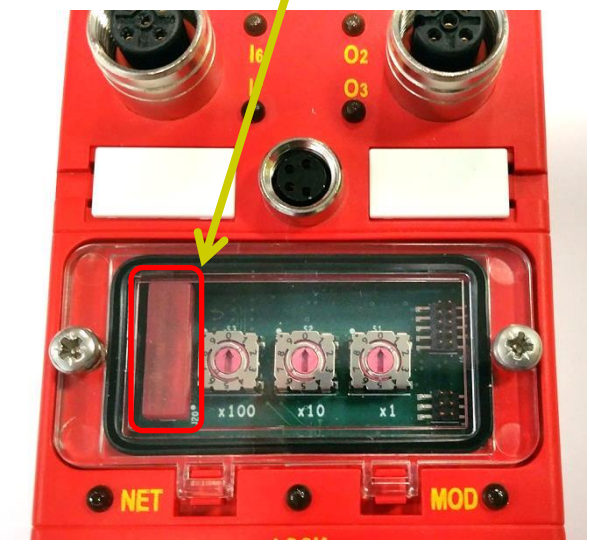
- Sicherheitshandbuch; diese vorliegende Anleitung.

  Hinweis!
  Vor dem Start der Produktbereitstellung wird dringend empfohlen, das gesamte Sicherheitshandbuch zu lesen.

- Software Network Configuration Tool (auch SNCT genannt)
- Beschreibungsdateien für das Sichere E/A-Modul (EDS)
- Technische Hinweise
- CAD-Dateien

11.3. Speicherschlüssel

Es wird ein Speicherschlüssel mitgeliefert. Auf dem Schlüssel werden alle Informationen einschließlich der Modulparameter sowie der "sicheren" und der "nicht sicheren" Konfiguration gespeichert.

Speicherschlüsselfenster
Größe: 18 x 6 x 7 mm 


Verhalten

Warnung!

Der nicht-flüchtige Speicherschlüssel DARF nur eingesetzt und entfernt werden, wenn das Modul von der Spannungsversorgung getrennt ist.

Warnung!

Wenn der nicht-flüchtige Speicherschlüssel nicht erkannt wird (lockerer Sitz im Anschluss, Schlüssel im Betrieb entfernt), wird das Modul unverzüglich in den ausfallsicheren Zustand geschaltet. In dem Fall blinken alle E/A-LEDs rot.

Hinweis!

Das Sichere E/A-Modul kann nur betrieben werden, wenn ein einzelner Schlüssel eingesetzt ist. Wenn ein zweiter Schlüssel erkannt wird, wird das Modul unverzüglich in den ausfallsicheren Zustand geschaltet. In dem Fall blinken alle E/A-LEDs rot.

12. Web-Server-Schnittstelle

In diesem Kapitel werden die Informationen des Sicheren E/A-Moduls beschrieben, die nach der Verbindung des Web-Servers des Moduls verfügbar sind.

12.1. Verbinden des Web-Servers

Die Web-Server-Schnittstelle stellt dem Benutzer eine komfortable und einfache Methode für die Diagnose des Sicheren E/A-Moduls über einen Web-Browser (Internet Explorer, Firefox usw.) bereit.

Gehen Sie dazu folgendermaßen vor:

- Verbinden Sie den Computer, auf dem sich das Sichere E/A-Modul befindet, mit dem Netzwerk.
- Starten Sie den Web-Browser.
- Geben Sie die IP-Adresse des Sicheren E/A-Moduls in die Adresszeile des Web-Browsers ein.

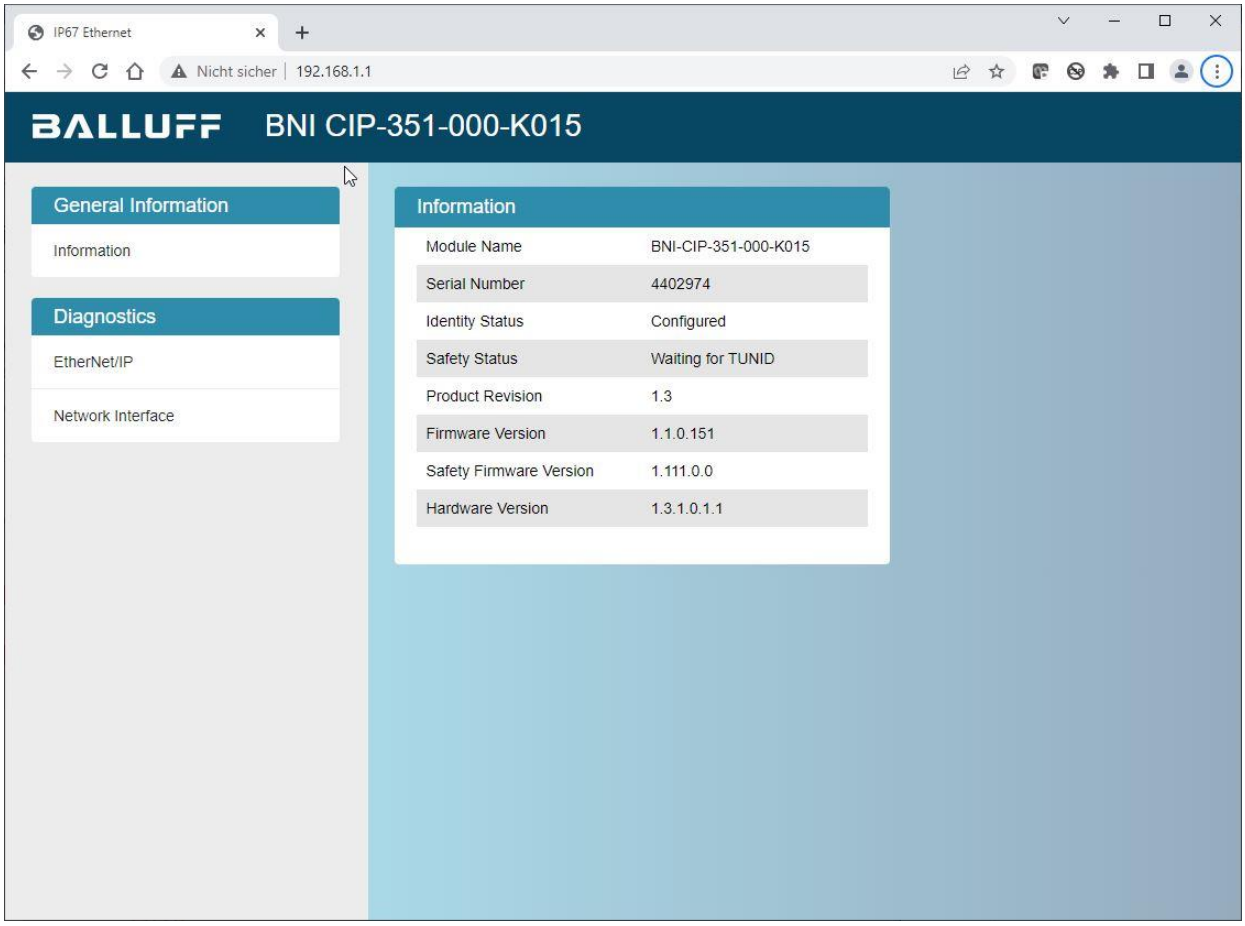
Warnung!
Achten Sie besonders auf die Optionen im Internet Explorer; Parameter wie “Proxy-Server” können den Zugriff auf die Web-Server-Schnittstelle des Sicheren E/A-Moduls blockieren.

Hinweis!
Der Zugriff auf die Web-Schnittstelle erfolgt ohne Anmeldung und ohne Kennworteingabe.

Hinweis!
Alle angezeigten Informationen sind schreibgeschützt. Es ist nicht möglich, die Modulkonfiguration mit dem Web-Server zu ändern.

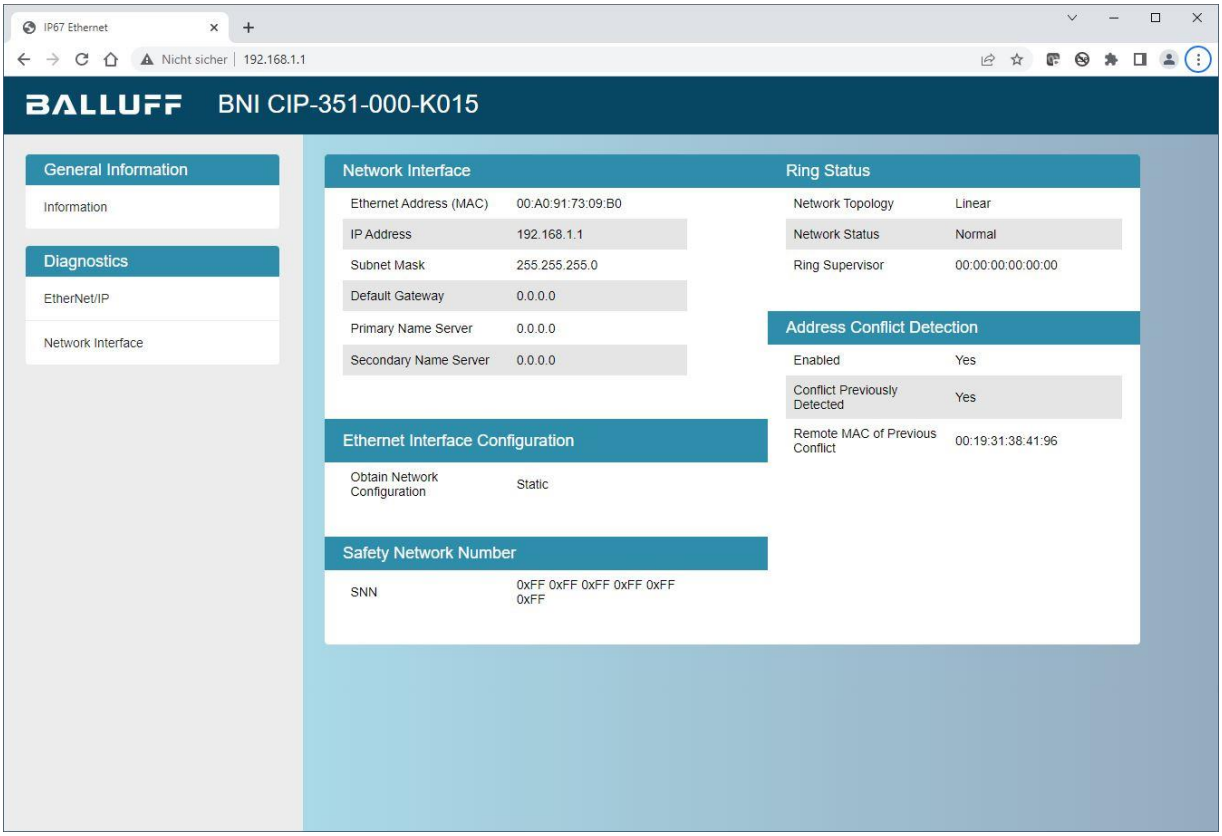
12.2. Allgemeine Informationen

Auf dieser Seite werden die Informationen des Sicheren E/A-Moduls angezeigt.

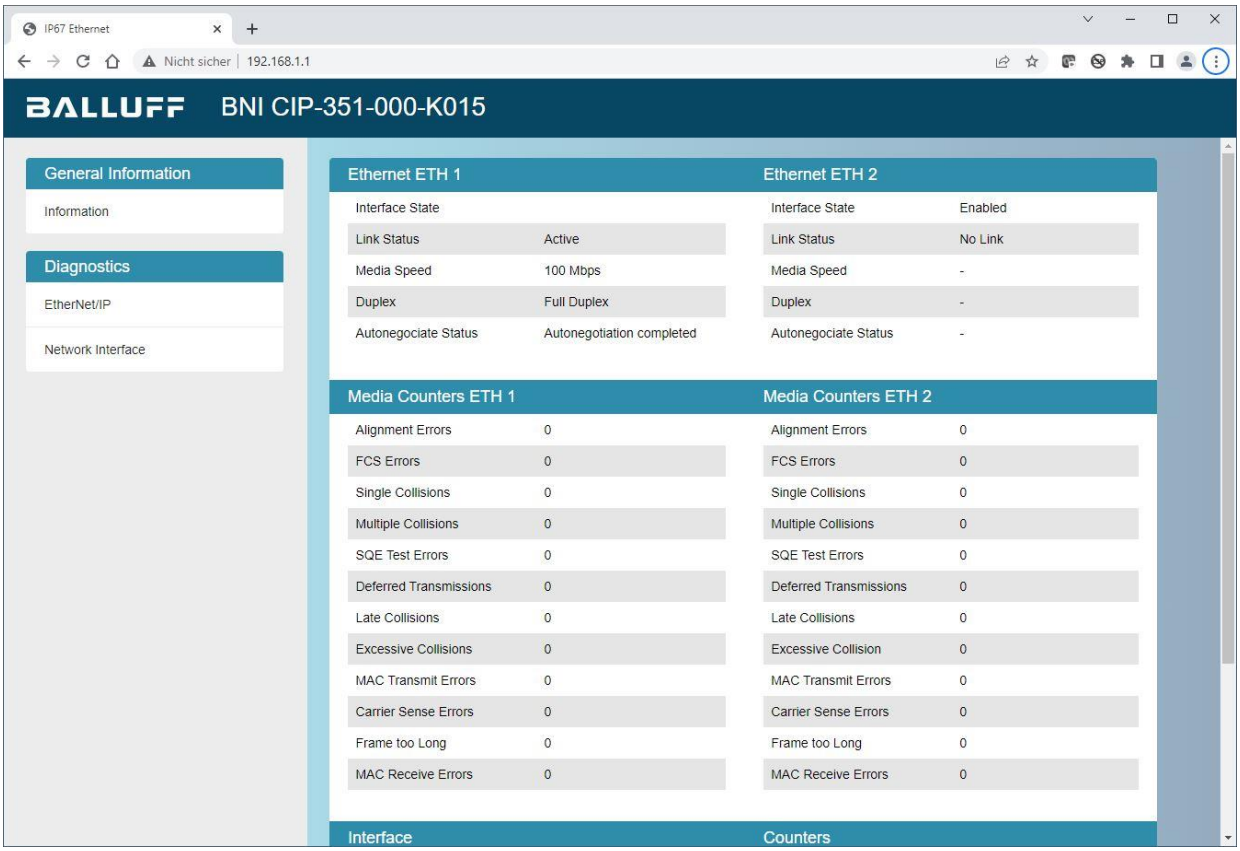


12.3. Diagnoseinformationen

Auf dieser Seite werden die Diagnoseinformationen für die Netzwerkschnittstelle angezeigt.



Auf dieser Seite werden die Ethernet- und EtherNet/IP-Diagnoseinformationen angezeigt.



13. Produktsupport

14.1. Garantiebedingungen

Die Garantiebedingungen finden Sie auf der Website von Balluff: (www.balluff.com).

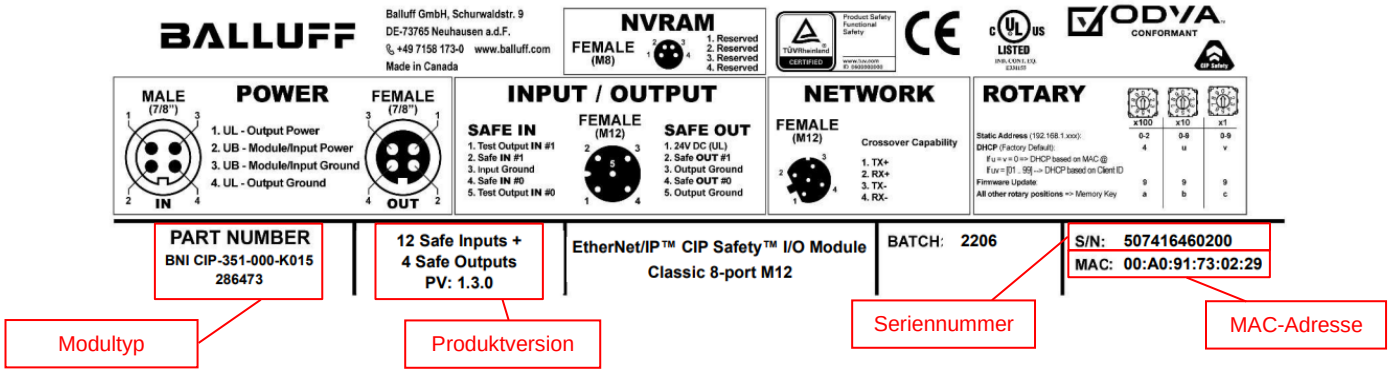
14.2. Produktinformationen

Halten Sie bitte die folgenden Informationen bereit, bevor Sie sich an den technischen Support wenden:

- Modultyp und Seriennummer
- Details zu den Problemen und zu den Begleitumständen, die das Problem verursacht haben können.

Hinweis:

Die Typenschilder des Sicheren E/A-Moduls befinden sich an der Seite und an der Rückseite des Moduls.



14.3. Technischer Support

Um die Benutzer bei der Verwendung der Produkte zu unterstützen, stellt Balluff auf seiner Website technische Informationen bereit:

Balluff Support und Download

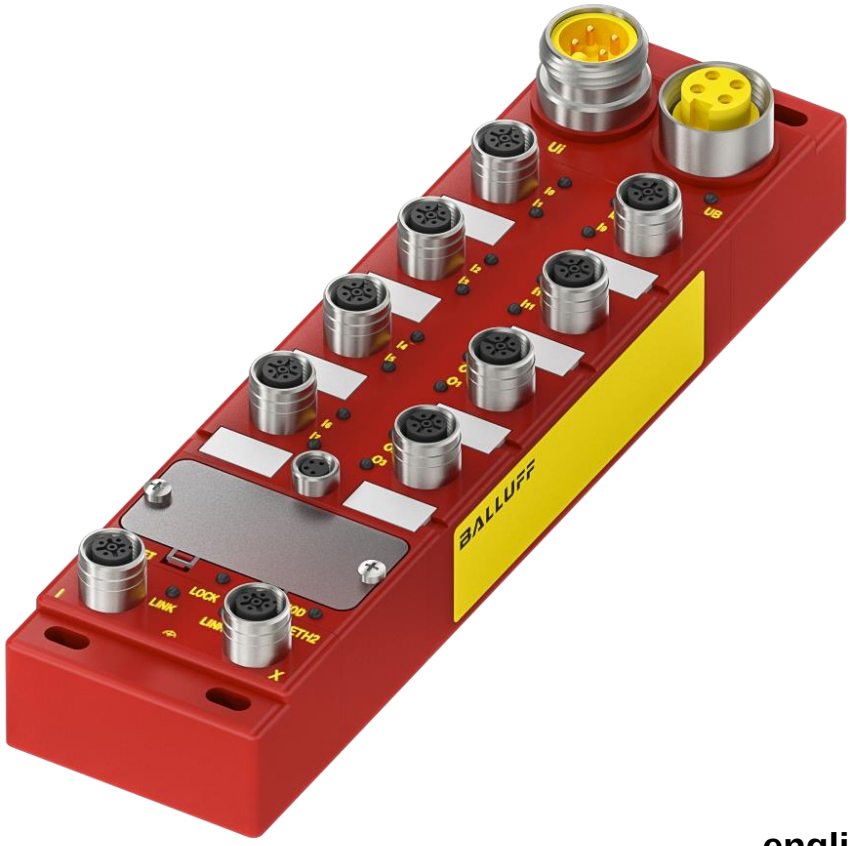
Hier finden die Benutzer verschiedene Ressourcen, u.a.:

- Download-Center
- Formular für Supportanfragen
- Knowledge Base
- Kontakte für den weltweiten technischen Support

955362_AC · DE · H22; Änderungen vorbehalten. Ersetzt G22.

EtherNet/IP™ CIP Safety™
Safe I/O Module
BNI CIP-351-000-K015 (BNI00HN)

User's guide



EtherNet/IP™

CIP Safety™

english

www.balluff.com

Original instructions

All rights reserved. Protected within the legally permissible limits of the United States and internationally. This document may not be copied or modified without prior written permission from Balluff.

All the trademarks and names appearing here are for identification purposes only. Some of these trademarks may be registered trademarks of the respective owners.

Balluff is not liable for any technical or printing errors, removal of the text contained herein or unintended damage resulting from use of the material.

1. About This Manual 6
1.1. About this manual 6

2. General Safety Instructions 9
2.1. Intended use 9
2.2. Responsibility of the user 9
2.3. Documentation 10
2.4. Maintenance 11
2.5. Spare parts 11
2.6. Shipping 11
2.7. Disposal 11
2.8. Education of the personnel 11
2.9. Personal protective equipment 12
2.10. Special hazards 13
2.11. Sign-posting 14

3. About this product 15
3.1. Product description 15
3.2. Ordering Information 15
3.3. Application 16
3.4. Functional safety - safety relevant parameters 17
3.5. Product environmental and safety instructions 18
3.6. Product features 20
3.7. Ethernet topologies 21

4. Functional Safety Functions 22
4.1. Safety States 22
4.2. Safety Inputs 23
4.3. Safety Outputs (BNI CIP-351-000-K015) 28
4.4. I/O Status 31
4.5. Behavior in case of fault 32
4.6. Response Time 34

5. Product Characteristics 35
5.1. Hardware characteristics 35
5.2. Mechanical characteristics 41
5.3. Physical I/O mapping 42
5.4. Safety I/O assemblies 43
5.5. Safety I/O connections 44
5.6. Safety I/O data mapping 46
5.7. Pin assignment 54
5.8. LED assignment 55

6. Product installation and wiring 59
6.1. Power supply 59
6.2. Ethernet connection 60
6.5. Module grounding 63
6.6. I/O wiring 64

7. Product Deployment 70
7.1. Getting Started 70
7.2. IP address setting 70
7.3. EDS files 78
7.4. Import the Safe I/O Module – Safety EDS into Rockwell library 80
7.5. Configure Safe I/O Module into Rockwell RSLogix 5000 project 89
7.6. Safety I/O assemblies 92
7.7. Configure Safe I/O Module in BALLUFF SNCT 95
7.8. Connection and testing of the Safe I/O Module in RSLogix 5000 114

8. EtherNet/IP Behavior 118
8.1. I/O behavior 118
8.2. IDLE behavior 118
8.3. Duplicate IP address 118
8.4. EtherNet/IP Object Classes 119

9. Product Replacement 127
9.1. Before to start 127
9.2. Replacement procedure 128
9.3. Verification 129

10. SNCT Configuration Software 130
10.1. Overview 130
10.2. Safety Reset 132
10.3. Lock / Unlock Configuration 139
10.4. Stored IP Address using DHCP Server 145
10.5. IP Address Conflict 146
10.6. Ethernet Port Diagnostics 147
10.7. Module Information 148
10.8. Set/Reset password 150
10.9. Additional Information 154
10.10. Download Firmware 156
10.11. Print module configuration 160
10.12. Log (Emergency Mode) 163

11. Product Package 164
11.1. Product package 164
11.2. USB Stick 164
11.3. Memory Key 165

12. Web Server Interface 166

12.1. How to connect the web server 166
12.2. General information 167
12.3. Diagnostic information 168

13. Product Support 170

14.1. Warranty conditions 170
14.2. Product Information 170
14.3. Technical Support 171

1. About This Manual

This user`s guide describes the IP67 digital CIP Safety I/O Module BNI CIP-351-000-K015 (BNI00HN) from Balluff.

1.1. About this manual

General Safety Instructions
This chapter gives an overview of all important safety aspects for optimum protection of the personnel, as well as for the safe and fault-free operation.

Product Overview
This chapter gives an overview of the product usage and main features.

Safety Functions
This chapter gives a presentation of the characteristics of the Safety Inputs and Safety Outputs of the module.

Product Characteristics
This chapter gives an overview of characteristics and technical data of the Safe I/O Module.

Product Installation and Wiring
This chapter details the wiring possibilities and associated safety categories.

Product Deployment
This chapter presents an example of how to proceed with the commissioning of the Safe I/O Module based on the Rockwell Automation RSLogix™ 5000 software.

Product Behavior
This chapter gives a presentation of the Safe I/O Module behaviors related to EtherNet/IP communication.

Product Replacement
This chapter describes the strategy in case of replacement of commissioned Safe I/O Module.

SNCT Configuration software
This chapter presents the important features that are available in the SNCT software used for the Safe I/O Module commissioning.

Product Package
This chapter details the contents of the product package.

Web Server Interface
This chapter presents the Safe I/O Module information available by connecting the module web server.

Product Support
This chapter describes how to identify the product and contact information the technical support.

Target audience

The manual is targeted at users who have a background in automation and networking technology, including safety application, EtherNet/IP™ and CIP Safety™.

Structure of the manual

The manual consists of chapters. Every chapter provides a self-contained description of a specific topic.

Availability

The manual is available in electronic form as PDF-file (Adobe Acrobat Reader) in English language. It is important to warrant that the product will be implemented by a body having the right skill to understand English.

Icon headings

Important passages in the text are highlighted by following icons and headings:

Danger!

Immediate danger to life and limb of personnel and others. Non-compliance will cause death or serious injury.

Warning!

Hazardous situation to life and limb of personnel and others. Non-compliance may cause death or serious injury.

Attention!

Designates a possibly harmful situation. Non-compliance can damage the product or something in its environment.

Note!

Supplementary information and useful tips.

Liability Limitation

All data and notes in these instructions were prepared with consideration to the statutory standards and regulations, the present state of technology, as well as our many years of knowledge and experience.

The manufacturer accepts no liability for damage caused because:

- Non-compliance with the instructions
- Non-specified use
- Use of untrained personnel

The actual scope of delivery can, by special designs, deviate from the explanations and presentations given here, because of the utilization of additional order options, or because of the most recent technical changes.

The user is responsible for the execution of service and commissioning according to the safety instructions of the prevailing standards and other relevant national and local instructions concerning conductor dimensioning

and protection, earthing, overcurrent protection and so on.

The individual, who has carried out the mounting or the installation, is liable for damages which result from the mounting or from the connection.

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly. Necessary corrections are included in subsequent editions.

Suggestions for improvement are welcome.

The manufacturer is no liable for damage resulting from missing or insufficient knowledge of the manual. Therefore, it is recommended to the operator to obtain written instructions from qualified people.

Modifications or functional alterations on the product are not allowed due to safety reasons. Any modification on the product not explicitly authorized by the manufacturer will result in loss of any liability claims to the vendor. The same applies if non-authorized parts or equipment are used.

Copyright

This manual is to be treated confidentially. It has been provided only for the personnel, which uses the product. The transfer of this document to third parties without the authorization in writing of the vendor is prohibited.

Note!

The contents, texts, drawings, pictures and any other illustrations are copyrighted and subject to other protection rights. Any person unlawfully using this publication is liable to criminal prosecution.

Use of this manual

This user`s guide contains information for the intended use of the BNI CIP-351-000-K015 safety module.

Knowledge of regulations and the proper technical implementation of the safety instructions detailed in this manual performed by qualified personnel are prerequisites for safely planning, engineering, programming, installing and starting up the BNI CIP-351-000-K015 safety modules as well as for ensuring safety during their operation and maintenance.

Balluff will not be held liable for severe personal injuries, damage to property or the surroundings caused by any of the following: unqualified personnel working on or with the devices, de-activation or bypassing of safety functions or failure to comply with the instructions detailed in this manual.

The manual contains safety instructions, description of the modules and information about life cycle.

2. General Safety Instructions

This chapter gives an overview of all important safety aspects for optimum protection of the personnel, as well as for the safe and fault-free operation.

2.1. Intended use

The modules have been engineered and designed exclusively for the proper use described in this documentation. The modules are intended to be used if considering all references and information of this manual.

Warning!

Danger by not intended use!

Each use of the product, which differs from the intended use, can lead to dangerous situations.

Therefore:

Use the product only as intended.

Use the product only together with the recommended components.

Consider all the data in this manual.

Ensure that only qualified personnel works with the product.

Ensure during configuration that the product is operated within its specifications.

Ensure that the power supply corresponds to the given specifications.

Only use the product in a technically adequate condition.

Only use the product in combination with approved components.

Changes and modifications at the product

To avoid endangerments and to ensure the optimal operating, neither changes nor modifications should be made to the product, which are not specially approved by the manufacturer.

2.2. Responsibility of the user

The product is used in the factory automation environment. The user of the product is subject of the statutory duties to work safely.

In addition to the safety instructions in this manual, for the usage environment of the product, adhere to the relevant accident prevention and environmental protection regulations.

- The user must be informed about the valid industrial safety regulations in order to evaluate additionally dangers, which arise as a result of the special conditions for the product in the place of operation. This is to be transcribed with working instructions for the operation of the product.
- These working instructions must be kept in the direct environment of the product and accessible at any time for people who work with the product.
- Fully adhere to the working instructions.
- The product is only to be operated in a technically flawless and reliable condition.

2.3. Documentation

Every person working with the product must have read and understood the operating instructions before carrying out any work. The manual must be available to all personnel involved in:

- project design
- installation
- commissioning
- operation
- decommissioning

The following conditions must be met before using or commissioning the components described in this manual

Warning!

- Modification to the process control system should only be carried out when the system has been disconnected from power!
- Installation and modifications shall only be performed by properly trained personnel
- The national rules and regulations of the respective country must be satisfied (installation, safety, EMC ...)

Danger!

To prevent hazards and ensure optimum performance, no changes, modifications or conversions may be made to the product that have not been expressly approved by the manufacturer.

2.4. Maintenance

The corresponding safety module is maintenance-free.

2.5. Spare parts

Please use only original spare parts of Balluff.

Warning!
Incorrect or faulty spare parts can cause damage, malfunction or failure as well as affect security and safety function.

2.6. Shipping

For shipping always use the original packaging.

2.7. Disposal

National rules and regulations apply to the disposal of the unit. Please check with the local authorities for the correct local disposal procedures.

2.8. Education of the personnel

Warning!
Risk of injury resulting from insufficient qualification!
Improper use can cause considerable personal injury and material damage.

Qualification

The automation system may only be operated by persons, which are trained, instructed and authorized. Troubleshooting, maintenance, cleaning, and replacement must be performed only by skilled or trained personnel.

Qualified personnel
These persons have to know the instruction manual and have to act accordingly. Commissioning and training should only be performed by qualified personnel.

Operating personnel
These are electrical engineers and electricians of the customer or third party, which are authorized by the manufacturer and which have learned installation and commissioning by the manufacturer and are allowed to ground, mark and install electrical circuits and devices in accordance to the standard safety technology.

Qualified personnel is trained and instructed according to the corresponding valid standards in safety technology in the care and use of appropriate safety equipment.

2.9. Personal protective equipment

During work, the wearing of personal protective equipment is needed to minimize health hazards.

- Always wear the necessary protective equipment for the corresponding job.
- For your own safety regard the signs, which are in your work space.

Work clothing

is close-fitting clothing with low tensile strength, with tight sleeves and without a protruding part. Depending on the application it should be prevented, that the carrier gets serious injured or is exposed to health risk during work.

For reasons of injury no jewelry like rings and chains should be worn.

Protective helmet

for protection against falling and flying objects.

Safety shoes

for protection against falling heavy objects.

Protective gloves

To protect hands from friction abrasions, punctures or injuries, as well as from contact with hot objects

Eye protector

To protect eyes from flying parts and liquid splashes

2.10. Special hazards

In the following section the residual risks are identified, which result from the hazard analysis.

Regard the listed safety warnings here and the notes in the whole manual to reduce health hazards and to avoid dangerous situations.

Electric current

Danger!

Risk of death by electric current!

Contact with live parts is immediate danger to life. Damage of the insulation or of components can be danger to life.

Therefore:

Immediately turn off the power supply when the insulation is damaged. Work on the electrical system only by qualified personnel.

Always power-off and secure the electrical system during work.

Risk by residual energy

Danger!

Risk of death by electric current!

After disconnecting the device from main voltage, parts such as power connections should only be touched when the capacitors are discharged in the device.

Therefore:

Regard discharge time of the capacitors; do not touch live parts before having observed a period of 1 minute.

If there are additional connected capacitors on the link, the discharge of the link can last considerably longer. In this case you have to determine the required waiting period or even to measure whether the device is safe.

Moving objects

Warning!

Risk of injury from moving parts!

Rotary and linear moving parts can cause serious injuries.

Therefore:

Do not touch moving parts during operation. Do not open the cover during operation.

The mechanical residual energy depends on the application.

Driven components rotate respectively move for a certain time even after switching off the power supply.

Fire fighting

Danger!

Risk of death by electric current!

Risk of an electrical shock when using a conducting firefighting medium.

Therefore use the following firefighting medium:

- ABC powder / CO2

Behavior with dangers and accidents

Preventive measures

- Always be prepared for accidents or fire!
- Keep first-aid equipment (first aid kit, blankets etc.) and fire extinguishers handy.
- Make personnel familiar with accident message, first aid and rescue mechanisms.

In case of emergency: act correctly

- Set immediately the device with emergency stop out of operation.
- Initiate first-aid measures.
- Rescue persons from the danger zone.
- Inform responsible on-site.
- Call medical and / or fire department.
- Clear the access routes for emergency vehicles.

2.11. Sign-posting

Warning!

Danger of injury by illegible symbols

In course of time stickers and symbols on the equipment can get dirty or otherwise become unrecognizable.

Therefore:

Please always maintain all safety warnings and operation instructions on the device in easily readable condition.

3. About this product

3.1. Product description

EtherNet/IP™ CIP Safety™ module provide a reliable solution for the monitoring of safety input devices (interlock switches, emergency stops, light curtains, laser scanners, etc.) as well as the control of safety output devices (relays, muting lamps, fail-safe motor starters, etc.) with industrial safety controllers in harsh duty environments. Contained in an IP67 rated housing, the Safe I/O Module can be machine mounted and are able to withstand areas were liquids, dust or vibration may be present.

EtherNet/IP™ CIP Safety™ module serves mainly applications for automotive manufacturers and machine builders looking for on-machine safety I/O connection to reduce cabinet space. The IP67 60mm housing with M12 connectors make the Safe I/O Module ideally suited for many safety applications including material handling equipment, automated assembly machinery and automotive applications running robots into cells.

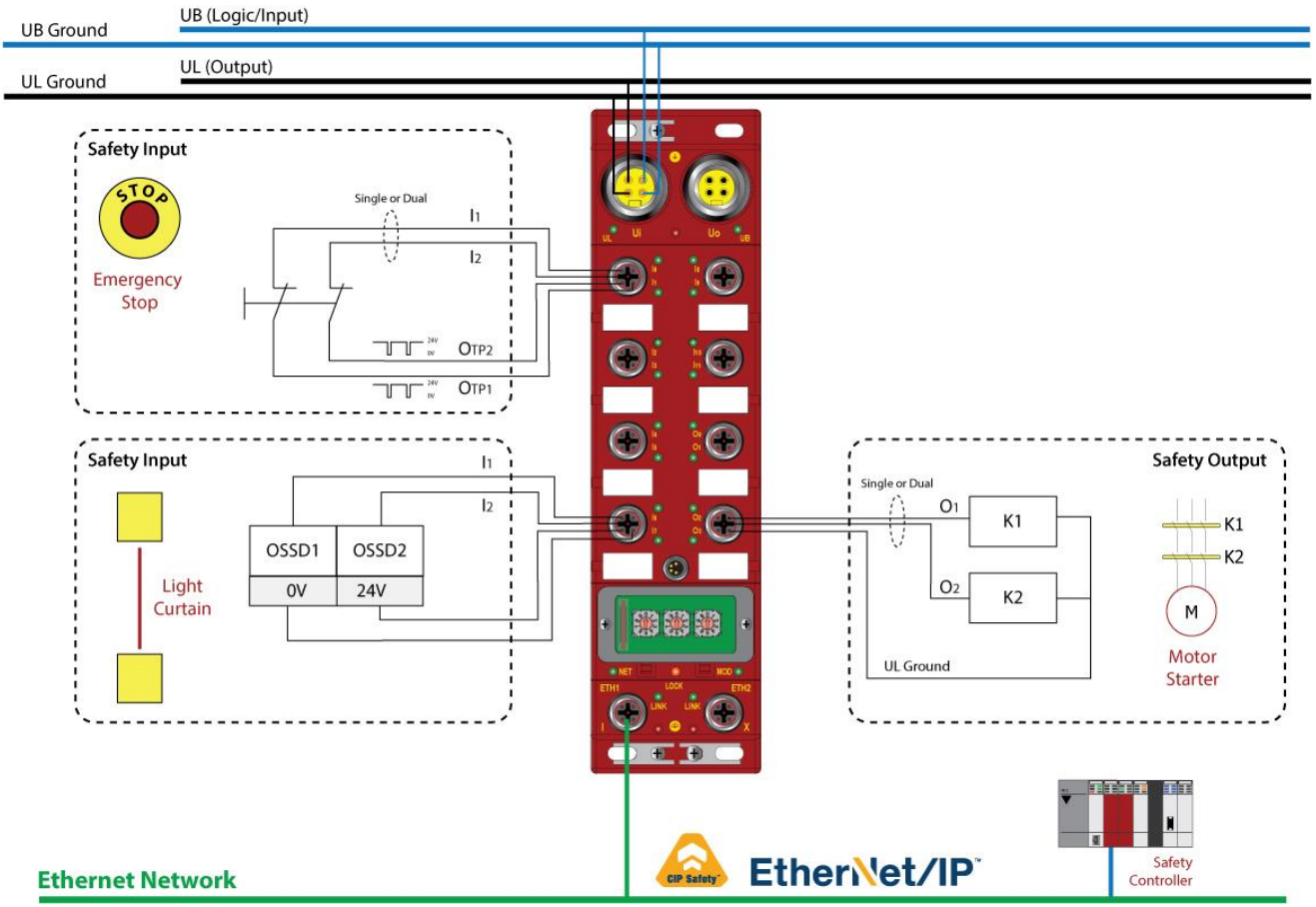
3.2. Ordering Information

Product Name	Order Code
BNI CIP-351-000-K015	BNI00HN

3.3. Application

The combination of EtherNet/IP and CIP Safety protocols allow exchanging safety process I/O and diagnostics information over a single Ethernet network. The modules need to be configured in order to suit with the safety function definitions, up to SIL 3 as defined by IEC 61508 or CAT 4/ PLe as defined by ISO 13849-1 (in particular, inputs and outputs could be set for use as dual-channel).

The diagram below shows some examples of safety I/O wirings.



3.4. Functional safety - safety relevant parameters

This chapter describes parameters associated to functional safety. In according to IEC 61508, Safety means first that a system is free from unwarrantable risks. Functional safety is a part of the total safety, which guarantees the fail-safe response of a safety system according to the input conditions. Here internal safety-relevant device errors must be detected and lead to a safe condition.

Safety relevant parameters may always be found in the according manuals of the modules.

BNI CIP-351-000-K015 (BNI00HN) product:

Parameters according to IEC 61508	Meaning
PFH = 4.95 × 10^{-9}/h	**P**robability of **f**ailure per **H**our: Probability of danger failure per hour
PFDavg = 4.30 × 10^{-4}	**P**robability of **F**ailure on **D**emand **av**era**g**e: Average of probability of failure on demand
SFF according SIL 3	**S**afe **F**ailure **F**raction: Fraction of failure, which lead to a safe state.

BNI CIP-351-000-K015 (BNI00HN) product:

Parameters according to DIN EN ISO 13849-1	Meaning
MTTFd: High	**M**ean **T**ime **T**o **d**angerous **F**ailure
DCavg: High	**D**iagnostic **C**overage **av**era**g**e
Service Life: 20 years	During the expected life of the device of up to 20 years, no proof test is required

3.5. Product environmental and safety instructions

Approvals, directives, standards

The Safe I/O Module has been designed to comply with the following directives and standards:

Conformity and approval		
CE*	2006/42/EC	Machinery directive
	2011/65/UE	RoHS 2 directive
	2014/30/EU	EMC directive for industrial use (Class-B)
UL Listed	UL 508	Approval for USA and Canada
IEC 61508	Ed 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)
ISO 13849-1	Ed 2015	Safety of machinery
IEC 62061	Ed 2021	Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems
IEC 61131-2	Ed 2007	Programmable logic controllers - Equipment Requirements and Tests
ODVA conformance	Vol 2 – 1.18	EtherNet/IP™
	Vol 5 – 2.6	CIP Safety™
IEC 60529	Ed 2010	IP67 degree of protection
IEC 61326-3-1	Ed 2017	Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)

*CE Declaration of conformity can be found on the Balluff website: (www.balluff.com).

The Safe I/O Module has been designed and produced specifically for:

- communication and process control
- general control and automation applications
- industrial applications
- operation within the environmental conditions specified in the technical data

This product was EMC tested for use in industrial areas. If it is to be used in personal or business and trade environments, the resulting system must go through EMC qualification.

Explosive environments

Danger!
This device is not certified for applications in

- explosive environments (EX-zone)

Power supply and Electrical safety

The device is developed for operation on 24 VDC power supplies, which correspond to the PELV-/SELV regulations in accordance to EN 50178.

Risk of injury by electric current!

There may only devices be connected to the module, which have a safe separation from the mains (such as 120V/230V/600V) power.

The power supply to generate 24 V power must correspond to the requirements for PELV/SELV according to EN 50178.

IP67 rating

The product complies with IP67 when installed. All caps of non-used connectors shall be mounting on the product to maintain the IP67 rating during operation.

Danger!
Risk of electric power!
Contact with live parts is immediate danger to life.

Mission time

The expected life time of the Safe I/O Module is up to 20 years with no proof test necessary.

Warning!
If the user calculates their safety application with the specified data for >20 years, the Safe I/O Module has to be decommissioned and replaced. A proof test cannot be established by the user.

Earthing

Warning!
Connections to earth shall be wired accordingly to the relevant chapter of this manual in order to warrant EMC characteristics of the product.

3.6. Product features

EtherNet/IP CIP Safety I/O Module main features include:

- Safety Inputs
  - To connect safety devices, such as emergency stop push buttons, gate switches, and safety light curtains.
  - Single or dual channel modes supported.
  - Dual-channel mode evaluates consistency between two input signals (channels), which allows use of the module for Safety Category 3 and 4. The time of a logical discrepancy between two channels can be monitored using a discrepancy time setting.
  - Each safety input has its own associated test output to check external wiring short-circuit.
  - Independently adjustable ON and OFF delay are available per channel.
- Test Outputs
  - Separate test outputs are provided for external short circuit detection of a safety input.
  - Power (24 V) can be supplied to devices, such as safety sensors.
  - Test outputs can be configured as standard non-safe outputs.
  - 2 test outputs can be used for broken wire detection of a muting lamp.
- Safety Outputs
  - Up to 1A for safety outputs.
  - Dual-channel mode evaluates consistency between two output signals (channels).
  - Safety outputs can be pulse tested to detect field wiring shorts to 24 VDC.
- I/O Safety RPI with up to 10ms cycle time
- IP67 rated enclosure that when properly installed provides protection against the ingress of dust, water
- Integrated 2-port unmanaged Ethernet switch with cross-over and DLR capability
- Isolated grounding to able to use 2 separate power supplies to energize the module logic/inputs and outputs.
- Protective earth (for power supplies)
- Functional earth (for Ethernet connectors)
- Diagnostic visible LEDs
- Easy commissioning via Balluff Safety Network Configuration Tool (SNCT)
- On-board memory key allowing to store module configuration and perform replacement in few minutes without any special tool or re-commissioning.
- 3 rotary switches to set IP address

3.7. Ethernet topologies

EtherNet/IP CIP Safety I/O Module can be used with a protocol compliant scanner as part of control system architecture. The module built-in 2-port Ethernet DLR capable switch allowing to use the network topology that meets the application needs. These topologies include the following:

- Star
- Daisy-chain
- Combination of star and daisy-chain
- DLR for Ethernet media ring redundancy

Note!

When considering the daisy chain topology, note that:

- Performing maintenance on any module not physically located at the end of the daisy chain – for example, by removing the network cable, or by cycling power to the module – affects any modules located down the chain from the maintained module.
- The embedded dual port Ethernet switch located in each module eliminates the need for additional Ethernet switches

4. Functional Safety Functions

EtherNet/IP CIP Safety I/O Module can achieve the following safety classes by making suitable parameter settings and wiring.

Safety Classes		
I/O Configuration	**Per IEC 61508 / IEC 62061**	**Per ISO 13849-1**
Dual I/O Channel	SIL 3	PL e / Cat. 4
Single I/O Channel	SIL 2	PL d / Cat. 2

4.1. Safety States

The safety states of the I/O module are defined as the following:

- Safe Outputs are switched OFF
- Safe Inputs are reported in the OFF state on the network

Warning!
The Safe I/O Module are to be used in systems where the OFF state is the safety state.

4.2. Safety Inputs

Safety inputs are used to report the state of safety input devices.

A safety input can be configured as:

- **Not Used** (default) - the input is disable and doesn't participate in any safety function
- **Safety** - the input participates to the safety function, but does not have a dependency on a test output
- **Safety Pulse Test** - the input participates to the safety function and has a dependency on an associated test output configured as "Pulse Test"
- **Standard** - The input doesn't participate in any safety function (allows to connect non-safe input device). Nevertheless a **Standard** input behaves exactly like an input configured as **Safety**.

Using Safety Inputs on Single-Channel

The inputs are configured as 2 distinct safety inputs on the same M12 connector.

The process Input value is set to safety device physical input value and status is "1" (good) as long as no fault is detected. On fault detection, the process Input value is turned OFF and status is "0" (bad).

BNI CIP-351-000-K015 (BNI00HN) behavior when used as single safe inputs:

Safety Device Physical State	Fault Detected(1)	Safe Input Process Value	Safe Input Process Status	Safe Input Led Status
0 = OFF	No	**0** (safe)	**1**	**OFF**
1 = ON	No	**1** (active)	**1**	**YELLOW**
0 = OFF	Yes	**0** (fault) (2)	**0**	**RED**
1 = ON	Yes	**0** (fault)	**0**	**RED**

Notes!

- (1) When single channel input is configured as "Standard" or "Safety", only internal hardware faults can be detected. Input shall be configured as "Safety Pulse Test" to allow external short to ON detection.
- (2) This state is a transitory state only as it corresponds to fault reset condition (physical value set to OFF). If physical fault still exist on the wiring, fault will be detected again at next ON transition.

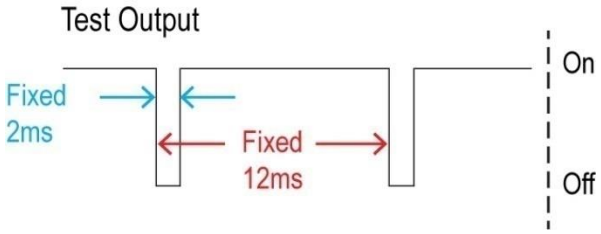
Using a Test Output

A test output can be configured as

- **Pulse Test** – When the external contact of the safety device is closed, the test output pulse allows diagnosing external wiring faults as stuck with the power supply or short with the other safety input from the same M12 connector.

Note!
Characteristics of the pulse test

- Pulse test length: 2ms
- Pulse test period: 12ms



Note!
A pulse test can be configured to each safety Input of the M12 connector. It can be also associated to the both inputs.

- **Power Supply** – The test output is used as a power supply to supply 24 VDC for the safety input device.
- **Standard** – The test output is used as a non-safe digital output.

Note!
No status led is associated to test outputs. Test output values and status can nevertheless be monitored via Inputs process image.

- **Muting Lamp** – The test output diagnoses whether the circuit and lamp are operational.

Warning!
When test outputs are configured for **Power Supply** or **Muting Lamp**, the use of double isolation cable could be required depending on the application and on the expected SIL/CAT to achieve.

When test output is activated, Muting Lamp feature controls the output current. Below 5mA, a fault is detected and the status is 0=OFF. Above 25mA is normal operation, the status is 1=ON.

Below is a typical scenario for muting lamp broken wire detection:

Test Output Process Value	Muting Lamp Physical State	Muting Lamp Status
Step #1: 1 = ON	Lamp good	1
Step #2: 1 = ON	Lamp broken	0
Step #3: 0 = OFF	Lamp broken	0
Step #4: 0 = OFF	Lamp replaced	1

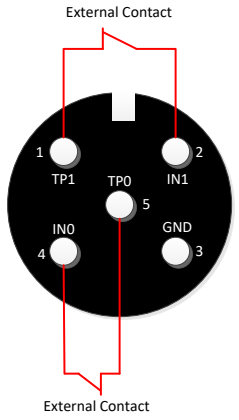
Notes!

- Only *Test Output 3* and *Test Output 7* can be configured in Muting Lamp mode.
- When Test Output is not activated, no broken wire fault can be detected. However, once a default has been detected (step 2), the lamp replacement is diagnosed even if the Test Output is deactivated (step 3)
- Broken wire detection is performed at a 3 second period. Two consecutive detections are required before the status is reported as BAD, so up to 6 seconds can be required before muting lamp status to be set to BAD

Typical wiring of safety inputs

M12 pining and wiring of the safety inputs with the associated pulse test outputs

- 1: Test Output #1 (TP1, 24 VDC powered from UB)
- 2: Safe Input #1 (IN1)
- 3: Ground Logic/Input (UB GND)
- 4: Safe Input #0 (IN0)
- 5: Test Output #0 (TP0, 24 VDC powered from UB)



Set Dual-channel Mode and Discrepancy Time

To support redundant channel safety devices, the consistency between signals on two input channels can be evaluated. This type of redundant wiring is called dual-channel mode.

Note!

- The dual-channel feature can only work by using the 2 safety input signals of the same M12 port of the Safe I/O Module.
- A total of six redundant channel safety devices can be connected to the Safe I/O Module. One redundant channel safety device per M12 port.

Either “Equivalent” or “Complementary” evaluation mode of the safety input pair has to be selected. In dual-channel mode, the Safe I/O Module monitors the time during which there is a discrepancy between the two channels.

Note!

Using the Balluff SNCT software,

- The discrepancy time can be configured from 10ms to 30s, in increments of 10ms.
- The discrepancy time default value is 10ms.

BNI CIP-351-000-K015 (BNI00HN) behavior when used as equivalent dual safe inputs:

Safety Device Physical State		Fault Detected(*1)		Safe Input Process Value		Safe Input Process Status		Safe Input Led Status	
Input (Pin 4)	Input+1 (Pin2)	Input	Input+1	Input	Input+1	Input	Input+1	Input	Input+1
0 = OFF	0 = OFF	No	No	**0** (safe)	**0** (safe)	**1**	**1**	**OFF**	**OFF**
0 = OFF	1 = ON	No	No	**0** (fault)	**0** (fault)	**0**(a)	**0**(a)	**RED**(b)	**RED**(b)
1 = ON	0 = OFF	No	No	**0** (fault)	**0** (fault)	**0**(a)	**0**(a)	**RED**(b)	**RED**(b)
1 = ON	1 = ON	No	No	**1** (active)	**1** (active)	**1**	**1**	**YELLOW**	**YELLOW**
-	-	Yes	-	**0** (fault)	**0** (fault)	**0**	**0**	**RED**	**BLINKING RED**
-	-	-	Yes	**0** (fault)	**0** (fault)	**0**	**0**	**BLINKING RED**	**RED**

(a): At “1” until discrepancy time expired.
(b): OFF until discrepancy time expired.

BNI CIP-351-000-K015 (BNI00HN) behavior when used as complementary dual safe inputs:

Safety Device Physical State		Fault Detected (1)		Safe Input Process Value		Safe Input Process Status		Safe Input Led Status	
Input (Pin 4)	Input+1 (Pin2)	Input	Input+1	Input	Input+1	Input	Input+1	Input	Input+1
0 = OFF	0 = OFF	No	No	**0** (fault)	**1** (fault)	**0**(a)	**0**(a)	**RED**(b)	**RED**(b)
0 = OFF	1 = ON	No	No	**0** (safe)	**1** (safe)	**1**	**1**	**OFF**	**YELLOW**
1 = ON	0 = OFF	No	No	**1** (active)	**0** (active)	**1**	**1**	**YELLOW**	**OFF**
1 = ON	1 = ON	No	No	**0** (fault)	**1** (fault)	**0**(a)	**0**(a)	**RED**(b)	**RED**(b)
-	-	Yes	-	**0** (fault)	**1** (fault)	**0**	**0**	**RED**	**BLINKING RED**
-	-	-	Yes	**0** (fault)	**1** (fault)	**0**	**0**	**BLINKING RED**	**RED**

(a): At “1” until discrepancy time expired.
(b): OFF until discrepancy time expired.

Notes!

- (1) When dual channel inputs are configured as “Standard” or “Safety”, only internal hardware faults and discrepancy between inputs can be detected. Inputs shall be configured as “Safety Pulse Test” to allow external short to 1 detection
- At inputs transition, during the discrepancy time, inputs are reported at the safe state

Safety Input Fault Recovery

Note!

If a fault is detected, the safety input (or safety inputs) process value remains in the safety state until the following procedure is applied:

1. Removed the cause of the fault.
2. Set the safety input to his safety state.

Input Delay

On-delay and Off-delay can be configured individually for each input.

On-delay

The On-delay is the minimum time necessary for a physical input switched to ON to be reported as “1” on the network. For example, if the On-delay is set to 5ms, the Input will be reported on the network at level “1”, after the Input has been evaluated at ON during at least 5ms.

Off-delay

The Off-delay is the minimum time necessary for a physical input switched to OFF to be reported as “0” on the network. For example, if the Off-delay is set to 5ms, the Input will be reported on the network at level “0”, after the Input has been evaluated at OFF during at least 5ms.

Note!

Using the Balluff SNCT software,

- On-delay and Off-delay parameters can be configured from 0 to 1000ms, in increments of 1ms.
- On-delay and Off-delay default values are 0.

Input Error Latch Time

The Input Error Latch Time is a unique parameter that applies for all the Inputs.

The purpose for latching input errors is to make sure that intermittent faults that can only exist for a few milliseconds are latched long enough to be read by the controller. It defines the minimal duration a detected fault on any safe inputs shall be reported on the network in order to able the controller to detect it.

Note!

Using the Balluff SNCT software,

- Input Error Latch Time default parameters can be configured from 0 to 65530ms, in increments of 10ms.
- Input Error Latch Time default value is 1000ms.
- The amount of time to latch the error must be based on the RPI of the safety connection, the application safety task watchdog, and other application specific variables.

4.3. Safety Outputs (BNI CIP-351-000-K015)

Safety sourcing outputs are used to drive the state of output devices.

Note!
The safe outputs are:

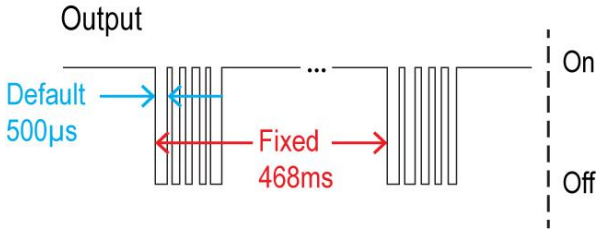
- current sourcing at max. 1A
- short circuit protected
- pulse test configurable

A Safety Output can be configured as:

- **Not Used** (default) - The output is disable and doesn't participate in any safety function.
- **Safety Pulse Test** - The output generates pulse tests (when the output is active) to monitor short-circuit between output pin and power supply (stuck at "1"), or short with other active output from the same M12 connector.

Notes!
Using the Balluff SNCT software,

- The Pulse tests length is configurable from 300µs to 10ms, in increments of 100µs.
- Pulse tests length default value is 500µs
- Pulse tests period: 468ms



- In addition to external shorts detection, all safety functions involved in outputs switch-off are also diagnosed at each period. So a series of 4 pulse tests are applied on each safety output.

Note!
The pulse test should be configured according to the impedance of the connected device. The Safe I/O Module has been designed to control a wide range of device by using an active discharge circuit. For each pulse test higher than 500µs (or equal), if a residual voltage is present, a 50mA current is clamped during 300µs. Nevertheless, if it is not enough and output goes into safe state due to the capacitive load of the connected equipment, the pulse length can be increased (up to 10ms).

Notes!

- Safety Sourcing outputs should not be used to provide power to a device or sub-system whom the resistive and capacitive load could vary during operation.

Warning!

Be careful of the response time of the output device to prevent any malfunction because of pulse test.

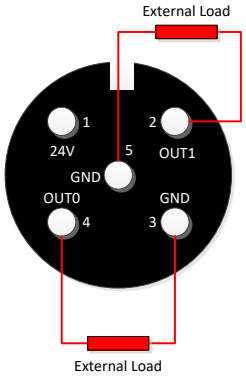
- **Safety No Pulse Test** - The output is used without pulse test.

Note!

In this mode, diagnostics are done on the output. When a sourcing output is switched off, the measured state can be different to the expected one due to the capacitive load of the connected equipment. The Safe I/O Module have been designed to control a wide range of equipment by using an active discharge circuit. When a sourcing output is switched off, if a residual voltage is present, a 50mA current is clamped during 2ms.

M12 pining and wiring of the safety sourcing outputs:

- 1: 24 VDC (powered from UL)
- 2: Safe Output #1 (OUT1)
- 3: Ground Output (UL GND)
- 4: Safe Output #0 (OUT0)
- 5: Ground Output (UL GND)



Note!

The maximum current available on the Pins #1 (24 VDC) of the 2 Output sourcing ports is 3.5A.

Using Safety Outputs in Single-Channel Outputs

Outputs from the same M12 connector are configured as 2 single channel outputs.

When activated by the logic controller, output is turned ON and status is “1” (good) as long as no fault is detected. On fault detection, Output is forced to safe state OFF and status is set to “0” (bad).

BNI CIP-351-000-K015 (BNI00HN) behavior when used as single safe outputs:

Safe Output Process Value	Fault Detected	Safety Device Physical State	Safe Output Process Status	Safe Output Led Status
0	No	0 = OFF (safe)	**1**	**OFF**
1	No	1 = ON (active)	**1**	**YELLOW**
-	Yes (on output itself)	0 = OFF (fault)	**0**	**RED**
-	Yes (on the partner)	0 = OFF (fault)	**0**	**BLINKING RED**

Note!

When a fault is detected on a single channel output, both outputs on the same M12 connector will switch to safe state.

Note!

- When no pulse test is configured on a safety output, only read back value is used to detect fault, so only short to 1 when output is driven to 0 and short to 0 when output is driven to 1 are detected
- When pulse tests are activated, internal faults as well as short to 1 can be then detected

Using Safety Outputs as Dual-Channel outputs

Outputs from the same M12 connector can be configured as an output pair.

When both output process values are activated by the logic controller, the dual outputs are turned ON and status is “1” (good) as long as no fault is detected. On hardware fault detection or discrepancy of output process values, outputs are forced to safe state OFF and status is set to “0” (bad).

BNI CIP-351-000-K015 (BNI00HN) behavior when used as dual safe outputs:

Safe Output Process Value		Fault Detected		Safety Device Physical State		Safe Output Process Status		Safe Output Led Status	
Output	Output+1	Output	Output+1	Output (Pin 4)	Output+1 (Pin2)	Output	Output+1	Output	Output+1
0	**0**	No	No	0 = OFF (safe)	0 = OFF (safe)	**1**	**1**	**OFF**	**OFF**
0	**1**	No	No	0 = OFF (fault)	0 = OFF (fault)	**0**	**0**	**RED**	**RED**
1	**0**	No	No	0 = OFF (fault)	0 = OFF (fault)	**0**	**0**	**RED**	**RED**
1	**1**	No	No	1 = ON (active)	1 = ON (active)	**1**	**1**	**YELLOW**	**YELLOW**
-	-	Yes	-	0 = OFF (fault)	0 = OFF (fault)	**0**	**0**	**RED**	**BLINKING RED**
-	-	-	Yes	0 = OFF (fault)	0 = OFF (fault)	**0**	**0**	**BLINKING RED**	**RED**

Safety Output Fault Recovery

Note!

If a fault is detected, the safety output (or safety outputs) physical value remains in the safety state until the following procedure is applied:

- Removed the cause of the fault.
- Set the safety output to his safety state.

Output Error Latch Time

The Output Error Latch Time is a unique parameter that applies for all the Outputs.

The purpose for latching output errors is to make sure that intermittent faults that can only exist for a few milliseconds are latched long enough to be read by the controller. It defines the minimal duration a detected fault on any safety outputs shall be reported on the network in order to able the controller to detect it.

Note!

Using the Balluff SNCT software,

- Output Error Latch Time default parameters can be configured from 0 to 65530ms, in increments of 10ms.
- Output Error Latch Time default value is 1000ms.
- The amount of time to latch the error must be based on the RPI of the safety connection, the application safety task watchdog, and other application specific variables.

4.4. I/O Status

The Safe I/O Module provides status information to monitor the I/O circuit. The status information can be read by the EtherNet/IP scanner.

Note!

When a fault is detected, the status value is “0” meaning bad. On normal operation, the status value is “1” meaning good.

Each individual point listed below has its own individual status:

- Safety Input Status
- Test Output Status
- Safety Output Status

4.5. Behavior in case of fault

Detected fault	Fail safe state applied on	Method to recover	Fieldbus communication availability
Safety Input pulse test failure (single channel)	Faulted safe input	1. Remove the fault 2. Switch input in the safe state Wait latch error time expired	Yes
Safety Input pulse test failure (dual channel)	Safety inputs pair	1. Remove the fault 2. Switch input in the safe state Wait latch error time expired	Yes
Safety input pair discrepancy (dual channel)	Safety inputs pair	1. Remove the fault 2. Switch input in the safe state Wait latch error time expired	Yes
Safety output pulse test failure or read back value error (single channel)	Both single safety outputs on same connector	1. Remove the fault 2. Switch outputs in the safe state Wait latch error time expired	Yes
Safety output pulse test failure or read back value error (dual channel)	Safety output pair	1. Remove the fault 2. Switch outputs in the safe state Wait latch error time expired	Yes
Safety output discrepancy error (dual channel)	Safety Output pair	1. Remove the fault 2. Switch outputs in the safe state Wait latch error time expired	Yes
Overvoltage/under voltage error on input power (UB)	Whole module (all safety inputs and outputs)	Power cycle needed	Yes
Overvoltage error on output power (UL)	Whole module (all safety inputs and outputs)	Power cycle needed	Yes
Under voltage error on output power (UL)	All Safety outputs	1. Remove the fault 2. Switch outputs in the safe state	Yes
Overcurrent on input power (UB)	Whole module (all safety inputs and outputs)	Power cycle needed	Yes
Overcurrent on output power (UL)	Whole module (all safety outputs)	Power cycle needed	Yes

Temperature error	Whole module (all safety inputs and outputs)	Power cycle needed	NO → Critical Error All I/O leds blinked
Internal hardware error (CPU, RAM, ADC 3,3V,…)	Whole module (all safety inputs and outputs)	Power cycle needed	NO → Critical Error All I/O leds blinked
CIP Safety communication error (input connection)	All safety inputs	Originator to restart connection	Yes
CIP Safety communication error (output connection)	All safety outputs	Originator to restart connection	Yes
Rotary Change Value	Whole module (all safety inputs and outputs)	Power cycle needed	Yes
Remove External Key	Whole module (all safety inputs and outputs)	Power cycle needed	Yes

4.6. Response Time

Calculate the response time

In order to calculate the response time of a safety function, the worst-case response times of all components involved must be added to the delays on the communication paths. Below are the response times of the Safe I/O Module to perform these calculations.

Warning!
The safety function is not guaranteed if the following response times are calculated incorrectly.

1. **Maximum response time of a digital safety input (single and dual-channel modes)**
   Calculate the maximum response time of a safety Input in error-free state. The response time is calculated from the instant of the physical event happened to a connected sensor and the emission of the corresponding telegram on the EtherNet/IP network by the Safe I/O Module.

   Calculation Delay Times

Response time of the connected sensor/switch	+ _____	ms
Input delay configured + 500µs tolerance	+ _____.5	ms
Internal maximum processing time of Safe I/O Module PT_{IN} max	+ 10.5	ms
	---	
Maximum response time of a digital safety input	**= _____**	**ms**

2. **Maximum response time of a digital safety output (single and dual-channel modes)**
   Calculate the maximum response time of a safety output in error-free state. The response time is calculated from the moment a telegram is received by the Safe I/O Module and the actuator physical processes the switch-off physical event.

   Calculation Delay Times

Internal maximum processing time of the Safe I/O Module PT_{OUT} max:	+ 4.5	ms
Pulse test configured	+ _____	ms
Switch-off time of connected actuator/relay	+ _____	ms
Additional Switch-off delay (physical signal time commutation)	+ _____	ms
	---	
Maximum response time of a digital safety output	**= _____**	**ms**

Note!
The maximum response type of a detected safety error is 10ms (emission of the corresponding telegram on the EtherNet/IP network by the Safe I/O Module).

5. Product Characteristics

5.1. Hardware characteristics

Type	**12x Safe Inputs + 4x Safe Outputs**
Product Reference	BNI CIP-351-000-K015
Safety	
SIL (per IEC 61508 / IEC 62061)	Up to SIL3 (when configured in dual I/O Channel)
CAT (per ISO 13849-1)	Up to Cat. 4 (when configured in dual I/O Channel)
PL (per ISO 13849-1)	Up to PL e (when configured in dual I/O Channel)
PFH	4.95×10^{-9}/h
PFDavg	4.30×10^{-4}
DCavg	96.32%
MTTF	105 years
Service Life	20 Years
Power	
Power IN connector	Mini Change (7/8”), 4-pin male, stainless steel, shielded, Maximum 8 A
Power OUT connector	Mini Change (7/8”), 4-pin female, stainless steel, shielded, Maximum 8 A
Module & Input power (**UB**)	24 VDC, -15% / +20% (protected against power crossing).
Operating current (**UB**)	<100 mA
Output power (**UL**)	24 VDC, -15% / +20% (protected against power crossing)
Operating current (**UL**)	<20 mA (without load)
Safe Inputs	
Channels	12 channels
Connector	M12 Ultra-Lock, 5-pin, female, A-Coded, stainless steel, unshielded(*)
Input type	IEC61131-2 type 3
Input voltage	**UB**
On / Off delay	Configurable from 0 to 1000ms (0 by default)

Warning!
If **UB** is over 36 V for a period of 2 seconds or more. The safety module will go in fail state (all LEDs are blinking in red) and considered as destroyed. Indeed, the internal surge protections are irreversibly damaged and therefore the module cannot operate anymore.

Pulse Test Output	
Test rate interval	Max. 12ms
Pulse test length	2ms
Sensor power supply	0.7A
Max short circuit current	2A at 25°C
Safe Outputs	
Output type	Sourcing (PNP)
Channels	4 channels, 2-wires
Output voltage	UL
Connector	M12 Ultra-Lock, 5-pin, female, A-Coded, stainless steel
Test rate interval	Max. 2s
Rated Output current	1A per channel
Maximum Short circuit current (transitory before safety switch-off)	6.5 A

Note!
Shields of I/O connectors are not connected to earth. If shielded cable is used, then customer should connect the cable shield to the earth.

Fieldbus	
Ethernet connectors	M12, 4-pin, female, D-Coded, stainless steel, shielded
IP setting	DHCP based on MAC (infinite lease), DHCP based on Name, Static IP
Protocol	CIP Safety EtherNet/IP Adapter according specification Vol 5 – 2.21 (CIP Safety) and Vol 2 – 1.26 (EtherNet/IP)
Data access	Implicit messages for I/O data transfer
Implicit (I/O) connection	• 1x Exclusive Owner (EO) connection (safe information) • 2x Input Only (IO) connection (to share safe process data with a non-safe scanner) • Up to 7 Listen Only (LO) (to share safe process data with a non-safe scanner)
Explicit (EM) connection	• Up to 8 connections
CIP safety connection	Type 1 and Type 2

Supported CIP Objects	• 0x01 – Identity object
	• 0x02 – Message Router object
	• 0x04 – Assembly object
	  ○ Safety Input Profiles
	  ▪ 0x20C (T→O)
	  ▪ 0x21C (T→O)
	  ▪ 0x22C (T→O)
	  ▪ 0x243 (T→O)
	  ▪ 0x25C (T→O)
	  ▪ 0x27C (T→O)
	  ○ Safety Input Vendor Specific
	  ▪ 0x300 (T→O)
	  ○ Safety Output Profiles
	  ▪ 0x233 (O→T)
	  ○ Safety Output Vendor Specific
	  ▪ 0x301 (O→T)
	  ○ Configuration
	  ▪ 0x302 (T→O)
	• 0x06 – Connection Manager object
	• 0x23 – Safety discrete IO Profile
	• 0x37 – File Object
	• 0x3B – SDOP object
	• 0x3D – SDIP object
	• 0x3F – SDCO object
	• 0x47 – DLR object
	• 0x48 – QoS (Quality of Service)
	• 0x80 – SDCI object
	• 0xF5 – TCP/IP Interface object
	• 0xF6 – Ethernet Link object

Integrated Switch	• 2x ports integrated switch • Speed: 100Mbps • Auto negotiation • Auto crossing • Auto polarity • 1x status Led per port • Storm Protection against network loop (Broadcast, Multicast and Unicast packets)

Request Packet Interval (RPI)	For safety Inputs (configurable per Scanner connection) → ≥10ms minimum For safety Outputs (single Scanner connection) → ≥10ms minimum
IP Address Conflict Detection	Yes (ACD supported)
DLR	Yes (beacon node)
ODVA conformance	Yes (CT18EN – CT18ES)

Default Ethernet setting:

- IP address: DHCP
- Subnet mask: DHCP
- Gateway: DHCP
- ETH1 port: Auto negotiation + Auto-MDI
- ETH2 port: Auto negotiation + Auto-MDI
- ACD Enabled

Mechanical	
Housing dimension	235 x 60 x 44 mm (9.25"x2.36x1.73")
Housing material	PBT VALOX 420 SEO RED 7701
Flammability Standard	UL 94 V-0
Corner mounting hole	4 mounting holes, 5 x10 mm
Ground stud	Yes, stainless steel (allows the continuity of the ground when the module is mounted on the chassis machine)
Memory Key	Internal window key
Operating temperature	-25°c … +70°C
Storage temperature	-40°c … +90°C
Installation Altitude	Max. 2000m
Vibration resistance	Operating: 7mm p-p (5-15.7Hz), 7g (15,7Hz to 500Hz), 3 axis
Shock resistance	Operating: 15g, 11ms, 3 axis Non-operating: 50g, 6ms, 3 axis
Relative humidity	10 % to 95 %, non-condensing
Protection Class	IP67
MTBF	523 750 hours / 59,8 years at 25°C 345 000 hours / 39.4 years at 40°C 136 000 hours / 15.5 years at 70°C

Note!

7/8” accessories (cordsets, plugs …) connected to the module power connectors shall be screw with a torque of 2.0Nm to ensure a correct sealing to achieve IP67 rating.

M12 accessories (cordsets, plugs …) connected to the module I/O and network connectors shall be screw with a torque of 2.0Nm to ensure a correct sealing to achieve IP67 rating.

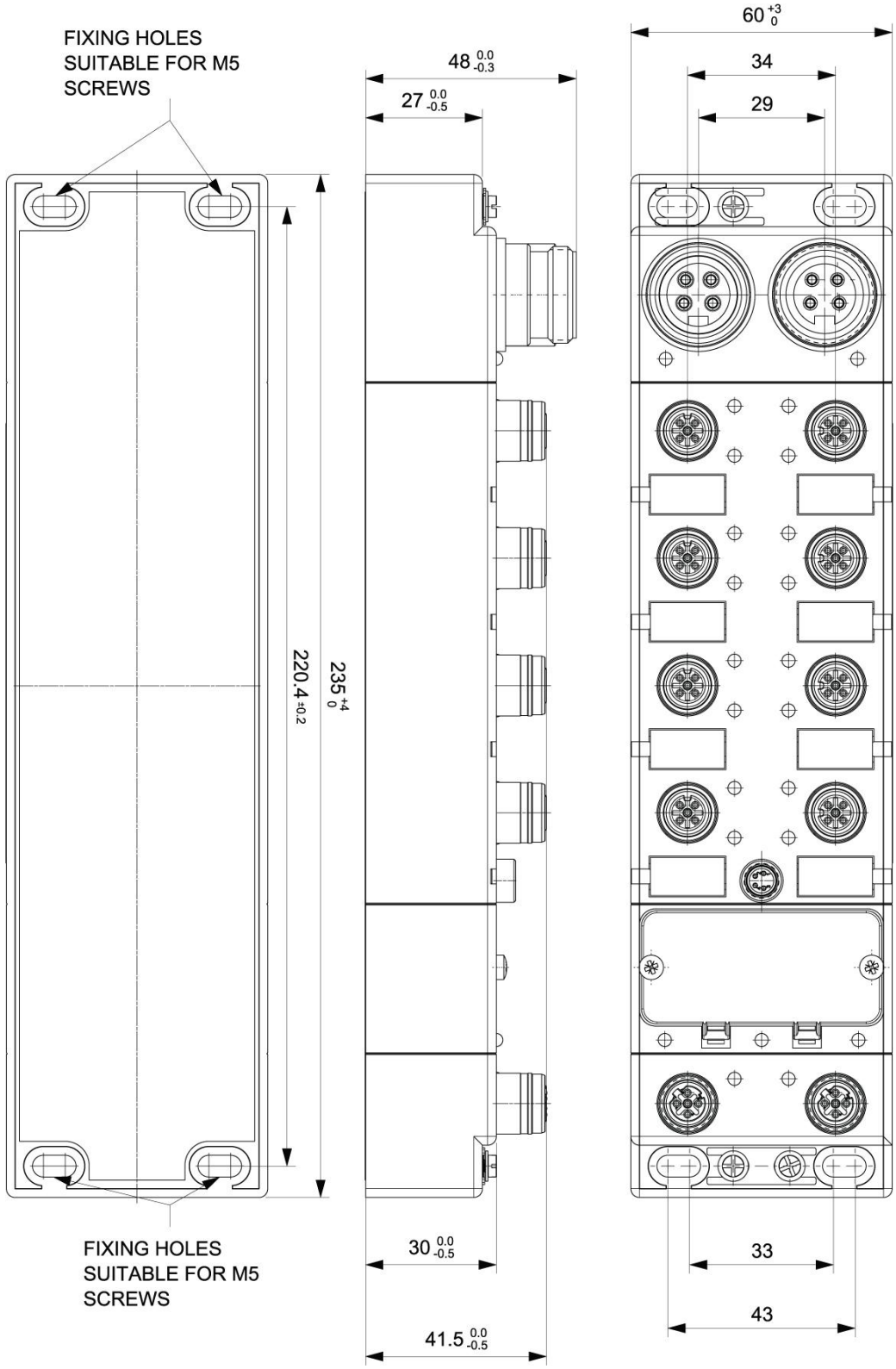
M8 accessories (cordsets, plugs …) connected to the module I/O and network connectors shall be screw with a torque of 2.0Nm to ensure a correct sealing to achieve IP67 rating.

Electromagnetic compatibility (EMC)	Standard		Comment
Noise immunity zone B	EN 61000-6-2		Immunity standard for industrial environments
Emission Standard for Industrial Environments	EN 61000-6-4 Class A (Industrial area)	EN 61000-4-2	ESD 8kV air discharge 6kV contact discharge
		EN 61000-4-3	High-frequency electromagnetic field 80MHz … 1000MHz, 20V/m, 80% AM (1kHz) 1.4GHz ... 2.0GHz, 10V/m, 80% AM (1kHz) 2.0GHz ... 6.0GHz, 3V/m, 80% AM (1kHz)
		EN 61000-4-4	Burst +/- 3kV 5/50 ns, 5 kHz on power ports +/- 2kV 5/50 ns, 5 kHz on I/O ports +/- 2kV 5/50 ns, 5 kHz communication ports
		EN 61000-4-5	Surge 1kV line to line, 2kV line to earth on power ports 2kV line to line on I/O ports 2kV line to earth on communication ports
		EN 61000-4-6	Conducted disturbances, induced by radio 150kHz … 80MHz, 10V, 80% AM (1kHz)
		EN 61000-4-16	Test for Immunity to conducted, common mode disturbances 0 Hz … 150 KHz

Warning!
Balluff devices comply with EU directives and conform (DoC) to the related EMC standards so that they can be easily integrated into other devices or machines. However, EMC compliance of the whole system remains under system builder responsibility.

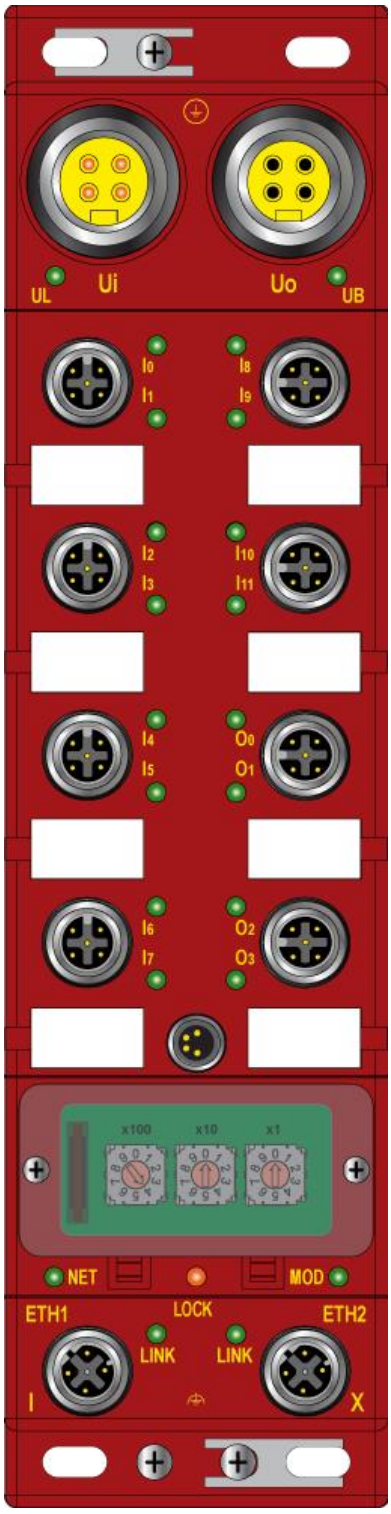
5.2. Mechanical characteristics

Size and dimensions (in mm)



5.3. Physical I/O mapping

BNI CIP-351-000-K015 (BNI00HN)



5.4. Safety I/O assemblies

The I/O process data are available through the EtherNet/IP assemblies which depend on the required data:

- Safety Input Process Data
    - Safety Discrete Input Profiles
        - Assembly 524 (20C Hex)
        - Assembly 540 (21C Hex)
        - Assembly 556 (22C Hex)
        - Assembly 579 (243 Hex)
        - Assembly 604 (25C Hex)
        - Assembly 636 (27C Hex)
    - Vendor Specific
        - Assembly 768 (300 Hex):
- Safety Output Process Data
    - Safety Discrete Output Profile
        - Assembly 563 (233 Hex)
    - Vendor Specific
        - Assembly 769 (301 Hex)
- Configuration Data
    - Vendor Specific
        - Assembly 770 (302 Hex)

5.5. Safety I/O connections

The I/O module supports

- 1x Exclusive Owner (EO) connection for controlling safe Input/Output process data.
- 2x Input Only (IO) connections for reading safe Input/Output process data with a safe or non-safe EtherNet/IP scanner.
- Up to 7 Listen Only (LO) (to read safe process data with a non-safe EtherNet/IP scanner).

Exclusive owner

This connection is bi-directional: the originator (safety PLC) produces data consumed by the target Safe I/O Module and the target produces data that is consumed by the originator. This connection type is called an Exclusive Owner (EO) connection or the controlling connection.

The Exclusive Owner (EO) connection is used to control the safe Input and safe Output process data. No more than one I/O EO connection can be an Input/Output connection.

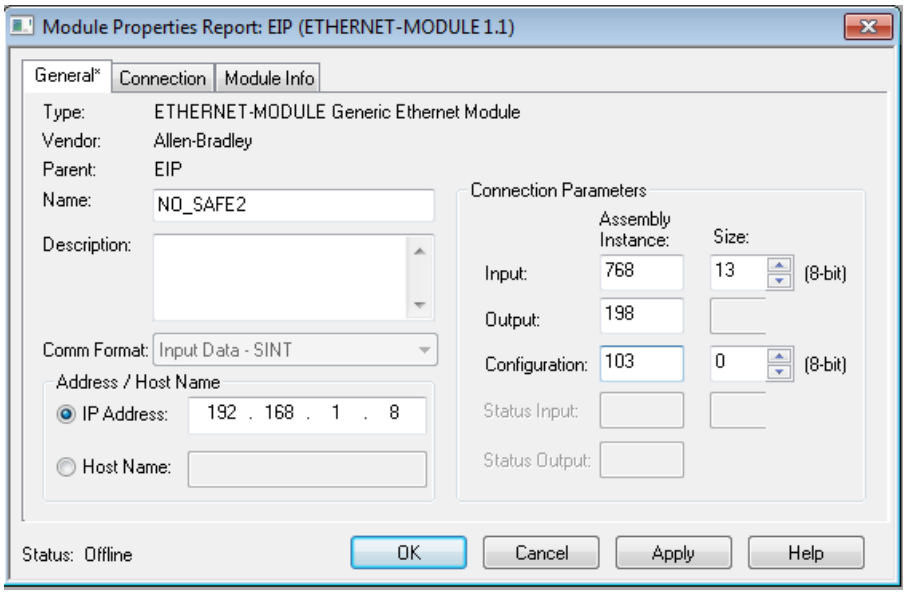
Input Only

For this connection type, only the target (Safe I/O Module) produces data, which is consumed by the originator (safety PLC). The originator will only send a heartbeat packet, sometimes at a reduced interval (less frequently than the RPI) used to allow the Safe I/O Module to identify when the connection is broken. This input only connection can be either unicast, either multicast.

Note!

Upload EDS file from the safety module to easily configure the connection.

Input Assembly	768 (300 Hex), Size 13 bytes
Output Assembly (Heartbeat)	198 (C6 Hex), Size 0 bytes
Configuration Assembly	103 (67 Hex), size 0 byte



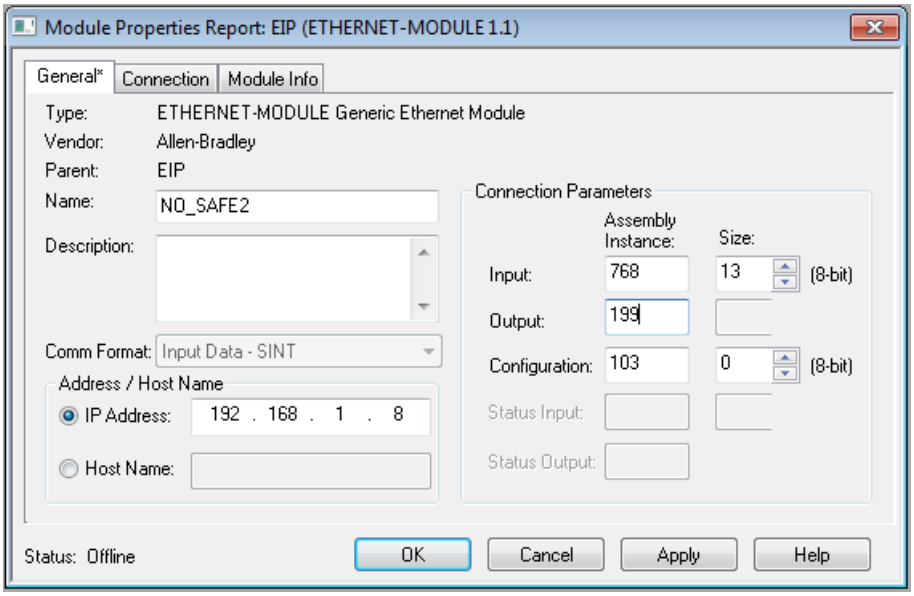
Listen Only

This connection type is identical to an Input Only connection type, with a single exception: a Listen Only connection can only exist when one of the other I/O connection (EO) types has been established. That is, a Listen Only connection cannot be established until an Input/Output or Input Only connection has been established, and conversely when the last non-Listen-Only connection has been closed or has timed out, the Listen Only connection will automatically close as well. This connection type is the least-frequently used type.

Note!

Upload EDS file from the safety module to easily configure the connection.

Input Assembly	768 (300 Hex), Size 13 bytes
Output Assembly (Heartbeat)	199 (C7 Hex), Size 0 bytes
Configuration Assembly	103 (67 Hex), size 0 byte



5.6. Safety I/O data mapping

Safe Inputs assemblies

Safety Discrete Input Profiles

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Input Data (Assembly 524 - 20C Hex), Size: 2 byte(s)																	
Safety Inputs	00	n/u	n/u	n/u	n/u	Safety Input I_{11}	Safety Input I_{10}	Safety Input I_9	Safety Input I_8	Safety Input I_7	Safety Input I_6	Safety Input I_5	Safety Input I_4	Safety Input I_3	Safety Input I_2	Safety Input I_1	Safety Input I_0

n/u: Not used
Safety Input Ix: Safety Input process value on channel Ix

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Input Data (Assembly 540 – 21C Hex), Size: 2 byte(s)																	
Safety Inputs + Global Safety Input Status	00	Comb. Safety Input Status **CIS**	n/u	n/u	n/u	Safety Input I_{11}	Safety Input I_{10}	Safety Input I_9	Safety Input I_8	Safety Input I_7	Safety Input I_6	Safety Input I_5	Safety Input I_4	Safety Input I_3	Safety Input I_2	Safety Input I_1	Safety Input I_0

n/u: Not used
Safety Input Ix: Safety Input process value on channel Ix
Combined Safety Input Status CIS: Set to “0” when an error is detected on any of the safety inputs.

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Input Data (Assembly 556 - 22C Hex), Size: 3 byte(s)																	
Safety Inputs + Safety Input Status	00	Safety Input Status I_3	Safety Input Status I_2	Safety Input Status I_1	Safety Input Status I_0	Safety Input I_{11}	Safety Input I_{10}	Safety Input I_9	Safety Input I_8	Safety Input I_7	Safety Input I_6	Safety Input I_5	Safety Input I_4	Safety Input I_3	Safety Input I_2	Safety Input I_1	Safety Input I_0
	02									Safety Input Status I_{11}	Safety Input Status I_{10}	Safety Input Status I_9	Safety Input Status I_8	Safety Input Status I_7	Safety Input Status I_6	Safety Input Status I_5	Safety Input Status I_4

n/u: Not used
Safety Input Ix: Safety Input process value on channel Ix
Safety Input Status Ix: Set to “0” when an error is detected on safety input Ix

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Input Data (Assembly 579 - 243 Hex), Size: 1 byte(s)																	
Safety Output Status	00									n/u	n/u	n/u	n/u	**Safety Output Status O_3**	**Safety Output Status O_2**	**Safety Output Status O_1**	**Safety Output Status O_0**

n/u: not used
Safety Output Status Ox: Set to “0” when an error is detected on safety output Ox

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Input Data (Assembly 604 - 25C Hex), Size: 2 byte(s)																	
Safety Inputs + Global Safety Input Status + Global Safety Output Status	00	**Comb. Safety Input Status CIS**	**Comb. Safety Output Status COS**	n/u	n/u	**Safety Input I_{11}**	**Safety Input I_{10}**	**Safety Input I_9**	**Safety Input I_8**	**Safety Input I_7**	**Safety Input I_6**	**Safety Input I_5**	**Safety Input I_4**	**Safety Input I_3**	**Safety Input I_2**	**Safety Input I_1**	**Safety Input I_0**

n/u: not used
Safety Input Ix: Safety Input process value on channel Ix
Combined Safety Input Status CIS: Set to “0” when an error is detected on any of the safety inputs
Combined Safety Output Status COS: Set to “0” when an error is detected on any of the safety outputs

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Input Data (Assembly 636 - 27C Hex), Size: 3 byte(s)																	
Safety Inputs + Global Safety Input Status	00	**Comb. Safety Input Status CIS**	n/u	n/u	n/u	**Safety Input I_{11}**	**Safety Input I_{10}**	**Safety Input I_9**	**Safety Input I_8**	**Safety Input I_7**	**Safety Input I_6**	**Safety Input I_5**	**Safety Input I_4**	**Safety Input I_3**	**Safety Input I_2**	**Safety Input I_1**	**Safety Input I_0**
Safety Output Status	02									n/u	n/u	n/u	n/u	**Safety Output Status O_3**	**Safety Output Status O_2**	**Safety Output Status O_1**	**Safety Output Status O_0**

n/u: not used
Safety Input Ix: Safety Input process value on channel Ix
Combined Safety Input Status CIS: Set to “0” when an error is detected on any of the safety inputs
Safety Output Status Ox: Set to “0” when an error is detected on safety output Ox

Vendor Specific

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Input Data (Assembly 768 - 300 Hex), Size: 13 byte(s)																	
Safety Inputs	00	n/u	n/u	n/u	n/u	Safety Input I_{11}	Safety Input I_{10}	Safety Input I_9	Safety Input I_8	Safety Input I_7	Safety Input I_6	Safety Input I_5	Safety Input I_4	Safety Input I_3	Safety Input I_2	Safety Input I_1	Safety Input I_0
Safety Input Status	02	n/u	n/u	n/u	n/u	Safety Input Status I_{11}	Safety Input Status I_{10}	Safety Input Status I_9	Safety Input Status I_8	Safety Input Status I_7	Safety Input Status I_6	Safety Input Status I_5	Safety Input Status I_4	Safety Input Status I_3	Safety Input Status I_2	Safety Input Status I_1	Safety Input Status I_0
Test Output Value	04	n/u	n/u	n/u	n/u	Test Output TO_{11}	Test Output TO_{10}	Test Output TO_9	Test Output TO_8	Test Output TO_7	Test Output TO_6	Test Output TO_5	Test Output TO_4	Test Output TO_3	Test Output TO_2	Test Output TO_1	Test Output TO_0
Test Output Status	06	n/u	n/u	n/u	n/u	Test Output Status TOS_{11}	Test Output Status TOS_{10}	Test Output Status TOS_9	Test Output Status TOS_8	Test Output Status TOS_7	Test Output Status TOS_6	Test Output Status TOS_5	Test Output Status TOS_4	Test Output Status TOS_3	Test Output Status TOS_2	Test Output Status TOS_1	Test Output Status TOS_0
Safety Output Monitoring	08	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	Safety Output Monitoring O_3	Safety Output Monitoring O_2	Safety Output Monitoring O_1	Safety Output Monitoring O_0
Safety Output Status	10	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	Safety Output Status O_3	Safety Output Status O_2	Safety Output Status O_1	Safety Output Status O_0
Miscellaneous	12									Input Over Current Error **UB**	Output Over Current Error **UL**	Muting Lamp Status TO_7	Muting Lamp Status TO_3	Comb. Safety Input Status **CIS**	Comb. Safety Output Status **COS**	Input Power Error **UB**	Output Power Error **UL**

n/u: not used

Safety Input Ix: Safety Input process value on channel Ix
Test Output TOx: Safety process value on channel Test Output TOx
Safety Output Monitoring Ox: Safety Output process value on channel Ox for PLC monitoring.

Safety Input Status Ix: Set to “0” when an error is detected on safety input Ix
Test Output Status TOSx: Set to “0” when an error is detected on the Test Output TOx
Safety Output Status Ox: Set to “0” when an error is detected on safety output Ox

Combined Safety Input Status CIS: Set to “0” when an error is detected on any of the safety inputs
Combined Safety Output Status COS: Set to “0” when an error is detected on any of the safety outputs
Muting Lamp Status TOx: Set to “0” when an muting lamp broken wire error is detected on channel x

Output Power Error UL: Diagnostic bit for Output power supply (UL)

- Set to “1”, if UL is out of valid range
- Set to “0”, if UL is within valid range

Input Power Error UB: Diagnostic bit for Logic/Input power supply (UB)

- Set to “1”, if UL is out of valid range
- Set to “0”, if UL is within valid range

Note!
Safety inputs configured as “not used” will report a process value of 0 and a safety status of 1.

Safety Outputs

Safety Discrete Output Profile

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Output Data (Assembly 563 - 233 Hex), Size: 1 byte(s)																	
Safety Outputs	00									n/u	n/u	n/u	n/u	Safety Output O_3	Safety Output O_2	Safety Output O_1	Safety Output O_0

n/u: not used
Safety Output Ox: Safety Output process value on channel x

Vendor Specific

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Output Data (Assembly 769 - 301 Hex), Size: 4 byte(s)																	
Safety Outputs	00	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	n/u	Safety Output O_3	Safety Output O_2	Safety Output O_1	Safety Output O_0
Test Outputs	02	n/u	n/u	n/u	n/u	Test Output TO_{11}	Test Output TO_{10}	Test Output TO_9	Test Output TO_8	Test Output TO_7	Test Output TO_6	Test Output TO_5	Test Output TO_4	Test Output TO_3	Test Output TO_2	Test Output TO_1	Test Output TO_0

n/u: not used
Safety Output Ox: Safety Output process control value on channel x
Test Output TOx: Test Output process control value on channel x

Notes!
Values provided for Safety outputs are ignored if corresponding outputs are configured as “not used”
Values provided for Test Outputs are ignored if corresponding Test Outputs are not configured as a “Standard Output”

Configuration Data

Note!

The data size can be set to “0” if the EtherNet/IP CIP Safety Scanner doesn’t need to send configuration data at the establishment of the connection (Safety Forward Open request), which is the case for example for Rockwell Safety controllers.

Note!

The description of the configuration data in the below table are for information purpose only. In fact, the configuration data are managed and sent directly by Balluff SNCT software.

Vendor Specific

	Byte Offset	Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Configuration (Assembly 770 - 302 Hex), Size: 123 bytes																	
Version	00	**Minor Version**								**Major version**							
Test Output Mode	02	**Test Output O1**								**Test Output O0**							
	04	**Test Output O3**								**Test Output O2**							
	06	**Test Output O5**								**Test Output O4**							
	08	**Test Output O7**								**Test Output O6**							
	10	**Test Output O9**								**Test Output O8**							
	12	**Test Output O11**								**Test Output O10**							
Output Error Latch Time	14	**Output Error Latch Time**															
Output Mode & Pulse test Length	16	**Pulse test Length O0**								**Output Mode O0**							
	18	**Pulse test Length O1**								**Output Mode O1**							
	20	**Pulse test Length O2**								**Output Mode O2**							
	22	**Pulse test Length O3**								**Output Mode O3**							
Dual Safe Output Mode	24	**Dual Output Mode O3 / O2**								**Dual Output Mode O0 / O1**							
Input Error Latch Time	26	**Input Error Latch Time**															
Parameters – Input I0	28	**OFF → ON Delay Input I0**															
	30	**ON → OFF Delay Input I0**															
	32	**Test Source Input I0**								**Input Mode I0**							
Parameters – Input I1	34	**OFF → ON Delay Input I1**															
	36	**ON → OFF Delay Input I1**															
	38	**Test Source Input I1**								**Input Mode I1**							

Parameters – Input I2	40		**OFF → ON Delay Input I2**
	42		**ON → OFF Delay Input I2**
	44	**Test Source Input I2**	**Input Mode I2**
Parameters – Input I3	46		**OFF → ON Delay Input I3**
	48		**ON → OFF Delay Input I3**
	50	**Test Source Input I3**	**Input Mode I3**
Parameters – Input I4	52		**OFF → ON Delay Input I4**
	54		**ON → OFF Delay Input I4**
	56	**Test Source Input I4**	**Input Mode I4**
Parameters – Input I5	58		**OFF → ON Delay Input I5**
	60		**ON → OFF Delay Input I5**
	62	**Test Source Input I5**	**Input Mode I5**
Parameters – Input I6	64		**OFF → ON Delay Input I6**
	66		**ON → OFF Delay Input I6**
	68	**Test Source Input I6**	**Input Mode I6**
Parameters – Input I7	70		**OFF → ON Delay Input I7**
	72		**ON → OFF Delay Input I7**
	74	**Test Source Input I7**	**Input Mode I7**
Parameters – Input I8	76		**OFF → ON Delay Input I8**
	78		**ON → OFF Delay Input I8**
	80	**Test Source Input I8**	**Input Mode I8**
Parameters – Input I9	82		**OFF → ON Delay Input I9**
	84		**ON → OFF Delay Input I9**
	86	**Test Source Input I9**	**Input Mode I9**
Parameters – Input I10	88		**OFF → ON Delay Input I10**
	90		**ON → OFF Delay Input I10**
	92	**Test Source Input I10**	**Input Mode I10**
Parameters – Input I11	94		**OFF → ON Delay Input I11**
	96		**ON → OFF Delay Input I11**
	98	**Test Source Input I11**	**Input Mode I11**
Dual Safe Mode	100	n/u	**Dual Safe Input Mode I1 / I0**
Dual Safe Discrepancy Time	102		**Discrepancy Operation Input I1 / I0**
Dual Safe Mode	104	n/u	**Dual Safe Input Mode I3 / I2**
Dual Safe Discrepancy Time	106		**Discrepancy Operation Input I3 / I2**

Dual Safe Mode	108	n/u	**Dual Safe Input Mode I5 / I4**
Dual Safe Discrepancy Time	110		**Discrepancy Operation Input I5 / I4**
Dual Safe Mode	112	n/u	**Dual Safe Input Mode I7 / I6**
Dual Safe Discrepancy Time	114		**Discrepancy Operation Input I7 / I6**
Dual Safe Mode	116	n/u	**Dual Safe Input Mode I9 / I8**
Dual Safe Discrepancy Time	118		**Discrepancy Operation Input I9 / I8**
Dual Safe Mode	120	n/u	**Dual Safe Input Mode I11 / I10**
Dual Safe Discrepancy Time	122		**Discrepancy Operation Input I11 / I10**

Test Output Mode
- 0: Not Used
- 1: Standard
- 2: Pulse Test
- 3: Power Supply
- 4: Muting Lamp (only possible for Input 3 and Input 7)

Output Error Latch Time (in ms)
A value between 0 and 65530; shall be a multiple of 10.

Output Mode
- 0: Not Used
- 1: Safety
- 2: Safety Pulse Test

Output Pulse test Length (in ms)
A value between 3 and 100.

Dual Safe Output Ox/Ox+1 Mode
- 0: Single
- 1: Dual

Input Error Latch Time (in ms)
A value between 0 and 65530; shall be a multiple of 10.

Input Ix Off → On Delay (in ms)
A value is between 0 and 1000.

Input Ix On → Off Delay (in ms)
A value is between 0 and 1000.

Input Ix Mode
- 0: Not Used
- 1: Safety Pulse Test
- 2: Safety
- 3: Standard

Input Ix Test Source (only test output on same connector can be used in this list):

- 0: Not Used
- 1: Test Output 0
- 2: Test Output 1
- 3: Test Output 2
- 4: Test Output 3
- 5: Test Output 4
- 6: Test Output 5
- 7: Test Output 6
- 8: Test Output 7
- 9: Test Output 8
- 10: Test Output 9
- 11: Test Output 10
- 12: Test Output 11

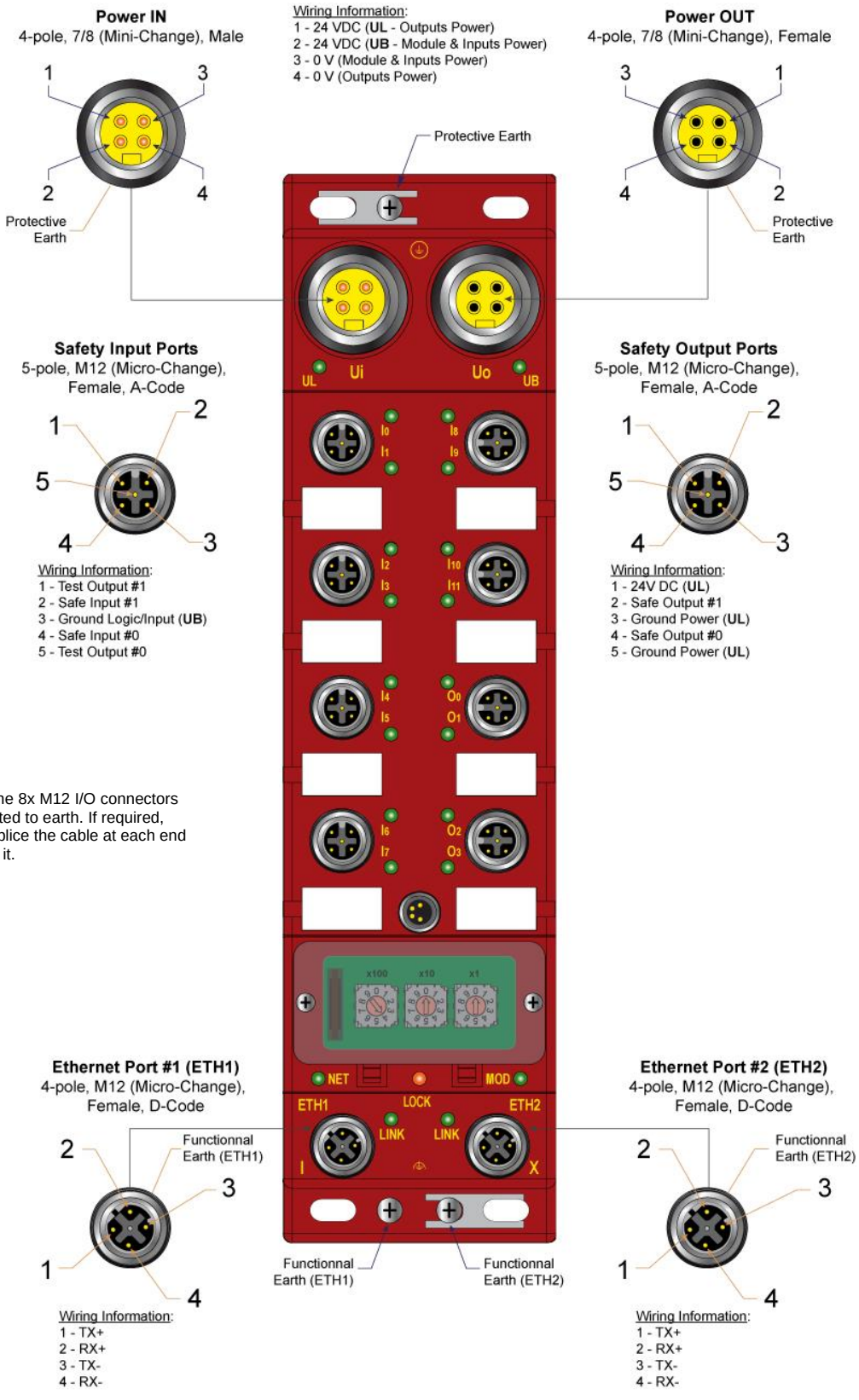
Input Ix/Ix+1 Dual Safe Mode

- 0: Single
- 1: Equivalent
- 2: Complementary

Dual Safe Input Ix / Ix+1 Discrepancy Time (in ms)

A value between 10 and 30000; shall be a multiple of 10.

5.7. Pin assignment



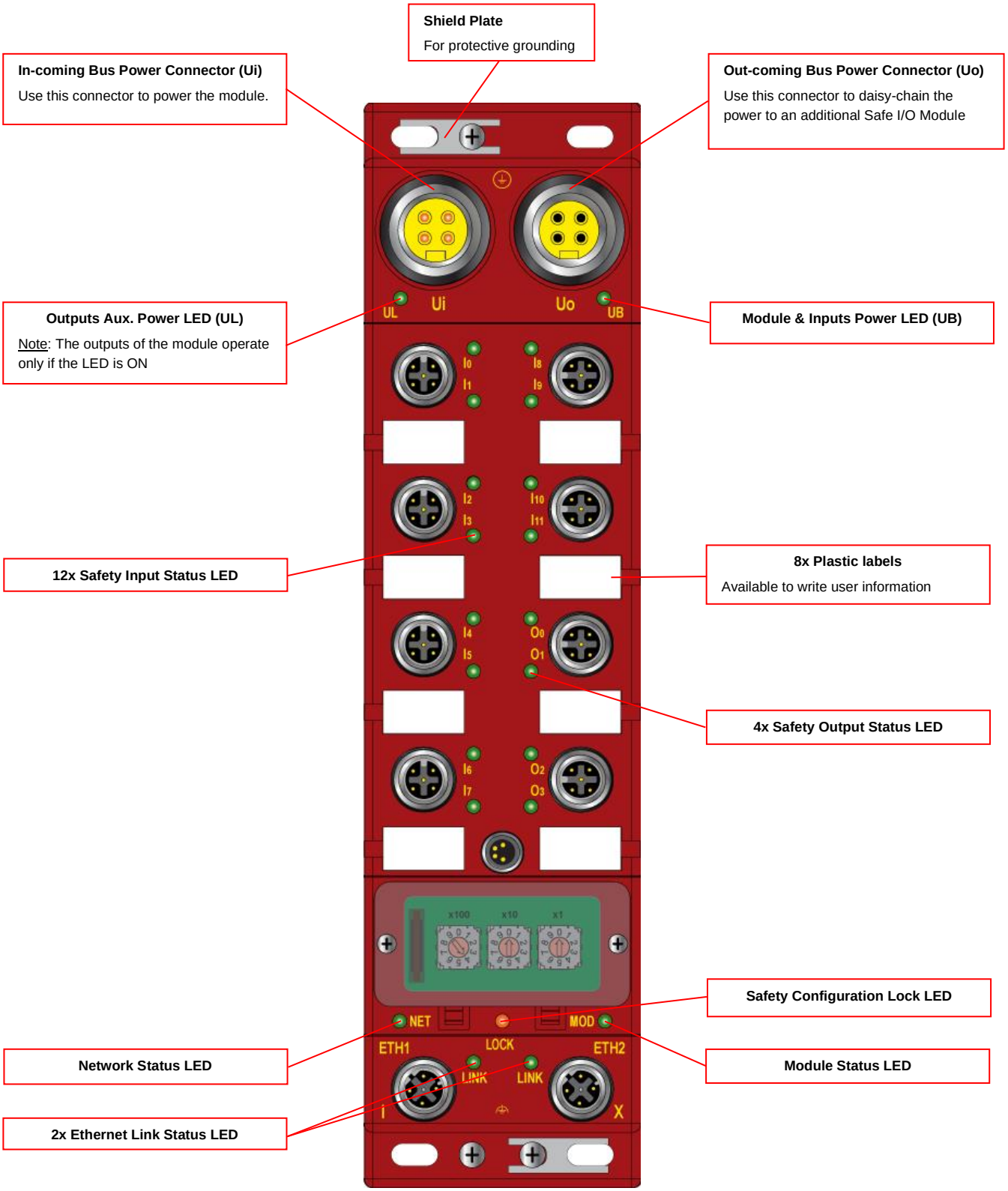
Note!

The shell of the 8x M12 I/O connectors is not connected to earth. If required, You should splice the cable at each end for grounding it.

5.8. LED assignment

LED positions

Warning: LEDs are NOT reliable indicators and cannot be guaranteed to provide accurate information. They should ONLY be used for general diagnostics during commissioning or troubleshooting. Do not attempt to use LEDs as operational indicators.



LED assignment

Module Logic and Input Power Status LED (UB)

LED State	Description
OFF	Module power supply not connected
GREEN	Module power supply is connected and in is the valid range (24 VDC → -20% to +25%)
YELLOW	Module power supply is detected but is outside the valid range (24 VDC → -20% to +25%)

Module Output Auxiliary Power Status LED (UL)

LED State	Description
OFF	Module power supply not connected
GREEN	Module power supply is connected and in is the valid range (24 VDC → -20% to +25%)
YELLOW	Module power supply is detected but is outside the valid range (24 VDC → -20% to +25%)

Safe Input Status LEDs (Ix)

LED State	Safety Input Status	Description
OFF	Good	Input is OFF or module being configured.
YELLOW	Good	Input is ON
RED	Fault	A fault in the input circuit has been detected, or a discrepancy error between the two Inputs of a dual input pair has been detected.
BLINKING RED	Fault	A fault in the Input circuit of the Input partner of a dual Input pair has been detected or unrecoverable detected faults affecting all inputs of the module.

Safe Output status LEDs (Ox)

LED State	Safety Output Status	Description
OFF	Good	Output is OFF, or module being configured
YELLOW	Good	Output is ON
RED	Fault	A fault in the output circuit has been detected, or values received from network for the two outputs used as dual output pair are different.
BLINKING RED	Fault	A fault in the other output circuit has been detected (whatever the output mode configuration: single or dual) or unrecoverable detected faults affecting all outputs of the module.

Link and Network Activity Status LEDs (LINK)

LED State	Speed Negotiate	Description
OFF		No network link.
BLINKING GREEN	100 Mbps	Link is established with no activity.
GREEN		Link is established with activity.
BLINKING YELLOW	10 Mbps	Link is established with no activity.
YELLOW		Link is established with activity.

Module Status LED (MOD)

LED State	Speed Negotiate	Description
OFF	No power	No power applied to the device.
GREEN	Executing	The device is operating in a normal condition.
BLINKING GREEN	Idle state	The device is in the Idle or Standby State.
RED	Critical Fault	The device has an unrecoverable fault, may need replacing.
BLINKING RED	Self-test	The device is in Self-Test or the device needs commissioning due to configuration or TUNID missing, incomplete or incorrect.

Network Status LED (NET)

LED State	Status	Description
OFF	No Power / No IP Address	The module is not online. The module may not be powered, look at Module Status LED (MOD).
FLASHING GREEN	Online / Not Connected	The module is Online but has no connection in the established state (IDLE mode).
GREEN	Link OK / Online / Connected	The module is Online and has connections in the established state (EXECUTING mode).
FLASHING RED	Connection Time-out	One or more I/O connections are in the timed–out state.
RED	Critical link failure	Failed communication device. The module has detected an error that has rendered it incapable of communicating on the network.
FLASHING RED / GREEN	Communication faulted	A specific communication faulted (device uses this indication to allow maintenance personnel commissioning the TUNID in a safety device).

Module Configuration Lock Status LED (LOCK)

LED State	Mode	Description
OFF	either no configuration or either configured by a CIP Safety Originator	The module is not configured or has been configured by a safety originator (FW Open Type 1).
YELLOW	Configuration Locked	Valid configuration received and locked.
FLASHING YELLOW	Configuration not Locked	Valid configuration received and not locked.
RED	Module faults	Bad safety configuration

6. Product installation and wiring

This chapter describes wiring possibilities and associated Safety categories.

6.1. Power supply

The safe I/O module shall be powered with 2 separate power supplies:

- 1x 24 VDC for module logic and safety Inputs power
- 1x 24 VDC for safety Outputs auxiliary power

Warning!

To comply with CE directive, the module shall be powered from a safety extra-low voltage (SELV) or a protected extra-low voltage source.

Note!

The 2 grounds are separated (means isolated from each other).

Warning!

- The maximum total current shall not exceed 8 A for Logic/Input power (UB).
- The maximum total current shall not exceed 8 A for Output power supplies power (UL).
- The current is monitored to be able to go in fail safe state if a current exceeds the maximum.

Warning!

Personnel in charge of safety application must verify that the maximum current consumption is lower than the maximum limit on all the range of temperature supported.

Warning!

An overcurrent protection should be added before the Safe I/O Module to avoid destruction of the module in case of overcurrent situation.

The pin description of the module power connectors is available here.

6.2. Ethernet connection

6.3. Port Identification

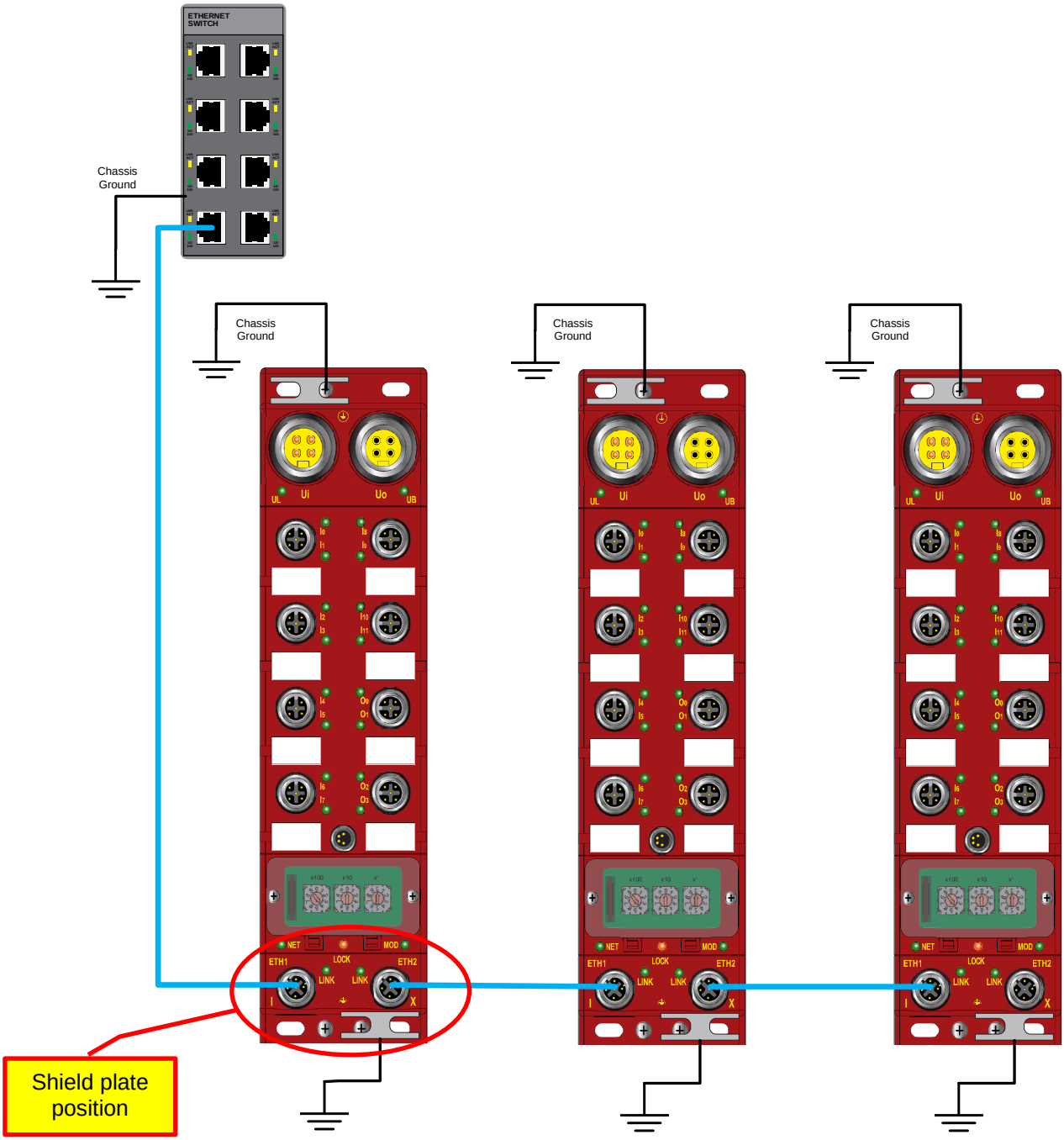
The Safe I/O Module embeds a dual-port Ethernet switch identified by **ETH1** and **ETH2**.

6.4. Wiring

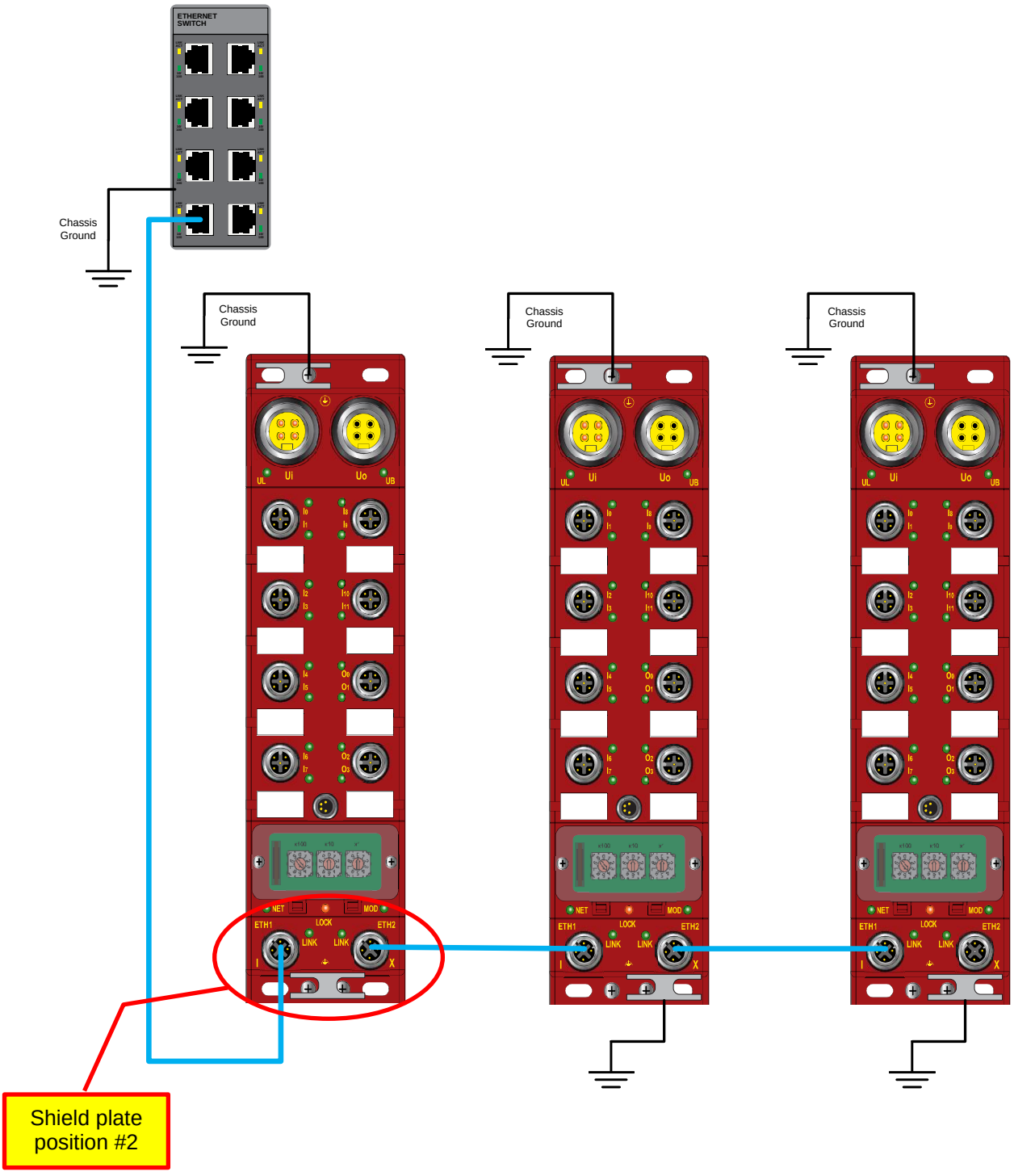
By default, the Safe I/O Module is delivered to be compliant with ODVA recommendations:

- The left M12 connector (ETH1) shield is not connected to functional earth.
- The right M12 connector (ETH2) shield is connected to the functional earth (FE)

This configuration allows the following wiring:



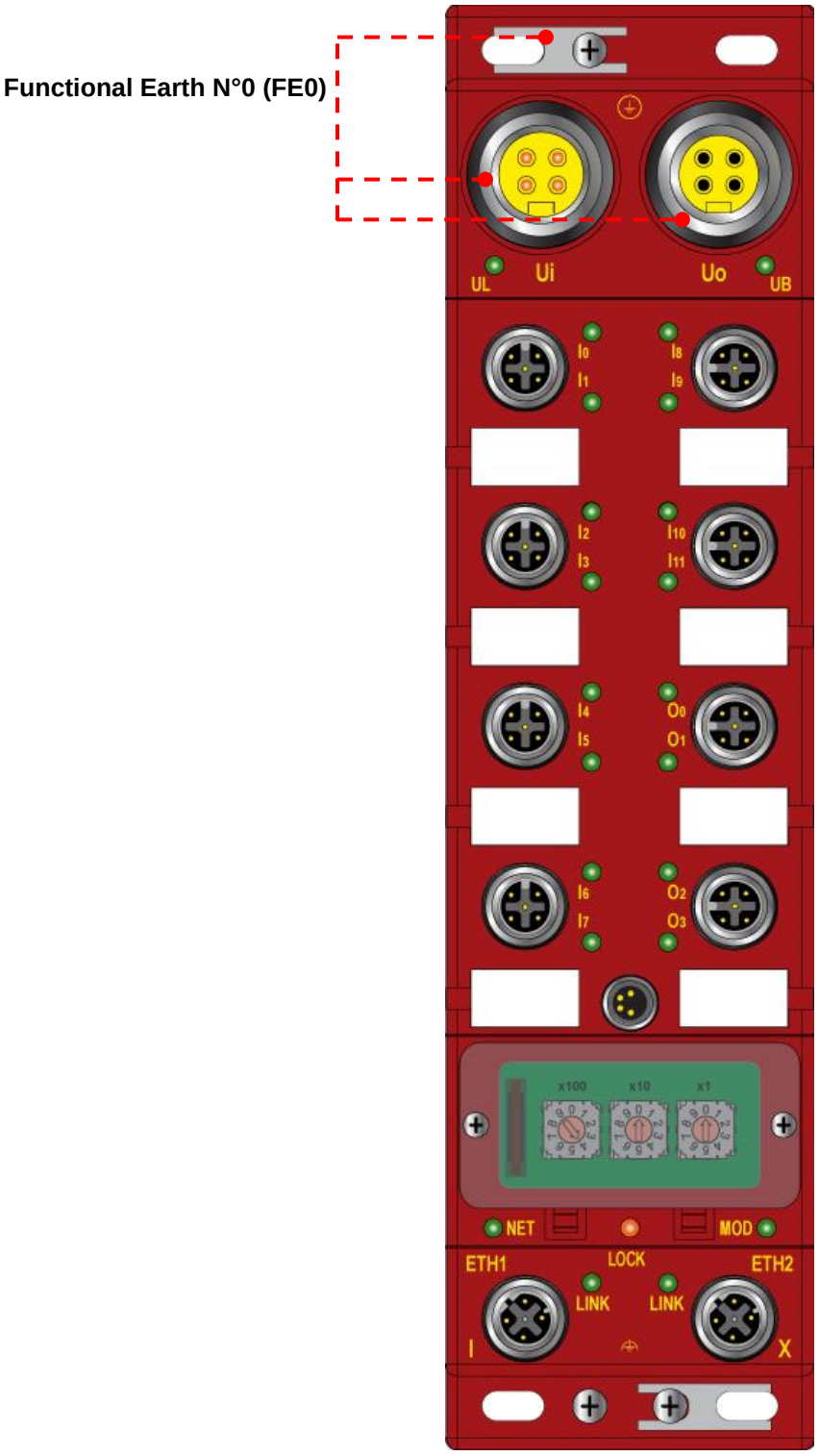
An external shield plate is provided to allow the connection between the two Ethernet shield connector, in order to achieve the following wiring:



6.5. Module grounding

Attention!

For the proper operation of the module, it is recommended that at least one of the earth connections (shown on the schematics below) should be grounded.

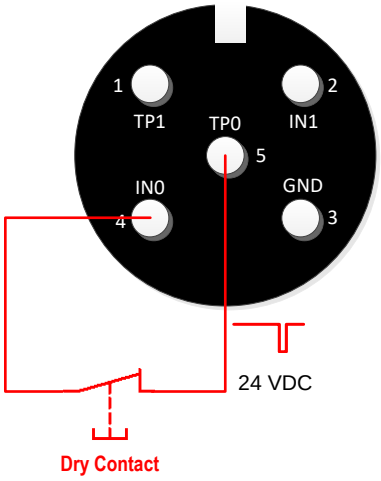
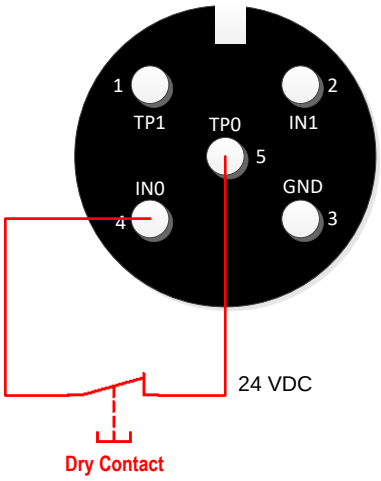


6.6. I/O wiring

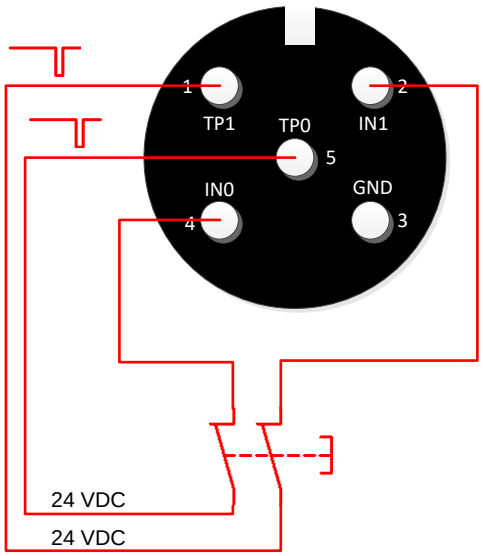
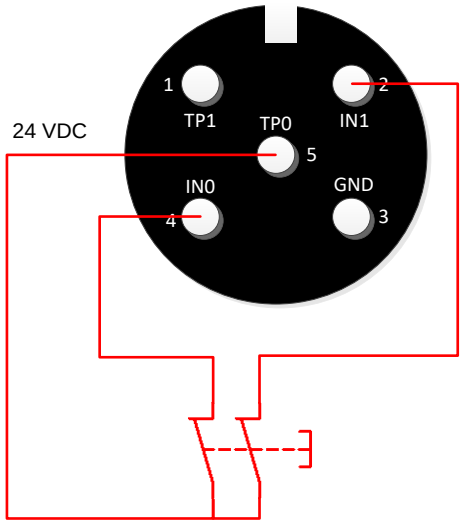
The following table shows different safety I/O wiring with their corresponding safety categories:

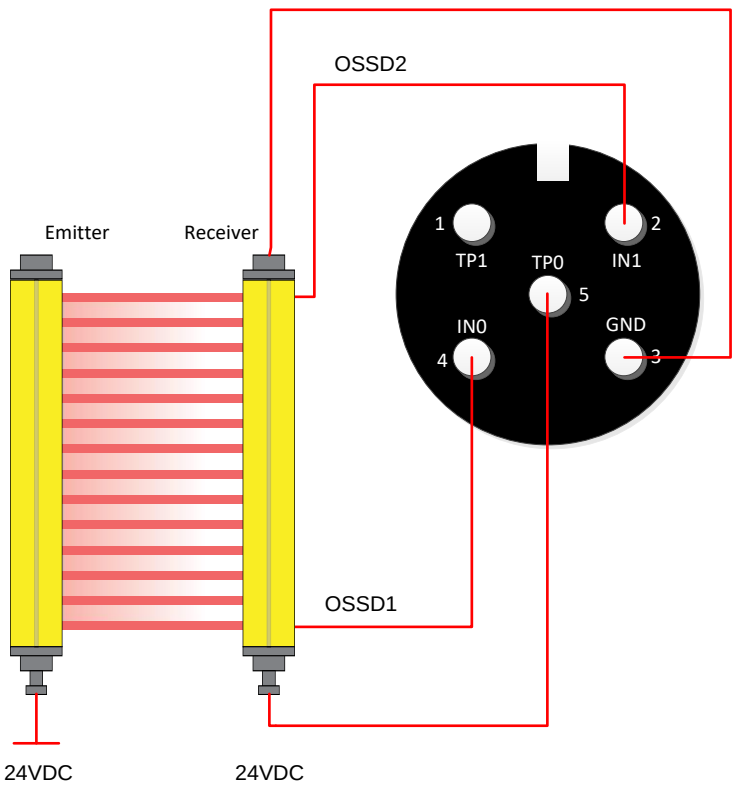
Safety Input wirings

Single Channel

Device	Pulse test from Test Output	M12 Port Wiring	Safety Category
Push Button	Yes TP0 is configured as 24 V power supply with pulse test		2
	No TP0 is configured as 24 V power supply		1

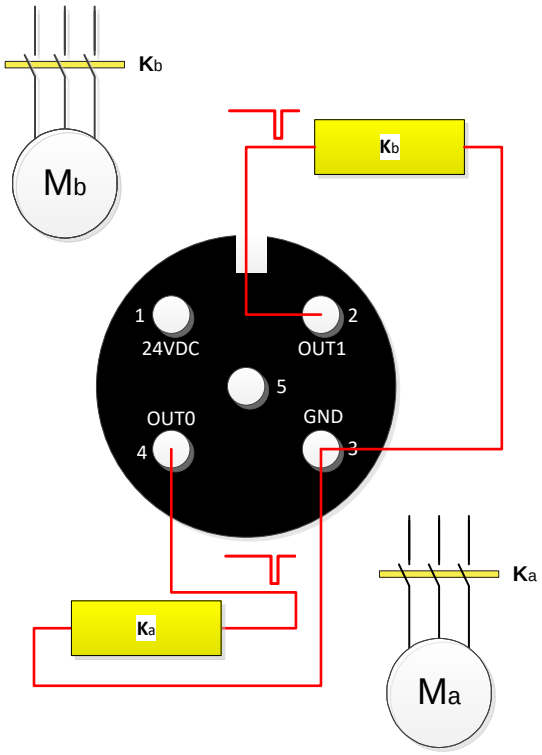
Dual Channel

Device	Pulse test from Test Output	M12 Port Wiring	Safety Category
E-Stop **or** **Door Monitor**	Yes TP0 and TP1 are configured as 24 V power supply with pulse test		4
	No TP0 is configured as 24 V power supply		3

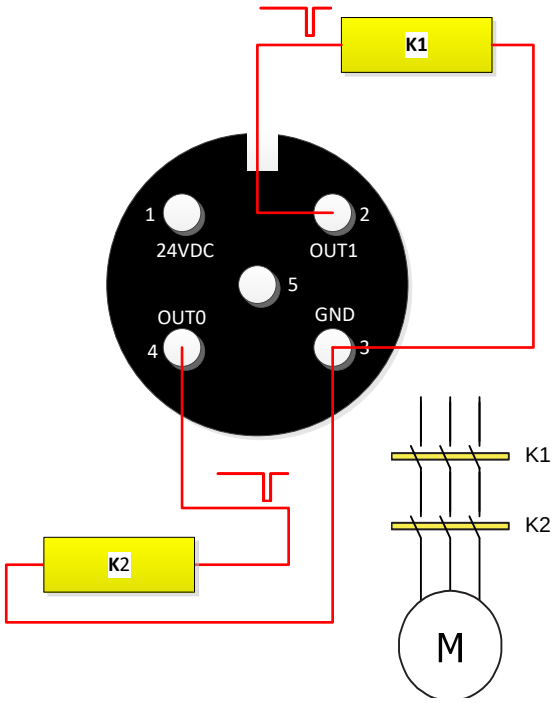
Device	Pulse test	M12 Port Wiring	Safety Category
Light Curtain	No TP0 is configured as 24 V power supply		3 or 4 depending on light curtain

Safety Output wiring

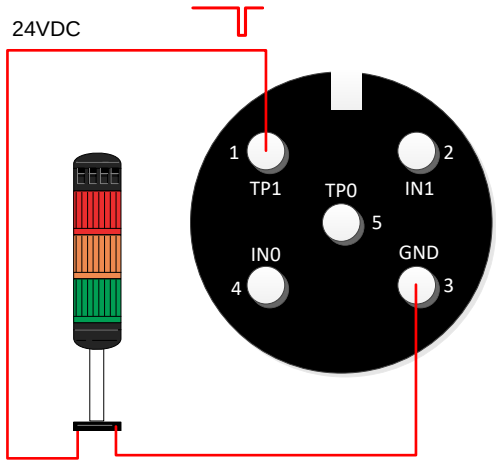
Single Channel

Device	Pulse test	M12 Port Wiring	Safety Category
Relay	**Yes** OUT0 and OUT1 are configured as single channel with pulse test		3

Dual Channel

Device	Pulse test	M12 Port Wiring	Safety Category
Relay	**Yes** OUT0 and OUT1 are configured as dual channel with pulse test		4

Muting Lamp wiring

Device	Pulse test from Test Output	M12 Port Wiring	Safety Category
Muting Lamp	Yes Feature only available when TO_3 or TO_7 are configured as a muting lamp output		ns

Note!
A muting lamp is not a safety device.

7. Product Deployment

This chapter presents an example of how to proceed with the commissioning of the Safe I/O Module based on the Balluff SNCT configuration tool and Rockwell Automation RSLogix™ 5000 software version 20.

7.1. Getting Started

Warning!
Uncontrolled processes can lead to personal injury and material damages.

Warning!
Use only components complying with safety standard corresponding to the required safety level.

It is recommended to consult a certification body regarding the assessment of the entire system.

You will need to define the type of safety components to be used, including the Safe I/O Module.
This will be necessary to calculate the parameters of the whole safety function.

The safety function shall be the result of a risk assessment study.

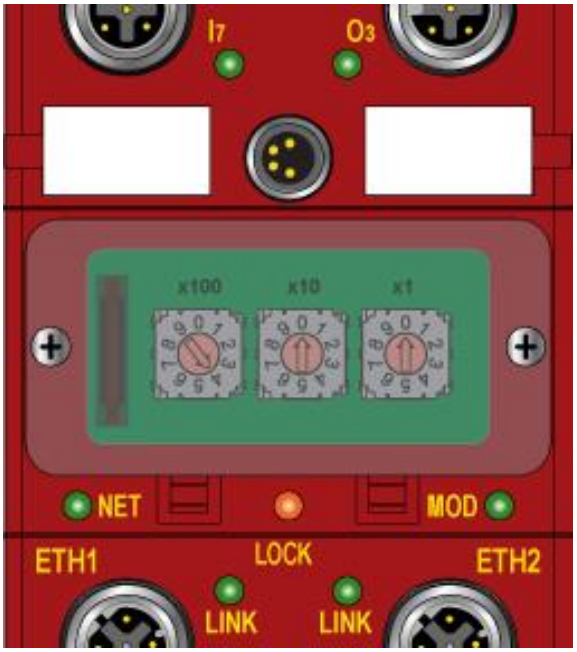
7.2. IP address setting

The Safe I/O Module is configured in DHCP mode by default.

When connecting to a network with a DHCP server, an IP address is automatically assigned to the module.

Setting IP address using the 3 rotaries

You can stop the DHCP procedure (in case of no DHCP server on the network) by selecting the 3 rotaries located in the window area of the module.



Warning!
Use a plastic screwdriver to turn the rotary switches or wear anti-static equipment.

Positions and behavior of 3 rotaries

Mode	x100 rotary	x10 rotary	x1 rotary	Descriptions
Static Address	**x** [0 to 2]	**y** [0 to 9]	**z** [0 to 9]	Overwrite the 4th byte of the IP address stored in Flash Memory. IP Address: **192.168.1.xyz** IP mask: 255.255.255.0 Gateway: **192.168.1.1** (except then the IP address is 192.168.1.1 then Gateway address is 0.0.0.0). **Note!** Addresses (**xyz**) in the range from 1 to 254 can be allocated. Invalid setting (e.g. 000 or 255 or 278…) lead to case (a,b,c of this table). **Note!** The IP mask address and Gateway address are the ones stored in the Flash memory of the module. To change these parameters, send explicit messages command to the module. See section here. **Note!** In this mode, it is not possible to store an IP address using CIP Explicit messages (0xF5 TCP/IP Object).
DHCP Mode	**4**	**u**	**v**	The Safe I/O Module gets its IP address, IP mask address and gateway address according DHCP method. **Note!** This mode requires that a DHCP server equipment is active on the network to deliver IP addresses. **Note!** If **u** = **v** = 0 → DHCP based on MAC address If **uv** = [01 .. 99] → DHCP based on Client ID

				Note! Module sends request indefinitely. **Note!** In this mode, it is not possible to store an IP address using CIP Explicit messages (0xF5 TCP/IP Object).

Update Firmware	**9**	**9**	**9**	The module enters in the update FPGA and firmware mode. **Note!** Please contact Balluff technical support for further information.

Stored Address (all other rotary positions)	**a**	**b**	**c**	The Safe I/O Module gets its IP address, IP mask address and gateway address according information stored in its Flash memory. **Note!** **a,b,c** designate any setting not described as part of this table above (e.g. the following positions: 000, [255 .. 399], [500 .. 998]). **Note!** In this mode, it is possible to store the TCP/IP address information using an EtherNet/IP commissioning tools (using 0xF5 TCP/IP Object). **Note!** If the module has never been commissioned, the Safe I/O Module starts in DCHP mode to obtain its first IP address.

Note!
The rotary switch position is ONLY read at the boot of the Safe I/O Module. Any modification of the position will require a power cycle (ON → OFF → ON) of the module.

Note!

When changing DHCP to Stored mode, all the IP settings are saved in the modules (address, mask, gateway) as it was set during DHCP transaction (given by the DHCP server).

Warning!

After setting the IP address, the window shall be closed and not open anymore during working operation.

Warning!

The module window shall be screwed with a torque of 0.4 Nm to ensure a correct sealing to achieve IP67 rating.

Setting module IP address using EtherNet/IP Explicit Messages

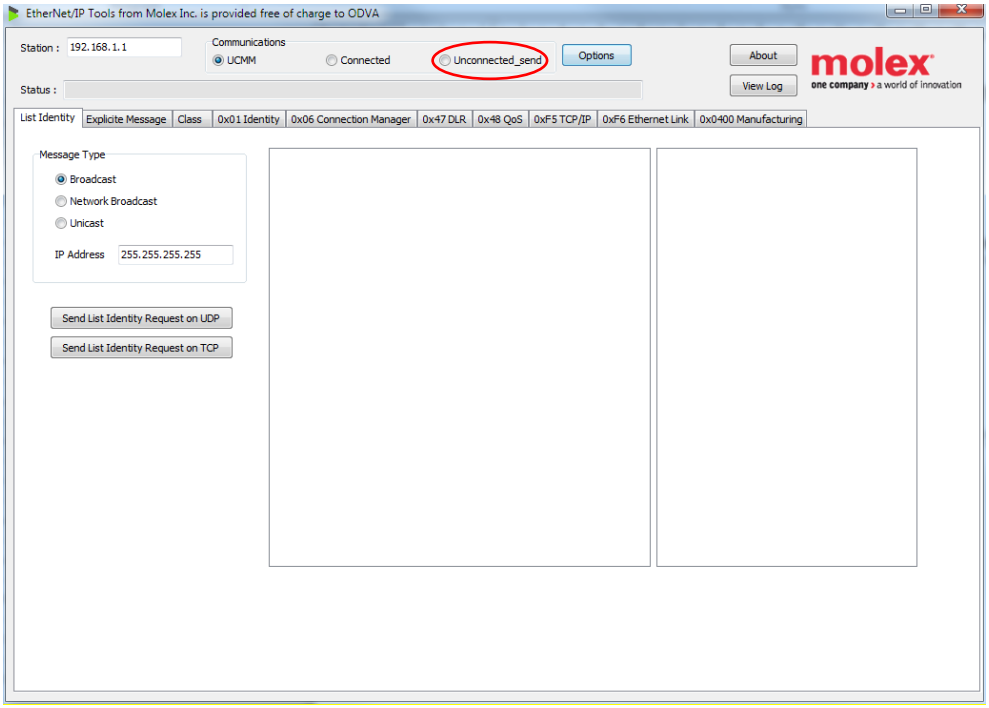
1. *Use of EtherNet/IP Tools*

   To change the IP settings of the module, you have to use a *Ethernet/IP software tool* that manages *Explicit Messaging* requests to access module CIP objects (0xF5 TCP/IP) to set parameters like:
   - Static or dynamic IP addressing
   - IP address
   - Network mask
   - etc.

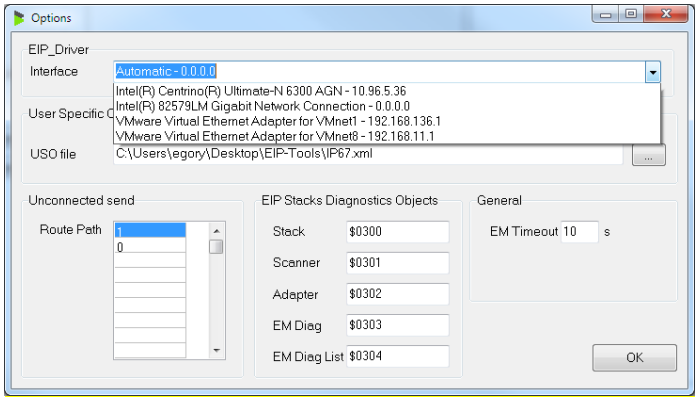
   A *EtherNet/IP software tool* can be download free-of-charge here.

   There is no installation setup. Just copy the files in a new folder and launch *EIP_Tools.exe*.

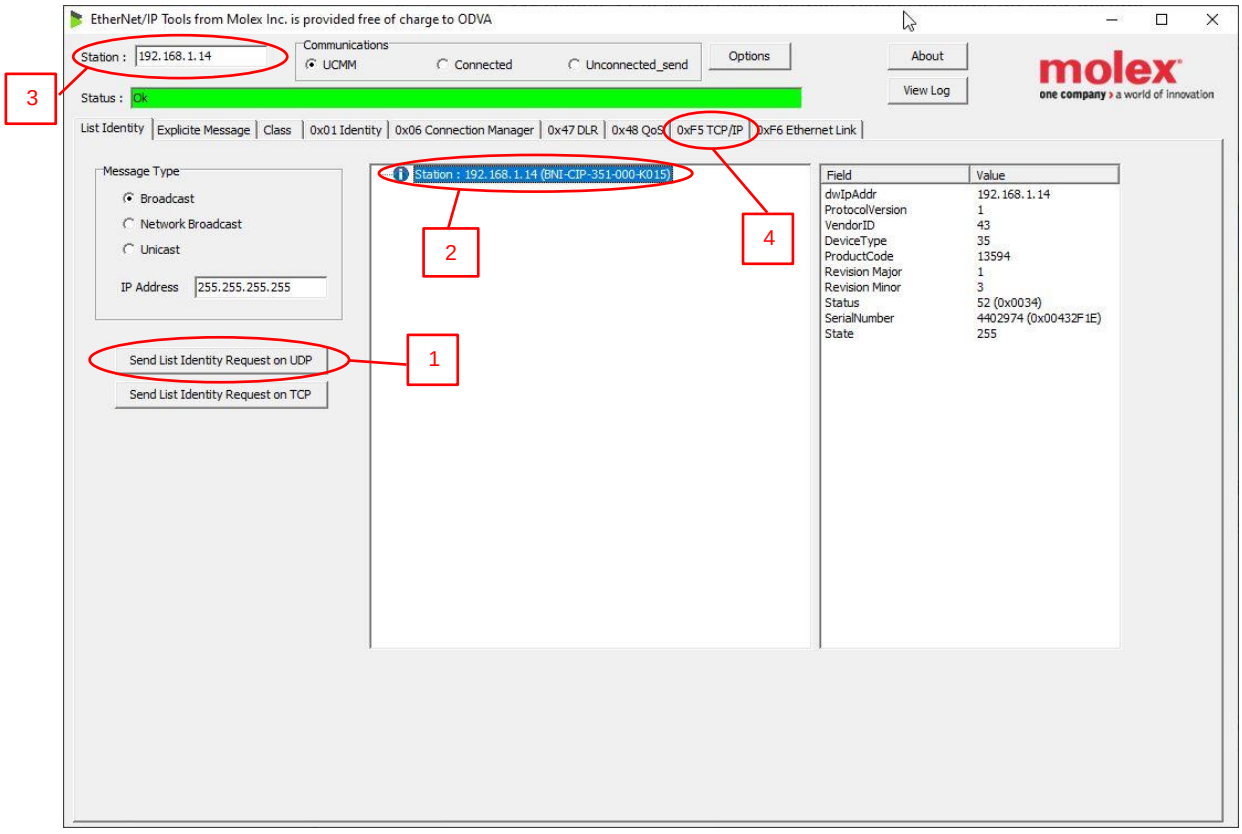
   Click on *Options*



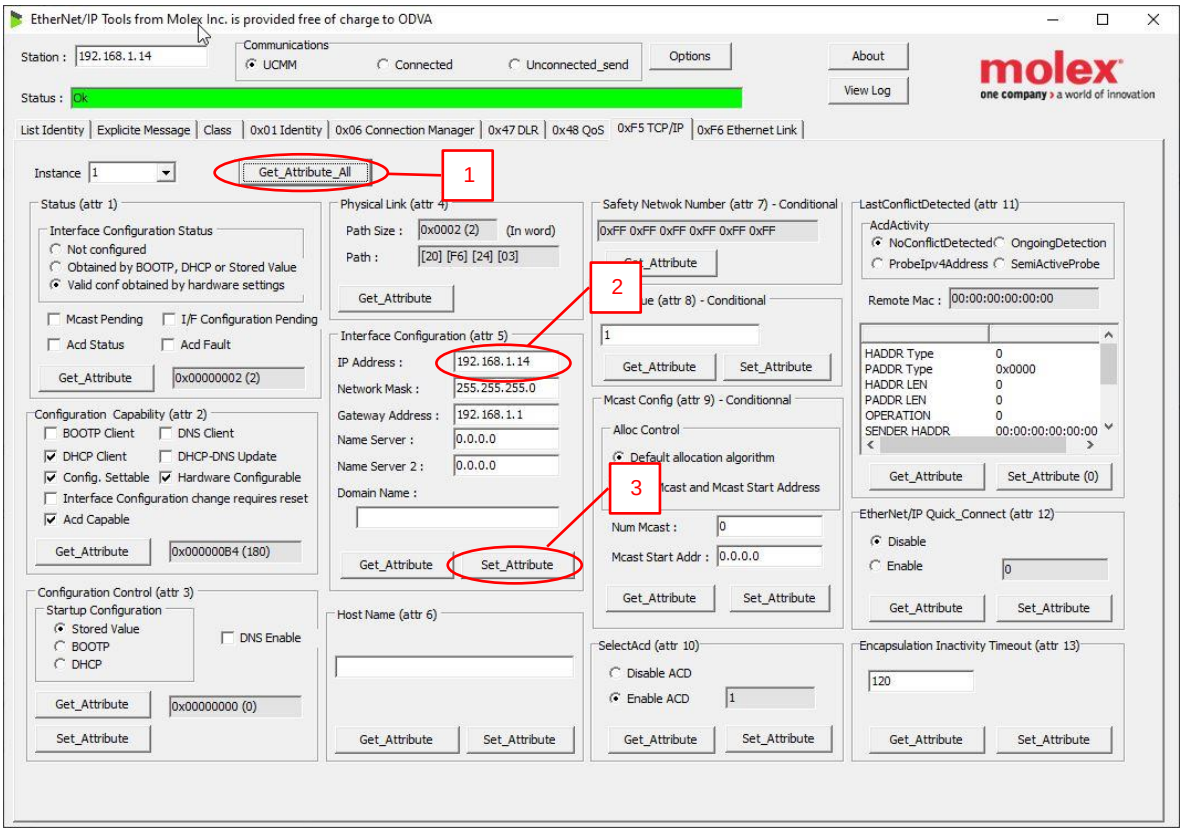
   Select the computer network Ethernet interface and click OK.



Select *Send List Identity Request on UDP* to discover all the EtherNet/IP devices connected to the network. Then select by clicking one EtherNet/IP device in the station list. The device selected should have its IP address set in the *Station:* <IP> area.



Click on *0xF5 TCP/IP* tab and then on *Get_Attribute_All*. The device parameters are displayed.



For example to modify the *IP Address* parameter, write the new IP and select *Set_Attribute* button to send the command.

Note!

The module is now configured with a new IP address stored in its flash memory.

Set the 3 rotary switches located in the window of the module to the position **000**.

Restart the module to apply the new IP address.

7.3. EDS files

The EDS files are simple text files used by network configuration tools to help identifying products and easily commission them on a network.

EDS file list according the associated EtherNet/IP CIP Safety I/O Module version:

Ordering Code #	Type Code #	EDS File Name	Product Code
BNI00HN	BNI CIP-351-000-K015	002B0023351A0103.eds	13594 0x351A

From USB Stick

The Safe I/O Module EDS files are available on the USB stick delivered in the product package and located in the *EDS files* folder.

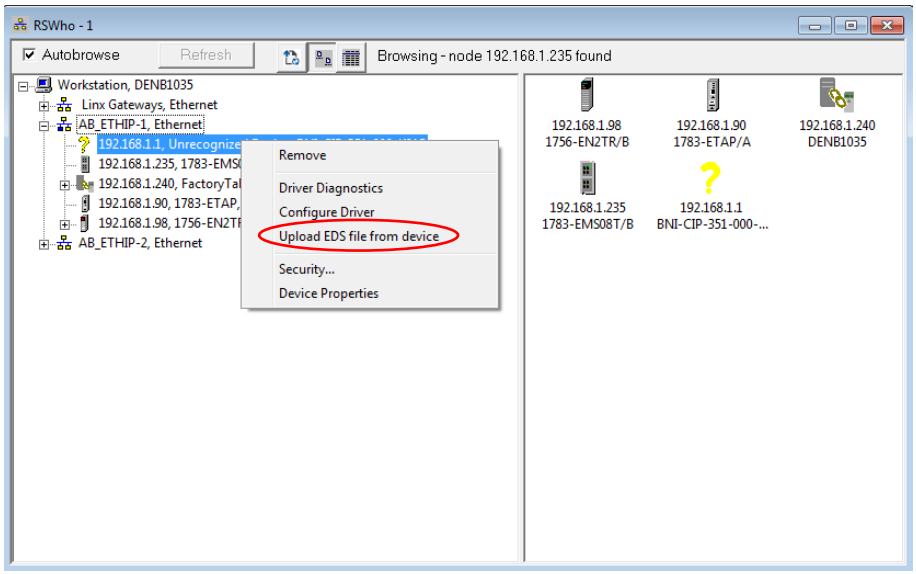
From Balluff website

The EDS files as well as the product documentation can be downloaded from the Balluff website.

https://www.balluff.com

Upload EDS from the module

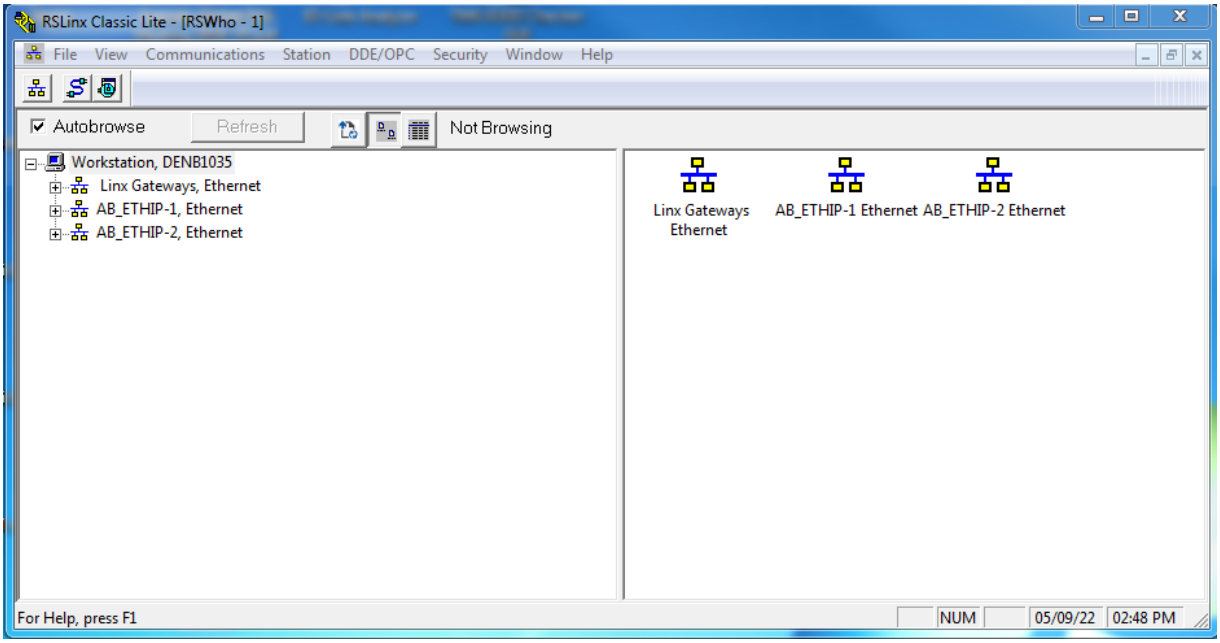
The EDS file can also be uploading from the Safe I/O Module. A tool like Rockwell RSLinx software can be used to call the *Upload EDS from device* service.



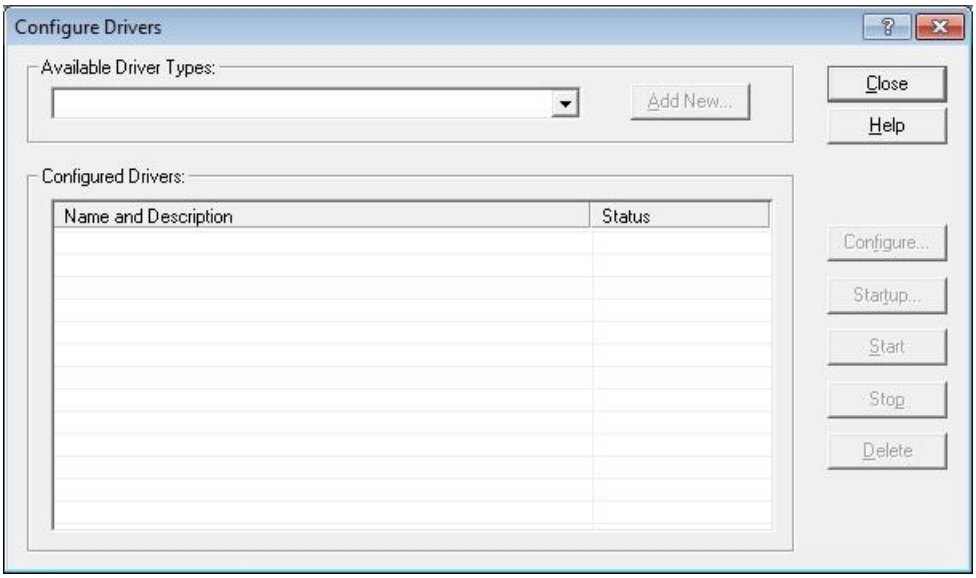
7.4. Import the Safe I/O Module – Safety EDS into Rockwell library

To start the commissioning, the first step is to import the Safe I/O Module – Safety EDS file into Rockwell hardware library by using Rockwell Automation RSLinx™ software.

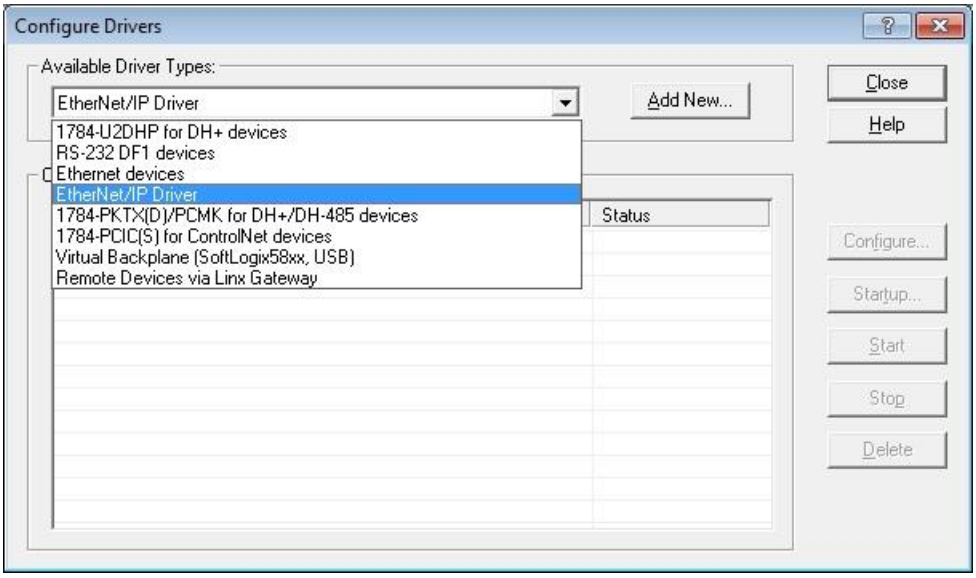
Start Rockwell RSLinx software.



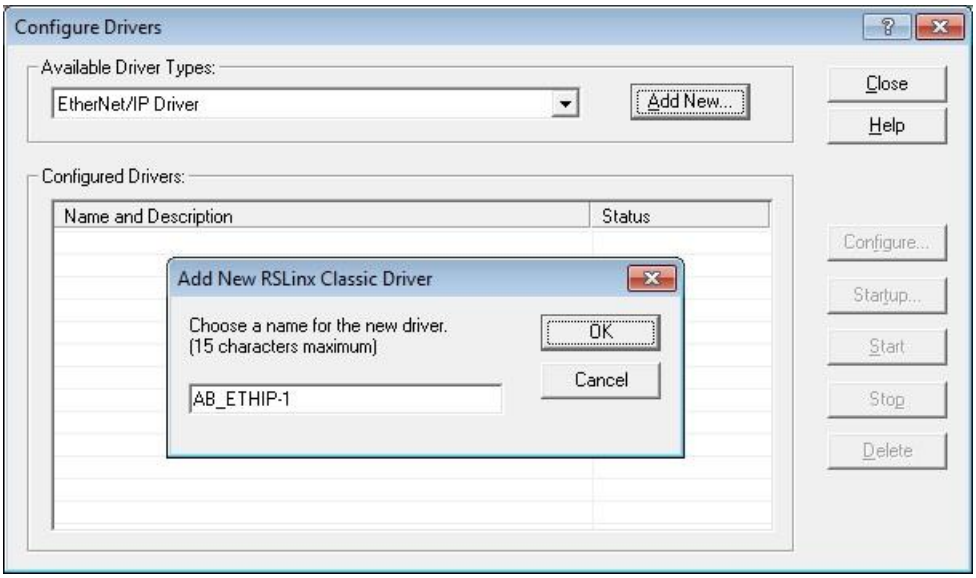
Select Menu *Communications*/*Configure Drivers*…



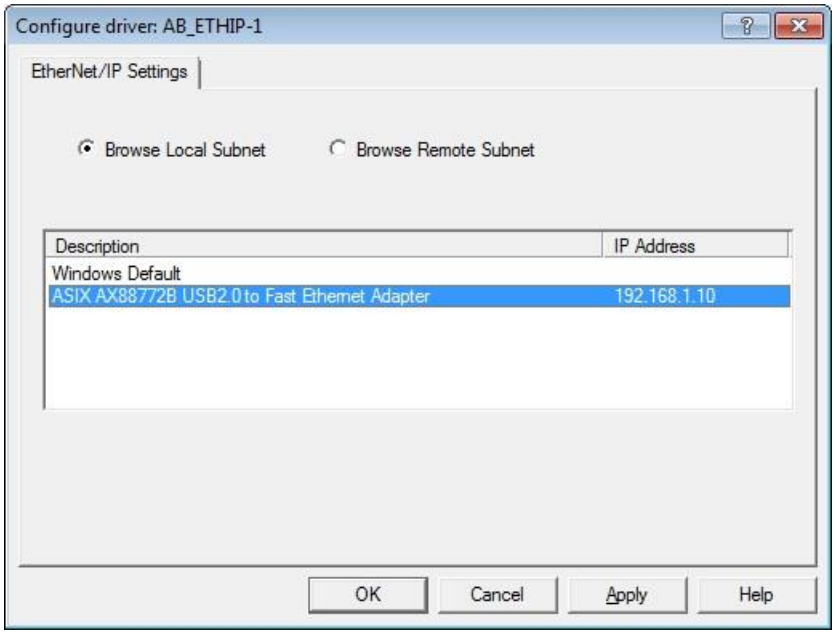
Select *EtherNet/IP Driver*



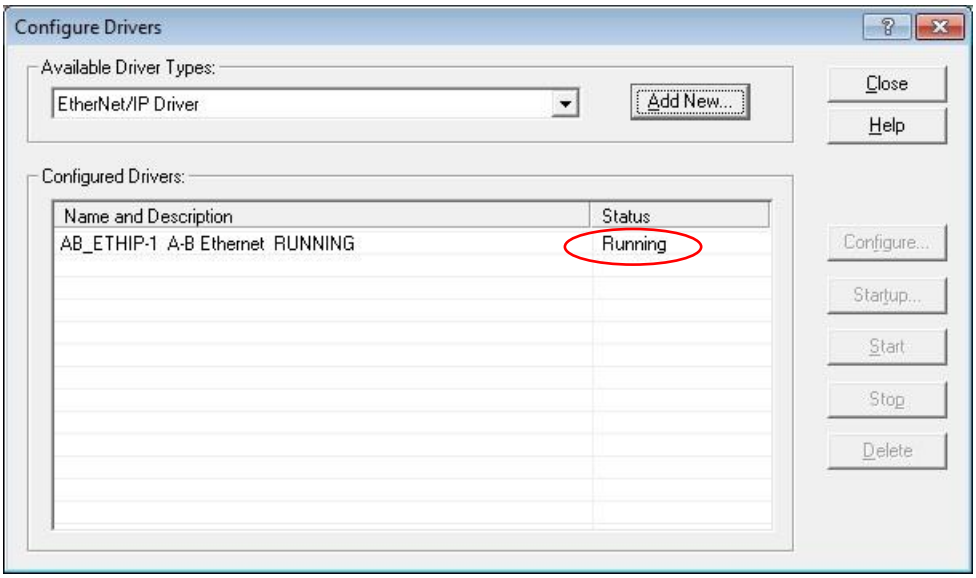
Set a name for the Driver.



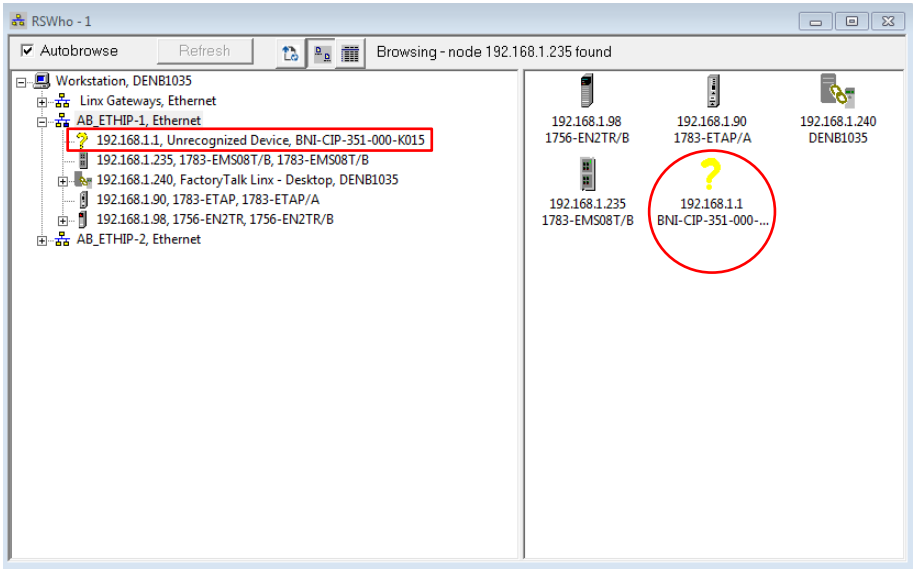
If there is multiple network interfaces in the computer, select the correct one to communicate with the Safe I/O Module.



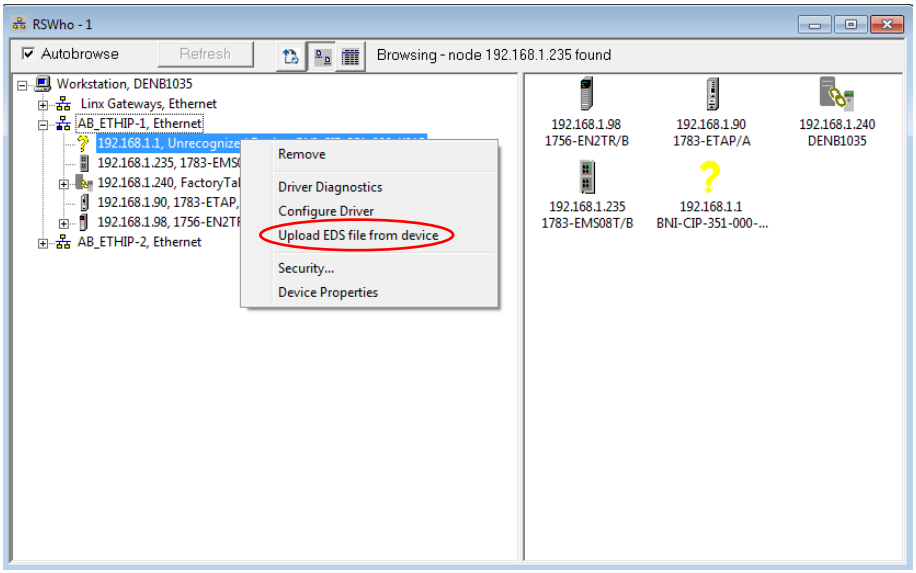
Check that the Driver is running.



RSLinx is now browsing the network to detect the EtherNet/IP devices. At this stage, the Safe I/O Module is detected but appears with an icon representing a question mark because the EDS file is not yet imported.

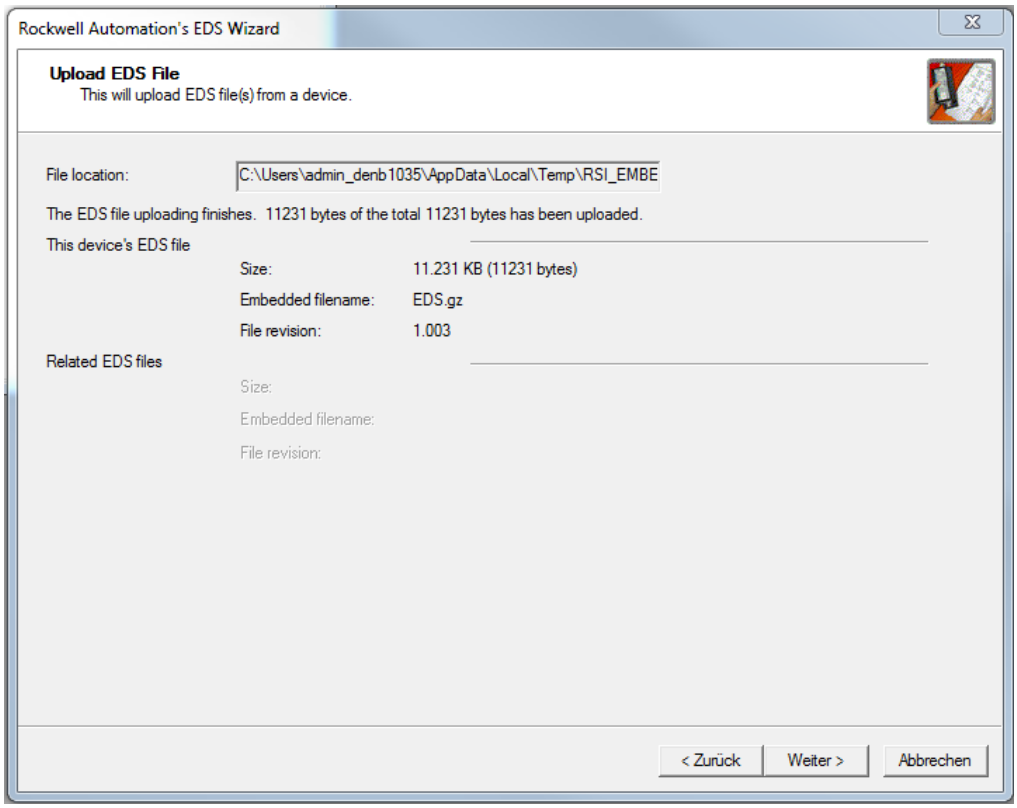


Select the Safe I/O Module, right-click on mouse and select *Upload EDS file from device*

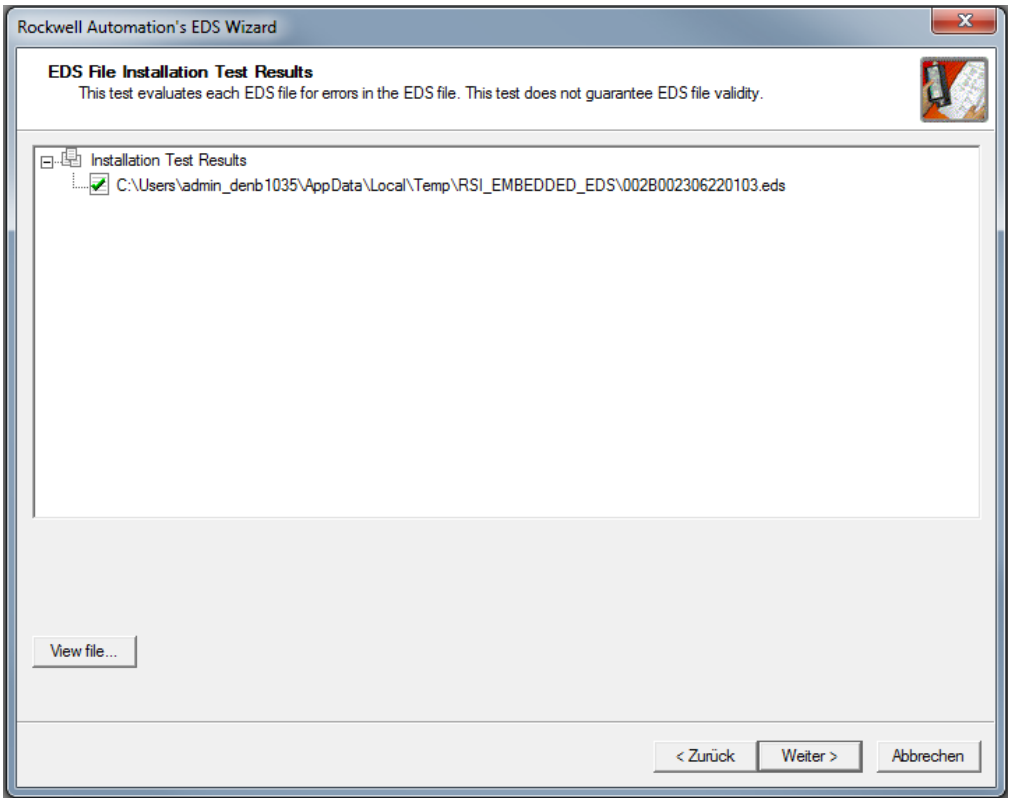


A new tool is launch. Select *Next* button.

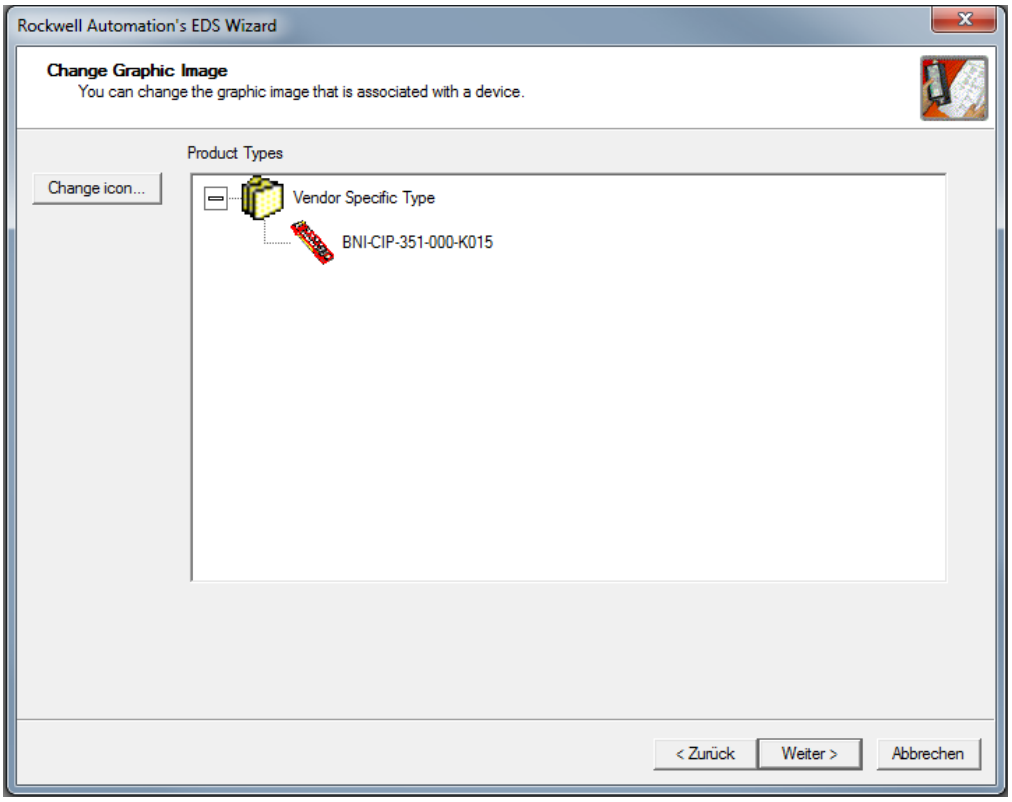
The EDS Wizard is checking the EDS file revision in the device.



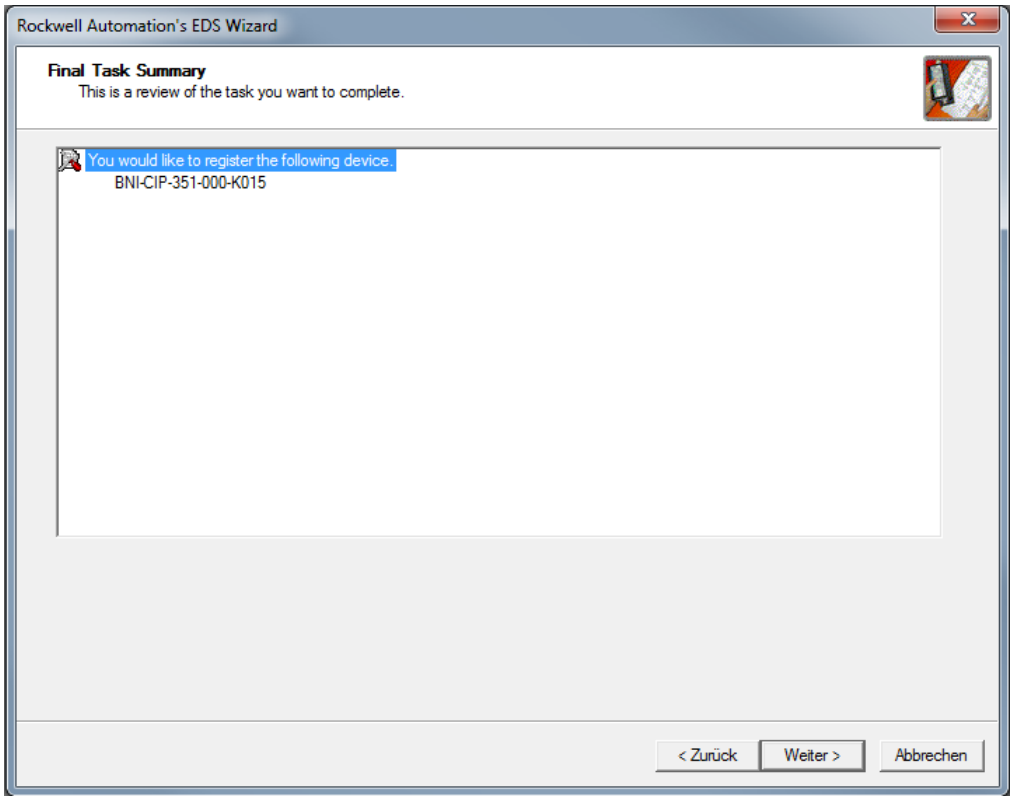
The EDS Wizard is checking integrity of the EDS file.



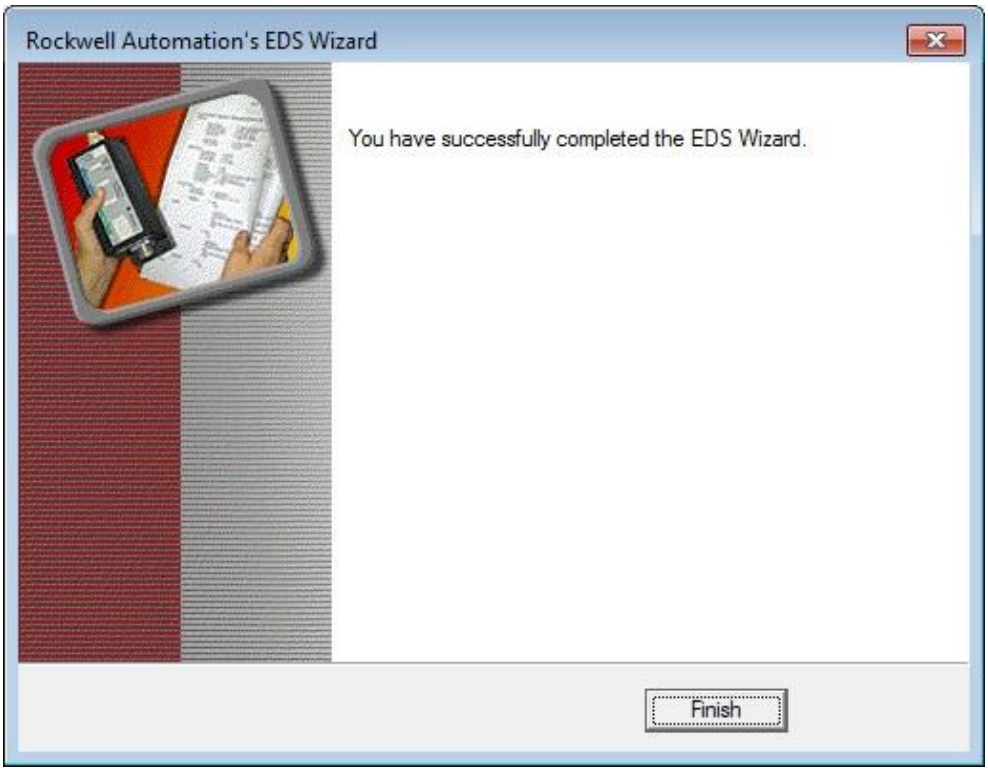
The EDS Wizard is checking integrity of the icon file.



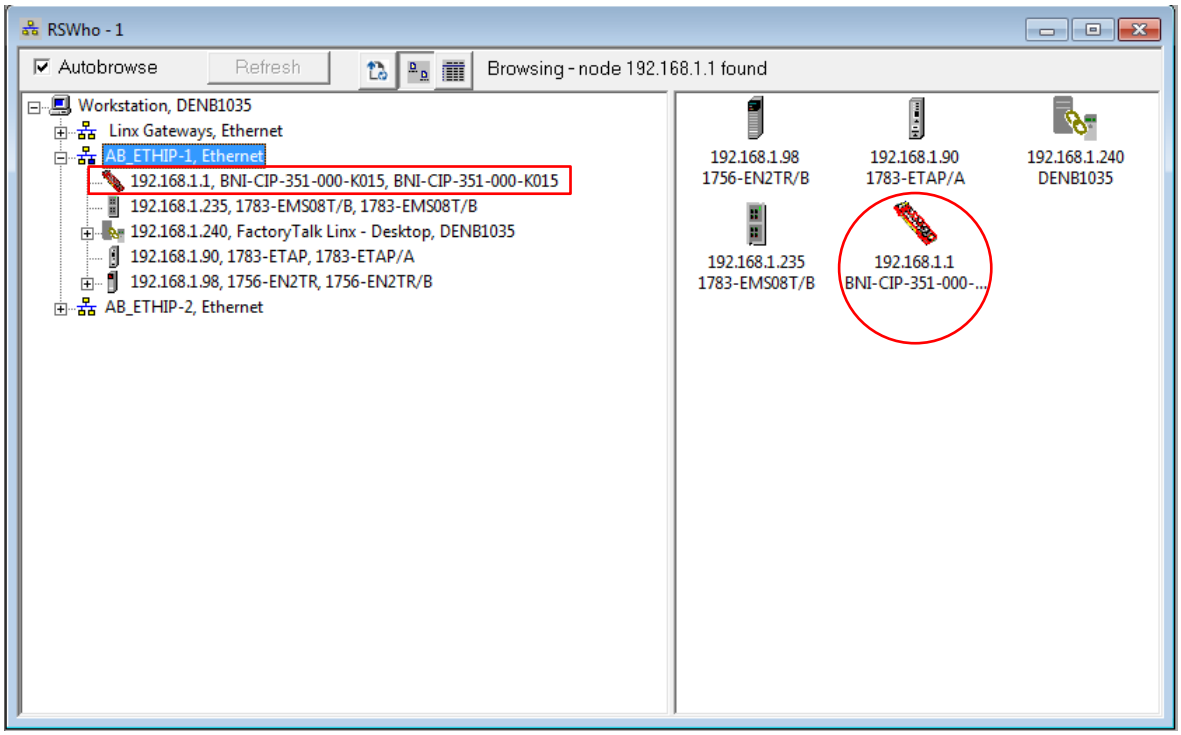
The EDS Wizard is importing the EDS file and icon in the Rockwell hardware library.



The EDS Wizard has successfully imported the files.



RSLinx has registered correctly the EDS file and displays now the correct icon of the Safe I/O Module.

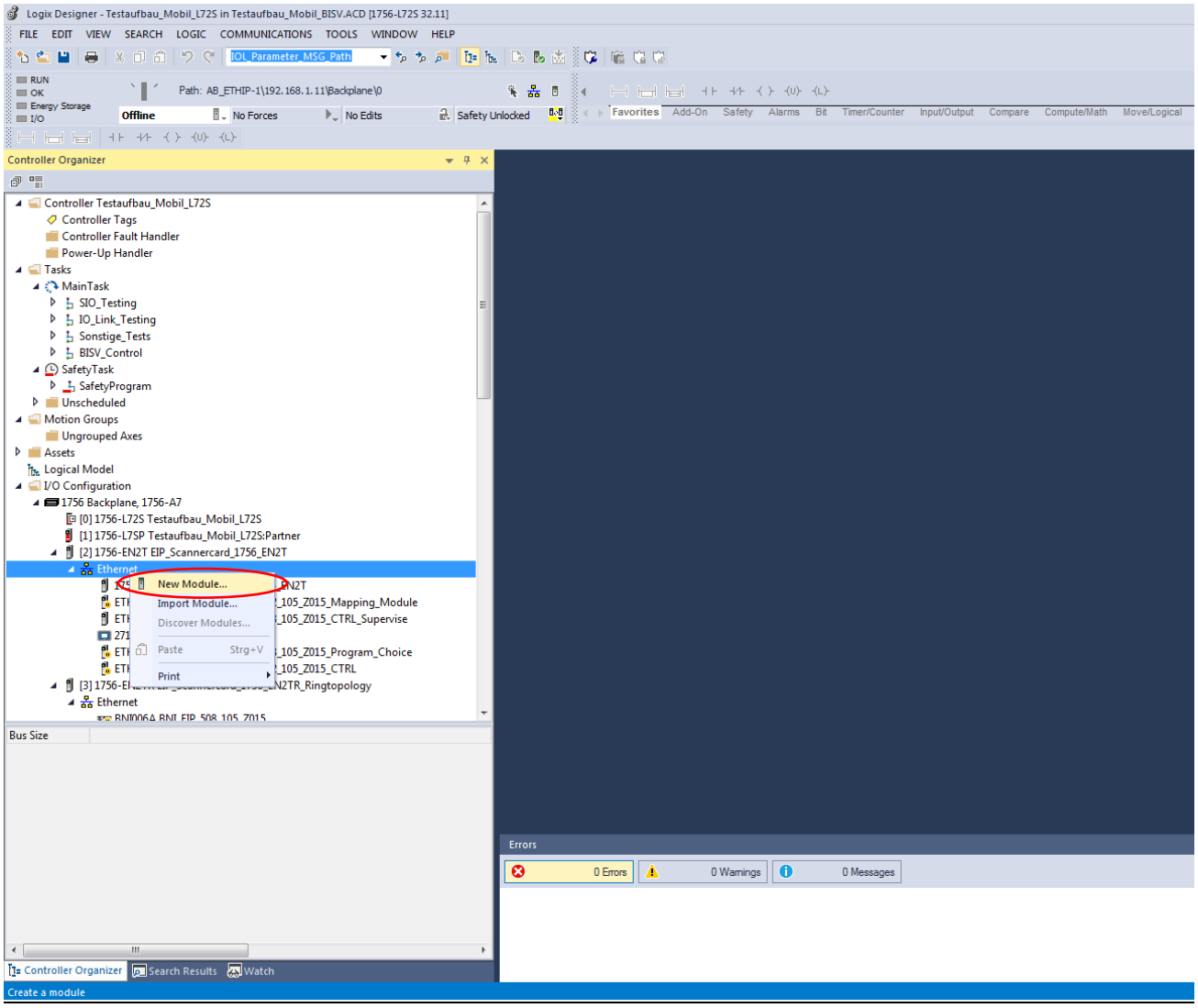


7.5. Configure Safe I/O Module into Rockwell RSLogix 5000 project

Start RSLogix5000 software.

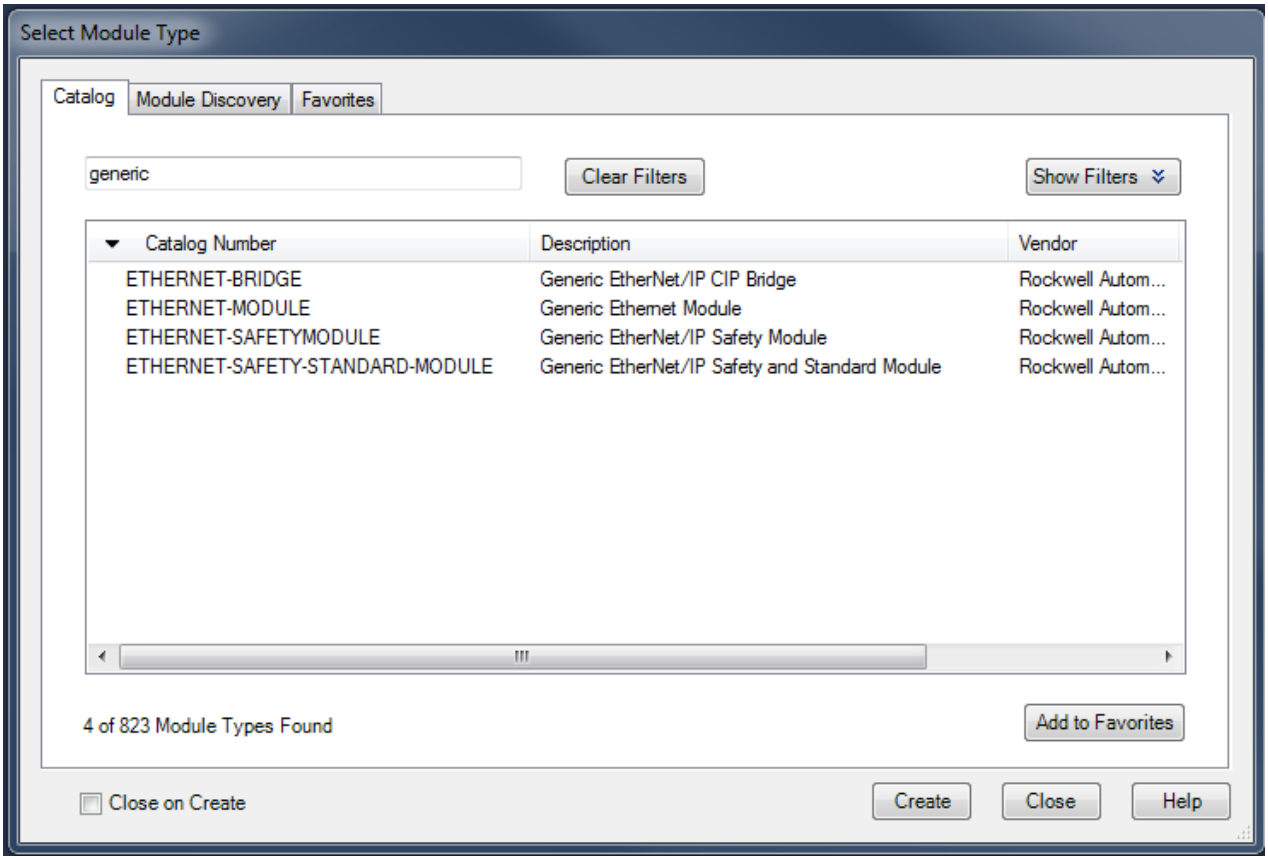
Select the *Ethernet* node of the EtherNet/IP connectivity channel.

Right-click on mouse and select *New Module…*

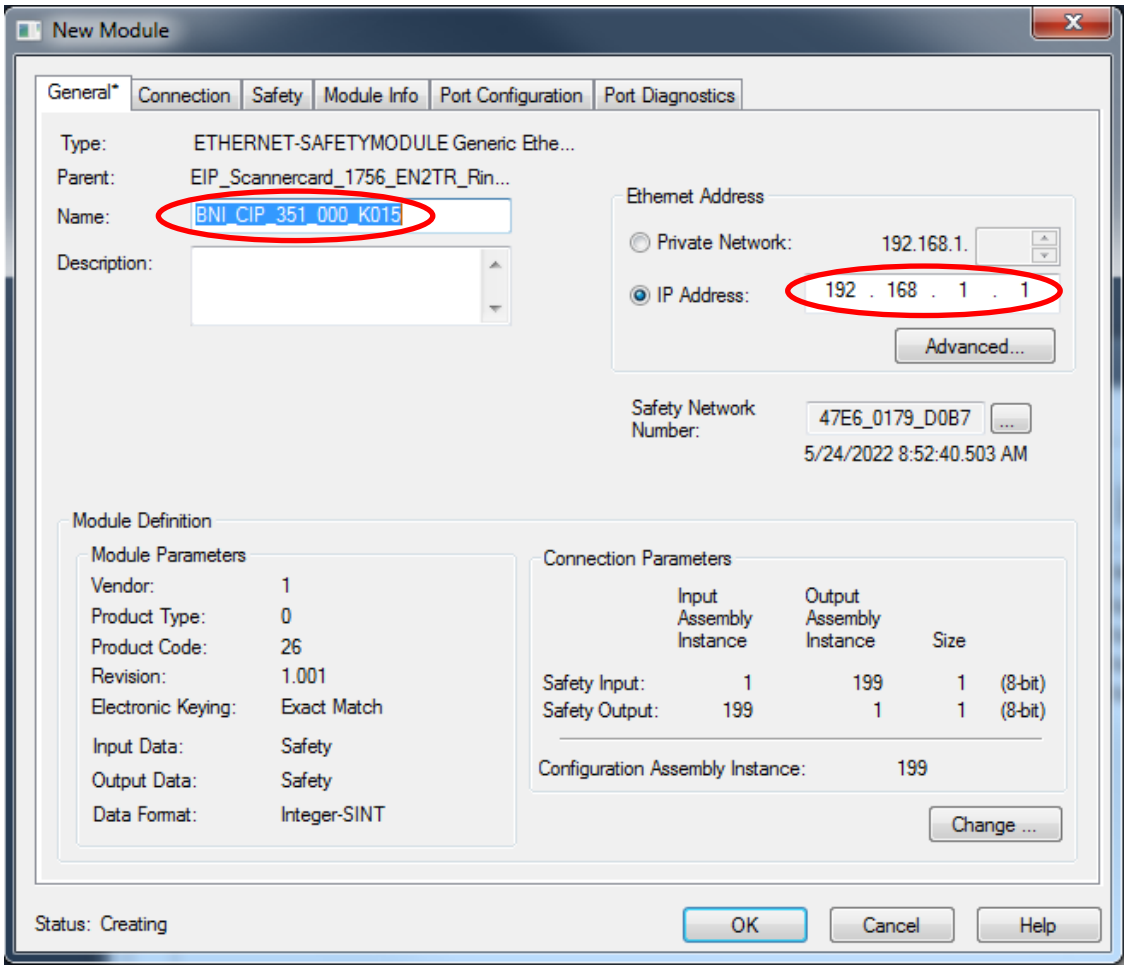


Look and select in the Catalog *Generic EtherNet/IP Safety Module*.

Select the module, right-click on mouse and select *Create*



Give a Name and set the module IP address that has been discovered by RSLinx.



RSLogix software creates automatically a Safety Network Number (also called SNN). The Safety Network Number is a unique identifier of 48-bit number to prevent the acceptance of connection requests that have been misdirected. This is to ensure that every module on the safety network can be uniquely identified.

Warning!

Safety controllers (Originator) that have an “Automatic” SNN setting feature should only use that feature when the safety system is not being relied upon

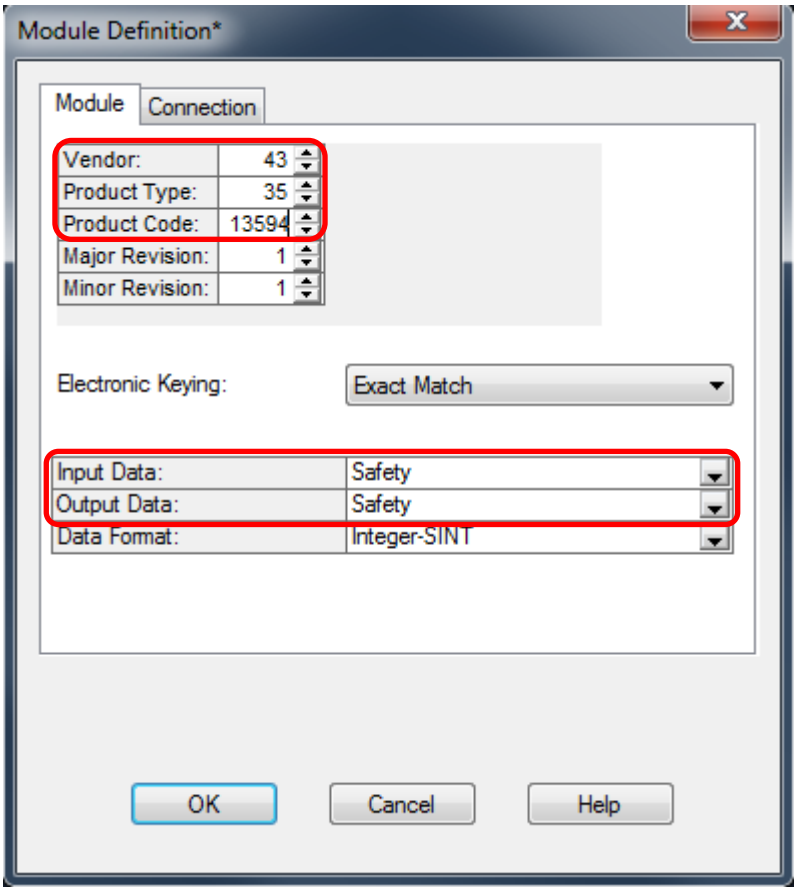
In the *Connection Parameters* area, select *Change*

In the Module tab, change the following parameters:

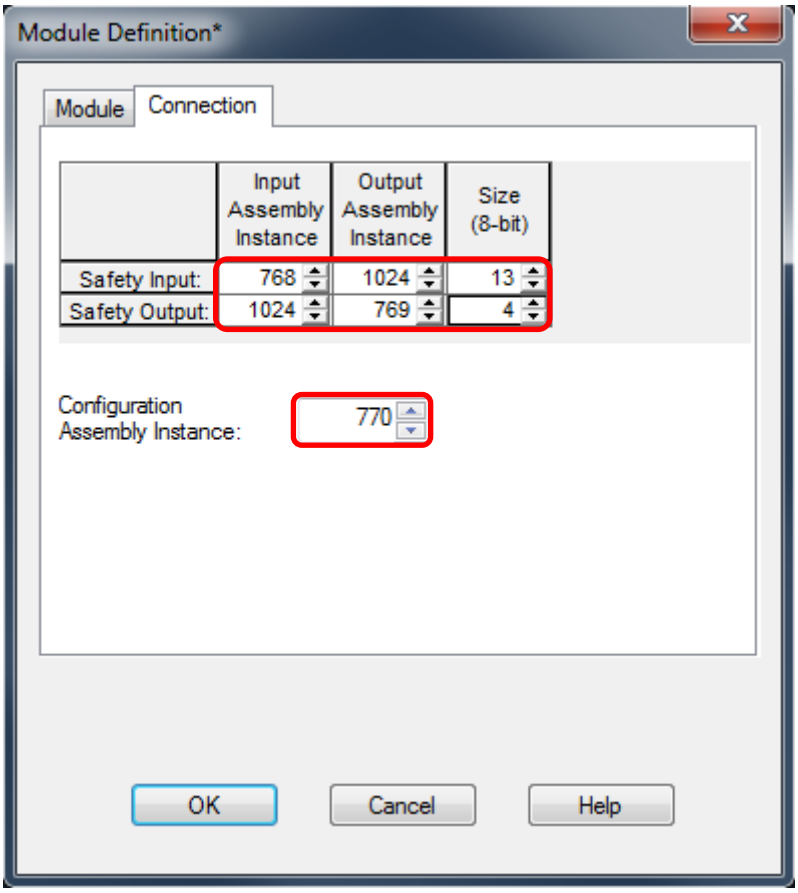
- Vendor: **43** (Balluff)
- Product Type: **35**
- Product Code: **13594**

7.6. Safety I/O assemblies

The Input Data and Output Data shall be set to *Safety*.



Change the Connection Assembly settings.

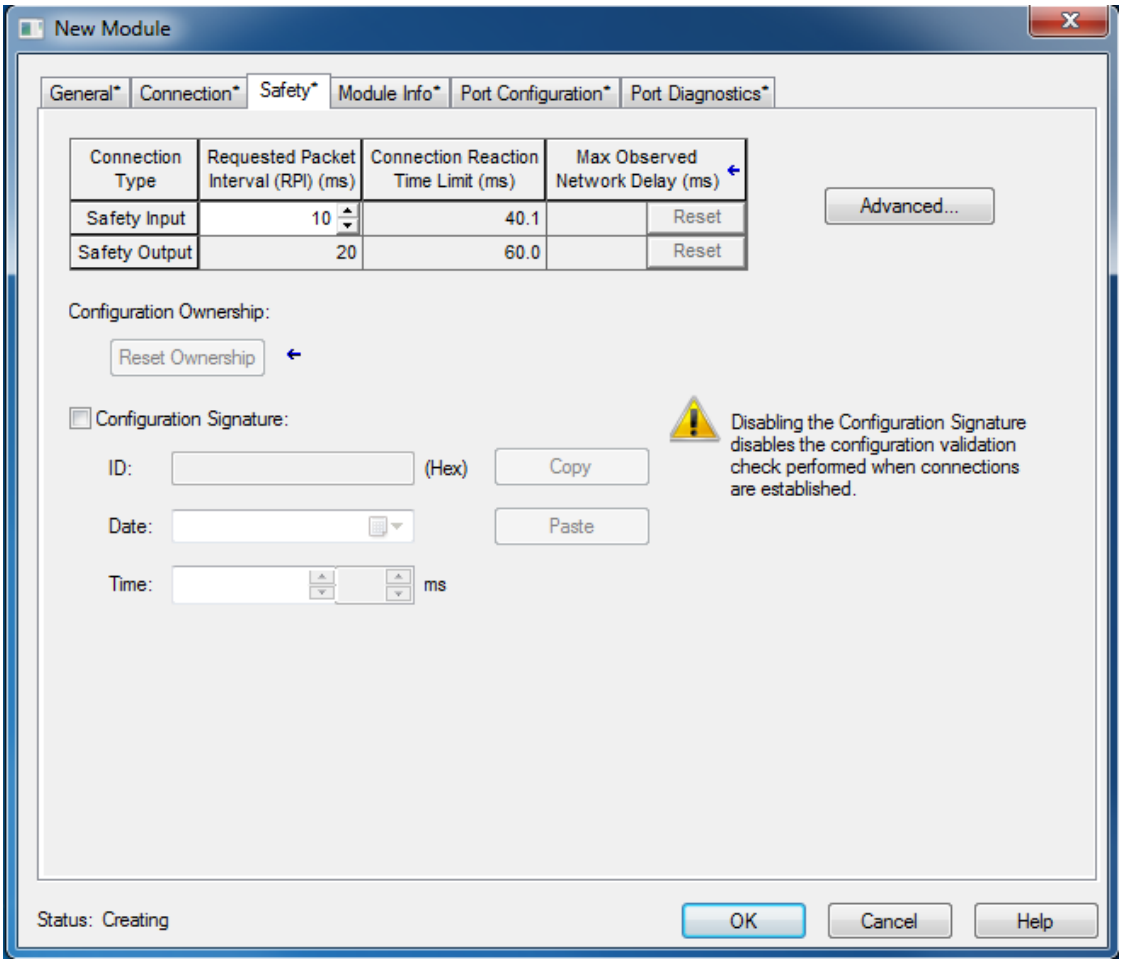


In our example, we are going to connect the Safety Input and Safety Outputs Vendor Specific assemblies.

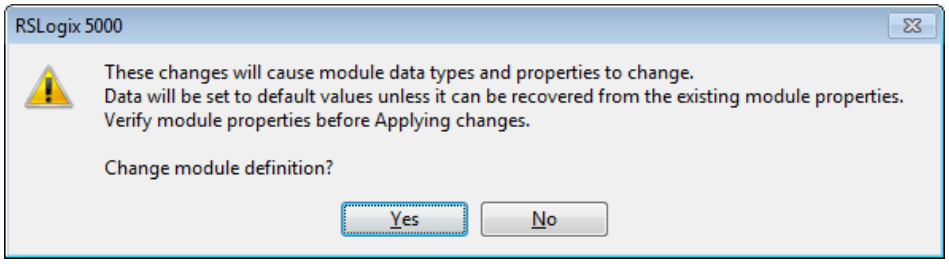
Note!
The Safe I/O Module supports different kind of safety I/O connections according the number and type of process data the application needs to access.

List of safety I/O connections are available in I/O data mapping.

Disable the *Configuration Signature* to apply the change.



Select *Yes* to apply the new parameters.



7.7. Configure Safe I/O Module in Balluff SNCT

Balluff Safety Network Configuration Tool (SNCT) is free software delivered on the USB stick included in the product package or can be downloaded from the Balluff website.

https://www.balluff.com

Warning!

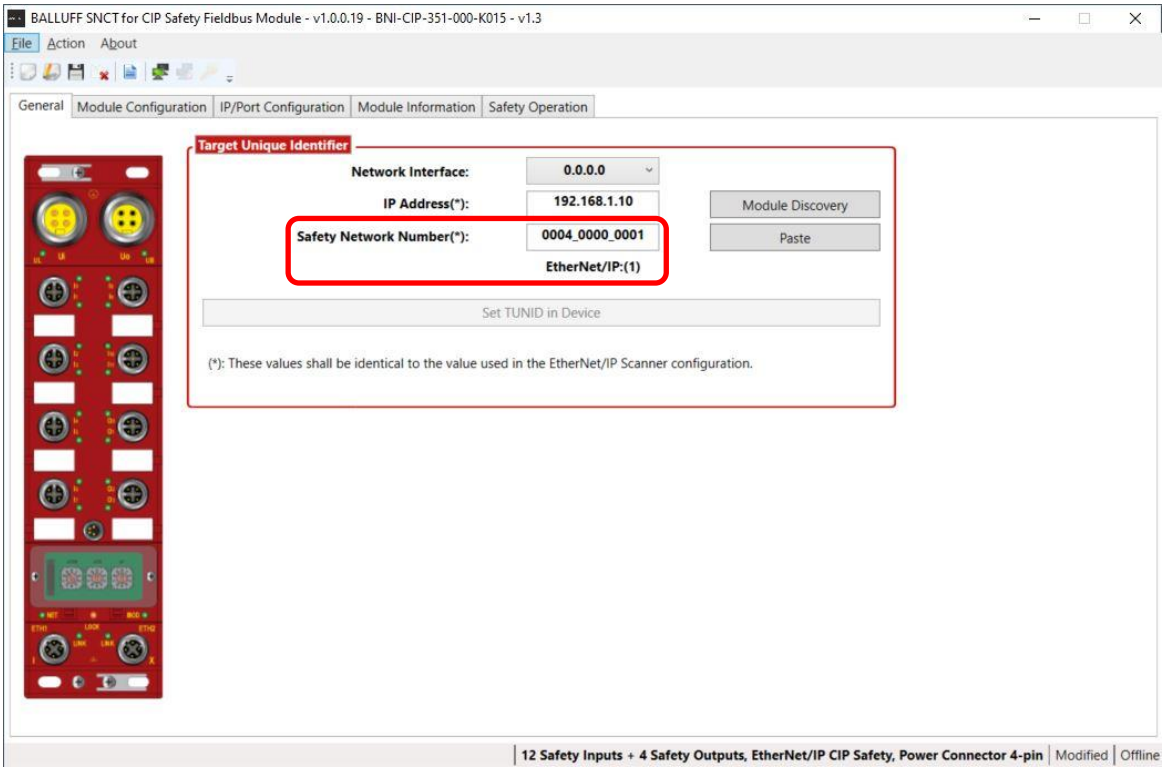
To browse and download software from the Balluff website, you must accept the use of cookies in the Internet explorer.

Start Balluff SNCT software.

And select File/New

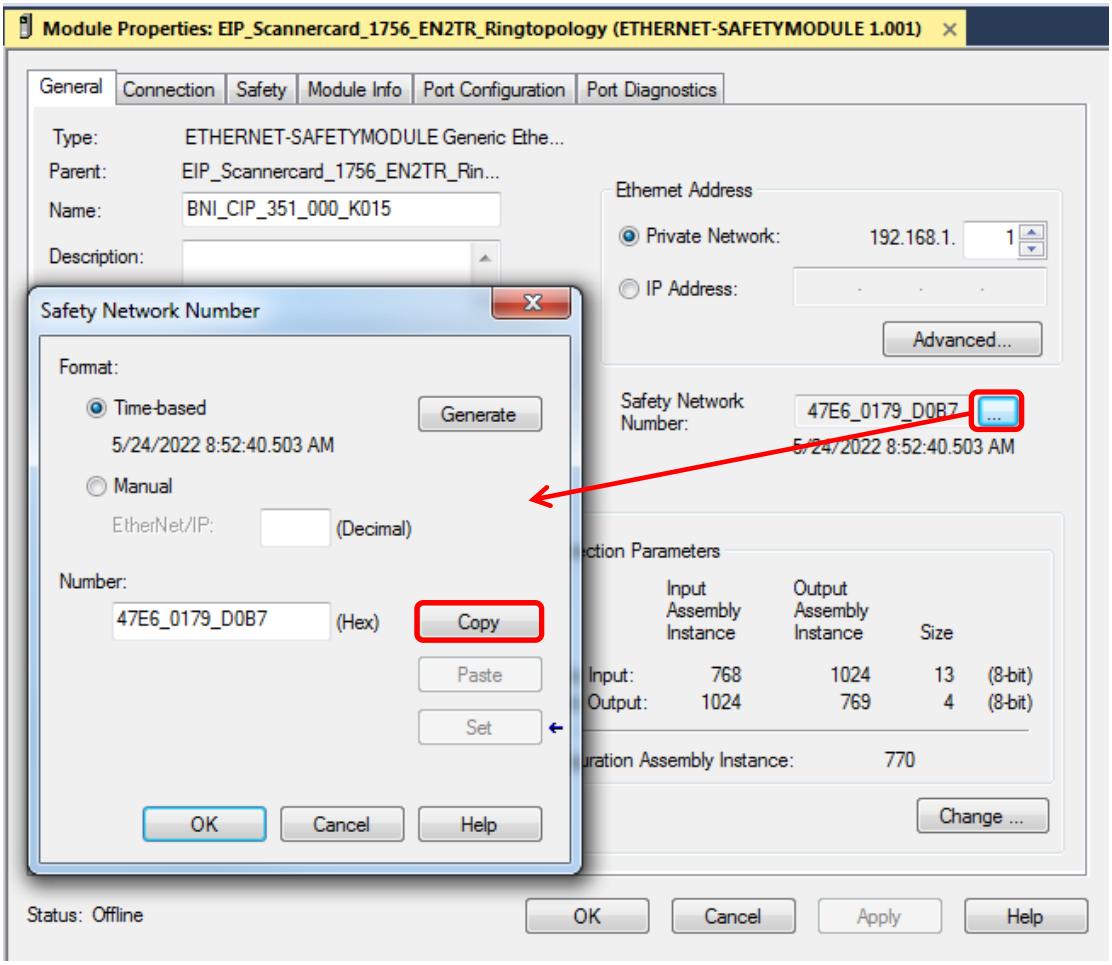
Select the Safe I/O Module and its version.

The next step is to setup the Safety Network Number.

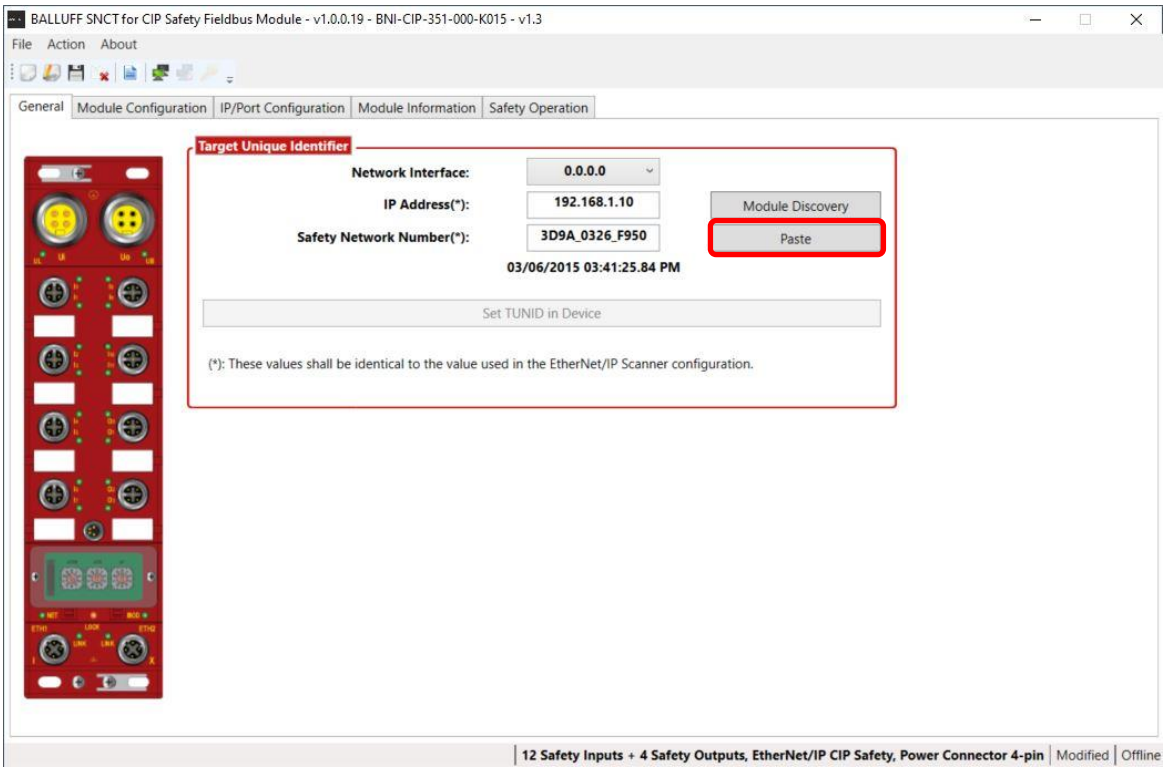


From the RSLogix 5000 software, go to Safe I/O Module properties dialog box.

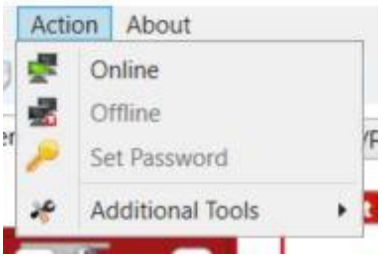
Select the Safety Network Number parameters button.



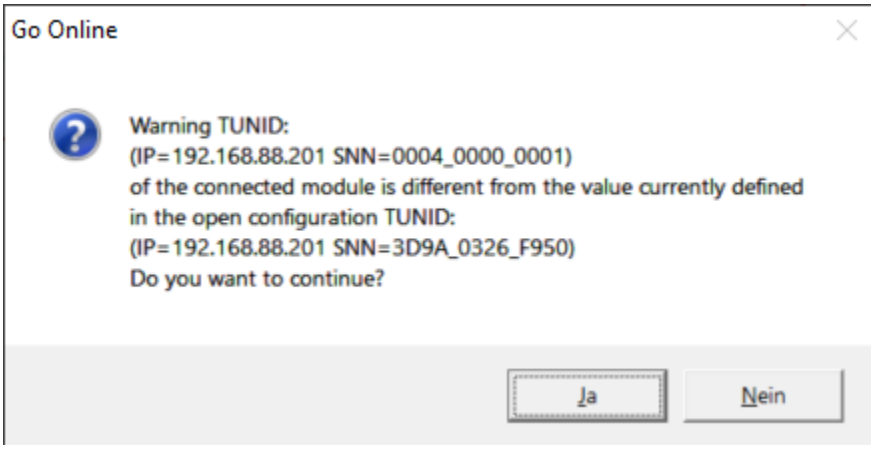
Copy the SNN in the clipboard and paste it in the SNCT software.



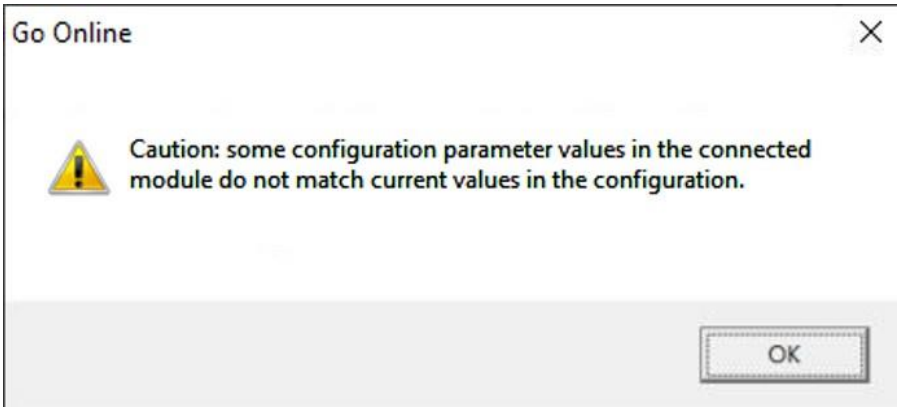
Connect to the module by choosing *Action* menu select *Online*



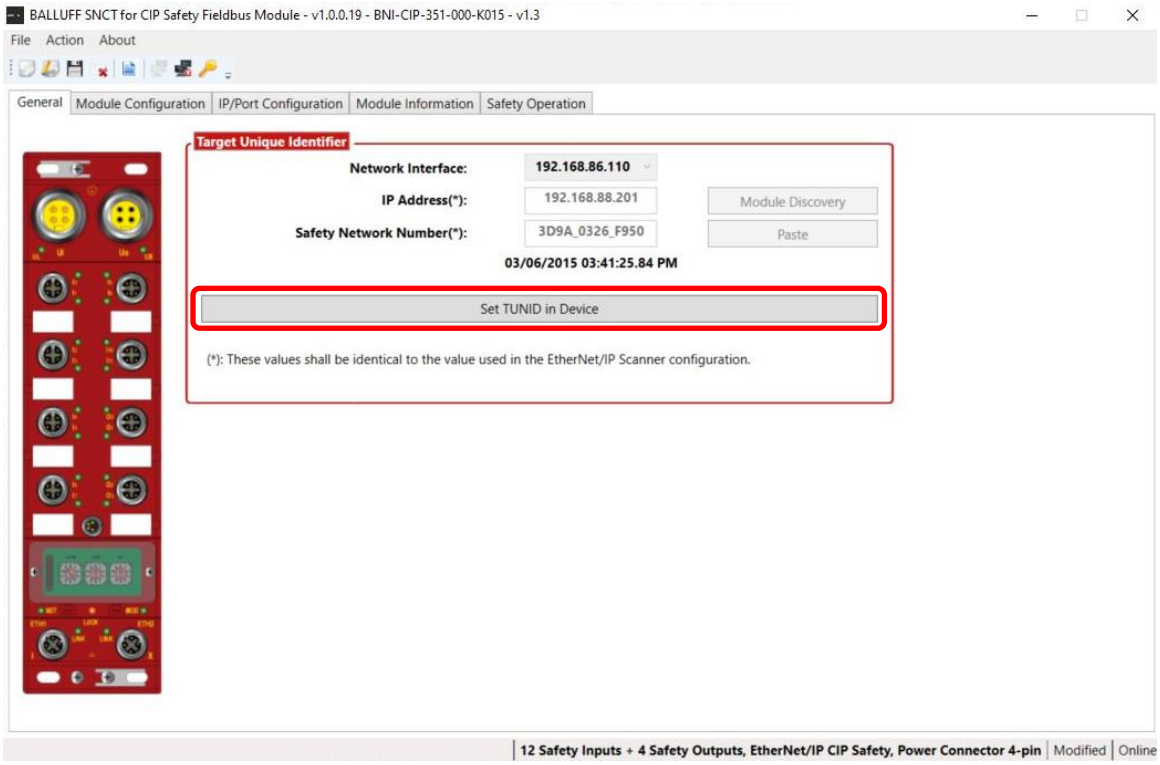
If the TUNID is different than the one configured in the module, the following message is displayed:



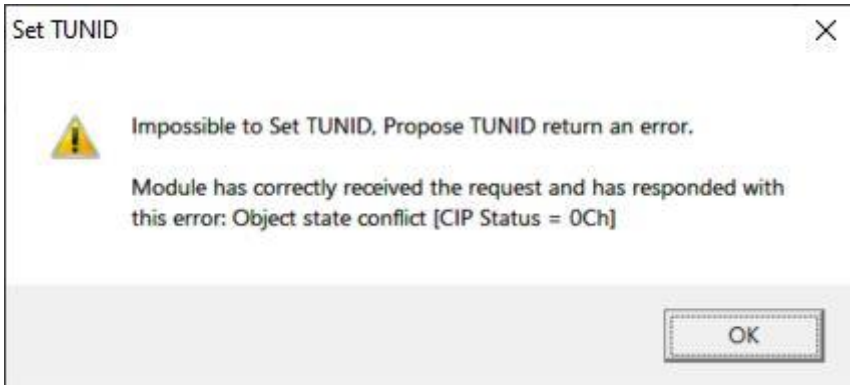
If some existing parameters were already set in the module, the following message is displayed:



Select *Set TUNID in Device button*.

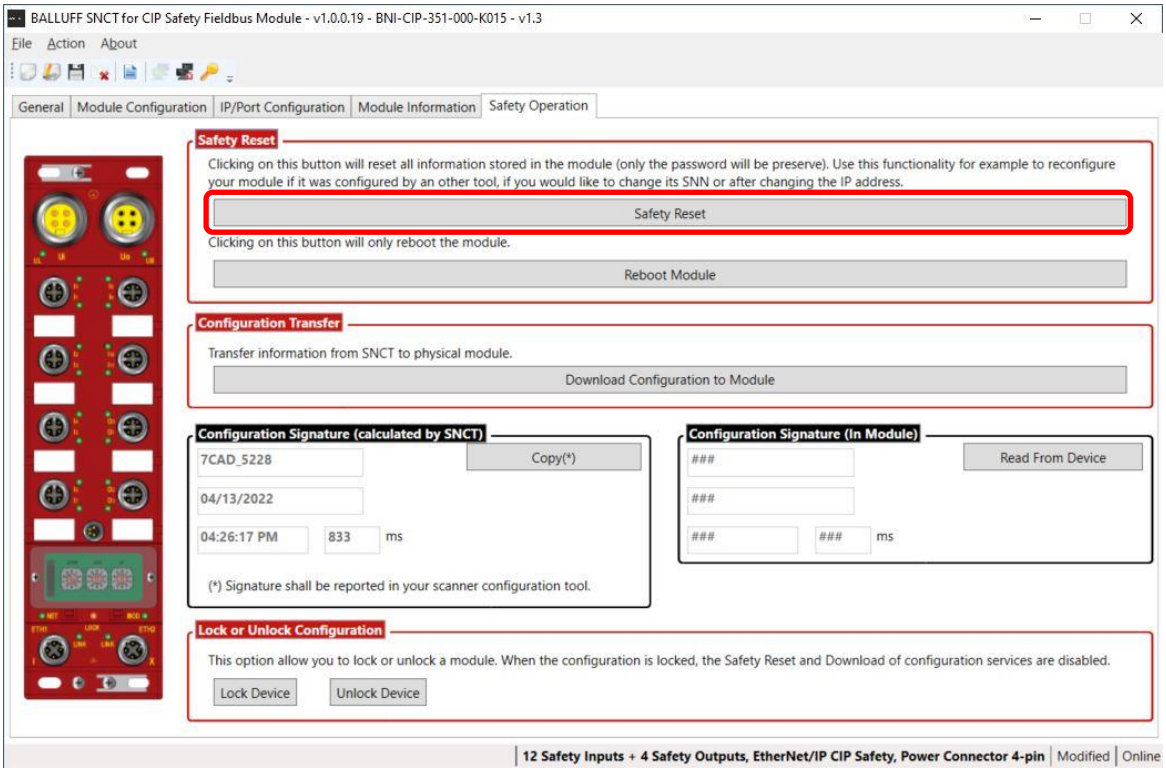


Note!
If you get the below message means that the module has already a TUNID configured.

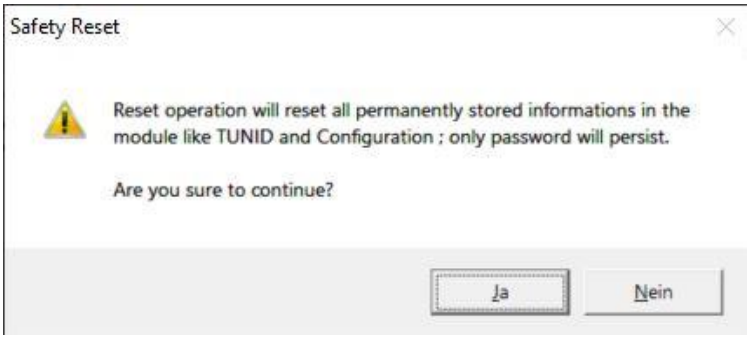


Perform a Safety Reset before to be able to set the TUNID.

Go to the Safety Operation tab and select the *Safety Reset* button.



Select Yes to reset the module TUNID and configuration.



The module is successfully reset.

Note!

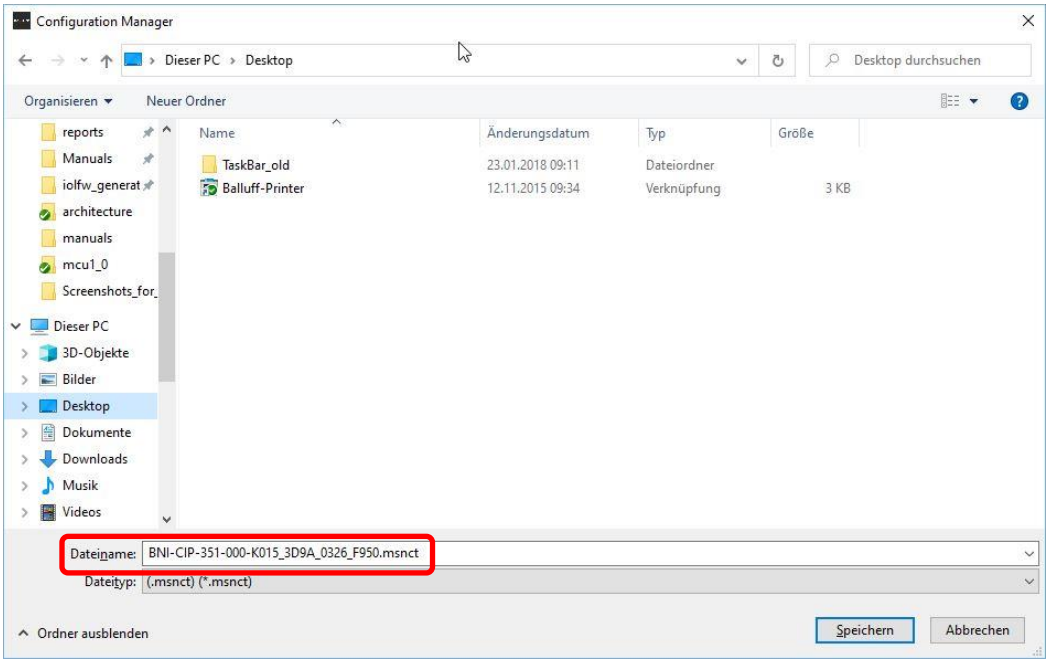
Be careful then setting TUNID that no EtherNet/IP Scanner I/O connections are open otherwise the setting of TUNID will failed.

The setting of TUNID is successful. The next step is to configure the module.

Note!
Now that the TUNID is configured, it is possible to save the module configuration.

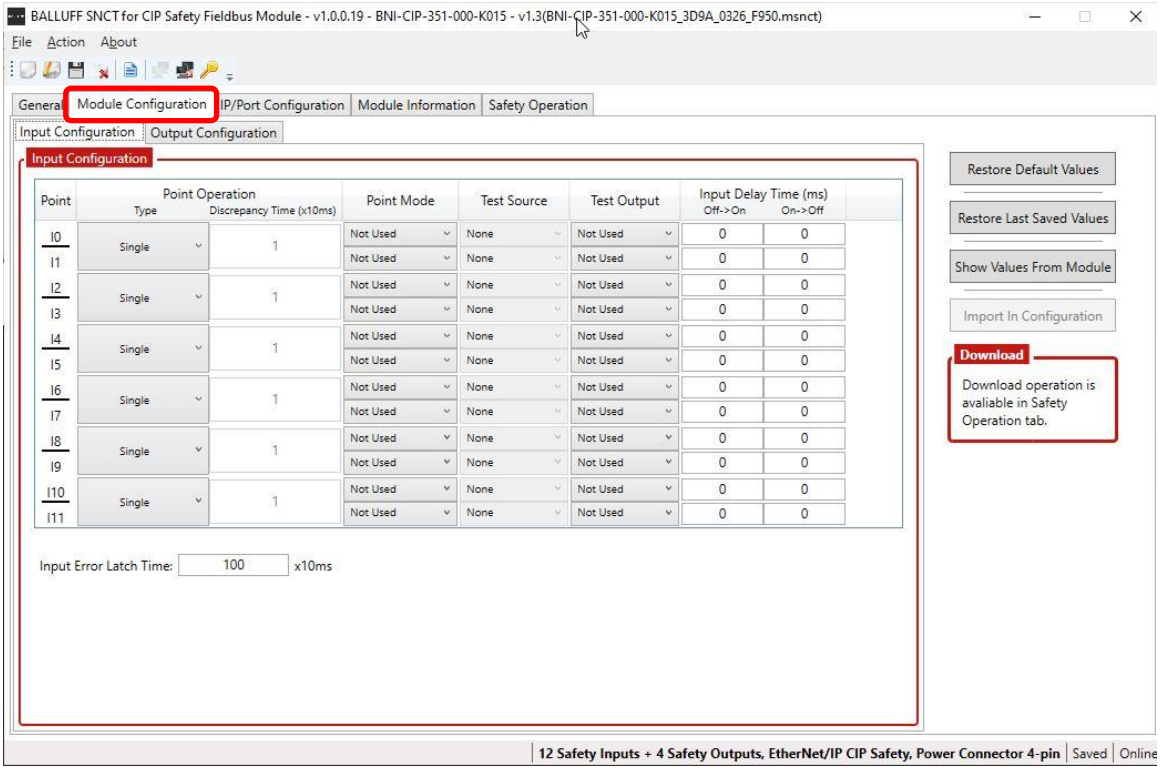
Select File / Save.

The default file name is the concatenation of the Safe I/O Module product number and TUNID configured in the module. The file name can be changed if necessary.



Select the *Module Configuration* tab to define the parameters for the Safety Inputs and Safety Outputs.

Safety Inputs Configuration



Point Operation Type

Type	Comments
Single	Safety Inputs are treated separately.
Equivalent	Safety Inputs are treated as an Equivalent dual-channel. The evaluation is done after discrepancy time.
Complementary	Safety Inputs are treated as a Complementary dual-channel. The evaluation is done after discrepancy time.

Point Mode

Mode	Comments
Not used	Input is disabled.
Safety	Input is enabled and no external pulse test is needed. This is commonly used when the Input device generates its own pulse test such as light curtain.
Safety Pulse Test	Input is enabled and a Pulse Test must be used as the 24 V. The pulse test is configured via the *Test Source* option.
Standard	Input is enabled but doesn't participate in any safety function. This is commonly used to connect non-safe input device.

Test Source

Select the appropriate Test Source for the Safety Input.

Note!

The Test source can only be selected when a Point Mode has been set to Safety Pulse Test.

Note!

The Test Source can only be set to one of the associated M12 connector.

Test Output

Mode	Comments
Not used	Test Output is disabled.
Standard	Test Output pin is configured to act as a non-safe output signal. The signal is control through the PLC in the process output image of the module.
Pulse Test	Test Output is configured to generate 24 VDC with a Pulse Test.
Power Supply	Test Output is configured to deliver 24 VDC power supply. At module power on, the Test Output is constantly energized (24 VDC).
Muting Lamp	Test Output is used to drive a muting lamp. The Test Output can detect a broken wire condition (check is done every 3s, and 2 consecutive fail tests are requiring to declare a fault).

Note!

Muting lamp selection is only available on Input #3 and Input #7.

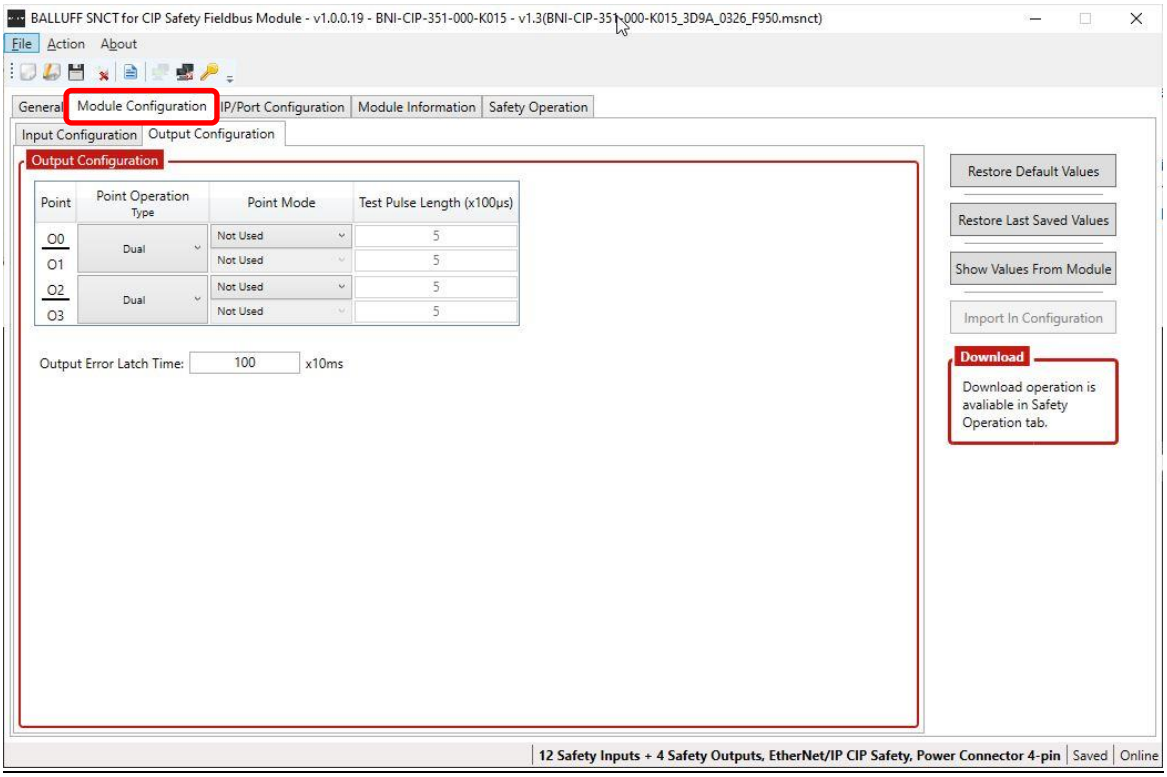
Input Delay

Define the filter time to the Safety Input transition. See Input Delay for more information.

Input Error Latch time

Define the time the module holds an error to make sure the safety controller can detect it. See Input Error Latch Time for more information.

Safety Outputs Configuration



Point Operation Type

Mode	Comments
Single	The Safety Outputs are treated separately.
Dual Channel	The Safety Outputs are treated as a dual-channel.

Point mode

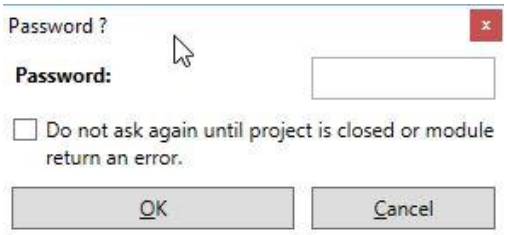
Mode	Comments
Not used	Output is disabled.
Safety No Pulse Test	Output is enabled and NO pulse test is generated.
Safety Pulse Test	Output is enabled and a pulse test is generated.

Pulse Test Length

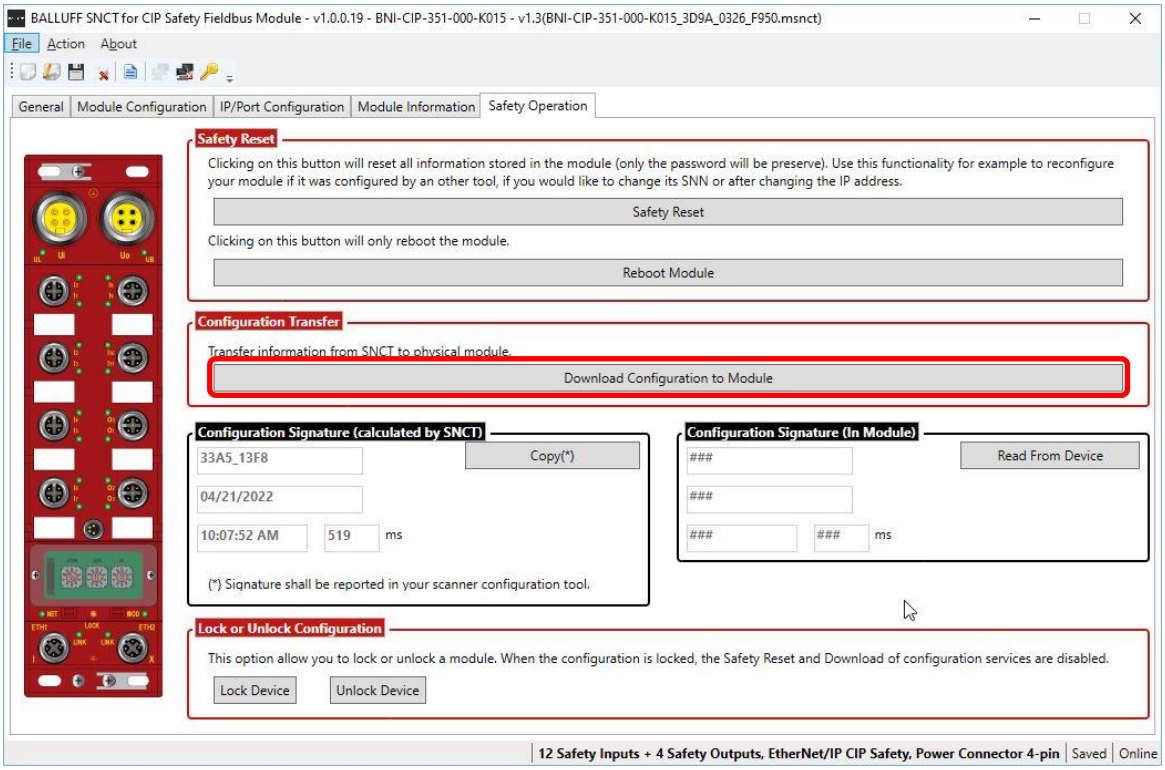
Define the pulse test length of the associated Output. See Output Pulse Test for more information.

When the safety I/O setting is completed, the next step is to download the configuration in the module.

Note!
If you have defined a password to protect the module configuration, the SNCT will ask to fill the password for the next Safety Operation.

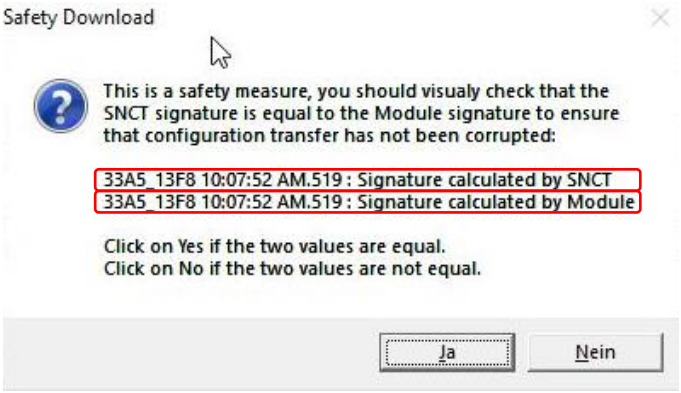


Select the *Safety Operation* tab and click on *Download Configuration to Device*.



Warning!
The validation of the configuration signature is an important step of the module commissioning.

It is the role as a Safety Expert to ensure that the configuration file sent to the module is correctly transferred by verifying the signature calculated by both SNCT software and Safe I/O Module.



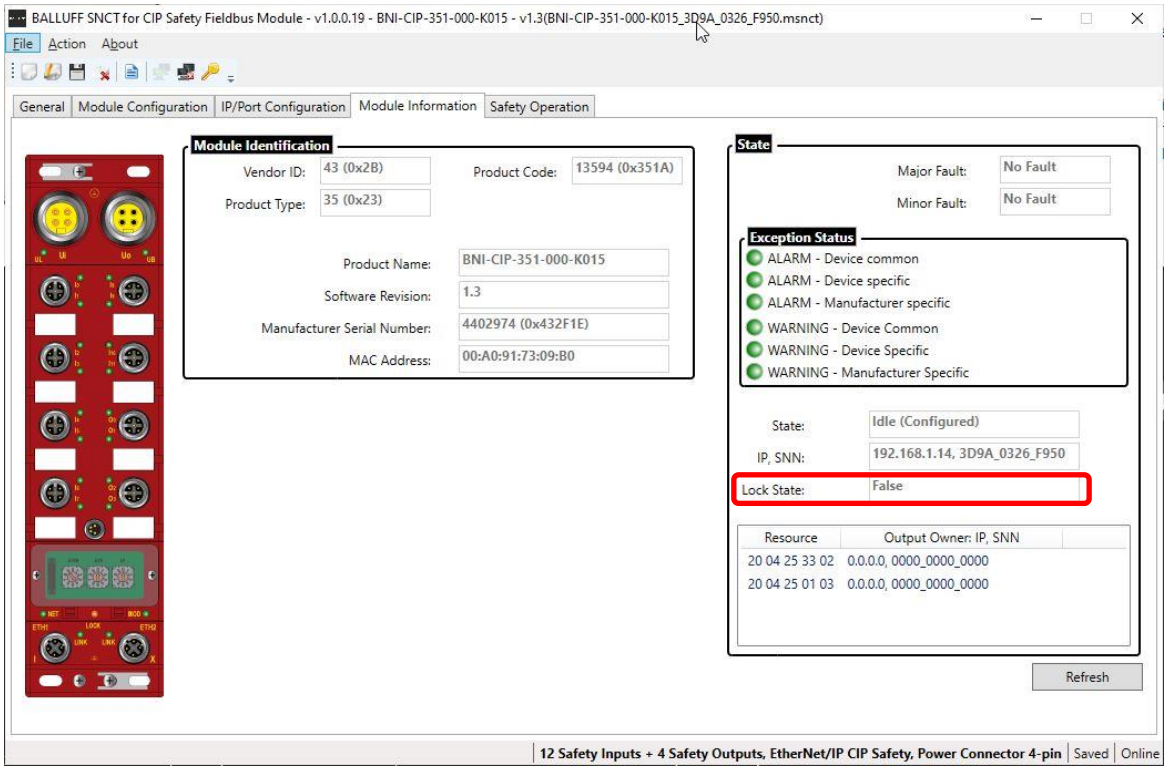
If the signatures are identical, click the *Yes* button otherwise click *No* to abort the operation.

Warning!
Each operation has to be done by a Safety Expert and requires knowing the module password to perform the operations.

Note!

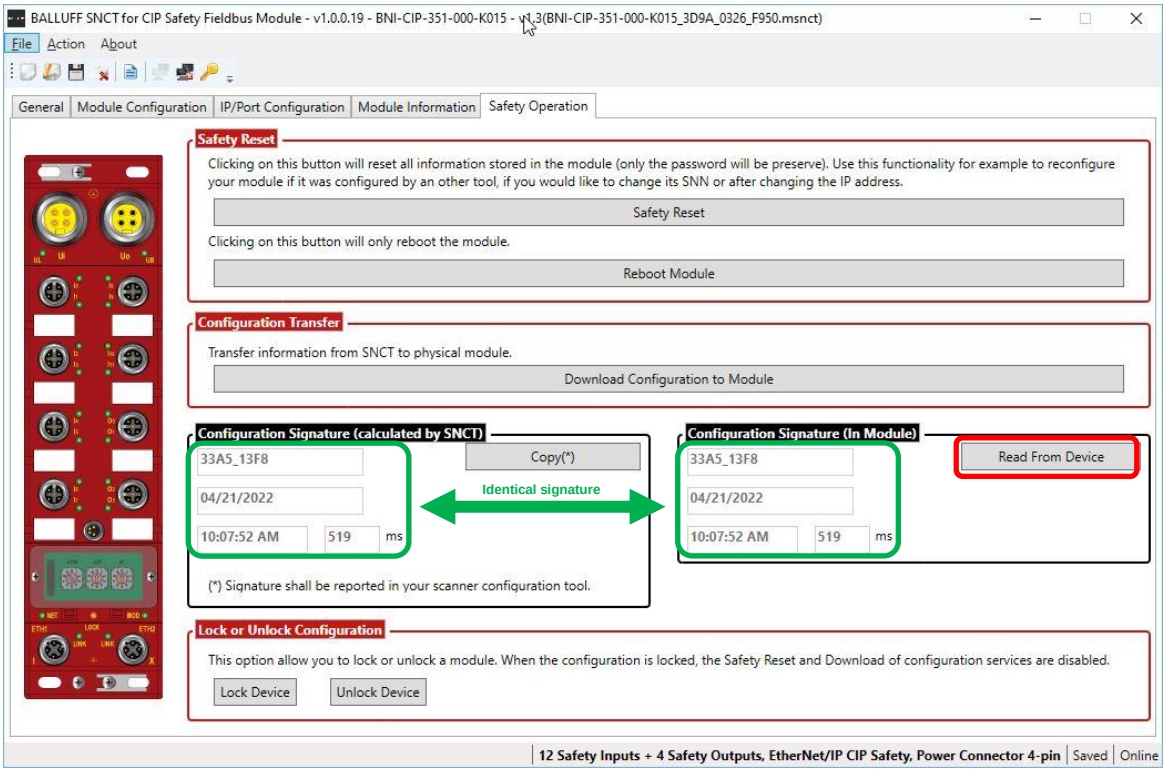
Before the download of file, please check that the module configuration is not locked.
This status can be visualized either looking the “Lock” yellow LED on the module

or using the Module Information Tab.

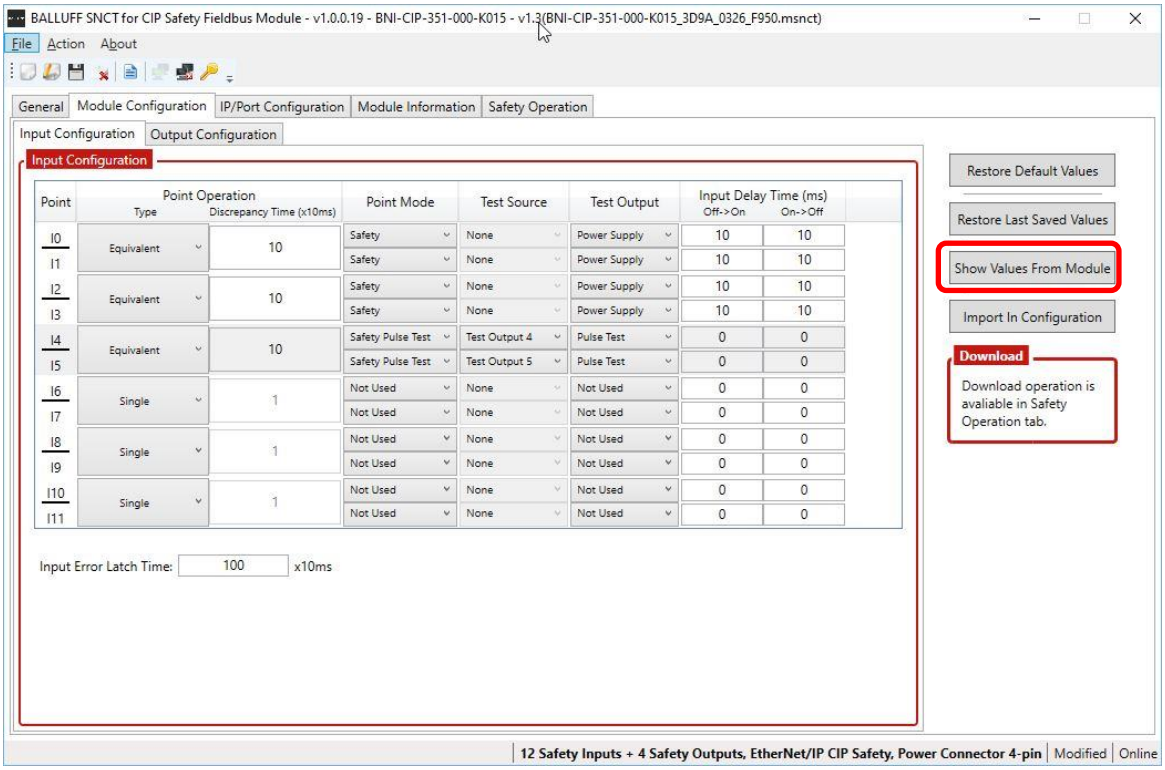


Verification of the transferred module configuration

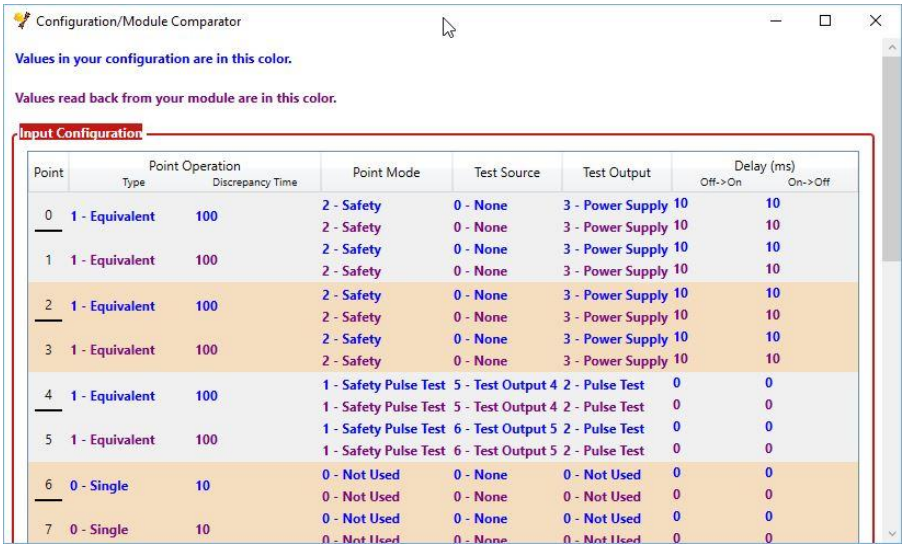
The module is configured now. You can verify the configuration signature by clicking the button *Read from device* to check that both SNCT configuration and Device configuration are identical.



It is also part of the safety process to control visually the correct match of the Safety Input and Safety Output parameters. Go to *Module Configuration* tab and click on *Show Values from Module*.



A window shows one-by-one the I/O parameters.



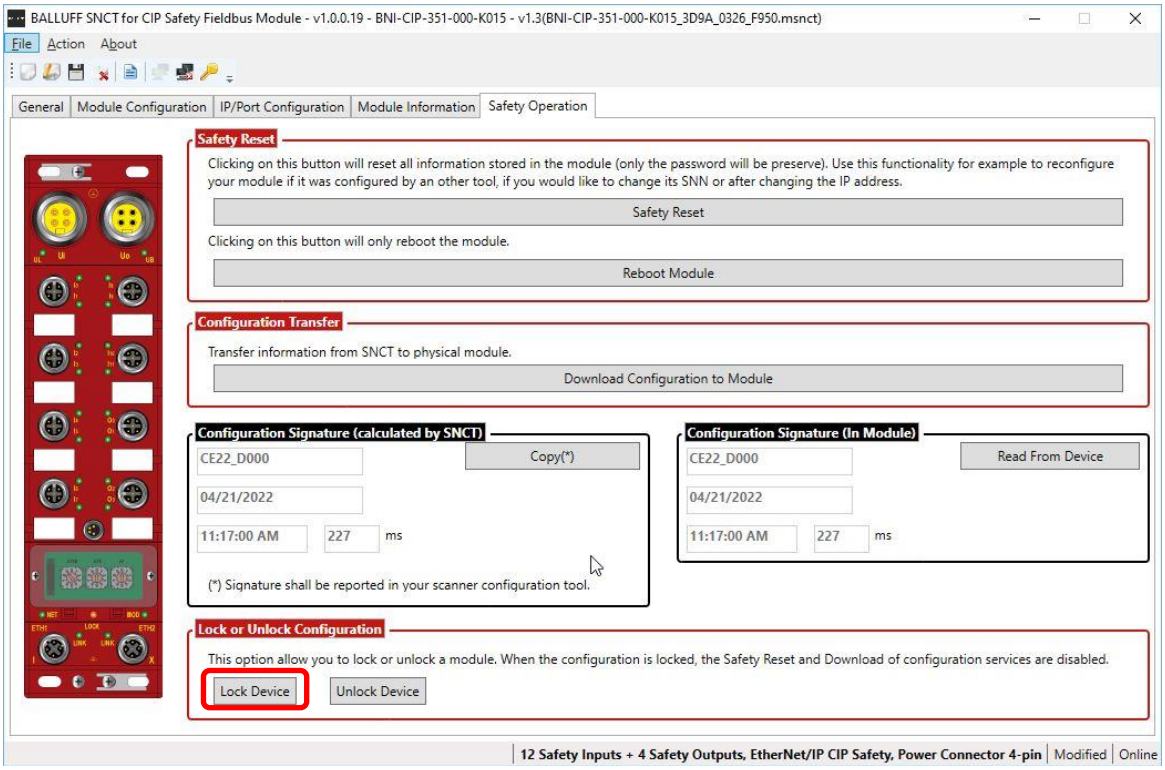
Note!

It is voluntary that the differences found are not highlighted because the checking has to be done by a Safety Expert body, and not by the SNCT software.

Warning!

It is part of the safety process to realize a test system of each safe input and safe Output configured. The tests have to be done by a Safety Expert body and consigned in a document.

Lock the configuration to protect it from any user modification.

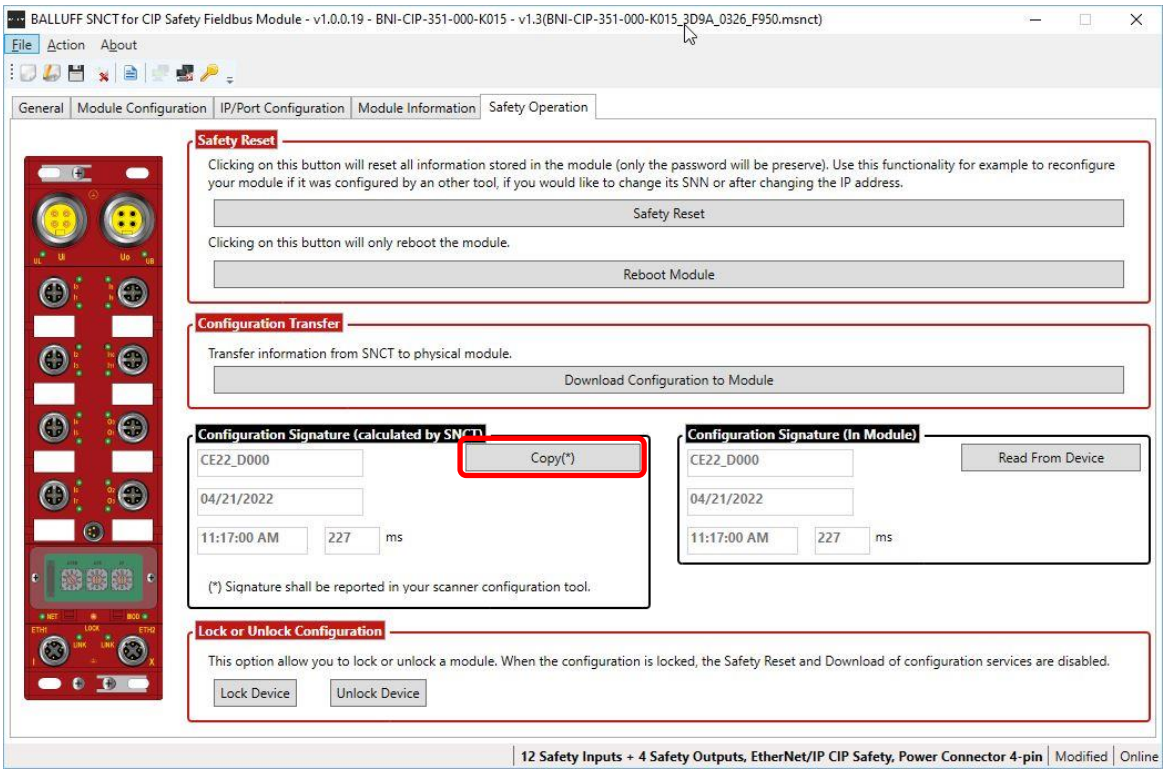


The module is now locked.

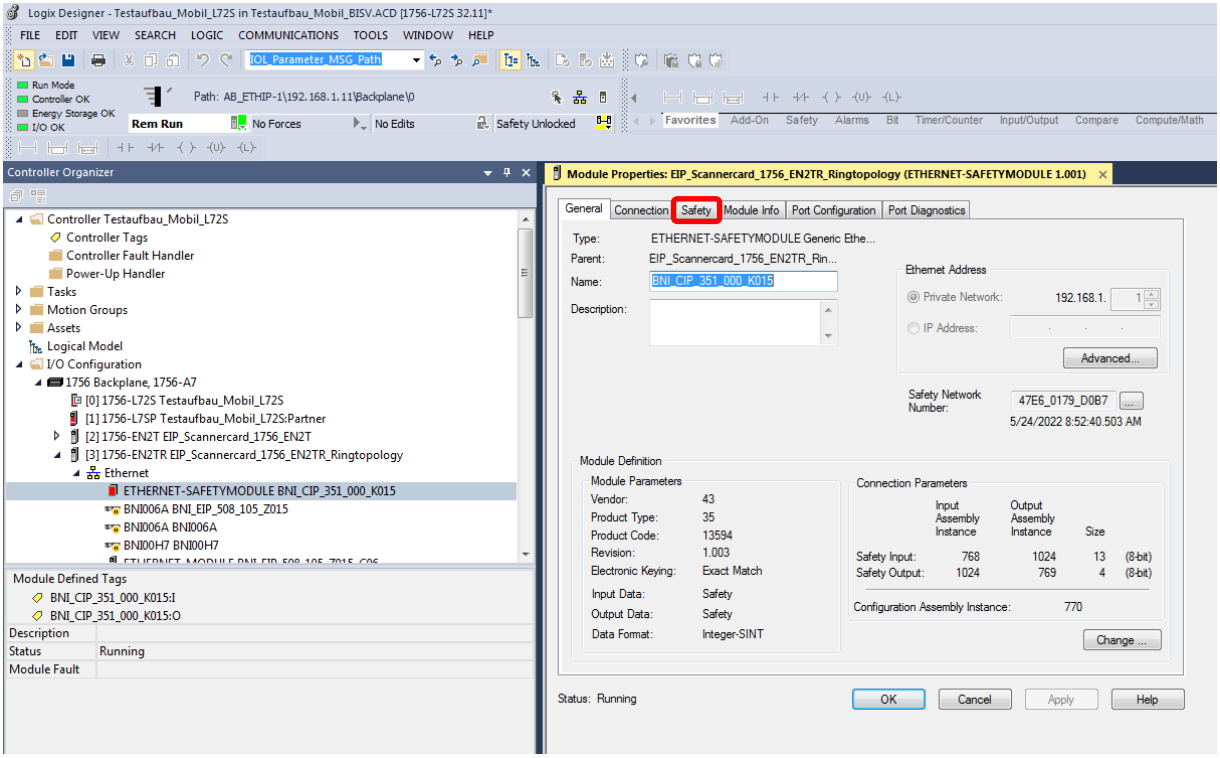
7.8. Connection and testing of the Safe I/O Module in RSLogix 5000

Importing the module signature in Logix5000

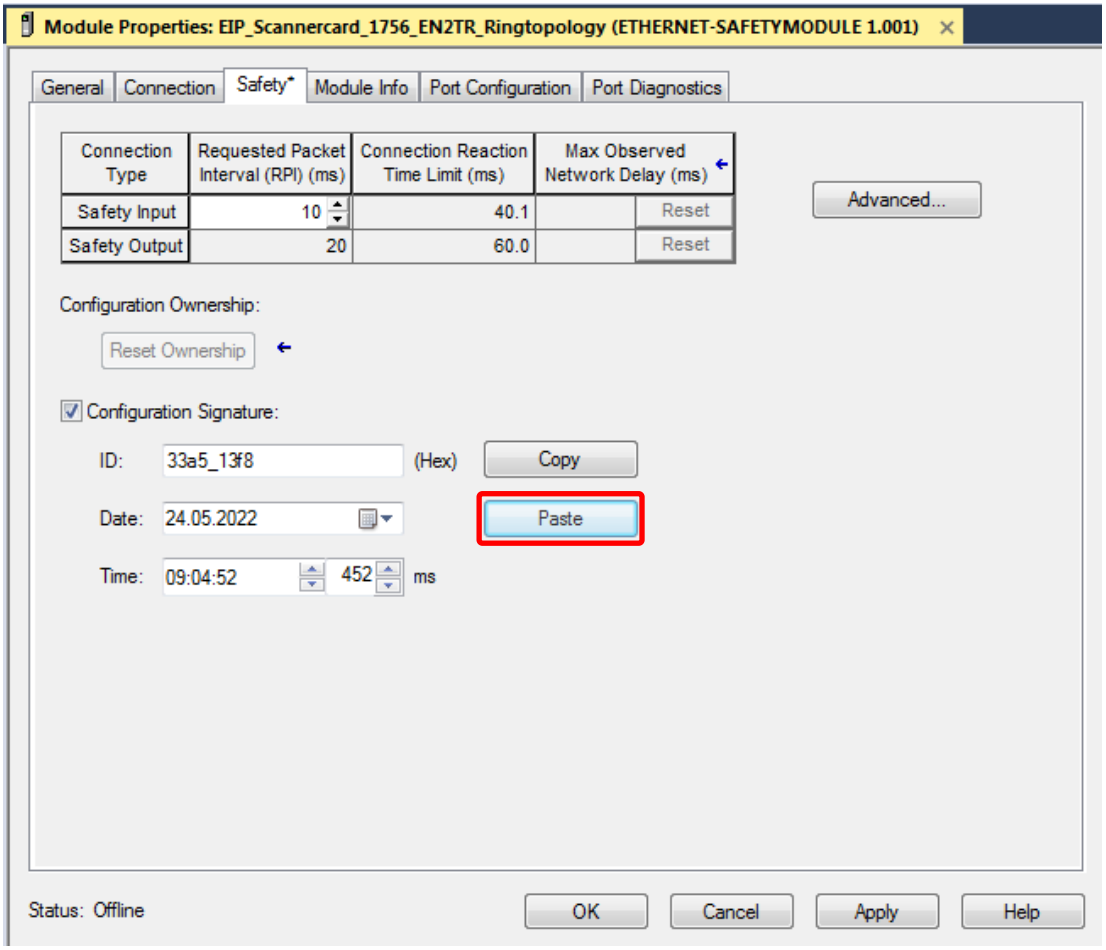
Go to *Safety Operation* and select *Copy*.



In RSLogix, open the Safe I/O Module Properties window and select *Safety* Tab.



Click on the *Paste* button.

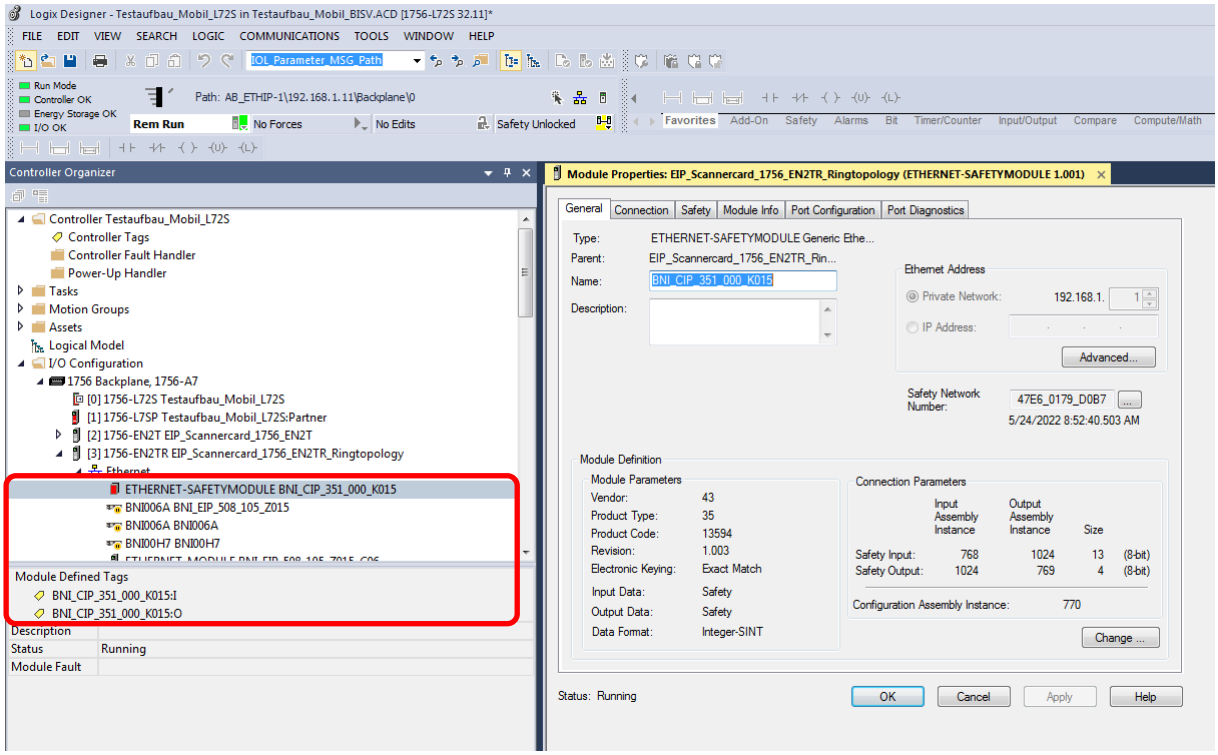


To finalize the configuration, adjust the RPI for the Safety Input connection at the required Value.

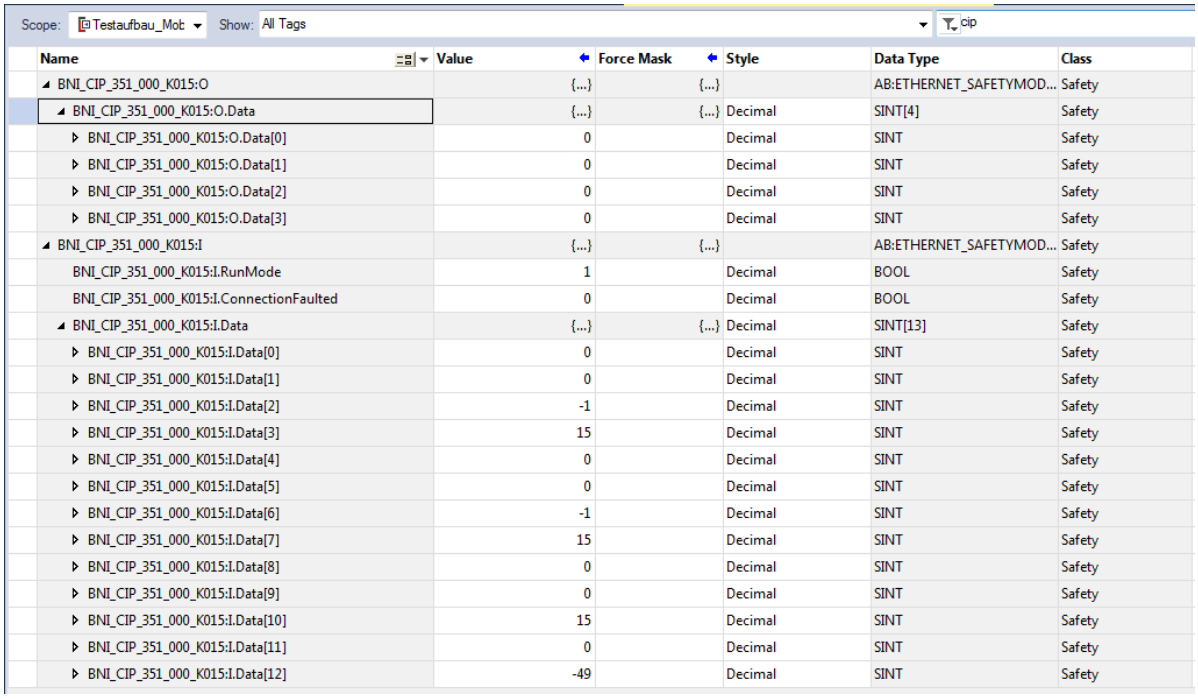
Warning!
The minimum RPI for the Safe I/O Module is 10ms.

Warning!
If configuration signature is unchecked, authorized personal needs to ensure that the Controller and Safe I/O Module have the correct configuration.

Go Online and download the controller project. Switch the safety controller in Run mode.



The Safe I/O Module connection is established and running. You can now access to the safety process data and start writing the safety control application.



Name	Value	Force Mask	Style	Data Type	Class
BNI_CIP_351_000_K015:O	{...}	{...}		AB:ETHERNET_SAFETYMOD...	Safety
BNI_CIP_351_000_K015:O.Data	{...}	{...}	Decimal	SINT[4]	Safety
BNI_CIP_351_000_K015:O.Data[0]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:O.Data[1]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:O.Data[2]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:O.Data[3]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I	{...}	{...}		AB:ETHERNET_SAFETYMOD...	Safety
BNI_CIP_351_000_K015:I.RunMode	1		Decimal	BOOL	Safety
BNI_CIP_351_000_K015:I.ConnectionFaulted	0		Decimal	BOOL	Safety
BNI_CIP_351_000_K015:I.Data	{...}	{...}	Decimal	SINT[13]	Safety
BNI_CIP_351_000_K015:I.Data[0]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[1]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[2]	-1		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[3]	15		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[4]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[5]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[6]	-1		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[7]	15		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[8]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[9]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[10]	15		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[11]	0		Decimal	SINT	Safety
BNI_CIP_351_000_K015:I.Data[12]	-49		Decimal	SINT	Safety

8. EtherNet/IP Behavior

This chapter gives a presentation of the Safe I/O Module behavior related to EtherNet/IP communication.

8.1. I/O behavior

When the Safe I/O Module is running (Scanner connection in progress) if the module detects a connection lost with the Scanner, the module sets automatically the safety output process data to “0”.

The detection of the connection lost with the Scanner is calculated based on the time-out (multiplier x RPI) defined in the I/O connection (Safety_Forward_Open request) sent by the Scanner.

8.2. IDLE behavior

An EtherNet/IP scanner can produce the safety output process data in IDLE mode (typically when it is in programming mode). In this case the controller maintains its I/O connections open but informs the devices the output process data must not be processed.

When the Safe I/O Module received safety output data in IDLE mode,

- the module sets all its safety output data to 0
- the module produces its safety input data to the scanner

8.3. Duplicate IP address

The Safe I/O Module performs a duplicate IP address checking according to ACD method (Ipv4 Address Conflict Detection) defined by ODVA and RFC 5227.

The goal of this feature is to ensure that the IP address is not used by another device on the network. This mechanism is done during boot up of the module, during module operation (if a new device inserted to the network is trying to use the same IP) or after software reset (CIP object 0x01, Instance 1 Service 5).

If the module detects another device with the same IP address, it will:

- Defend its IP address
- If conflict is confirmed
    - The module will release its IP address
    - The module diagnostics leds NET, LOCK and MOD are blinking **RED**

8.4. EtherNet/IP Object Classes

Identity (0x01)

This object allows reading the identity of the module.

Class Attributes

Id	Description	Get	Set	Limits
01h	Revision	●	○	1
02h	Max Instance	●	○	1
03h	Number of instances	●	○	1

● Supported ○ Not supported

Class Services

Id	Service	Param. Options
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instance Attributes

Id	Description	Get	Set	Limits
01h	Vendor Id	●	○	8
02h	Device Type	●	○	12
03h	Product Code	●	○	Depends on the product
04h	Revision	●	○	Depends on the revision
05h	Status	●	○	
06h	Serial Number	●	○	
07h	Product Name	●	○	Depends on the product

● Supported ○ Not supported

Instance Services

Id	Service	Param. Options
01h	Get_Attributes_All	
05h	Reset	
0Eh	Get_Attribute_Single	

Message Router (0x02)

Class Attributes

Id	Description	Get	Set	Limits
1	Revision	○	○	
4	Optional Attribute List	○	○	
5	Optional Service List	○	○	
6	Max ID of class attributes	○	○	
7	Max ID of instance attributes	○	○	

● Supported ○ Not Supported

Class Services

Service		Param. Options
Get_Attributes_All	○	
Get_Attribute_Single	○	

● Supported ○ Not Supported

Instance Attributes

Id	Description	Get	Set	Limits
1	Object List	○	○	
2	Maximum connections supported	○	○	
3	Number of active connections	○	○	
4	Active connections list	○	○	

● Supported ○ Not Supported

Instance Services

Service		Param. Options
Get_Attributes_All	○	
Get_Attribute_Single	○	

● Supported ○ Not Supported

Assembly (0x04)

This object allows to access I/O process data.

Class Attributes

Id	Description	Get	Set	Limits
01h	Revision	●	○	2
02h	Max Instance	●	○	199
03h	Number of instances	●	○	4

● Supported ○ Not supported

Class Services

Service		Param. Options
Get_Attribute_Single	●	

● Supported ○ Not Supported

Instance Attributes

Id	Description	Get	Set	Limits
03h	Data	●	●	Set command is not allowed if an exclusive owner connection is open

● Supported ○ Not supported

Instance Services

Id	Service	Param. Options
0Eh	Get_Attribute_Single	
10h	Set_Attribute_Single	

Connection Manager (0x06)

Class Attributes

Id	Description	Get	Set	Limits
01h	Revision	●	○	1
02h	Max Instance	●	○	1
03h	Number of instances	●	○	1

● Supported ○ Not supported

Class Services

Id	Service	Param. Options
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instance Attributes

Id	Description	Get	Set	Limits
01h	Open Requests	●	○	
02h	Open Format Rejects	●	○	
03h	Open Resource Rejects	●	○	
04h	Open Other Rejects	●	○	
05h	Close Requests	●	○	
06h	Close Format Requests	●	○	
07h	Close Other Requests	●	○	
08h	Connection Timeouts	●	○	

● Supported ○ Not supported

Instance Services

Id	Service	Param. Options
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	
4Eh	Forward_Close	
54h	Forward_Open	
5Bh	Large_Forward_Open	Class 3 only

TCP/IP Interface (0xF5)

Class Attributes

Id	Description	Get	Set	Limits
01h	Revision	●	○	2
02h	Max Instance	●	○	1
03h	Number of instances	●	○	1

● Supported ○ Not supported

Class Services

Id	Service	Param. Options
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instance Attributes

Id	Description	Get	Set	Limits
1	Status	●	○	
2	Configuration Capability	●	○	
3	Configuration Control	●	●	
4	Physical Link	●	○	
5	Interface Configuration	●	●	
6	Host Name	●	●	
7	Safety Network Number	●	●	
8	TTL Value	○	○	
9	Mcast Config	○	○	
10	Select ACD	●	●	
11	LastConflictDetected	●	●	
12	EtherNet/IP Quick_Connect	●	●	

● Supported ○ Not supported

Instance Services

Id	Service	Param. Options
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	
10h	Set_Attribute_Single	

Ethernet Link (0xF6)

Class Attributes

Id	Description	Get	Set	Limits
01h	Revision	●	○	3
02h	Max Instance	●	○	3
03h	Number of Instance	●	○	3

● Supported ○ Not supported

Class Services

Id	Service	Param. Options
0Eh	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instance Attributes

Id	Description	Get	Set	Limits
01h	Interface Speed	●	○	
02h	Interface Flags	●	○	
03h	Physical Address	●	○	
04h	Interface Counters	●	○	
05h	Media Counters	●	○	
06h	Interface Control	●	●	
07h	Interface Type	○	○	
08h	Interface State	○	○	
09h	Admin State	○	●	
10h	Interface Label	●	○	

● Supported ○ Not supported

Instance Services

Id	Service	Param. Options
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	
10h	Set_Attribute_Single	
4Ch	Get_and_Clear	

DLR (0x47)

Class Attributes

Id	Description	Get	Set	Limits
01h	Revision	●	○	3
02h	Max Instance	●	○	1

● Supported ○ Not supported

Class Services

Id	Service	Param. Options
0Eh	Get_Attribute_Single	

Instance Attributes

Id	Description	Get	Set	Limits
01h	Network Topology	●	○	0 indicates “Linear” 1 indicates “Ring”
02h	Network Status	●	○	0 indicates “Normal” 1 indicates “Ring Fault” 2 indicates “Unexpected Loop Detected” 3 indicates “Partial Network Fault” (not expected)
10h	Active Supervisor Address	●	○	IP and / or MAC address of the active ring supervisor
12h	Capability Flags	●	○	Value 0x02 Beacon-based Ring Node

● Supported ○ Not supported

Instance Services

Id	Service	Param. Options
01h	Get_Attributes_All	
0Eh	Get_Attribute_Single	

QoS (0x48)

Class Attributes

Id	Description	Get	Set	Limits
01h	Revision	●	○	1
02h	Max Instance	●	○	1
03h	Number of Instance	●	○	1

● Supported ○ Not supported

Class Services

Id	Service	Param. Options
0Eh	Get_Attributes_All	
0Eh	Get_Attribute_Single	

Instance Attributes

Id	Description	Get	Set	Limits
04h	DSCP Urgent	●	●	
05h	DSCP Scheduled	●	●	
06h	DSCP High	●	●	
07h	DSCP Low	●	●	
08h	DSCP Explicit	●	●	

● Supported ○ Not supported

Instance Services

Id	Service	Param. Options
0Eh	Get_Attribute_Single	
10h	Set_Attribute_Single	

9. Product Replacement

This chapter presents the strategy in case of replacement of commissioned the Safe I/O Module.

9.1. Before to start

This chapter explains how to replace a defective product in an existing application without having to redo the commissioning of a new module and by using the faulty module.

Note!
If the new module does not plan to use the memory key of the defective module. See section Product Deployment for a standard commissioning using the SNCT configuration tool.

Important!
In case of using the memory key for the device replacement, the end user must ensure that SIL3 integrity is applied by additional measures during the replacement verification.

If these measures can be applied, the memory key replacement procedure cannot be used. See section Product Deployment for a standard commissioning using the SNCT configuration tool.

This automatic product replacement operation is possible thanks to the memory key connected to the module. Use the Window internal key (see section Memory Key for details). The memory key saves all module information. Without the key, Safe I/O Module cannot operate.

Before replacing a defective product, check the following:

- The system (machine, application...) is stopped and in a safe state.

Note!
The module replacement will involve turning off power supply. This action may cause malfunctions on other devices depending of the system architecture (e.g. daisy chain / power supply topology).

- The new Safe I/O Module must be strictly similar to the defective product (identical part number, same product version → look the back and side label stickers to identify the product) otherwise **a new commissioning is required**.
- The new Safe I/O Module shall have no configuration (e.g. factory settings). If you are in doubt; you can perform a Safety Reset command to clear module configuration.
- Remember to locate and identify cables / cordsets connected to the module to avoid any inversion.
- You have the necessary skills to perform this replacement.

9.2. Replacement procedure

Follow these steps in order to perform a successful replacement of a module:

1. Disconnect the 7/8'' power supply cordsets.

Danger!

Risk of death by electric current!

After disconnecting the device from main voltage, parts such as power connections should only be touched when the capacitors are discharged in the device.

Therefore:

Regard discharge time of the capacitors; do not touch live parts before having observed a period of 30 sec.

If there are additional connected capacitors on the link, the discharge of the link can last considerably longer. In this case you have to determine the required waiting period or even to measure whether the device is safe.

2. Disconnect the Ethernet cordsets.
3. Disconnect the cables connected to safety I/O devices.
4. Take measures to prevent electrostatic discharge in the module or its accessories.
5. Remove the Safe I/O Module from the system support.
6. Note the position of the metallic ground plate of Ethernet connectors.
7. Note the position of the 3 rotary switches.
8. Remove the memory key, open the module window and disconnect the key using an appropriate. Avoid touching the exposed parts of the printed circuit board.
9. Store the defective module in an appropriate place (e.g. recycling disposal).

The first part of the procedure is completed. The defective module is removed and will be replaced by the new one.

10. Unpack the new module.
11. Remove the memory key and install the one of the defective module, open the module window and disconnect the existing key using an appropriate tool. Install the old key by paying attention to the key mounting direction and close the window.
12. Configure 3 rotary switches; open the module window and turn each rotary switch as noted in Step 7.
13. Place the metallic ground plate of Ethernet connectors as identify in Step 6.
14. Replace the module on its support.
15. Reconnect the cables connected to safety I/O devices.
16. Reconnect the Ethernet cordsets.
17. Reconnect the 7/8'' power supply cordsets.
18. Check that each port (7/8 '', M12, M8) not used on the module is closed with a plug.

9.3. Verification

The new Safe I/O Module starts. Several situations can occur:

1. All I/O diagnostic LEDs blink red. This information indicates that the new module does not accept the configuration stored in the memory key.
    a. Retry the procedure with another module.

    b. Perform a safety reset of the new module with the original memory key and try again the procedure.

2. After the boot self-test sequence, the module starts but is not reconnected by the network controller.
    a. Check the cordsets (power, network) are properly connected by inspecting the status of the diagnostic LEDs on the module.

    b. Test the communication with the module using a network tool:
        i. Sending a PING command from a DOS window
        ii. Use the Ethernet/IP tool software (available free-of-charge here) to detect the module.
        iii. Launch a web browser to connect to the module Web server.

3. After the boot self-test sequence, the module is reconnected by the network controller (MOD and NET LEDs are green or green flashing). **The replacement has been successfully completed**.

Note!

If the replacement failed, double check that the new module has no configuration. If you have any doubt, perform a Safety Reset command to clear module configuration.

Important!

The replacement of a safety device requires that a safety expert body checks the correct replacement and operation of the new device in the system.

10. SNCT Configuration Software

This chapter presents the important features that are available in the SNCT configuration software used for the Safe I/O Module commissioning.

10.1. Overview

Balluff *Safety Network Configuration Tool* (also called SNCT) is a Windows software tool used to do the safety configuration and commissioning of the Safe I/O Module.

Warning!

Balluff SNCT is a T3 software tool according to the definition provided by the IEC61508. For this reason, the user shall take all appropriate measures according to the standard for this type of software tool.

Note!

Before to use the SNCT tool, the Safe I/O Module must have its IP address already setup.

Note!

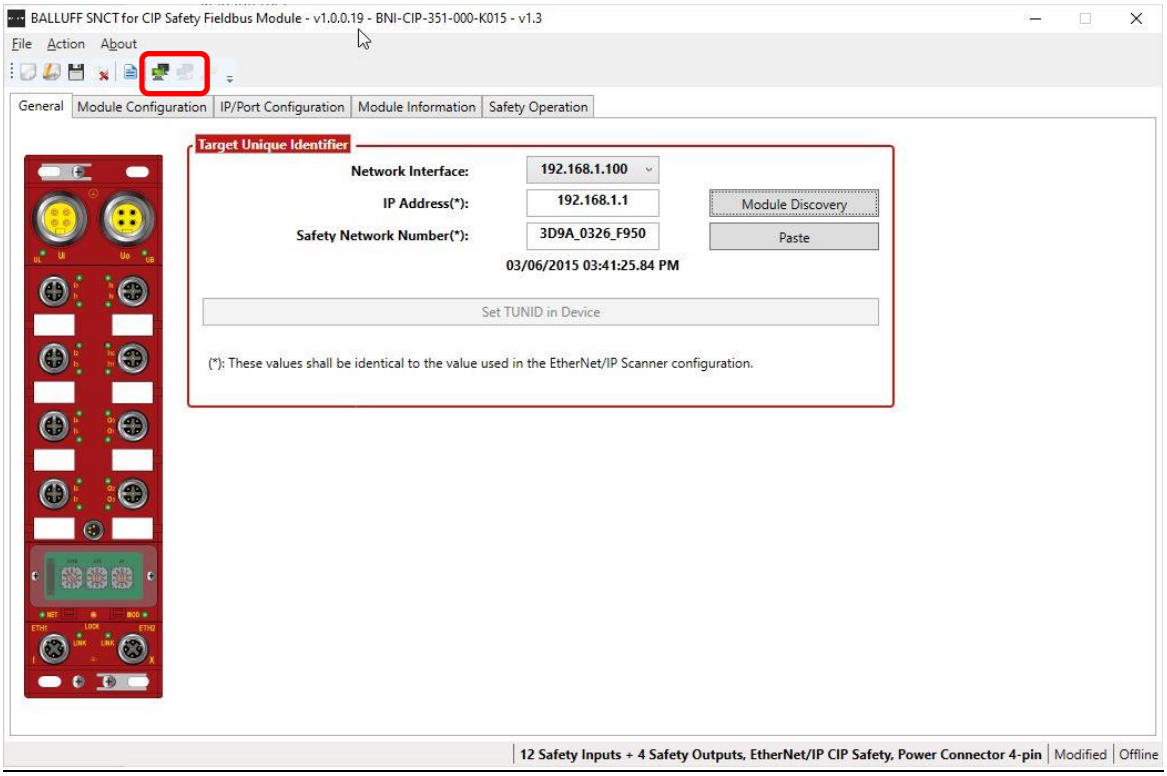
SNCT software is compatible with Windows 32-bit and 64-bit operating systems running under Windows XP and Windows Seven.

SNCT standard and safety features include:

- Create, Open and Save module configurations
- Preview and Print a module configuration
- Automatic module discovery
- Safety inputs and safety outputs parameters setting
- TCP/IP parameters setting
- Ethernet ports configuration and diagnostics
- Module identification and status information
- Safety Operations
    - Safety Network Number (SNN) setting
    - Safety Reset
    - Module Reset
    - Safety configuration transfer
    - Lock and Unlock of module configuration
- Set / Reset password for a configuration
- Advanced features
    - Emergency mode (allow to read information stored in the memory key)
    - Firmware Download

Most of the features are performed when the SNCT software is connected to the Safe I/O Module.

To go Online/Offline, select the *Action* menu or click on the following icon:



10.2. Safety Reset

The Safety Reset is a command to reset the ownership between the EtherNet/IP Scanner and a Safe I/O Module in case of one of the below parameter has changed:

- TCP/IP address
- Network Number (SNN)
- Module configuration signature

Note!
The command is useful if a Safe I/O Module already commissioned needs to be reset with the factory “out-of-box” configuration setting (meaning default SNN, no configuration signature and no stored IP address).

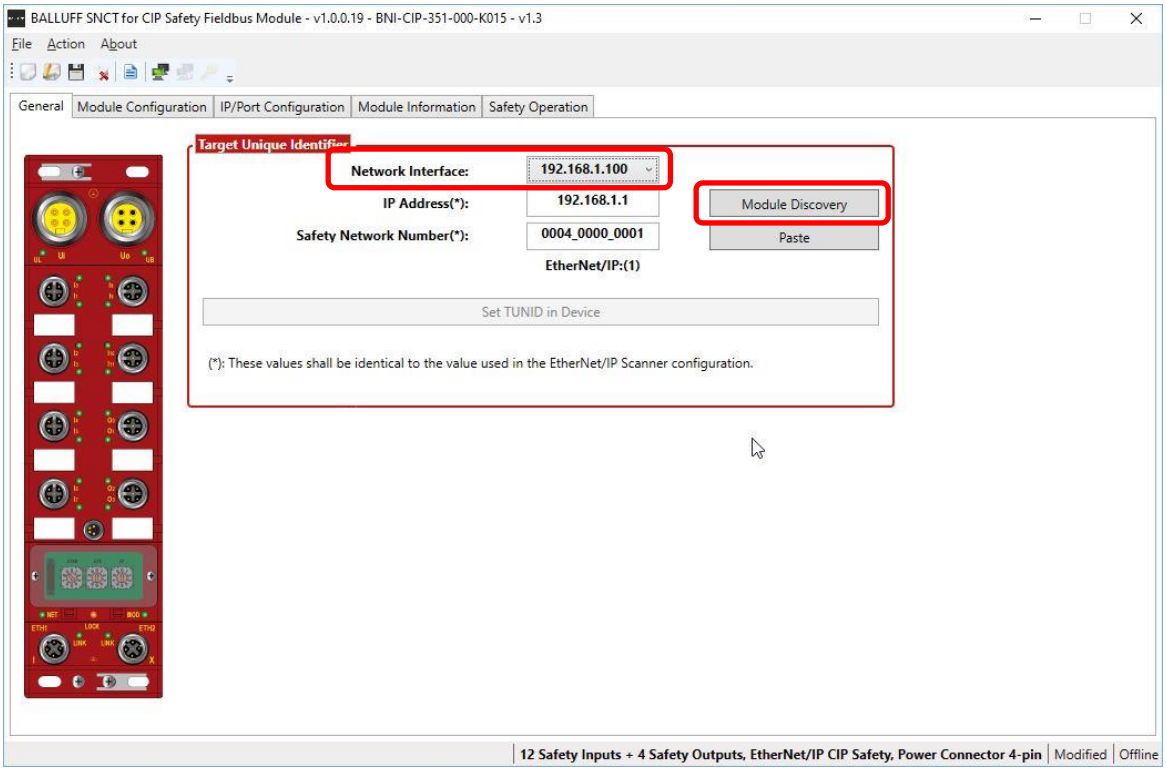
Note!
The procedure is based on the assumption that the module has been already commissioned and no information is known about the module (IP address, SNN, lock, signature, password…).

To perform a Safety Reset follows the below procedure:

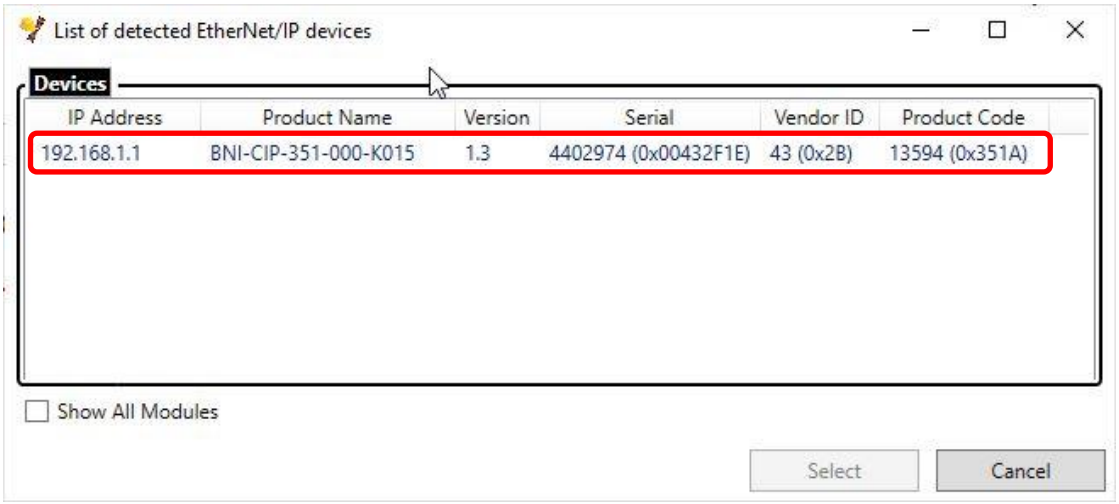
1. Set the computer network interface to **192.168.1.100**.
2. Open the Safe I/O Module window and set the 3 rotary switches to position **001** (corresponding to static IP address **192.168.0.1**)
3. Power up the module
4. Launch the SNCT
5. Create a new project (*File/New*)
6. Select the correct safety module model and version

7. Select the network interface

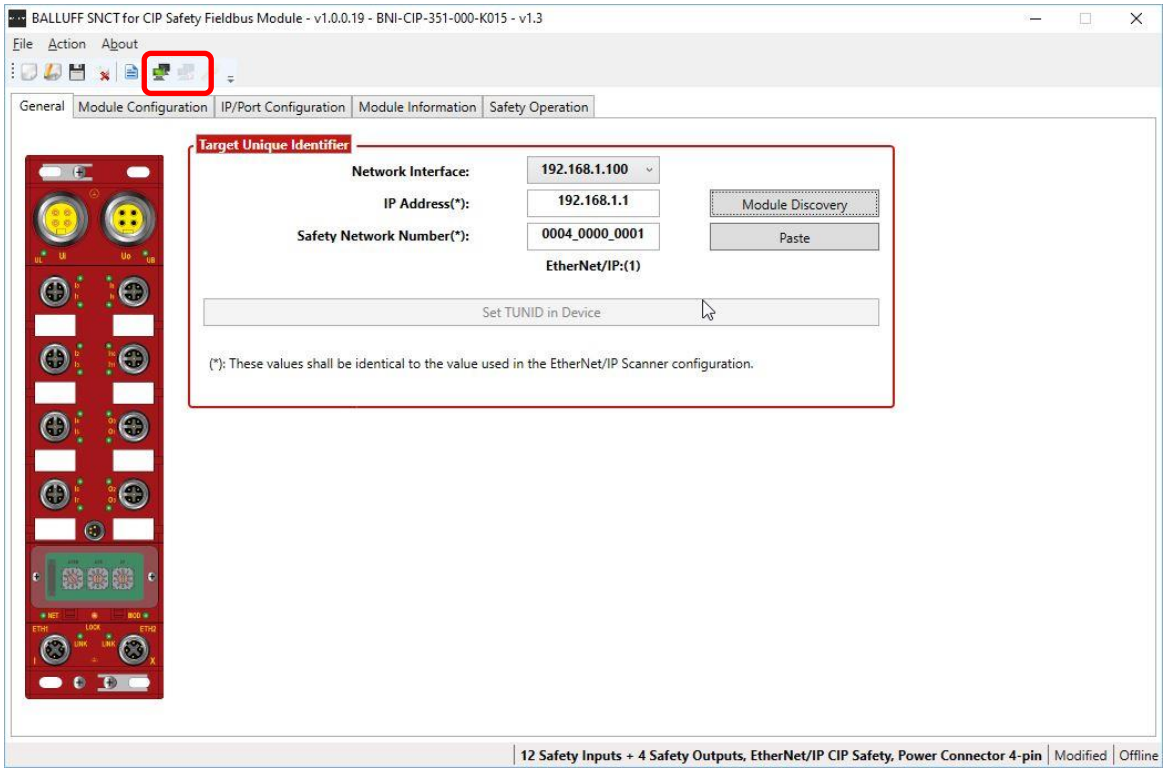
8. Perform a module discovery



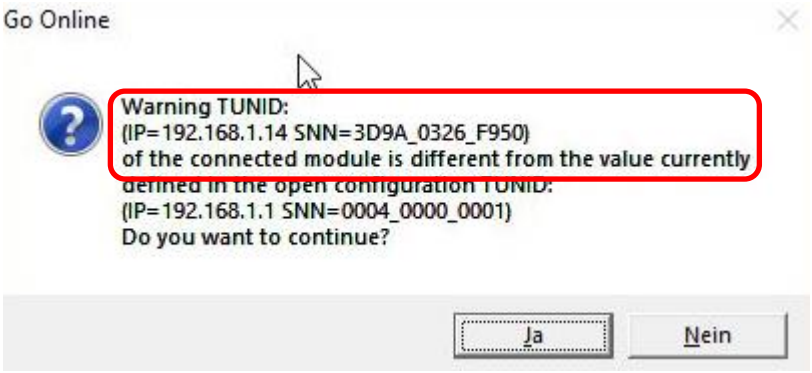
9. Double click on the module to select it.



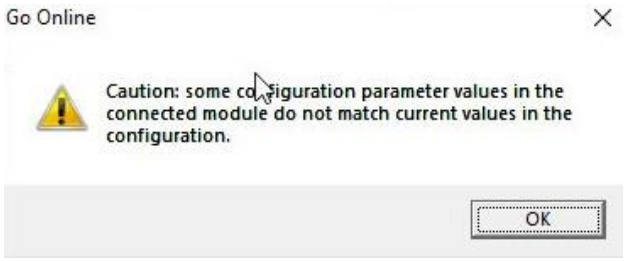
10. Go **Online** to connect the module (*Action/Online*)



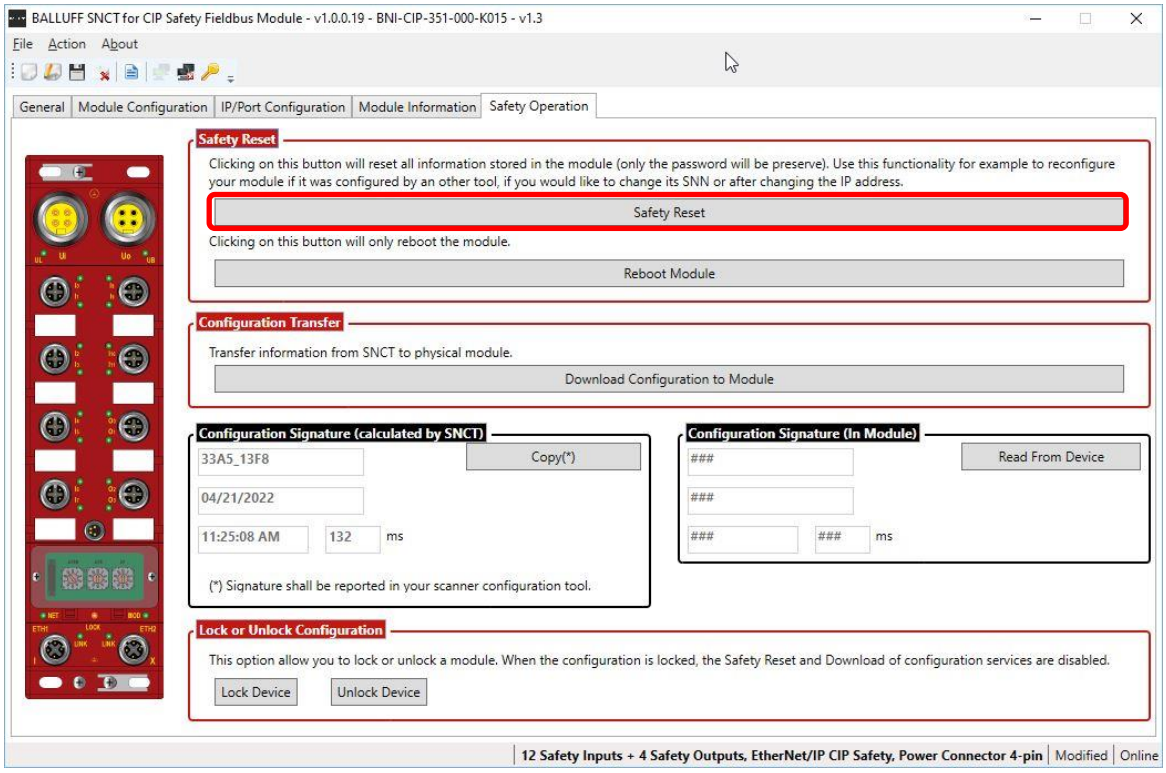
11. The SNCT detects a mismatch between the current TUNID set in the project (IP / SNN) and the TUNID stored in the physical module.



12. Select Yes and then OK.



13. Go to the *Safety Operation* tab



14. Select *Safety Reset* button

15. A notification box informs that all permanent information will be reset in the module (SNN, IP address, signature). Select Yes.

16. A notification box informs that the TUNID difference between the configured one in the project and the one in the physical module. Select Yes.

17. At this step, the SNCT is performing verification to know if:
    a. The module is locked
    b. The module has no password protection

18. If the module is locked, click on *Unlock Device* button

19. If the module is protected by a password, enter it and select *OK*. If the password is unknown, go to the section Reset Password

20. The Safety Reset service is successful.

21. Power OFF the module

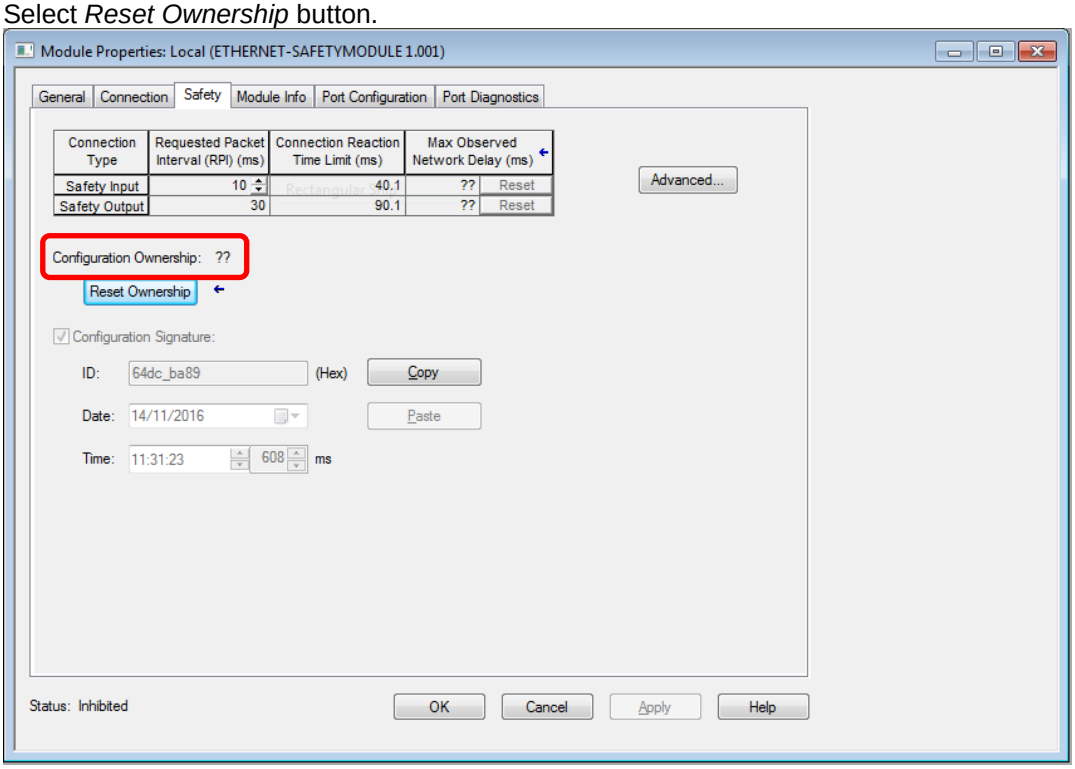
22. Go *Offline* and *Exit* SNCT

Note!
After a Safety Reset, the safety module is configured as follow:
- State: Waiting for TUNID
- Lock State: False
- IP Address: DHCP or Static (according the rotary switches position)

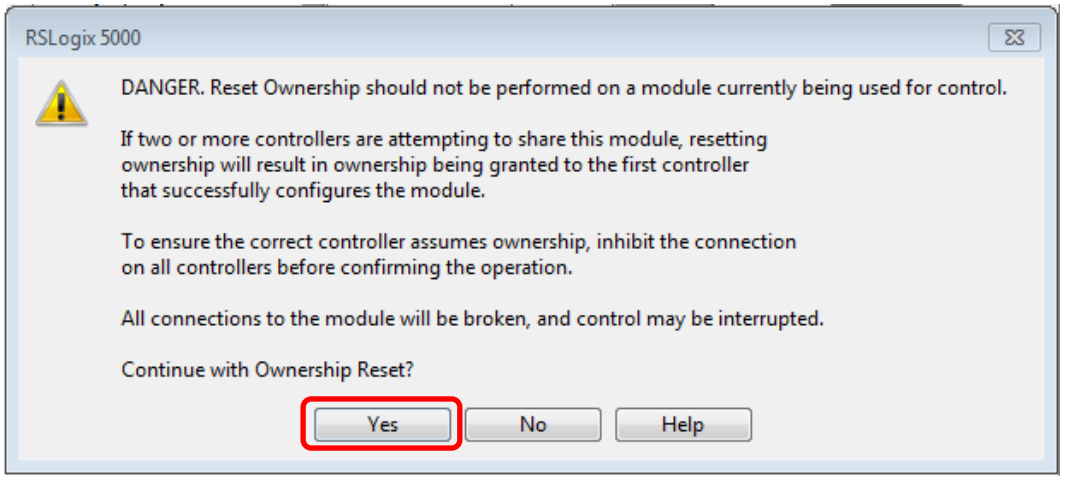
Note!
The safety reset service can also be performed using Rockwell Logix5000 / Studio5000 software.

Got to the module safety properties dialog box and select the *Safety* tab.

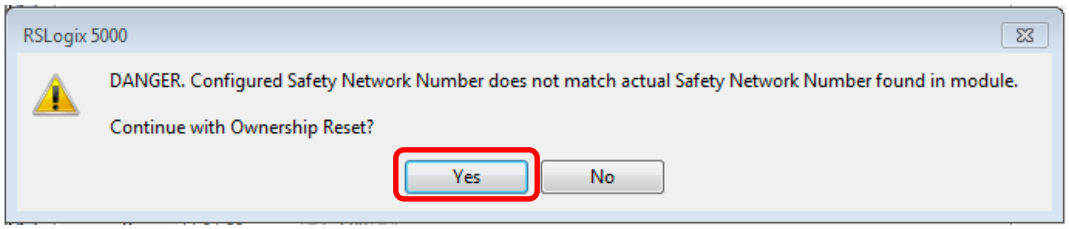
Select *Reset Ownership* button.



Select Yes.



Select Yes



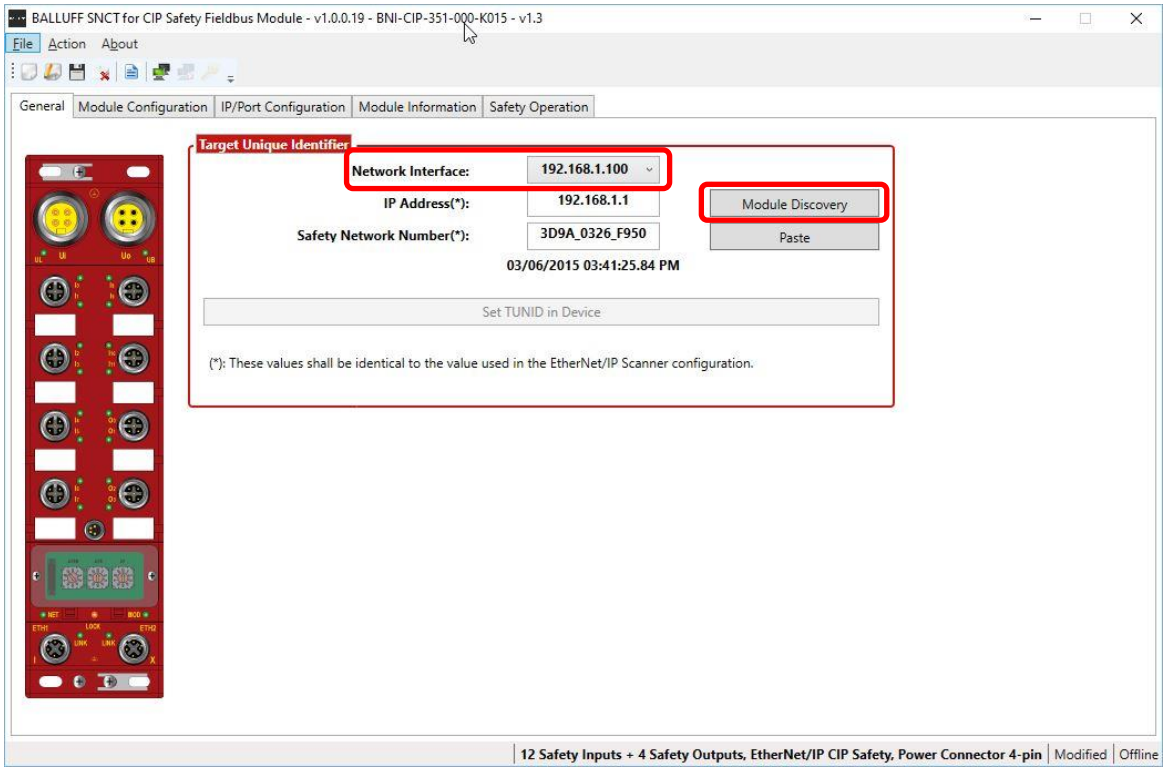
10.3. Lock / Unlock Configuration

The Lock is a feature protecting a Safe I/O Module to have its configuration modified after a commissioning by a Safety Expert body.

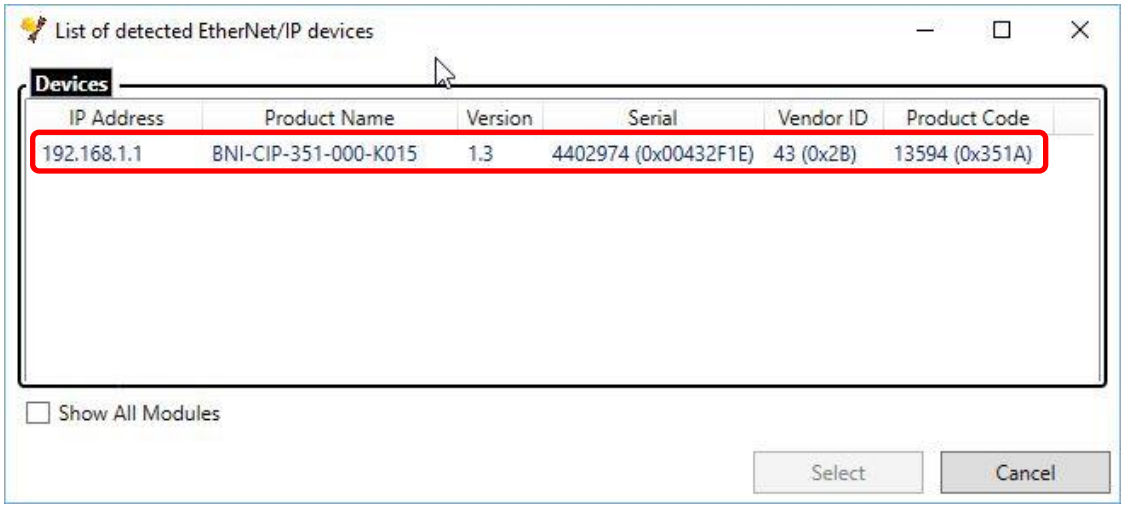
Note!
If the module is protected by Password, Lock and Unlock actions will require entering the password.

Lock a module configuration

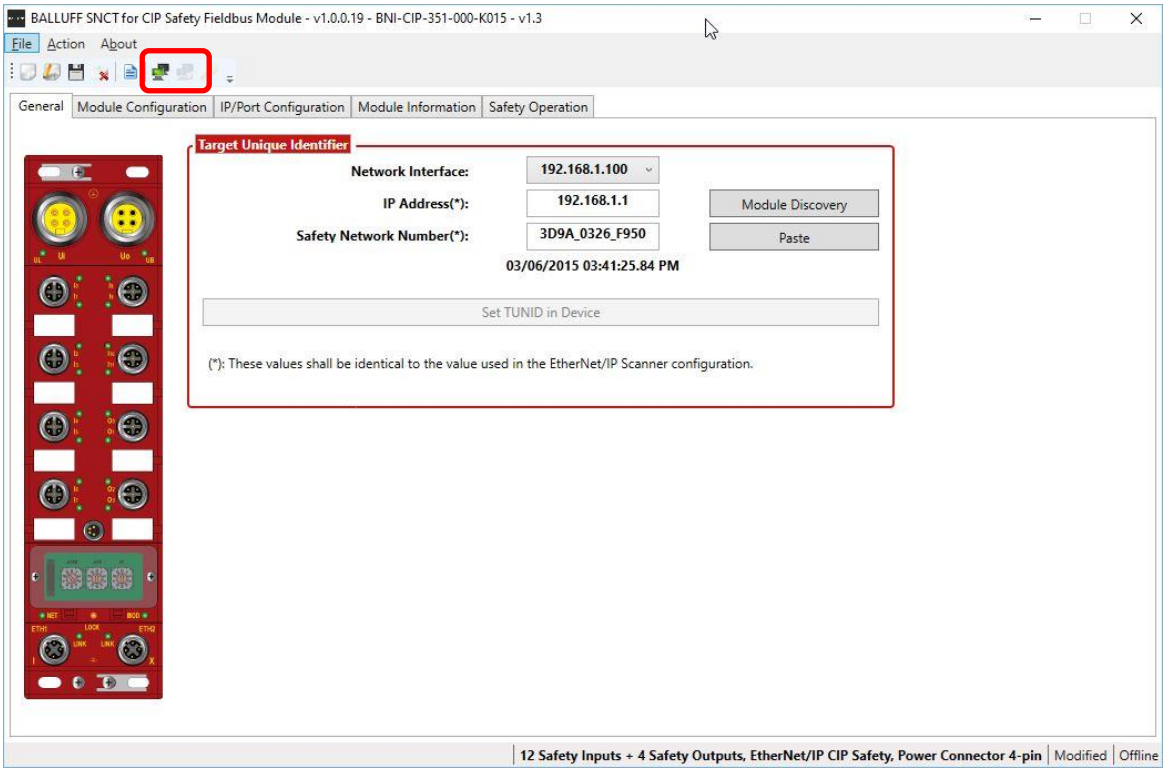
1. Launch the SNCT
2. Open the module configuration (File/Open)
3. Select the network interface
4. Perform a module discovery



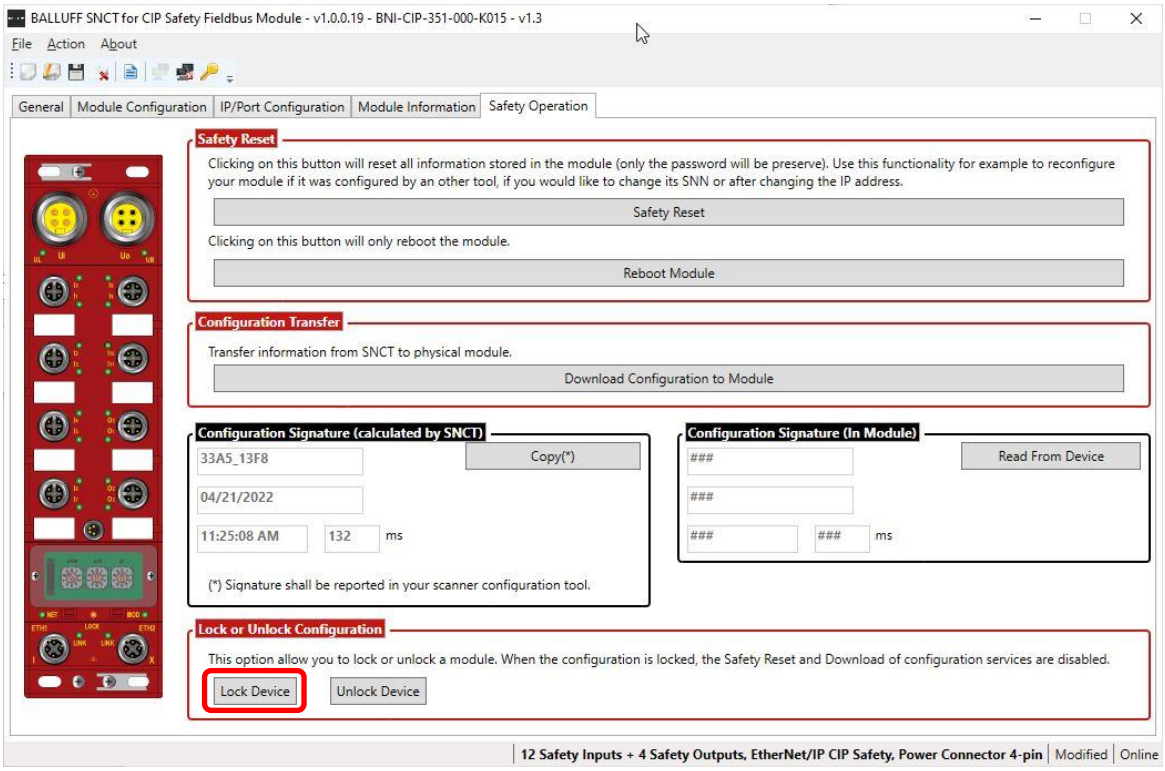
5. Double click on the module to select it.



6. Go *Online* to connect the module (Action/Online)



7. Go to the *Safety Operation* tab and Select *Lock Device* button

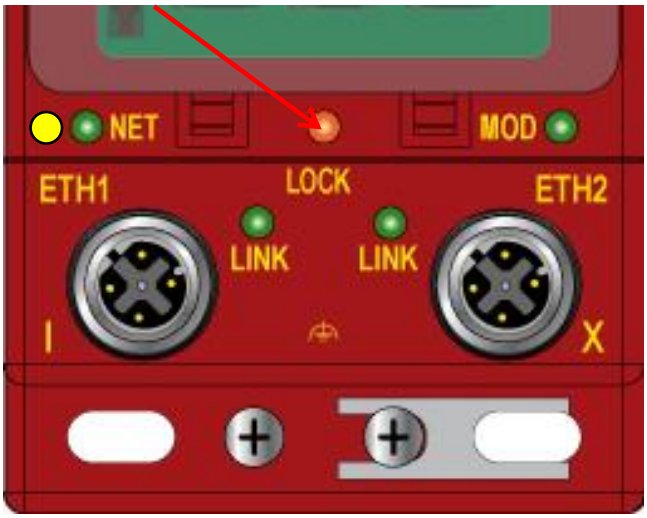


8. If the module is protected by a password, enter it and select OK. If the password is unknown, go to the section Reset Password

9. The Lock service is successful.

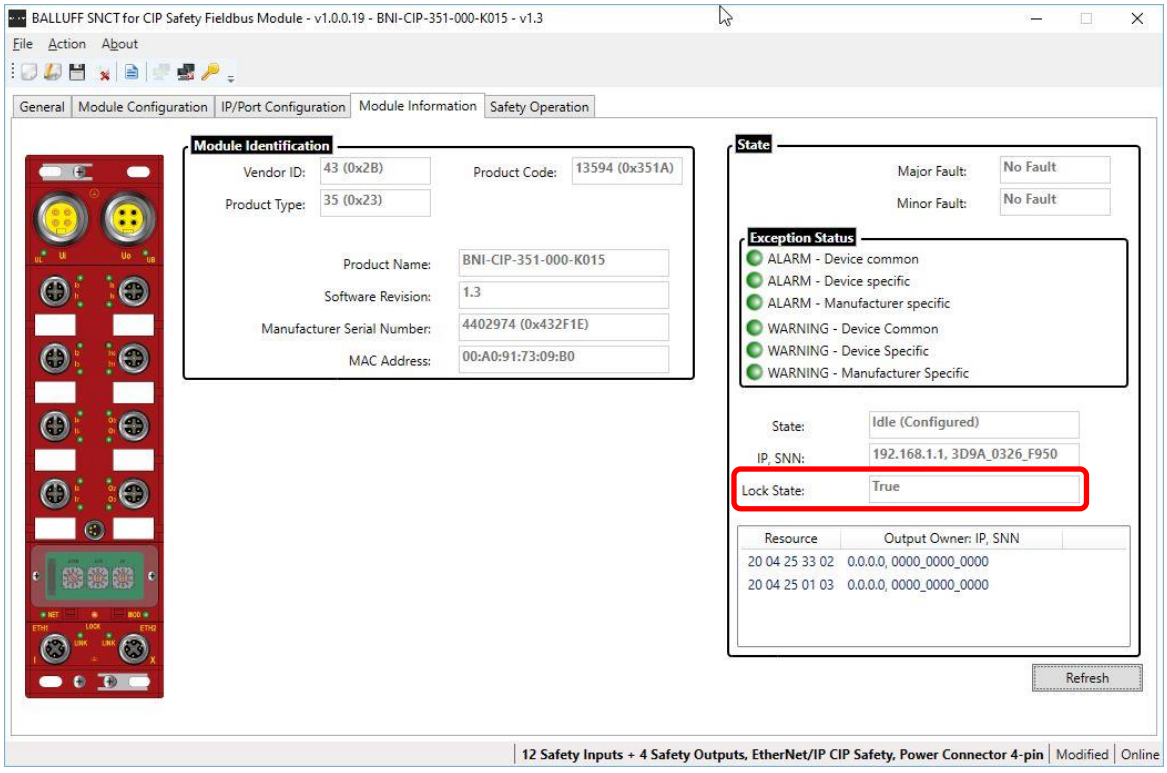
10. To verify the Lock state of the module,

    a. the Lock LED shall be solid Yellow.



or

b. Go to *Module Information* tab and click *Refresh* button to display the Lock State value

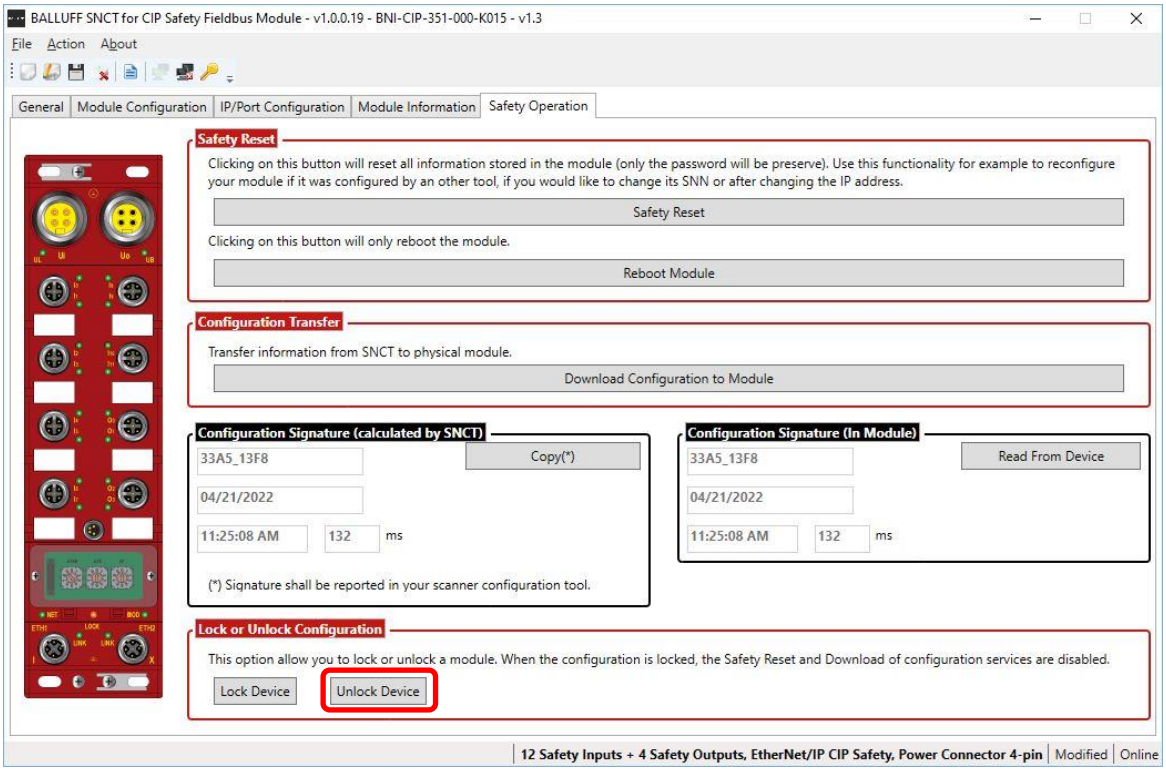


11. Go *Offline* and *Exit* SNCT

Unlock a module configuration

The steps to Unlock a module configuration are similar to the Lock procedure steps from 1 to 6.

7. Go to the *Safety Operation* tab and Select *Unlock Device* button

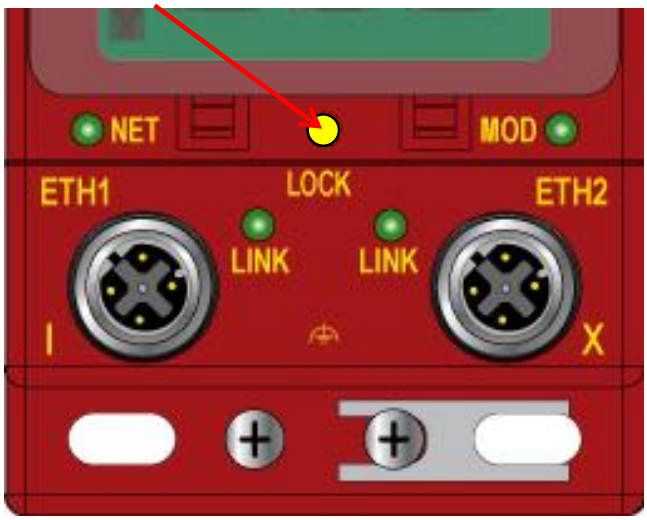


8. If the module is protected by a password, enter it and select OK. If the password is unknown, go to the section Reset Password

9. The Unlock service is successful.

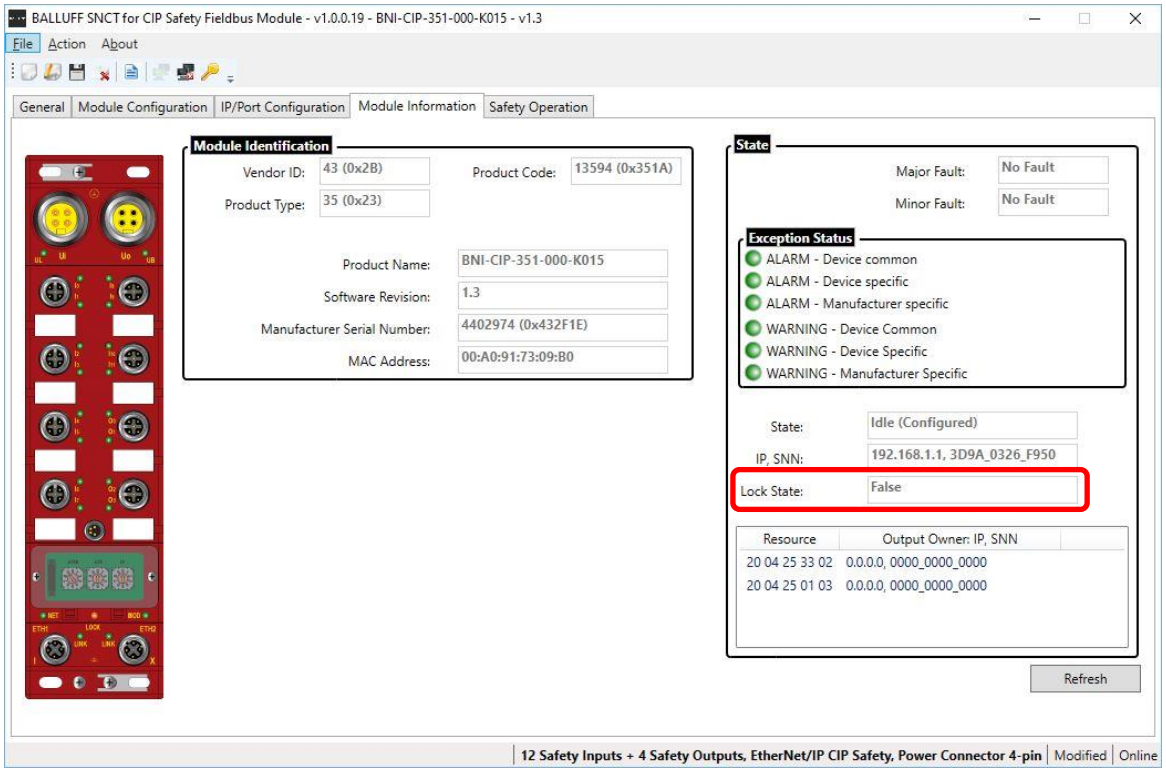
10. To verify the Lock state of the module,

    a. the Lock LED shall be blinking Yellow.



    or

    b. Go to Module Information tab and click Refresh button



11. Go *Offline* and *Exit* SNCT

10.4. Stored IP Address using DHCP Server

To store an IP address to an out-of-box module launch a *DHCP Server* application to manage the IP address configuration.

Start the SNCT tool. Create or open a project. Select the network interface. Enter IP address of the module or perform a module discovery and select the module.

1. Go *Online*
2. Go to *Module Information* tab and click on *Refresh*. Verify that the module is in “Waiting for TUNID” (if the module is really in out of box state that will be the case). If it not the cases you will not be allow to change IP of the module, so you will need to do a safety reset and restart the procedure at the step #1.
3. Go in *IP/Port Configuration* tab, click on the *Refresh* Button.
4. In *Configuration Control*, click on the *Change* Button
5. In the box, select *Static* and click Ok.
6. Modification is applied immediately and a message “Modification done with success” is displayed.
7. Click Ok
8. In Interface Configuration, click on the Change Button.
9. Provide the new IP address and network mask.
10. Modifications will be immediately applied.
11. SNCT will go Offline and then go Online automatically with the new IP address.

Note!
Due to the new IP address, a warning could be displayed indicating that configuration parameters are different between configuration and module.

10.5. IP Address Conflict

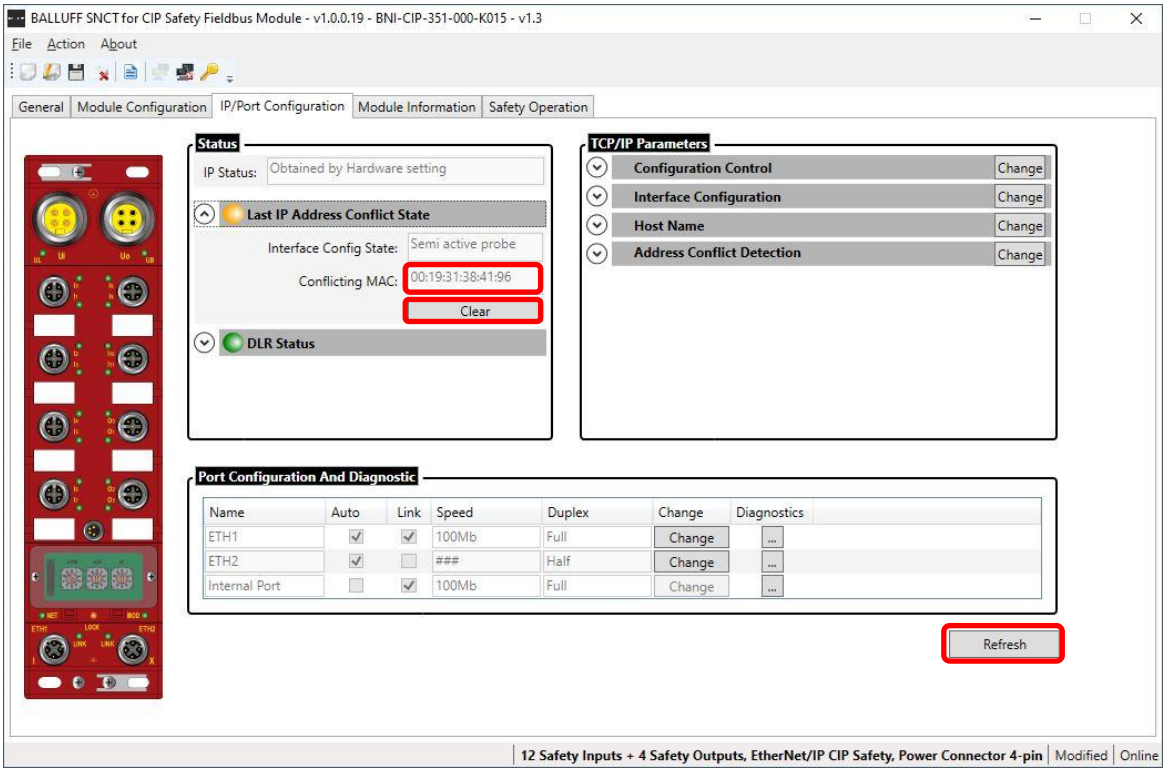
In case of IP conflict between the Safe I/O Module and other TCP/IP devices on the network, the module will be able to detect this issue (if ACD feature is enabled). The module will stop by itself to communicate on the network after detecting the problem.

Note!
In this case LED on the module will be **NET** = RED – **LOCK** = RED – **MOD** = RED Blinking.

SNCT will not be able at all to communicate with the module or a warning message will be displayed.

To verify an IP conflict state follows the below procedure:

1. Modify the rotary switch to generate an IP address available on the network and restart the module.
2. Start SNCT and go Online (Action/Go Online).
3. Go in IP/Port Configuration page, click on the Refresh Button.



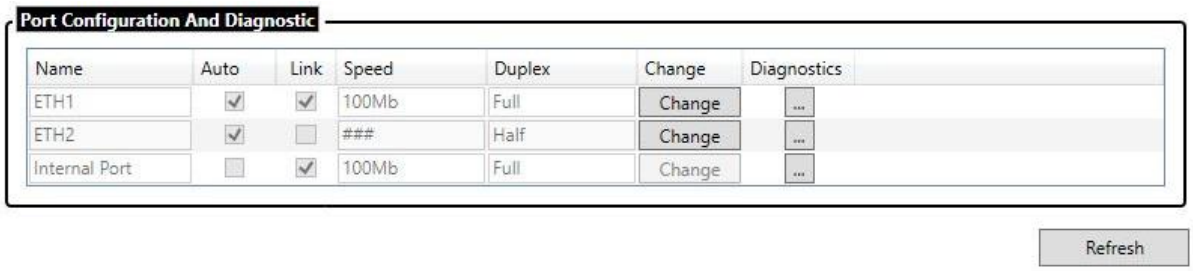
4. If the module is effectively in IP address conflict, the associated LED is yellow and the MAC address of the TCP/IP device in conflict is displayed. Click Clear Button to acknowledge the default.

10.6. Ethernet Port Diagnostics

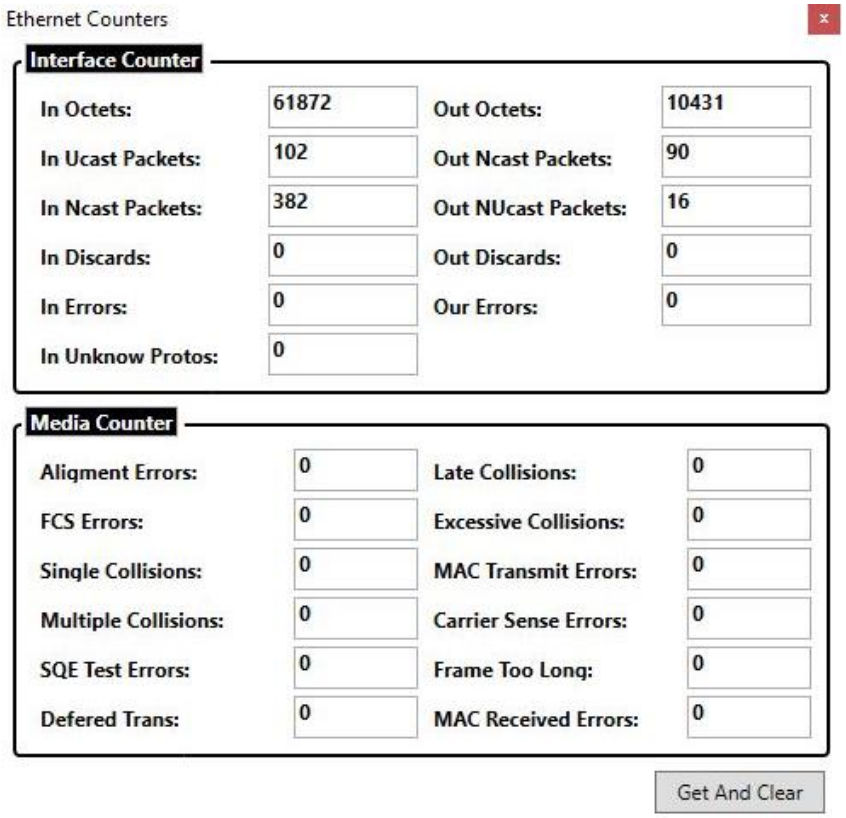
SNCT can provide diagnostic counter on each Ethernet port to monitor the traffic.

To get Ethernet port diagnostic follows the below procedure:

1. Start SNCT and Go online (Action/Go Online).
2. Go in *IP/Port Configuration* page, click on the *Refresh* Button.
3. Click on the "…" diagnostics button on the port that would like to analyze.



4. SNCT displays a dialog box with current value of the counters.



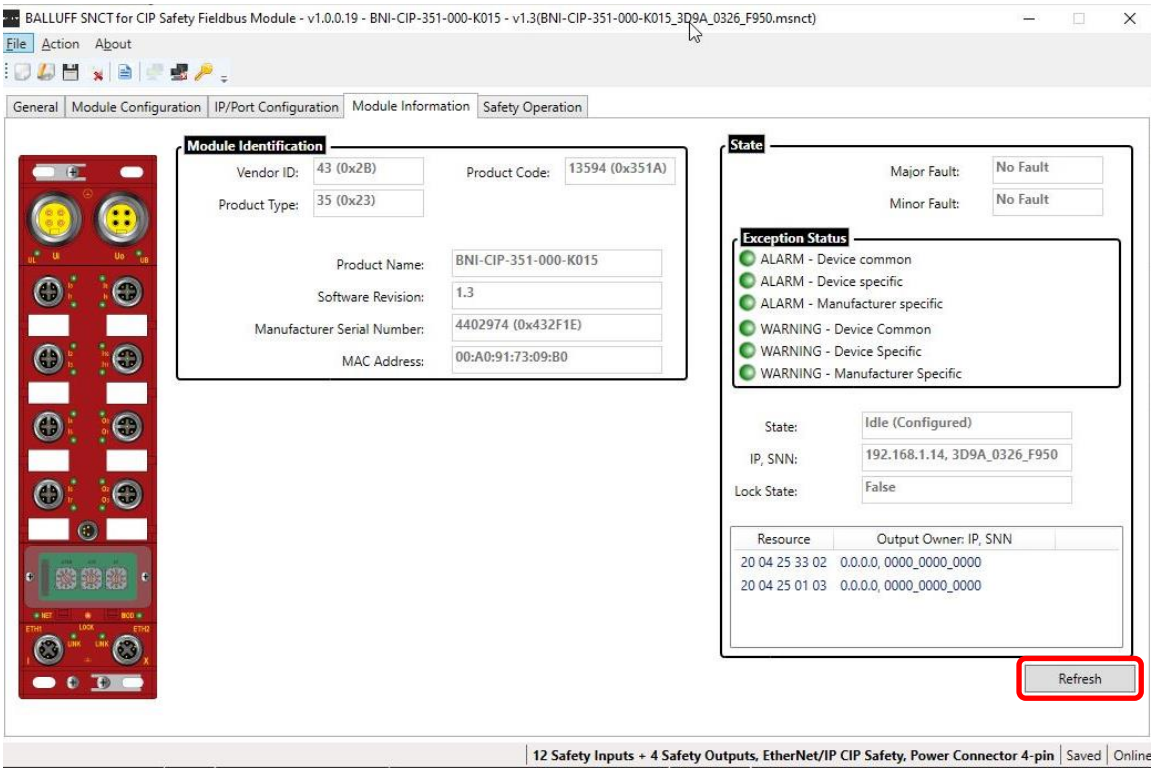
5. The counters can reset by clicking on the *Get and Clear* button.

10.7. Module Information

The module information feature allows getting data on the Safe I/O Module to monitor its current state.
To perform a module information follows the below procedure:

Note!
The procedure is based on the assumption that the module is in an unknown state but has a known IP address. If the module IP address is unknown, go to the Safety Reset section.

1. Launch the SNCT
2. Create a new project and select the module type.
3. Select the network interface.
4. Perform a module discovery and select the module.
5. Go *Online* to connect the module (Action/Online)
6. At this step, two warnings are displayed depending of the module state:
    a. TUNID configured is different from TUNID in the module (providing a TUNID is not mandatory to retrieve module Information).
    b. Parameters in the module are different from parameters in the configuration. This is normal because you have created a new project.
7. Select *Module Information* tabs and click on the *Refresh* Button.



8. SNCT displays the following information:

   - **Module Identification** provides information on the module, you will be able there to retrieved S/N of the module and module MAC address. Software Version displayed in this area provides a product version, more detailed version of the different elements that compose the module could be found in “Action\Additional Tools\Information…” (See Additional Information section)

   - **Major/Minor Fault**:
     - No fault: No problem has been detected.
     - Recoverable Fault: A fault has been detected like but not limited to:
       - Rotary switch position modified,
       - Memory key removed,
       - Safety problems on one input or output (short circuit…).

     Additional information on the problem could be found in Additional Information. You need correct the problem then restart the module to remove the fault.

     Not Recoverable Fault: A hardware major problem has been detected. You should not use any more the module, contact Balluff technical support team.

   - **State**: This value helps to known the state of the module and define the operations to do:
     - Waiting for TUNID: No TUNID is set in the module; Set one before to be able to do any other operation.
     - Configuring: Module have a TUNID but no configuration, download a configuration.
     - Idle (Configured): Module is configured and ready to execute but there is no EtherNet/IP scanner connected.
     - Executing: Module is configured and a EtherNet/IP scanner is connected.
     - Abort: Module has been triggered in safety state (see Major/Minor Fault below).

   - **IP/SNN**: This is the current TUNID affected to the module.

   - **Lock State**: Indicate if the module has been locked meaning that the module is considered as configured and tested.

   - **“Output owner”**: Indicate if an EtherNet/IP scanner owns the safety output assembly of the module.

     The first EtherNet/IP scanner that connects the output assembly will own it and only this EtherNet/IP scanner will be later authorized to connect this output assembly.

     If you would like to allow another EtherNet/IP scanner to connect the output assembly, it is necessary to perform a safety reset and reconfigure the module.

     This list show the two assembly formats:

     20 04 25 33 02: Assembly 0x0233 - Safety Discrete Output Profile

     20 04 25 01 03: Assembly 0x0301 - Vendor Specific

9. Go *Offline* and *Exit* SNCT

10.8. Set/Reset password

Set Password

The Set Password service allows protecting the use of the bellows SNCT features:

- Safety Reset
- Module Reboot
- Module Download
- Module configuration Lock/Unlock
- (Set Password)

After setting a password, this password will be requested each time one of the previous features are used.

The password is saved inside the module (and memory key) that means that the password is not link to the SNCT project but to the module. If the memory key is moved on a new module, the same password will be requested to access the features.

Warning!

Be sure to do not lose the password. Even SNCT provides a feature to Reset the password, this procedure takes time due the obligation to the contact to the Balluff technical support.

To perform a “Set Password”, follow the procedure:

1. Launch the SNCT
2. Open the module configuration (File/Open)
3. Select the network interface
4. Do a module discovery
5. Double click on the module to select it
6. Go *Online* to connect the module (Action/Online)
7. Do *Set Password* (Action/Set Password)
8. In the box:

   a. If the module does not have a password yet, let *Current Password* empty.
   b. If the module has already a password, enter current password value in *Current Password*

9. Enter the new password in *New Password* and enter it again in *New Password (Confirmation)*

10. Click OK
11. SNCT will display the message “*Password modified with success*”
12. Go *Offline* and *Exit* SNCT

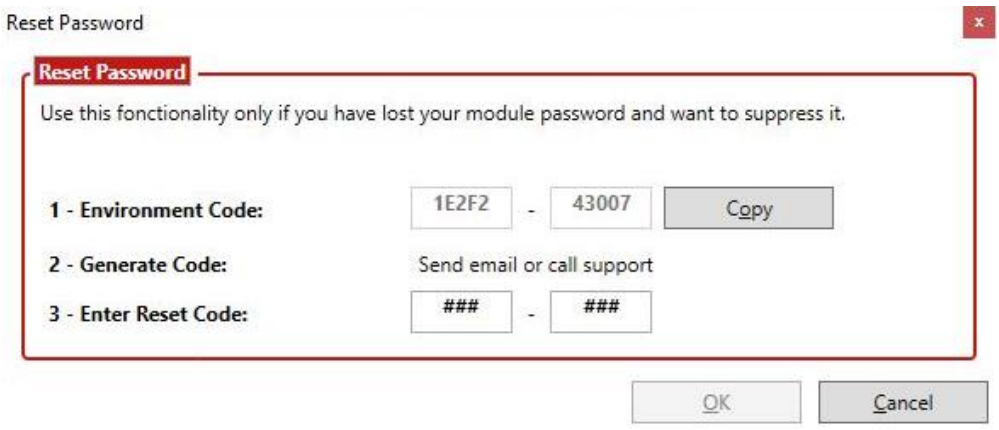
Reset Password

If the module password is lost, contact Balluff technical support to get a recovery code allowing resetting the module password.

Warning!
The Safety expert body is responsible to ensure that only authorized people have access to Balluff SNCT software to perform *Reset Password* command. Baluff does not ensure identification of the people asking a Reset code.

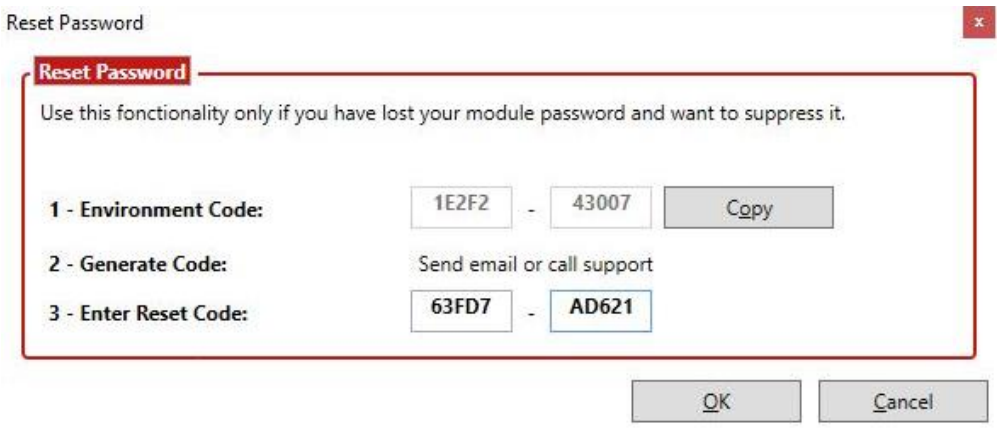
To perform a “Reset Password”, follow the procedure:

1. Launch the SNCT
2. Open the module configuration (File/Open)
3. Select the network interface
4. Do a module discovery
5. Double click on the module to select it
6. Go *Online* to connect the module (Action/Online)
7. Do Res*et Password* (Action / Additional Tools / Reset Password)



Warning!
The Environment Code is different for each module. A new Environment Code is generated after each *Reset Password* done successfully in a module, so Reset Code can used successfully only one time.

8. Visit the Balluff support site https://www.balluff.com/support. Send an email to the referenced support address:
   a. In the subject line “CIP Safety I/O Module – Reset Password Request”
   b. In the body, copy and paste the Environment Code (in this example “1E2F2-43007”)
9. Balluff Technical Support team will manage the request within the business open hours. A Reset Code will be provided in around 24h after reception of the request.
10. At reception of the answers redo operation 1 to 7 and then replace the ### in the *Enter Reset Code* fields by the received value:



Click OK.

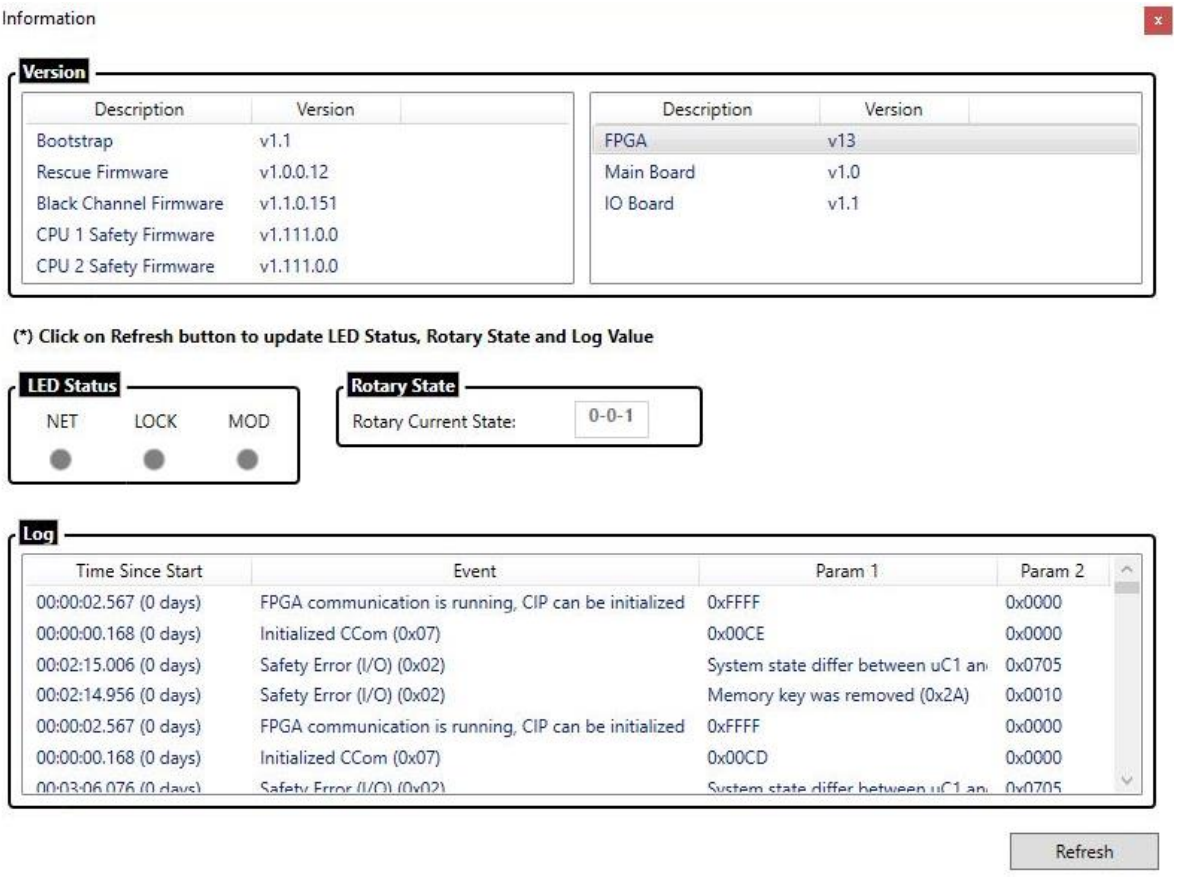
11. If the Reset Password is successful, a message will display "*The password has been correctly removed. It is recommended to set a new password in the module*".

10.9. Additional Information

The module additional information allows getting advanced information of the module.

To get additional information, follows the below procedure:

1. Launch the SNCT
2. Create a new project of the same model of the module
3. Select the network interface
4. Perform a module discovery and select the module
5. Go *Online* to connect the module (Action/Online)
6. At this step, two warnings are displayed depending on the module state:
    a. TUNID configured is different from TUNID in the module (providing a TUNID is not mandatory to retrieve module Information).
    b. Parameters in the module are different from parameters in the configuration. This is normal because a new project has been created.
7. Click on *Information* in the menu *Action/Additional* tools
8. SNCT will display this information's:



- **Version**: This section gives all the versions of the different firmware and hardware components.
- **LED Status**: Reflect the current state of the LEDs.
- **Rotary State**: Reflect the current positions of the 3 rotaries.
- **Log**: This area contains the log messages stored in the module memory. The first message is the most recent one. The messages are time stamped; time is based on the power-up of the module meaning that time return to 0 at each restart of the module.

  2 special messages are generated at the restart of the module. These messages are only informative:
  - Initialized CCom (0x07) – Param 1 indicates the number (in hexadecimal) of start of the module since its manufacturing.
  - FPGA communication is running, CIP can be initialized

Note!
This page is not refreshing cyclically; Click the *Refresh* button to update the contents.

10.10. Download Firmware

The feature allows updating the I/O Module firmware.

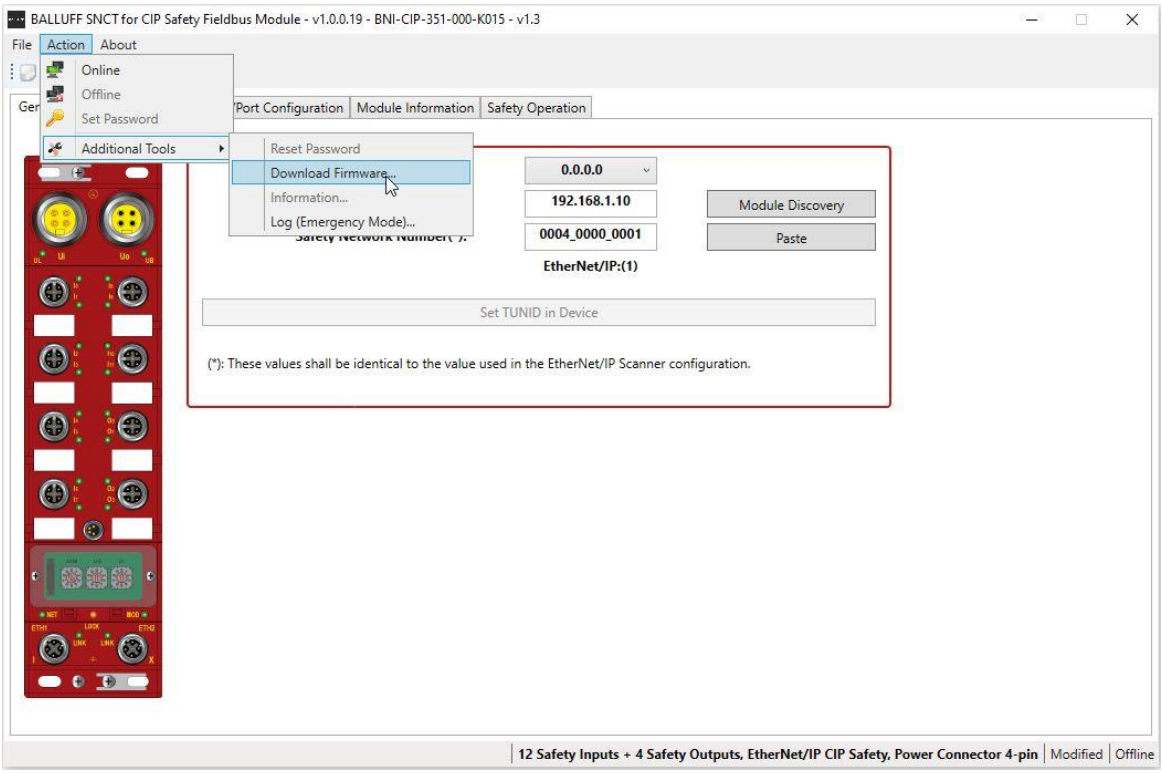
Note!
This procedure doesn't delete the configuration parameters stored in the Safe I/O Module.

Warning!
It is highly recommended to use a point-to-point Ethernet connection to transfer the firmware, between the computer and the Safe I/O module, to avoid disturbance during the file transfer.

Follow the below steps to download a firmware:

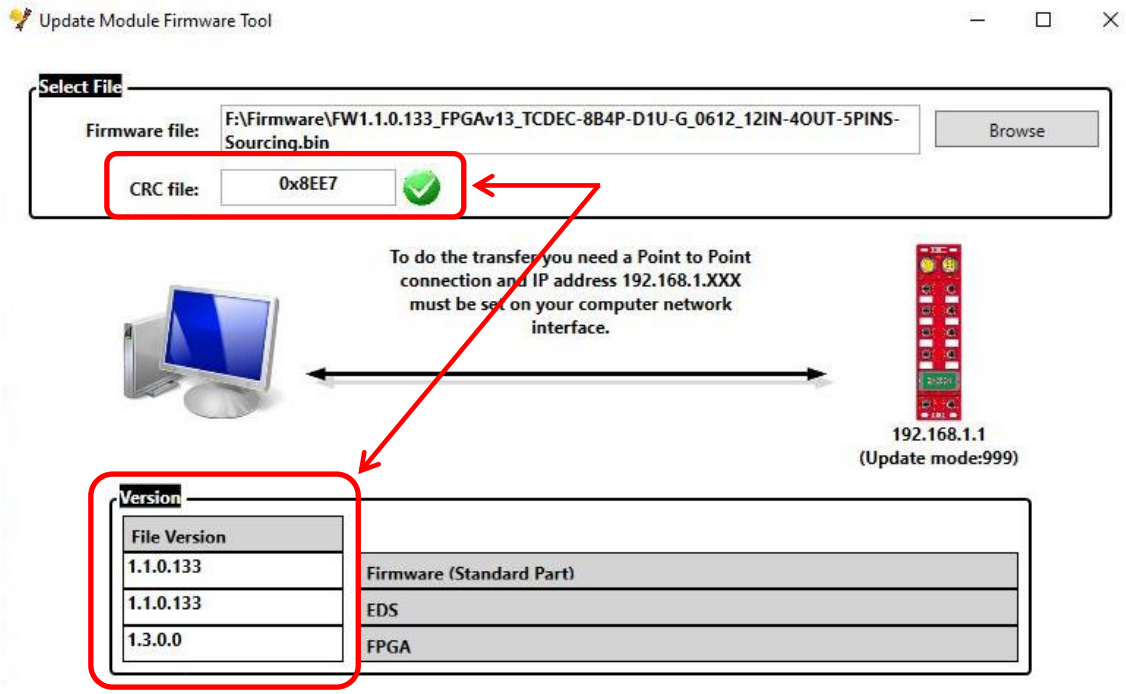
1. Set the computer network interface to **192.168.1.100**
2. Launch the SNCT
3. Open a new project (File/New)
4. Select the Safe I/O Module version

5. Select in the *Action* menu, *Additional Tools*/*Download Firmware*…

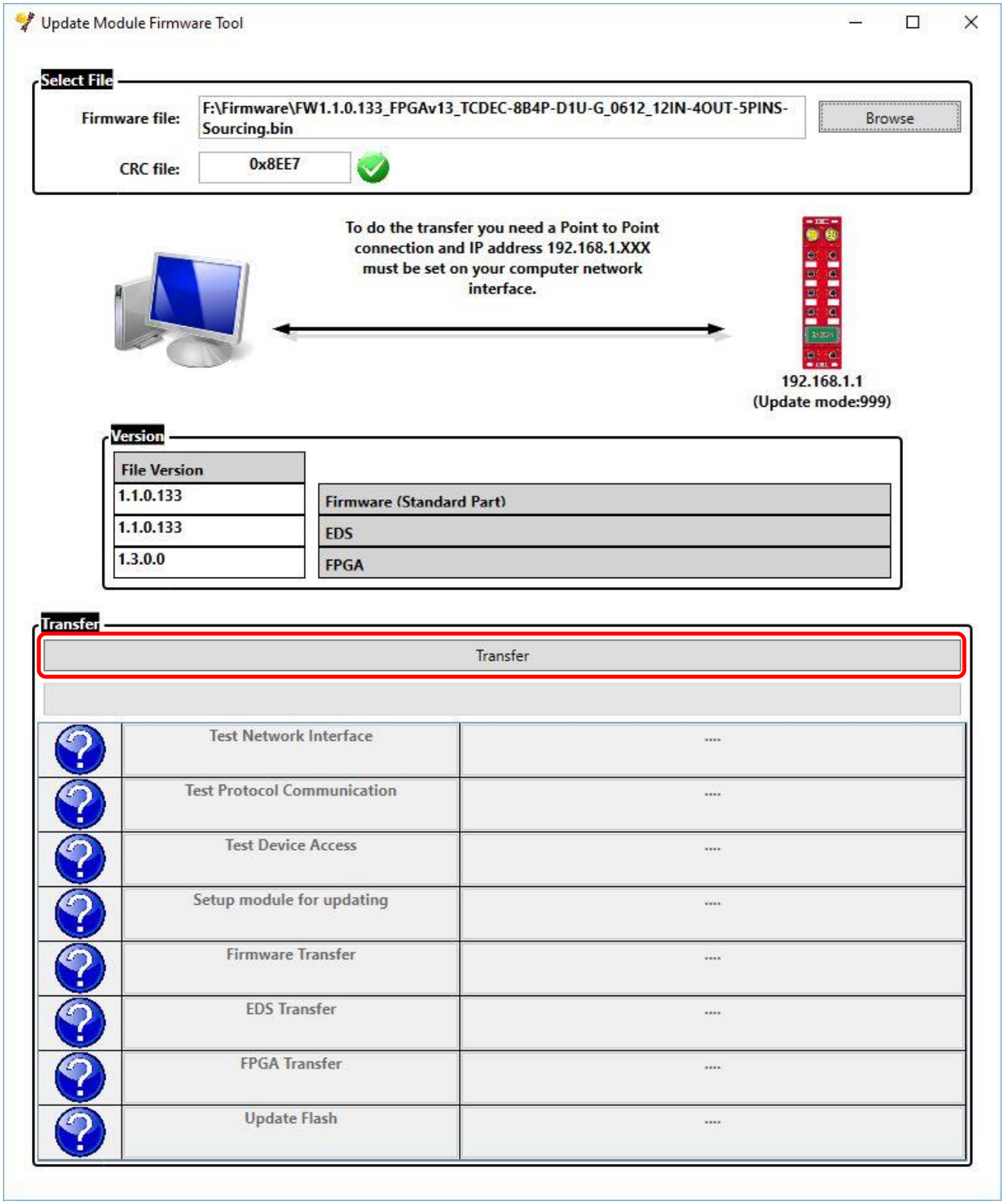


6. Browse the computer to locate the I/O Module firmware, select it and click *Open*.

7. SNCT checks the firmware CRC file and display version information.

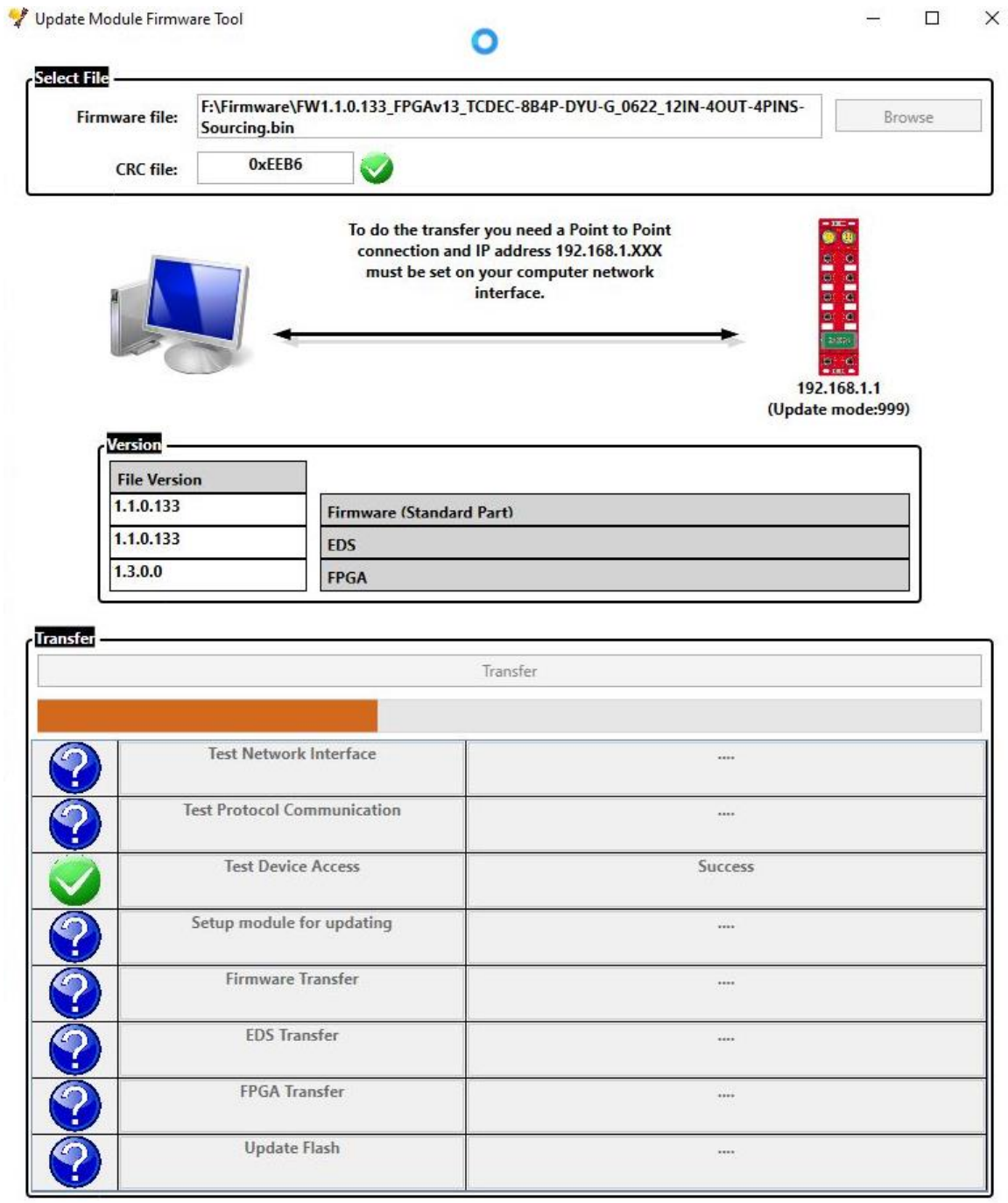


8. Click the *Transfer* button



9. Follow the instructions

10. SNCT starts the download and display information during the transfer that takes approximately 30 sec.



11. Transfer is done successfully. Follow the instructions to restart the module.

10.11. Print module configuration

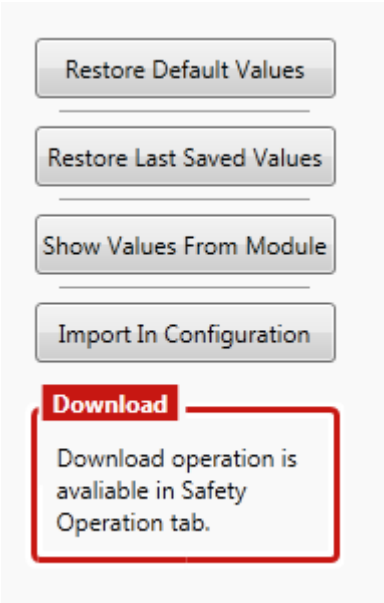
The feature allows generating a report that could be print or saved. This feature could also be used to verify that the configuration has been correctly applied to the module.

Warning!

Safety Expert body must perform safety measures to ensure that each parameter configured has been correctly applied in the module. The "*Show Value From Module*" feature can help to display these parameters.

Print functionality could also be used. In this two cases after verifying that the configuration signature *In SNCT* are equal to the signature *In Module,* Safety Expert shall verify individually that each parameters value in the section "Safety Inputs", "Safety Input X and Safety Input Y", "Safety Outputs", "Safety Output X and Safety Output Y" have the same values.

If the configuration signatures are equal but the verification shows differences contact Balluff technical support team.

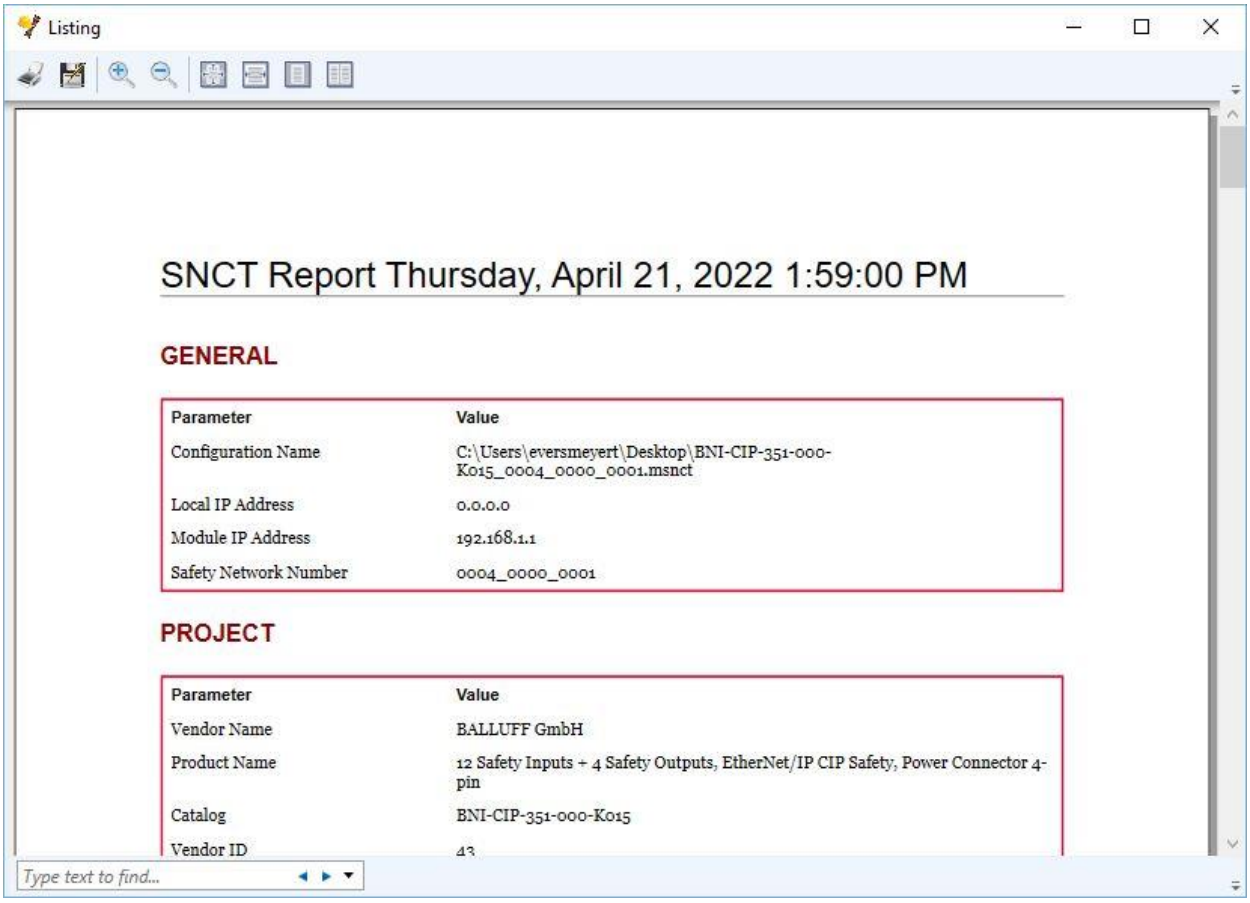


Follow the below steps to generate a listing:

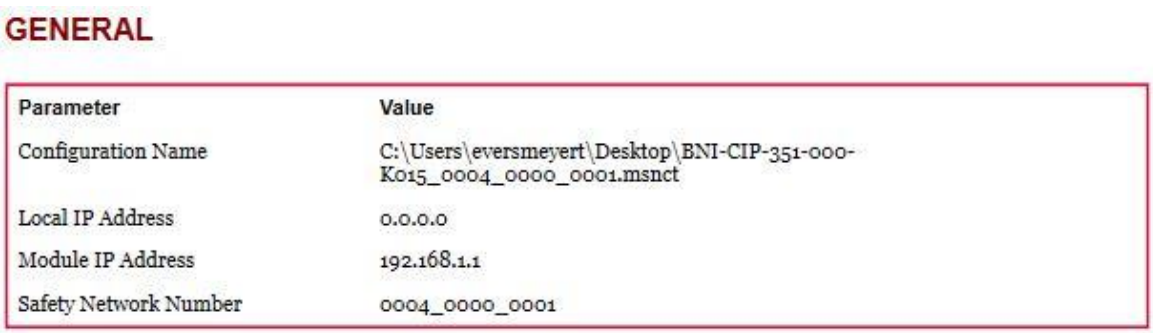
Note!
This procedure takes as hypothesis that the user has already downloaded a valid configuration in the module and has not do modification in the project since.

1. Launch the SNCT
2. Open the project.
3. Go *Online* to connect the module (Action/Online). At this step no warning message shall be generating due to the hypothesis done.

4. Generate the listing (*File/Print*)



5. Ensure that is the correct module by verifying in the listing the IP and SNN.



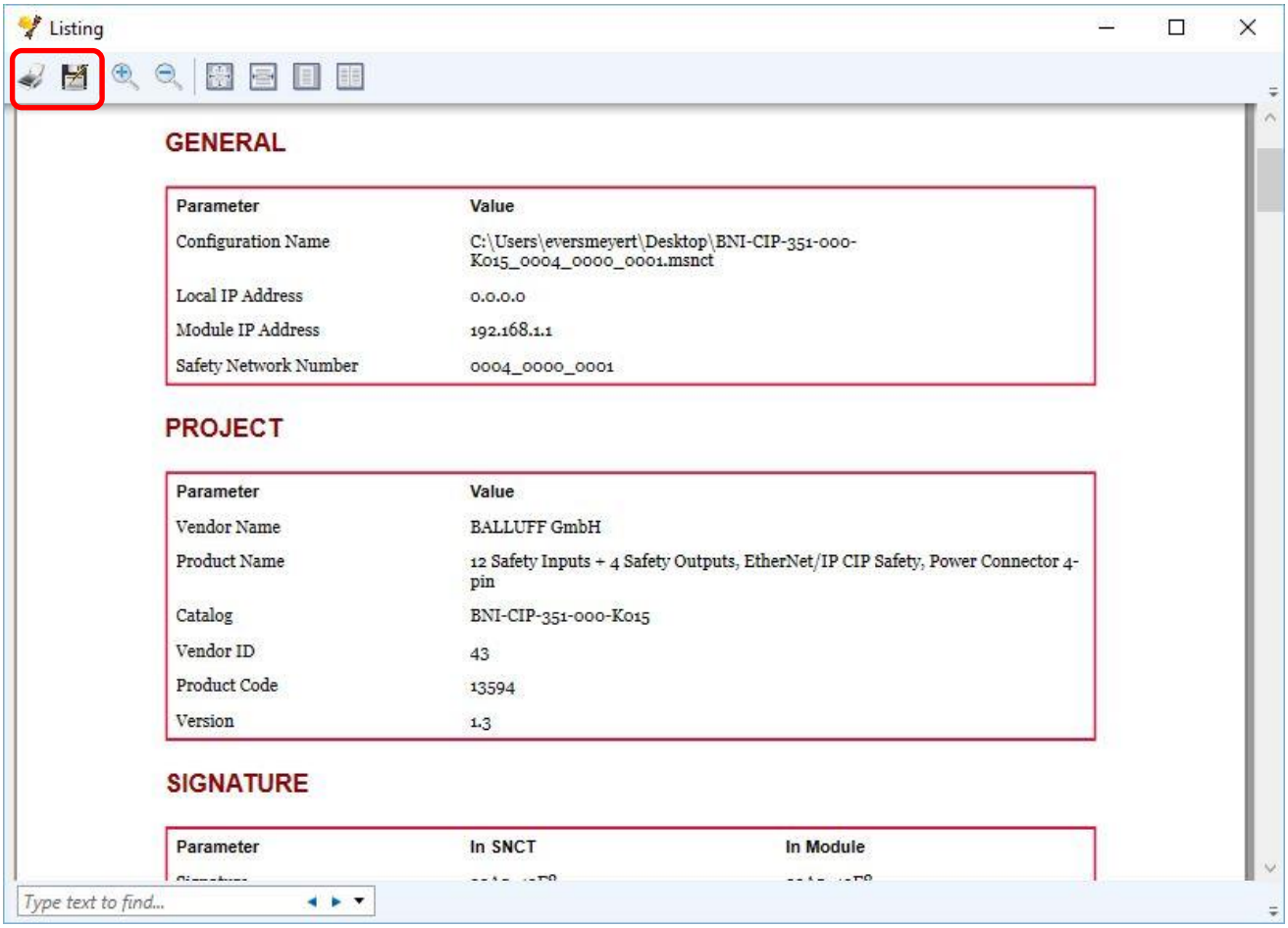
6. Compare the signatures (In SNCT / In Module) in the listing.

7. Compare each parameter in the section “Safety Inputs”, “Safety Input X and Safety Input Y”, “Safety Outputs”, “Safety Output X and Safety Output Y”

Note!
Values rounded below are value set in the configuration assembly and are described in the section “Safety I/O data mapping / Configuration Data”.

Parameter	In SNCT	In Module	Unit
Input Operation Type	0 - Single	0 - Single	
Discrepancy Time	10	10	x10ms
Input Io OffOn Delay	0	0	ms
Input Io OnOff Delay	0	0	ms
Input Io Mode	0 - Not Used	0 - Not Used	

8. Print or save the listing.



9. Go Offline / Close the SNCT.

10.12. Log (Emergency Mode)

This is an expert feature to retrieve the log information of the module that is not operating anymore.

Note!
This feature must be used only on request of the Balluff technical support team.

11. Product Package

This chapter details the contents of the product package.

11.1. Product package

The product package includes:

- An IP67 I/O module.
  The wiring information is available on the back label of the module.

- A memory key.
  This key is used to store the module configuration and allows a quick replacement without re-commissioning (see chapter – Product Replacement).

- An USB stick.
  The USB stick contents information important and software package to proceed to the commissioning of the module.

11.2. USB Stick

The USB stick contains important electronic material including:

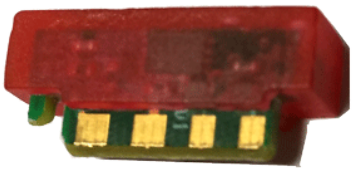
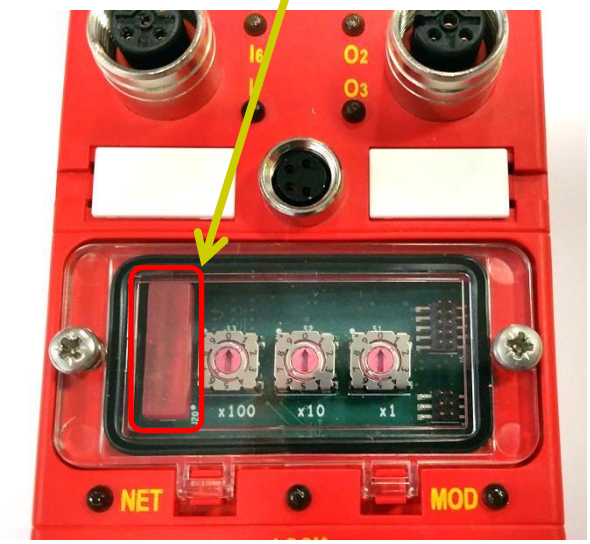
- Safety manual; this present manual.

Note!
Before starting the product deployment, it is highly recommended to read carefully the whole safety manual.

- Software Network Configuration Tool (also called SNCT)
- Safe I/O Module description files (EDS)
- Technical Notes
- CAD files

11.3. Memory Key

A memory key is delivered. The key stores all information including module parameters and "safe" and "non-safe" configuration.

Window Memory Key
Size: 18 x 6 x 7 mm 


Behavior

Warning!
Insertion and remove of the non-volatile memory key SHALL be done with the module disconnected from the power supply.

Warning!
If the non-volatile memory key is not detected (bad insertion in the connector, key removed during operation), the module is directly switching in fail safe mode and all the I/O leds will blink in red color.

Note!
The Safe I/O Module can operate only if a single key is inserted. If a second key is detected, the module is directly switching in fail safe mode and all the I/O leds will blink in red color.

12. Web Server Interface

This chapter presents the Safe I/O Module information available by connecting the module web server.

12.1. How to connect the web server

The web server interface offers the user a convenient and simple method for the diagnosis of Safe I/O Module thru a web browser (Internet Explorer, Firefox, etc…).

To do so:

- Connect the computer to the network where is located the Safe I/O Module
- Launch the web browser
- Enter the Safe I/O Module IP address in the address box of the web browser

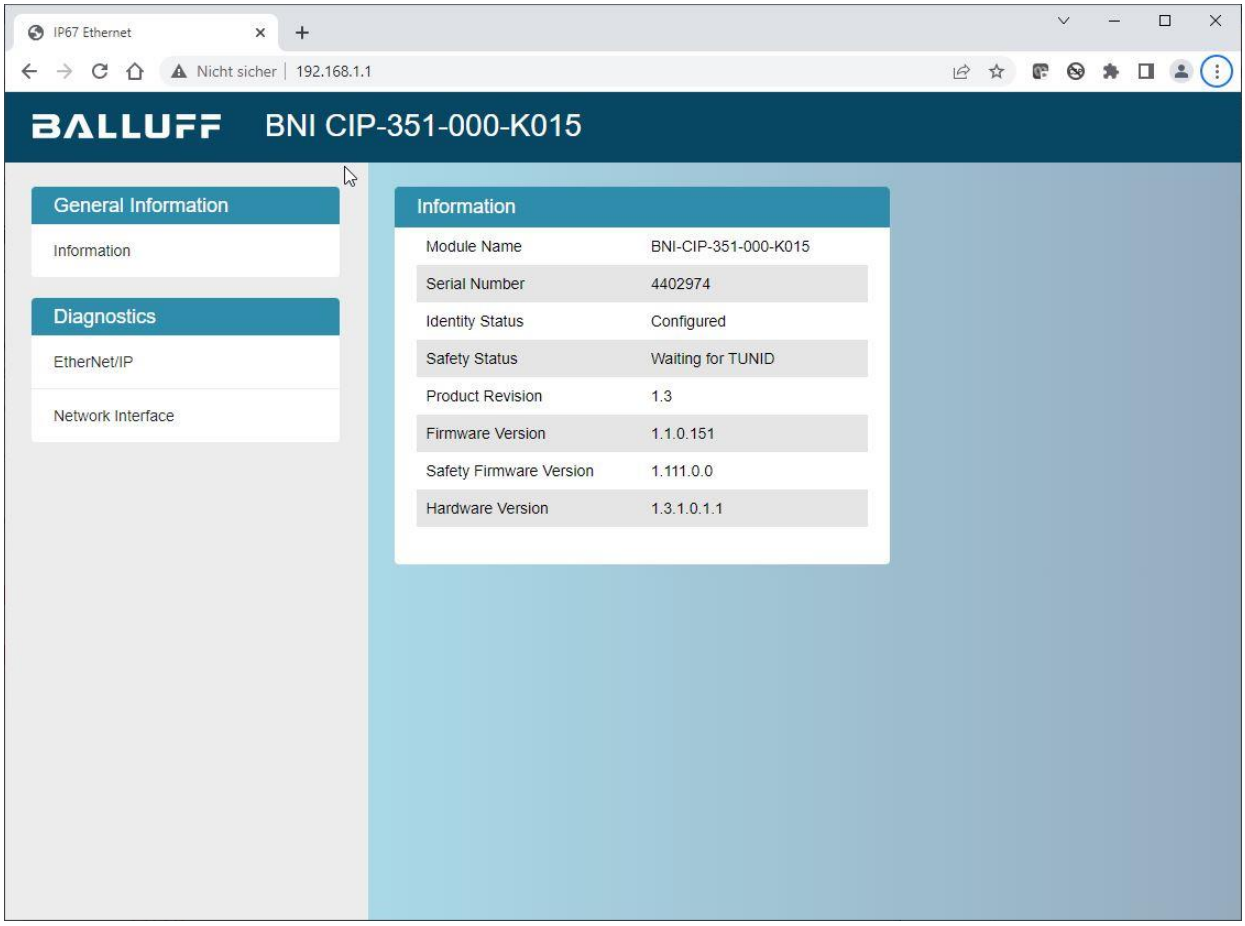
Warning!
Be careful about Internet Explorer options; parameters like “Proxy Server” can block the access to the Safe I/O Module web server interface.

Note!
There is no login and no password to access the web interface.

Note!
All the information displayed are in read only mode. It is not possible to modify the module configuration using the web server.

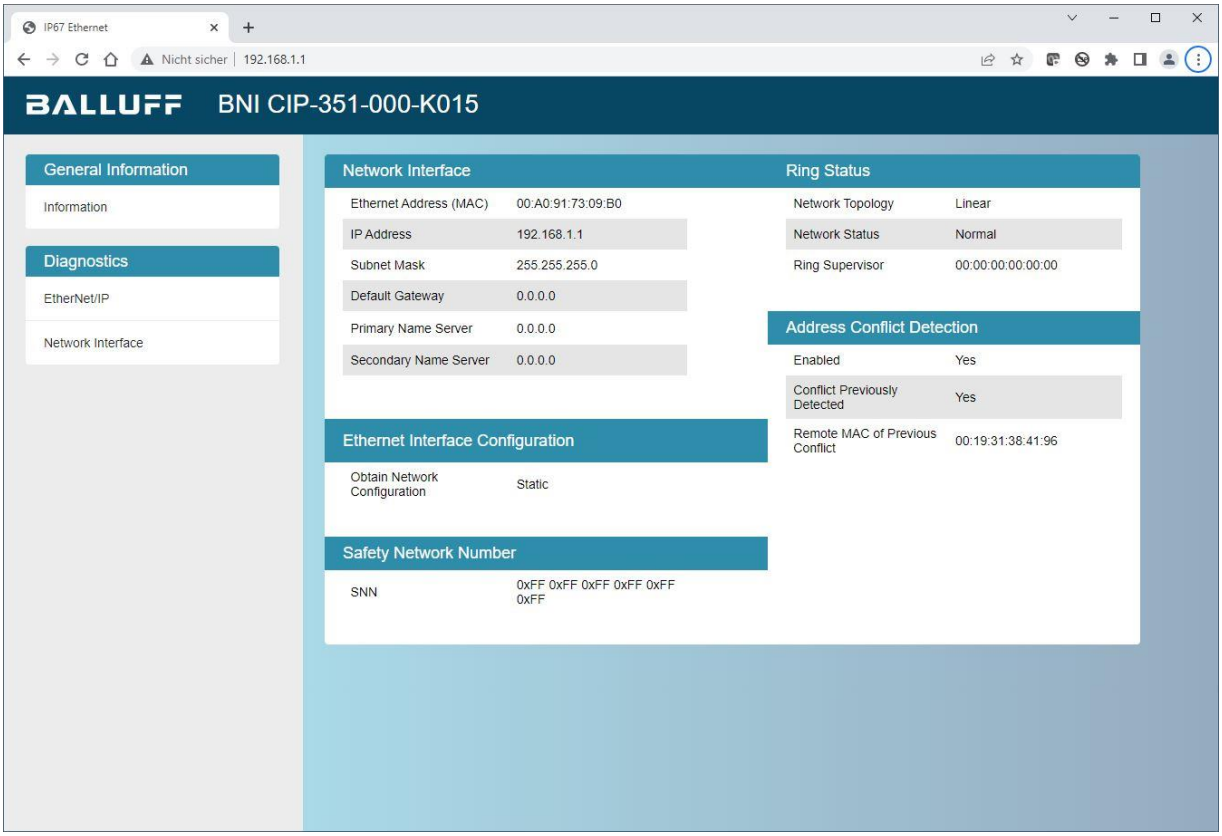
12.2. General information

This page shows the information of the Safe I/O Module.

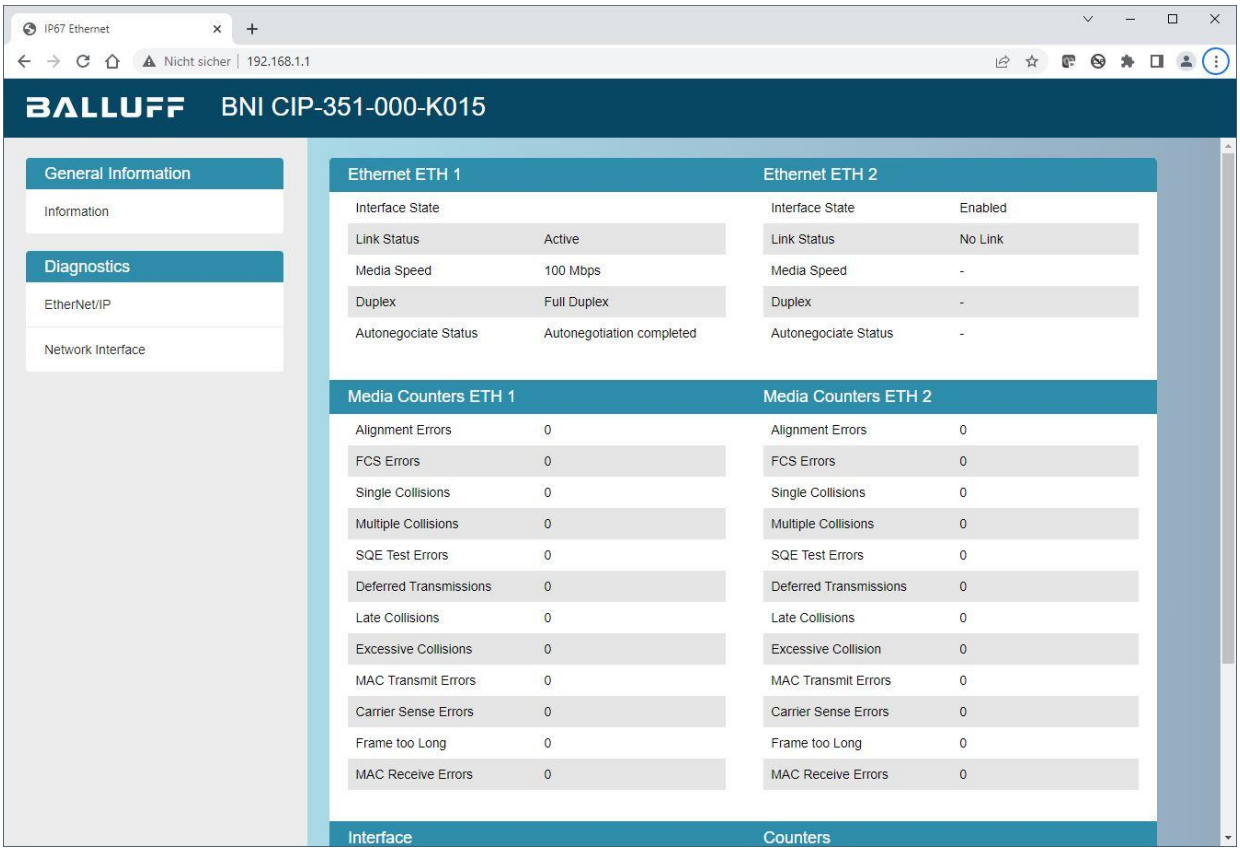


12.3. Diagnostic information

This page shows the network interface diagnostic information.



This page shows the Ethernet and EtherNet/IP diagnostic information.



13. Product Support

14.1. Warranty conditions

The warranty conditions may be found on the Balluff website: (www.balluff.com).

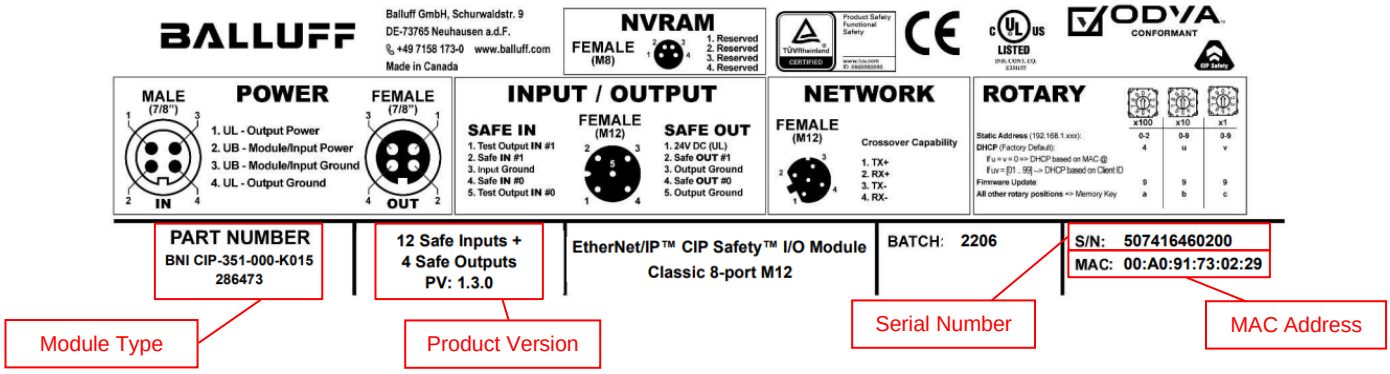
14.2. Product Information

Please ensure that the following information is available before calling for technical support:

- Module type and serial number
- Details of the issue and circumstances that may have caused the problem

Note:

The Safe I/O Module identification is located on the side and backside of the module.



14.3. Technical Support

To assist users in using the products, Balluff provides technical information on its website:

Balluff Support and Download

They can find particularly:

- Download center
- Support Request Form
- Knowledge Base
- Worldwide technical support contacts

955362_AC · EN · H22; subject to modification. Replaces G22.

innovating automation

Headquarters

Germany
Balluff GmbH
Schurwaldstrasse 9
73765 Neuhausen a.d.F.
Phone +49 7158 173-0
Fax +49 7158 5010
balluff@balluff.de

DACH Service Center

Germany
Balluff GmbH
Schurwaldstrasse 9
73765 Neuhausen a.d.F.
Phone +49 7158 173-370
service.de@balluff.de

Southern Europe Service Center

Italy
Balluff Automation S.R.L.
Corso Cuneo 15
10078 Venaria Reale (Torino)
Phone +39 0113150711
service.it@balluff.it

Eastern Europe Service Center

Poland
Balluff Sp. z o.o.
Ul. Graniczna 21A
54-516 Wrocław
Phone +48 71 382 09 02
service.pl@balluff.pl

Americas Service Center

USA
Balluff Inc.
8125 Holton Drive
Florence, KY 41042
Toll-free +1 800 543 8390
Fax +1 859 727 4823
service.us@balluff.com

Asia Pacific Service Center

Greater China
Balluff Automation (Shanghai) Co., Ltd.
No. 800 Chengshan Rd, 8F, Building A,
Yunding International Commercial Plaza
200125, Pudong, Shanghai
Phone +86 400 820 0016
Fax +86 400 920 2622
service.cn@balluff.com.cn

955362_AC/H22