Safety Systemhandbuch

Safety

Betriebsanleitung

Erstellungsdatum: 20.05.2010 | Versionsdatum: 18.08.2023 | Artikelnummer: 08-100-131-D

Herausgeber: SIGMATEK GmbH & Co KG
A-5112 Lamprechtshausen
Tel.: +43/6274/4321
Fax: +43/6274/4321-18
Email: office@sigmatek.at
WWW.SIGMATEK-AUTOMATION.COM

Copyright © 2010
SIGMATEK GmbH & Co KG

Originalsprache

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder in einem anderen Verfahren) ohne ausdrückliche Genehmigung reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Inhaltliche Änderungen behalten wir uns ohne Ankündigung vor. Die SIGMATEK GmbH & Co KG haftet nicht für technische oder drucktechnische Fehler in diesem Handbuch und übernimmt keine Haftung für Schäden, die auf die Nutzung dieses Handbuches zurückzuführen sind.

Safety Systemhandbuch

Inhaltsverzeichnis

1 Einführung 12

1.1 Allgemeine Hinweise 12

1.1.1 Verwendete Abkürzungen 12

1.1.2 Verwendete Symbole 13

1.1.3 Allgemeine Sicherheitshinweise 14

1.1.4 Bestimmungsgemäße Verwendung 16

1.1.5 Restrisiken 17

1.1.6 Besondere Sicherheitshinweise 18

1.2 Sicherheit der Maschine oder Anlage 19

1.3 Richtlinien und Normen 19

1.4 EU-Konformitätserklärung 19

1.5 Gebrauchsdauer, Verwendungszeit und Schaltzykluszeiten. 20

1.6 Verwendung von Modulen der Revision 1, Revision 2, Revision 3 und Revision 4 21

1.7 Dokumentation 22

1.8 Systemvoraussetzungen 24

2 Einführung in das C-DIAS und S-DIAS Sicherheits-System 25

2.1 Struktur des C-DIAS Safety-Systems 25

2.2 Struktur des S-DIAS Safety-Systems 27

2.3 Topologie des Safety-Systems 28

2.3.1 Generelle Topologie 28

2.3.2 Sicherheitsmodule 32

2.3.3 Sicherer Zustand 33

2.3.4 Handbediengerät ... 33
2.3.5 Safety-Interface ... 34
2.4 Kommunikation im Safety-System ... 36
2.5 Systemmerkmale ... 37
2.5.1 Konfigurationsmerkmale ... 37
2.5.2 Konfiguration des Systems ... 38
2.5.3 Änderungen am System ... 39
2.5.4 Reaktionszeit und Abschaltzeit ... 39
2.5.5 LEDs der Sicherheitsmodule ... 40
2.5.6 Diagnose ... 41
2.6 Betriebszustände ... 42
2.6.1 Post – Power On Self Test ... 43
2.6.2 Idle ... 45
2.6.3 ChkCfg – Check Configuration ... 46
2.6.4 OpTemp – zeitlich begrenzter Operational Zustand ... 47
2.6.5 Op – Operational ... 48
2.6.6 Service – Service Mode ... 49
2.6.7 Error – Fehlerzustand ... 51
2.6.8 SAI 041 – Auto-Quit ... 52

3 Installation und Montage ... 55
3.1 Montage eines Sicherheitsmoduls ... 55
3.2 Verdrahtung ... 55
3.2.1 Verdrahtungsbeispiele und Beispiele der Konfigurationserstellung ... 56

4 Inbetriebnahme und Konfiguration ... 77

4.1 Erstellen des Standard-Steuerungsprojekts 77

4.2 Erstellen der sicheren Applikation über den SafetyDesigner 77

4.2.1 Erstellen der Konfiguration 77

4.2.2 Konfiguration des Systems 78

4.3 Konfiguration über die SD-Karte 80

4.3.1 Beschreiben der SD-Karte 80

4.3.2 Konfigurieren einer Safety-CPU über die SD-Karte 81

4.4 Konfiguration eines sicheren Eingangs 82

4.4.1 Aufbau eines sicheren digitalen Eingangs 82

4.4.2 Konfiguration eines sicheren Eingangs 82

4.4.3 Beschaltungsbeispiele eines sicheren Eingangs 84

4.5 Konfiguration eines sicheren Ausgangs 94

4.5.1 Aufbau eines sicheren digitalen Ausgangs 94

4.5.2 Konfiguration eines sicheren Ausgangs 95

4.5.3 Verwendung unsicherer Freigabesignale 95

4.6 Konfiguration einer Safety-CPU 97

4.7 Berechnung der Monitoring Settings (ab Revision 2) 98

4.8 Reaktionszeit 98

4.8.1 Reaktionszeitbestimmung an einer Safety-CPU mit lokalen Ein- und Ausgängen 99

4.8.2 Bestimmung der Reaktionszeit bei einer Safety-CPU mit entfernten Ein- und Ausgängen bei Querschlusserkennung 102

4.8.3 Bestimmung der Reaktionszeit mit FSoE-Kommunikation 104

4.8.4 Fixe Zeitparameter, die Einfluss auf die Reaktionszeit haben 106

4.8.5 Konfigurierbare Zeitparameter, die Einfluss auf die Reaktionszeit haben 107

5 Betrieb 108

5.1 Abarbeiten der sicheren Applikation 108

5.2 Bedienung des Validierungstasters 108

5.2.1 Erklärung der einzelnen Sequenzen 109

5.3 Diagnose im Fehlerfall 113

5.3.1 Diagnose über die LEDs 113

5.3.2 Diagnose über den SafetyDesigner 114

5.3.3 Fehlerbehandlung 115

5.3.4 Fehler an sicheren Eingängen 116

5.3.5 Fehler an sicheren Ausgängen 116

5.3.6 Fehler beim Verteilen der Konfiguration 118

6 Änderungen am System 121

6.1 Update von Sicherheitsmodulen 121

6.2 Änderung der Konfiguration 121

6.3 Modultausch 122

6.3.1 Tausch einer Safety-CPU 123

6.3.2 Tausch eines sicheren Eingangs- bzw. Ausgangsmoduls 123

6.3.3 Tausch mehrerer sicherer Eingangs- bzw. Ausgangsmodule 123

6.3.4 Tausch sicherer Eingangs- bzw. Ausgangsmodule bei den Safety-Modulen SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211 123

6.4 Hinzufügen eines Sicherheitsmoduls 124

6.5 Entfernen eines Sicherheitsmoduls 124

6.5.1 Sicheres Eingangsmodul wird entfernt 124

6.5.2 Sichere CPU wird entfernt 125

6.5.3 Sicheres Ausgangsmodul wird entfernt 125

7 Besonderheiten im System 125

7.1 Verwendung optionaler Module (ab Revision 2) 125

7.2 Sicherheitsmaßnahmen und -hinweise 127

7.3 Verwendung von Interface-Variablen (ab Revision 2) 128

7.4 Master- und Slave-Mechanismus beim Modul SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211 128

7.5 Verwendung der Module SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211 im Standalone-Betrieb 129

7.6 Kommunikation über FSoE (Revison 4) 129

7.6.1 Was ist eine FSoE-Kommunikation 129

7.6.2 Erstellung einer FSoE-Verbindung zwischen zwei Modulen 129

7.6.3 Änderung der Werte 130

7.6.4 Watchdog-Zeit 132

7.7 Erstellung einer FSoE Verbindung über eine IP-Adresse 133

7.7.1 Einstellungen für die Verwendung der IP-Adresse und des Vergabeservices 133

7.7.2 FSoE-Dialog für schreibende Interfaces 135

7.7.3 FSoE-Dialog für lesende Interfaces 135

Monitoring Settings für lesende Interfaces 136

7.7.4 Ermittlung der maximalen Transmission Time 137

7.7.5 Vorteile des Vergabeservices 140

7.8 Kompatibilität der S-DIAS-Sicherheitsmodule 142

8 MDD 2000 (DIAS DRIVE 2000) 144

Allgemeine Beschreibung 144

8.2.1 Bestimmungsgemäße Verwendung 145

8.2.2 Systemvoraussetzungen 145

8.2.3 Geber ... 145
8.2.4 Sicherheitsfunktionen ... 146
8.2.5 Funktionsgerichtete Regelung des Drives ... 146
8.2.6 Standalone Betrieb ... 146
8.2.7 Betrieb mit einer Safety-CPU ... 148
8.2.8 Verifizierung der Geber ... 149
8.2.9 Referenzierung der Absolut-Position ... 151
8.2.10 Ablauf der Inbetriebnahme eines Drives im Standalone-Betrieb (ohne Safety-CPU) ... 152
8.2.11 Ablauf der Inbetriebnahme eines Drives mit einer Safety-CPU ... 153
8.2.12 Ablauf Gebertausch ... 154
8.2.13 Ablauf Tausch eines Drives ... 155
8.2.14 Ablauf Tausch einer Safety-CPU ... 156
8.2.15 Bremsentest ... 157
8.2.16 Beispiel zur Erstellung einer Konfiguration im Standalone-Betrieb ... 158
8.2.17 Beispiel zur Erstellung einer Konfiguration zusammen mit einer Safety-CPU ... 164

9 Wartung und Außerbetriebnahme ... 171

9.1 Allgemeines ... 171
9.2 Voraussetzungen ... 172
9.3 Anforderungen an den Netzwerkbetreiber ... 172

10 Konformitätserklärung ... 173

11 Zertifikat S-DIAS I/O System mit internem Bus ... 175

12 Anhang A: Fehlerbehandlung ... 176

13 Anhang B: Fehlerbehandlung MDD2000.....282

Verzeichnis der Bilder

Bild 1 Aufbau der Betriebsanleitung ... 23
Bild 2 Architektur einer dezentralen Steuerung ... 25
Bild 3 Safety Communication ... 26
Bild 4 Architektur einer dezentralen Steuerung ... 27
Bild 5 Architektur einer dezentralen Steuerung ... 28
Bild 6 Beispiel eines Safety-Systems ... 30
Bild 7 Anschluss eines Handbediengerätes ... 33
Bild 8 Anschluss eines HGW ... 34
Bild 9: Zustände eines Moduls ... 42
Bild 10: Zustand POST ... 43
Bild 11 Safety-CPU im POST ... 44
Bild 12 Safety-CPU im Idle Mode ... 45
Bild 13 Safety-CPU im Check Configuration Mode ... 46
Bild 14 Safety-CPU im temporary Operational Mode ... 47
Bild 15 Safety-CPU im Operational Mode ... 48
Bild 16 Safety-CPU im Service Mode ... 50
Bild 17 Safety-CPU im Error-Mode ... 51
Bild 18 Schematischer Aufbau der Bearbeitungsmaschine ... 57
Bild 19 C-DIAS Hardwareaufbau ... 59
Bild 20 S-DIAS Hardwareaufbau ... 60
Bild 21 Hardwaretree des Beispielprojekts 2 ... 63
Bild 22 Konfiguration des Starttasters S1_A ... 63
Bild 23 Lokales Netzwerk SafeCPU ... 64
Bild 24 Netzwerk 2 ... 65
Bild 25 C-DIAS Hardwareaufbau des Beispiels 3 ... 66
Bild 26 S-DIAS Hardwareaufbau des Beispiels 3 ... 67
Bild 27 Mögliche Sicherheitsapplikation ... 67
Bild 28 C-DIAS Ansteuerung einer Muting-Lampe ... 68
Bild 29 S-DIAS Ansteuerung einer Muting-Lampe ... 69
Bild 30 Möglicher Hardwareaufbau ... 70
Bild 31 Mögliche Sicherheitsapplikation ... 71
Bild 32 Möglicher Hardwareaufbau VARAN-System 1 ... 72
Bild 33 Mögliches Interface (Write) Bild 34 Mögliche Einstellungen ... 72
Bild 35 Mögliche Sicherheitsapplikation VARAN-System 1 ... 72
Bild 36 Möglicher Hardwareaufbau VARAN-System 2 ... 73
Bild 37 Mögliches Interface (Read) Bild 38 Mögliche Einstellungen ... 73
Bild 39 Mögliche Sicherheitsapplikation VARAN-System 2 ... 73
Bild 40 Mögliche Einstellung Speicherbereiche (VARAN-System 1) ... 74
Bild 41 Mögliche Einstellung Speicherbereiche (VARAN-System 2) ... 74
Bild 42 Einfacher fehlersicherer Ausgang ... 75
Bild 43 Zweikanaliger Ausgang ... 76
Bild 44 Aufbau eines digitalen Eingangs ... 82
Bild 45 Einkanaliges Einlesen eines Eingangs ... 85
Bild 46 Netzwerk einer einkanaligen Ansteuerung ... 85
Bild 47 Konfiguration der sicheren Eingänge ... 85

Bild 48 Einkanaliges einlesen eines Eingangs 87
Bild 49 Zweikanaliges Einlesen eines Eingangs 89
Bild 50 Netzwerk einer zweikanaligen Ansteuerung 89
Bild 51 Konfiguration der sicheren Eingänge 89
Bild 52 Schaltung einer Not-Halt-Funktion 92
Bild 53 Schematische Ausgangsschaltung 94
Bild 54 Verwendung unsicherer Freigabesignale 95
Bild 55 Hardwareklasse eines sicheren Ausgangsmoduls 96
Bild 56 lokaler Eingang - Safety-CPU - lokaler Ausgang 99
Bild 57 lokaler Eingang - Safety-CPU - lokaler Ausgang 100
Bild 58 Zweikanalig angeschlossene Sensoren 101
Bild 59 SIN: lokaler Eingang - Bus - Safety-CPU - Bus - SOUT: lokaler Ausgang 102
Bild 60 FSoE-Kommunikation 104
Bild 61 Kommandoeingabe über den Validierungstaster 109
Bild 62 FSoE Menü 130
Bild 63 FSoE-Verbindung 131
Bild 64 PropertyBrowser 133
Bild 65 PropertyBrowser 134
Bild 66 FSoE-Verbindung für schreibendes Interface 135
Bild 67 FSoE-Verbindung für lesendes Interface 135
Bild 68 Monitoring settings für lesendes Interface 136
Bild 69 Schreibendes Interface an 3 Projekten 138
Bild 70 3 schreibende Interfaces an einem Projekt 139
Bild 71 2 schreibende Interfaces an 2 Projekten 139
Bild 72 Schreibendes Interface an 50 Projekten 140
Bild 73 Connection ID Vergabeservice 141
Bild 74: Konzept bei Fernwartung 171

Verzeichnis der Tabellen

Tabelle 1 Abkürzungsverzeichnis 12
Tabelle 2 Gefahren und Warnhinweise 13
Tabelle 3 Hardwareklassenübersicht 29
Tabelle 4 LED-Beschreibung 40
Tabelle 5 Ein- und Ausgangs-LEDs 40
Tabelle 6 Validierungstaster LEDs 41
Tabelle 7 Mögliche Zustandswechsel von POST 43
Tabelle 8 Beschaltung der zentralen Sicherheitsmodule 61
Tabelle 9 Beschaltung der dezentralen Sicherheitsmodule 62
Tabelle 10 Modulzustände bezüglich der Konfiguration 97
Tabelle 11 Konfigurationsparameter einer einkanaligen Beschaltung 99
Tabelle 12 Konfigurationsparameter einer zweikanaligen Beschaltung 100
Tabelle 13 Konfigurationsparameter einer einkanaligen Beschaltung mit entfernten Sicherheitsmodulen 103
Tabelle 14 Konfigurationsparameter einer einkanaligen Beschaltung mit entfernten Sicherheitsmodulen 105
Tabelle 15 Fixe Zeitparameter 106
Tabelle 16 Einstellbare Zeitparameter 107
Tabelle 17 Validierungstaster-Befehle 111
Tabelle 18 Modulzustände und Kommandos 111
Tabelle 19 Validierungstasterkommandos 112
Tabelle 20 Permanente Fehler 115
Tabelle 21: Kompatibilität der S-DIAS-Sicherheitsbauteile 142

1 Einführung

1.1 Allgemeine Hinweise

1.1.1 Verwendete Abkürzungen

Abkürzung	Bedeutung
Hardware Tree	Graphische Darstellung des Aufbaus der Hardwarekonfiguration im Safety-Projekt
HSS	High Side Switch
Netzwerk	Graphisches Abbild des Ablaufcodes eines Safety-Moduls
PELV	Protected Extra Low Voltage, Schutzkleinspannung
Modul-Sicherheitsnummer	Weltweit eindeutige 4-Byte große Sicherheitsnummer zum Adressieren eines Safety-Moduls.
SPS-Applikation	Die Applikation in der SPS
VARAN	**V**ersatile **A**utomation **R**andom **A**ccess **N**etwork
Zykluszeit	Ist die Durchlaufzeit des Softwareteils in einem Safety-Modul, in dem folgende Aktivitäten stattfinden: Einlesen der Eingänge und im Eingangsabbild abspeichern Berechnung des Ausgangsabbildes durch die Applikation Ausgabe der Ausgänge anhand des Ausgangsabbildes Ausführen diverser Hintergrundtasks und Verwaltungsaufgaben
FSoE	Fail Safe over EtherCAT[1]

Tabelle 1 Abkürzungsverzeichnis

[1] FSoE bzw. EtherCAT sind eingetragene Warenzeichen der Firma Beckhoff Automation GmbH, Eiserstrasse 5, 33415 Verl, Deutschland.

1.1.2 Verwendete Symbole

Für die in den einschlägigen Anwenderdokumentationen verwendeten Warn-, Gefahren- und Informationshinweise werden folgende Symbole verwendet:

	Gefahr durch Stromschlag	**GEFAHR!** Beachten Sie unbedingt diesen Hinweis! Er warnt Sie vor unmittelbar drohenden Gefahren, die schwerste Körperverletzungen und Tod verursachen können und weist auf entsprechende Vorsichtsmaßnahmen hin.
	Warnung vor heißer Oberfläche	An thermisch leitenden Teilen können auf Grund der Verlustleistung hohe Temperaturen auftreten.
	Allgemeine Warnung	Beschreibt Situationen, von denen Gefahr für Leben und Unversehrtheit von Menschen ausgehen oder durch die das Produkt oder dessen Umgebung geschädigt werden kann und gibt entsprechende Vorsichtsmaßnahmen an.
	Wichtiger Hinweis	
	ESD-gefährdete Bauteile	Gefahrenzeichen für ESD-gefährdete Bauteile
	INFORMATION	Liefert Anwendungstipps, informiert über Besonderheiten und kennzeichnet besonders wichtige Textstellen.

Tabelle 2 Gefahren und Warnhinweise

1.1.3 Allgemeine Sicherheitshinweise

Dieses "Safety Systemhandbuch" ergänzt die Dokumentation. Beide Dokumente zusammen erfüllen die Anforderungen an eine Betriebsanleitung nach Maschinenrichtlinie 2006/42/EG. Laut Richtlinie 2006/42/EG ist die Betriebsanleitung Bestandteil eines Produktes.

- Bewahren Sie daher dieses Safety Systemhandbuch und das Handbuch stets griffbereit in der Nähe der Maschine auf, da sie wichtige Hinweise enthalten.

- Geben Sie beide Dokumente bei Verkauf, Veräußerung oder Verleih des Produktes weiter.

Bitte lesen sie vor jeder Handhabung eines Sicherheitsmoduls die dazu gehörigen Datenblätter, Bedienungsanleitungen und dieses Systemhandbuch gründlich durch. Für Schäden, die aufgrund einer Nichtbeachtung dieser Anleitungen oder der jeweiligen Vorschriften entstehen, übernimmt die Fa. SIGMATEK GmbH & Co KG keine Haftung.

Die technischen Daten der Sicherheitsmodule und die Hinweise zur Montage, vgl. Abschnitt 3, sind unbedingt einzuhalten.

Beachten Sie deshalb die in den folgenden Abschnitten aufgeführten allgemeinen und besonderen Sicherheitshinweise und die technischen Regeln und Vorschriften.

Technische Änderungen, die der Verbesserung der Geräte dienen, sind vorbehalten. Die vorliegende Dokumentation stellt eine reine Produktbeschreibung dar. Es handelt sich um keine zugesicherten Eigenschaften im Sinne des Gewährleistungsrechts.

Im Hinblick auf die mit der Nutzung der Maschine verbundenen Sicherheits- und Gesundheitsschutzanforderungen muss der Hersteller, bevor er eine Maschine in den Verkehr bringt, eine Risikobeurteilung gemäß Maschinenrichtlinie 2006/42/EG durchführen.

	Verwenden Sie die im Folgenden genannten Sicherheitsmodule der Serien C-DIAS und S-DIAS stets bestimmungsgemäß.
	C-DIAS: **CSCP 011 / CSCP 012**
	CSDI 161 / CSDI 162
	CSTO 081 / CSTO 082
	S-DIAS: **SCP 010 / SDI 100 / SRO 020 / STO 040**
	SCP 011 / SDI 101 / SRO 021 / SRO 022 / STO 081 / SDM 081 / SSI 021 / SIB 061 / SNC 021 / SAI 041
	SCP 111 / SCP 111-S / SCP 211
	DC 061 / DC 061-1 / DC 062 / DC 101 / DC 102 / ST 151
	HBG 0811 / HBG 0811-K / HBG 1011 / HBG 1011-1 / HBG 1011-H / HBG 1011-K / HGT 835 / HGT 835-TF / HGT 1035 / HGT 1035-H / HGT 1035-B / RBG 151 / HGT 1051 / HGW 1033-3 / HGW 0831-I / HGW 1033-32
	DRIVES **MDP/MDD 2xxx**

1.1.4 Bestimmungsgemäße Verwendung

Die durch die Sicherheitsmodule realisierten Sicherheitsfunktionen sind für den Einsatz in sicherheitsgerichteten Anwendungen im Rahmen einer SPS-Steuerung bestimmt und erfüllen alle notwendigen Anforderungen für einen sicheren Betrieb nach SIL 3 gemäß EN 62061 und nach PL e, Kat. 4 gemäß EN ISO 13849-1. Diese Sicherheitsschutzlevel beziehen sich auf 2 kanalige Anwendung. Im einkanaligen Betrieb haben manche Module geringere Sicherheitsschutzlevel. Bitte beachten Sie dazu die jeweilige EG-Baumusterprüfbescheinigungen (TÜV-Zertifikat).

Ein sicherheitsgerichtetes Minimalsystem kann beispielsweise bereits mit einem CSCP 011/012 Modul realisiert werden. Für den Betrieb von CSDI- und/oder CSTO-Modulen ist jedoch ein CSCP-Modul erforderlich.

Die Hinweise in dieser Dokumentation müssen beachtet werden.
Sicherheitsfunktionen dürfen nur von Netzteilen betrieben werden, die den Anforderungen von PELV nach EN60204 entsprechen.
Sachgemäßer Transport und sachgemäße Lagerung sind für einen einwandfreien Betrieb unerlässlich.
Installation, Montage, Programmierung, Inbetriebnahme, Betrieb, Wartung und Außerbetriebsstellung der Sicherheitsmodule **darf nur von geschultem Fachpersonal durchgeführt werden.**
Geschultes Fachpersonal in diesem Sinne sind Personen, die durch eine Ausbildung zur Fachkraft oder durch Unterweisung durch eine Fachkraft die Berechtigung erworben haben, sicherheitsgerichtete Geräte, Systeme und Anlagen unter Beachtung der einschlägigen Richtlinien und Normen der Sicherheitstechnik zu bedienen und zu betreuen. Die geltenden Umgebungsbedingungen müssen eingehalten werden.

Verwenden Sie die Sicherheitsmodule zu Ihrer und zur Sicherheit anderer Menschen nur bestimmungsgemäß.

Zur bestimmungsgemäßen Verwendung gehört auch die EMV-gerechte Installation.

Als nicht bestimmungsgemäß in diesem Sinne gilt

- jegliche an den Sicherheitsmodulen vorgenommene Veränderung jedweder Art oder der Einsatz beschädigter Sicherheitsmodule.
- der Einsatz der Sicherheitsmodule außerhalb des in dieser Bedienungsanleitung beschriebenen technischen Rahmens
- der Einsatz der Sicherheitsmodule außerhalb der in dieser Bedienungsanleitung beschriebenen technischen Daten (siehe auch die Abschnitte "Technische Daten" in der jeweiligen Produktdokumentation).

Beachten Sie ferner unbedingt die Sicherheitshinweise in den anderen Abschnitten dieser Anleitung. Diese Hinweise sind optisch durch Symbole besonders hervorgehoben.

Hinsichtlich der elektrischen Sicherheit gelten die Anforderungen der Norm EN 60204-1.

- Achten Sie zu Ihrer eigenen Sicherheit und zur Sicherheit anderer auf die Einhaltung der Umweltbedingungen.
- Der Schaltschrank und der Modulträger müssen einen korrekten Erdungskontakt besitzen.
- Trennen Sie das System immer vom Netz, wenn Wartung und Reparaturen durchgeführt werden. Prüfen Sie auf Spannungsfreiheit und stellen diese gegen wiedereinschalten sicher.

1.1.5 Restrisiken

Der Hersteller der Maschine muss bei der laut Richtlinie 2006/42/EG (Maschinenrichtlinie) durchzuführenden Risikobeurteilung die von den Sicherheitsmodulen möglicherweise ausgehenden Restrisiken berücksichtigen. Dazu gehören beispielsweise:

1. **Ungewollte Bewegungen angetriebener Teile der Maschine.**
2. **Ungewöhnliche Temperaturen, Emissionen von Gas, Partikeln, Geräuschen und Licht.**
3. **Gefährliche Berührungsspannungen**
4. **Wirkungen betriebsmäßiger elektrischer, magnetischer und elektromagnetischer Felder (beispielsweise auf Herzschrittmacher und Implantate).**
5. **Mögliche Einwirkungen von Geräten der Informationstechnik (Mobiltelefone, Smartphones usw.).**
6. **Freisetzung von nicht umweltgerechten Stoffen und Emissionen.**

1.1.6 Besondere Sicherheitshinweise

Gefahren durch spannungsführende Teile
Es gelten die Anforderungen der Norm EN 60204-1.

- Achten Sie zu Ihrer eigenen Sicherheit auf die Einhaltung der Umweltbedingungen.

Während Installation und Betrieb der Maschine besteht in besonderem Maße die von spannungsführenden Teilen ausgehende Gefahr des elektrischen Schlages. Spannungsführende Teile dürfen nicht berührt werden.

Unsachgemäße oder nicht bestimmungsgemäße Handhabung können Beschädigungen der Maschine und Personenschaden bis hin zu tödlichen Verletzungen verursachen.

Die elektrischen Anschlüsse dürfen nicht unter Spannung gelöst werden. Vor dem Lösen der Anschlüsse muss die Maschine kontrolliert abgeschaltet und von der Versorgung getrennt werden. Prüfen Sie auf Spannungsfreiheit und stellen diese gegen wiedereinschalten sicher.
Nach der Abschaltung bzw. der Trennung der Sicherheitsmodule von der Versorgungsspannung ist eine Wartezeit von 5 Minuten einzuhalten bevor spannungsführende Teile berührt oder Anschlüsse gelöst werden dürfen.
Zur Sicherheit ist die Spannung zu messen und zu warten bis diese ein Wert unter 40 Volt erreicht hat.

Nichtbeachtung der Anweisungen kann zu Schäden an der Anlage sowie zu schweren Verletzungen bis hin zum Tode führen!

Gefahren durch heiße Oberflächen
Während Installation und Betrieb können an thermisch leitfähigen Teilen (Kühlkörper) hohe Temperaturen auftreten. Vor einer Berührung ist die Temperatur dieser Teile daher zu prüfen; gegebenenfalls muss abgewartet werden bis die Temperatur auf unterhalb 40°C abgesunken ist.

Nichtbeachtung dieser Vorsichtsmaßnahmen kann zu schweren Verletzungen führen.

Es liegt in der Verantwortung des Maschinenherstellers, für den korrekten Umgang mit den Sicherheitsmodulen Sorge zu tragen und ggf. die Zugänglichkeit durch organisatorische Maßnahmen abzusichern!

1.2 Sicherheit der Maschine oder Anlage

Beachten Sie unbedingt die Sicherheitsrichtlinien, da sonst alle Gewährleistungs- und Garantieansprüche verloren gehen:

	Beachten Sie alle für den Einsatzort geltenden Regeln und Vorschriften der Unfallverhütung und Arbeitssicherheit.

1.3 Richtlinien und Normen

Die Sicherheitsmodule wurden so entwickelt, dass sie den Anforderungen der folgenden Normen erfüllen:

- EN / IEC 62061
- EN ISO 13849-1
- EN ISO 13849-2

Im Hinblick auf die Anwendung an einer Maschine hat der Anwender zunächst eine Risikoanalyse durchzuführen und dabei die folgenden Normen zu beachten:

- EN ISO 12100-1/-2 und EN ISO 14121
- EN 60204-1

Hinweis: Je nach Anwendung bzw. Art der Maschine kann die Einhaltung weiterer C-Typ Normen (z.B. Lift) erforderlich sein.

1.4 EU-Konformitätserklärung

CE-Konformitätserklärung

Die Sicherheitsmodule entsprechen den europäischen Normen für Speicherprogrammierbare Steuerungen.

- 2006/42/EG „Richtlinie des europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG“ (Maschinenrichtlinie)
- 2014/30/EU „Elektromagnetische Verträglichkeit“ (EMV-Richtlinie)
- 2011/65/EU „Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten (RoHS-Richtlinie)

Die EU-Konformitätserklärungen werden auf der SIGMATEK-Homepage zur Verfügung gestellt.

1.5 Gebrauchsdauer, Verwendungszeit und Schaltzykluszeiten

Gebrauchsdauer

Die maximale Gebrauchsdauer von allen Sicherheitsmodulen beträgt 20 Jahre. Spätestens nach Ablauf der Gebrauchsdauer muss das Sicherheitsmodul ersetzt werden. Stellen Sie daher durch geeignete Maßnahmen sicher, dass diese Anforderung erfüllt ist.

Verwendungszeit

In bestimmten Fällen, etwa bei Sicherheitsmodulen mit mechanischen Relaisausgängen, kann die Gebrauchsdauer durch die kürzere „Verwendungszeit“ reduziert werden, wenn beispielweise die maximale Anzahl der zulässigen mechanischen Schaltspiele erreicht ist. Bei Erreichen der Verwendungszeit muss die entsprechende Baugruppe ausgetauscht werden, auch wenn die Gebrauchsdauer noch nicht abgelaufen ist. Die Berechnungsformel für die Verwendungszeit wird in der jeweiligen Dokumentation angegeben.

Schaltzykluszeiten

Die Sicherheitskennzahlen (Diagnosemöglichkeiten) der sicheren Ein- und Ausgänge beruhen auf der Annahme, dass die sicheren Ein- und Ausgänge mindestens einmal pro Jahr geschalten werden.

Wenn ein regelmäßiges Schalten mit einem Intervall kleiner 1 Jahr in der Maschine nicht durch den normalen Betrieb sichergestellt werden kann, muss mindestens einmal jährlich manuell geschalten werden.

Notausschalter an Handbediengeräten müssen mindestens einmal innerhalb 30 Tage geprüft werden!

Stellen Sie daher durch geeignete Maßnahmen sicher, dass die Anforderungen hinsichtlich Gebrauchsdauer, Verwendungszeit und Schaltzykluszeiten erfüllt sind.

1.6 Verwendung von Modulen der Revision 1, Revision 2, Revision 3 und Revision 4

Die Revisionsnummern bezeichnen eine interne Unterscheidung der Hardware-Module und sind im Property-Browser der einzelnen Module ersichtlich. Die Unterscheidung ist nötig, da je nach Revision die Einstellparameter der Module (z.B. die Filterzeit) bzw. der Aufbau der Konfigurationsdaten (Daten für den Download zum Modul) unterschiedlich sind.

Module der Revision 1 sind:
- CSCP 011
- CSDI 161
- CSTO 081

Module der Revision 2 sind:
- CSCP 012
- CSDI 162
- CSTO 082
- SCP 010 mit Eingangs- und Ausgangskarten

Modul der Revision 3 ist:
- SCP 011 mit Eingangs- und Ausgangskarten

Modul der Revision 4 ist:
- SCP 111 mit Eingangs- und Ausgangskarten

Eine Vermischung der Module ist dem Anwender zwischen den C-Dias Safety Systemen sowie der SCP 010 und der SCP 011 erlaubt. Die Mischung mit dem SCP 111 ist nicht gestattet, da diese für die sicherheitsgerichtete Kommunikation das FSoE-Protokoll über VARAN benutzt. Bei einer Vermischung der Revisionen wird die Konfiguration auf Basis der Module mit der niedrigeren Revision generiert. Die Module SCP 010, SCP 011 und SCP 111 werden immer mit ihrer eigenen Revision generiert.

In den nachfolgenden Kapiteln wird der Anwender bei unterschiedlichen Arbeitsweisen zwischen den Revisionen durch folgende Beschreibung darauf hingewiesen.

	Für Revision 1 wird geschrieben **Revision 1**. Für Revision 2 wird geschrieben **Revision 2**. Für Revision 3 wird geschrieben **Revision 3**. Für Revision 4 wird geschrieben **Revision 4**.

1.7 Dokumentation

Die Dokumentation ist wie folgt aufgebaut: Das Safety-Systemhandbuch stellt das übergeordnete Dokument hinsichtlich des C-DIAS und S-DIAS Safety-Systems dar. Das LASAL-SafetyDesigner-Handbuch beschreibt die Bedienung des Konfigurationstools. Die Produktdokumentationen der einzelnen Sicherheitsmodule

- CSCP 011
- CSDI 161
- CSTO 081
- CSCP 012
- CSDI 162
- CSTO 082
- SCP 010
- SDI 100
- STO 040
- SRO 020
- SCP 011
- SDI 101
- STO 081
- SRO 021
- SRO 022
- SSI 021
- SNC 021
- SDM 081
- SCP 111
- SCP 111-S
- SCP 211
- SAI 041
- DIAS-DRIVE 2000
- Künftige Entwicklungen

beinhalten im Detail deren technische Daten sowie die erforderlichen Angaben für deren Anwendung.

Zum Einbinden des Safety-Systems in die Standardsteuerung steht das Systemhandbuch LASAL CLASS 2 der Standard-SPS zur Verfügung.

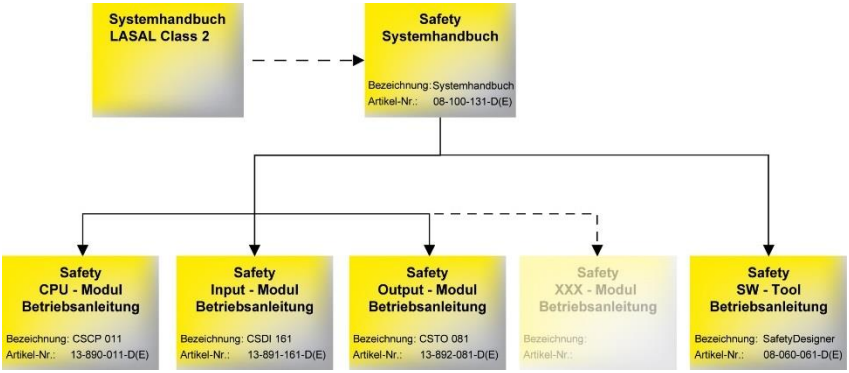


Bild 1 Aufbau der Betriebsanleitung

1.8 Systemvoraussetzungen

Die **C-DIAS-Safety**-Komponenten benötigen mindestens folgende Systemversionen:

LASAL-Betriebssystem: 01.02.076 oder höher
Hardwareklassenversion: 2.10 oder höher
SafetyDesigner-Version: 01.00.004 oder höher

Ab Revision 2:
LASAL-Betriebssystem: 01.02.190 oder höher
Hardwareklassenversion: 2.39 oder höher
SafetyDesigner-Version: 01.01.002 oder höher

Die jeweiligen Hardwareversionen der Sicherheitsmodule sind den entsprechenden Betriebsanleitungen zu entnehmen.

Die C-DIAS-Safety-Komponenten sind mit allen C-DIAS Produkten der Firma SIGMATEK GmbH & CO KG kompatibel.

Die S-DIAS-Safety-Komponenten benötigen mindestens folgende Systemversionen:

LASAL-Betriebssystem: 01.02.225 oder höher
Hardwareklassenversion: 1.0 oder höher (Klassen für SCP 010)
SafetyDesigner-Version: 01.01.003 oder höher

Ab Revision 3:
LASAL-Betriebssystem: 01.02.245 oder höher
Hardwareklassenversion: 1.0 oder höher (Klassen für SCP 011 und deren Ansteckkarten)
SafetyDesigner-Version: 01.01.007 oder höher

Ab Revision 4:
LASAL-Betriebssystem: 01.03.015 oder höher
Salamander OS: 09.01.140 oder höher
Hardwareklassenversion: 1.0 oder höher (Klasse für SCP 111)
SafetyDesigner-Version: 01.01.030 oder höher

Die Verwendung des MDD 2000 benötigt mindestes folgende Systemvoraussetzungen

Salamander OS: 09.03.190 oder höher
Hardwareklassenversion: 1.0 oder höher
Motion-Version: 1.0 oder höher
SafetyDesigner-Version: 01.01.070 oder höher

2 Einführung in das C-DIAS und S-DIAS Sicherheits-System

2.1 Struktur des C-DIAS Safety-Systems

Mit den Komponenten der Serie C-DIAS Safety wird das Steuerungssystem von SIGMATEK um Sicherheitsfunktionen ergänzt. Durch einen dezentralen Aufbau und die Modularität der Komponenten können **bestehende Anlagen einfach um Safety-Funktionen erweitert werden**. Basis der SIGMATEK Safety-Komponenten sind entsprechende Hardwarelösungen, die sich selbst überwachen, um so mögliche Fehler zu erkennen und die Maschine gegebenenfalls in einen sicheren Zustand zu bringen. **Das gesamte System entspricht den Normen** gemäß Performancelevel e (PL e) und Kategorie 4 nach EN ISO 13849 bzw. SIL 3 nach EN 62061.

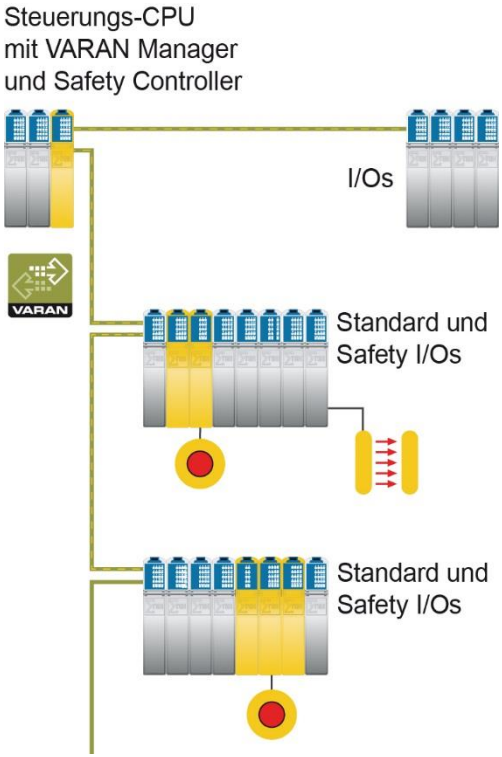


Bild 2 Architektur einer dezentralen Steuerung

Die Safety-Baugruppen sind vollständig in das Steuerungssystem integriert. **Durch den modularen Aufbau können die sicheren und nicht sicheren Systemkomponenten einfach kombiniert werden.** So lassen sich die individuellen Anforderungen unterschiedlichster Maschinentypen umsetzen.

Der Verdrahtungsaufwand reduziert sich gegenüber klassischen Sicherheitssystemen drastisch. Eine Beschreibung des Standard-Steuerungssystems ist in der Dokumentation LASAL Class 2 zu finden.

Auch für die Kommunikation ist **kein zusätzlicher Verdrahtungsaufwand** nötig. Es wird **nur ein Bussystem für sichere und nicht sichere Signale** genutzt und zwar der Ethernet-basierte, hart-echtzeitfähige VARAN-Bus (**V**ersatile **A**utomation **R**andom **A**ccess **N**etwork). Für die Kommunikation der Safety-Baugruppen wird das „Black-Channel"-Prinzip angewandt, bei dem der Bus keine sicherheitsrelevanten Aufgaben übernimmt, sondern nur als Übertragungsmedium dient. Dazu wird ein eigens entwickeltes sicheres Busprotokoll verwendet, bzw. bei der SCP 111 das FSoE-Sicherheitsprotokoll.

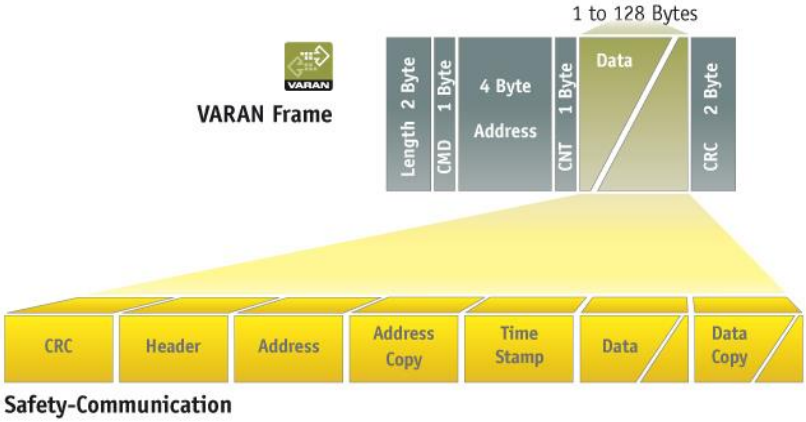


Bild 3 Safety Communication

2.2 Struktur des S-DIAS Safety-Systems

Das modulare Konzept des S-DIAS-Safety-Systems ermöglicht es, eine für den Kunden optimierte IO-Anforderung, einfach umzusetzen.

Bild 4 Architektur einer dezentralen Steuerung

Die obige Abbildung zeigt eine CPU-Einheit (hier beispielhaft: SCP 010) mit Erweiterungsmodulen (hier beispielhaft: 10 Eingänge, 4 Transistor-Ausgänge und 2 zweikanalige Relais-Ausgänge). Der minimale Aufbau besteht aus einer CPU-Einheit und einer Erweiterungsbaugruppe. Ein Standalone-Betrieb ohne Busanbindung ist möglich.

Die sicherheitsgerichtete Baugruppe erfüllt die Anforderungen nach **SIL 3** gemäß EN 62061 und **PL e, Kat. 4** gemäß EN ISO 13849-1.

Die Safety-Baugruppen sind vollständig in das Steuerungssystem integrierbar. **Durch den modularen Aufbau können die sicheren und nicht sicheren Systemkomponenten einfach kombiniert werden.** So lassen sich die individuellen Anforderungen unterschiedlichster Maschinentypen umsetzen.

Bild 5 zeigt exemplarisch eine durch Sicherheitsmodule der S-DIAS-Serie realisierte Topologie eines Steuerungssystems, die jener in Bild 2 entspricht. Auch das Mischen von Sicherheitsmodulen der C-DIAS- und S-DIAS-Serie in ein und derselben Applikation ist möglich (siehe hierzu Abschnitt 1.6). Das Mischen der beiden Systeme ist nicht möglich, wenn die SCP 111, SCP 111-S oder SCP 211 eingesetzt wird, da hier die sicherheitsgerichtete Kommunikation durch das FSoE-Protokoll über VARAN erfolgt.

Bild 5 zeigt eine dem Bild 2 entsprechende durch Baugruppen der S-DIAS-Serie realisierte Topologie.

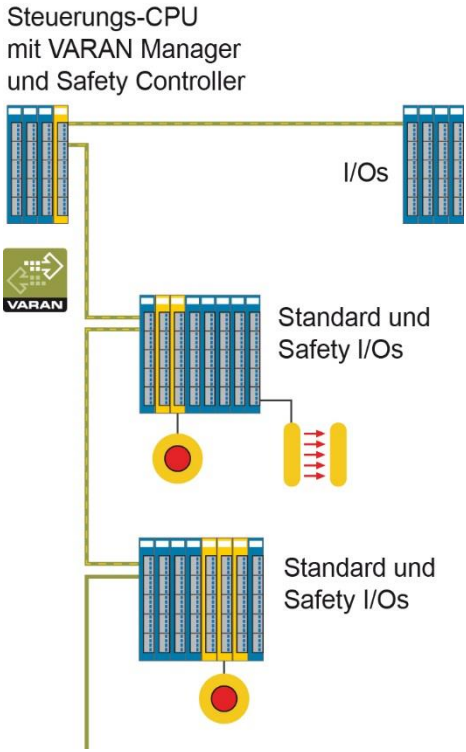


Bild 5 Architektur einer dezentralen Steuerung

2.3 Topologie des Safety-Systems

2.3.1 Generelle Topologie

Die Sicherheitsmodule werden in das Standard-Steuerungssystem von SIGMATEK GmbH & CO KG eingebettet. Zum Konfigurieren der Standard-SPS steht das Konfigurationstool LASAL Class 2 zur Verfügung. Dies ist eine objektorientierte Programmierumgebung, in der jedes verwendete Modul - gleichgültig ob Standardmodul oder Sicherheitsmodul - eine eigene Klasse besitzt.

In der objektorientierten Programmierung mit LASAL Class besteht ein Projekt aus mehreren Klassen, wobei jede Klasse Clients, Server und globale Methoden als Schnittstellen zu anderen Klassen besitzen kann. Mit Clients greift eine Klasse auf Daten oder Funktionalitäten außerhalb der Klasse zu und mittels Servern und globalen Methoden kann eine Klasse selbst Daten oder Funktionalitäten zur Verfügung stellen. Klassen, die die Aufgabe haben, Hardware anzusteuern, werden als Hardwareklassen bezeichnet.

Für die Sicherheitsmodule stehen folgende Hardwareklassen zur Verfügung:

Hardwareklasse	**Sicherheitsmodul**
CSDI161_IM	Sicheres Eingangsmodul CSDI 161
CSCP011_IM	Sichere CPU CSCP 011
CSTO081_IM	Sicheres Ausgangsmodul CSTO 081
CSDI162_IM	Sicheres Eingangsmodul CSDI 162
CSCP012_IM	Sichere CPU CSCP 012
CSTO082_IM	Sicheres Ausgangsmodul CSTO 082
SCP010	Sichere CPU SCP010
SCP011	Sichere CPU SCP011
SDI101	Sicheres Eingangsmodul SDI 101
STO081	Sicheres Ausgangsmodul STO 081
SRO021	Sicheres Relaismodul SRO 021
SRO022	Sicheres Relaismodul SRO 022
SSI021	Sicheres Gebermodul SSI 021
SNC021	SNC-Inkrementalgeber SNC 021
SDM081	Sicheres Mischmodul SDM 081
SCP111	Sichere CPU SCP 111
ST151	Schrittmotorkarte ST 151
_DriveMng_DC061	S-DIAS Achsmodul DC 061 und DC 061-1
_DriveMng_DC062	S-DIAS Achsmodul DC 062
_DriveMng_DC101	S-DIAS Achsmodul DC 101
_DriveMng_DC102	S-DIAS Achsmodul DC 102
MDD2000_Mng, MDD2000_Axis	MDD 2000

Tabelle 3 Hardwareklassenübersicht

Die C-DIAS Sicherheitsmodule müssen auf einem C-DIAS-Modulträger installiert werden. Der Modulträger ist entweder direkt oder über ein Koppelmodul (z.B. CIV 512) mit der Standard-SPS (z.B. einem C-IPC) verbunden.

Die Kommunikation der Koppelmodule erfolgt dabei z. B. über den VARAN-Bus. Der Bus-Master und die Safety CPU müssen auf einem Modulträger Platz finden.

Die S-DIAS Sicherheitsmodule können über ein Kopplermodul (z.B. VI 020) in das Standard-System eingebunden werden.

Die S-DIAS-Module (z.B. SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211) können auch in einer Standalone-Version verwendet werden. Die Module müssen dann nicht in das Standard-System integriert werden.

Ein typischer Aufbau eines Steuerungssystems ist in
Bild **6** dargestellt.

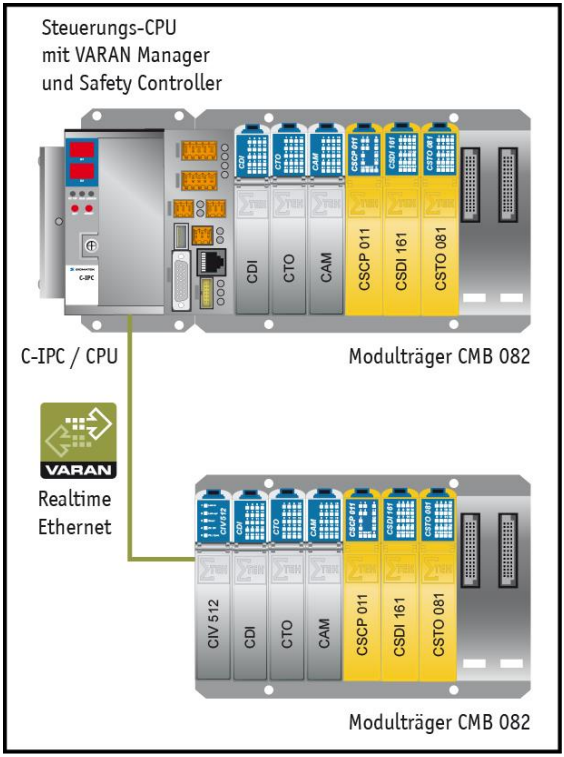


Bild 6 Beispiel eines Safety-Systems

Die Konfiguration der Sicherheitsmodule wird nicht über die Standard-SPS, sondern über den SafetyDesigner durchgeführt. Die sichere Applikation wird direkt in den Sicherheitsmodulen abgearbeitet (z.B. einer Safety-CPU).

Bei der Erstellung einer sicheren Steuerung ist wie folgt vorzugehen:

- Sicherheitsmodule installieren und verdrahten.

- Sicherheitsmodule in einem Standard-SPS-Projekt platzieren und die Schnittstelle mit der Standardsteuerung konfigurieren.
  In diesem Schritt ist die entsprechende Hardwareklasse für jedes Sicherheitsmodul zu platzieren und zu konfigurieren, z. B. ist der entsprechende Steckplatz auf dem C-DIAS-Busträger anzugeben.
  S-DIAS-Module im Standalone-Betrieb müssen in keinem Standard-SPS-Projekt platziert werden.

- Sicherheitsmodule über den SafetyDesigner konfigurieren.
  Über den SafetyDesigner wird die sichere Applikation, die auf den Sicherheitsmodulen ausgeführt wird, erstellt und hinuntergespielt.

- Validierung des sicheren Systems.
  Nachdem die sichere Applikation erstellt und auf die Sicherheitsmodule hinuntergespielt wurde, muss das System auf die korrekte Funktionalität hin überprüft werden.

2.3.2 Sicherheitsmodule

Generell gibt es vier verschiedene Modulgruppen.

- ***Sichere CPUs***
  Eine sichere CPU, wie das Sicherheitsmodul CSCP 011 besitzt vier sichere Eingänge und zwei sichere Ausgänge. Auf der Safety-CPU wird die Konfiguration entweder über den LASAL-SafetyDesigner oder z. B. über eine SD-Karte übertragen. Die Safety-CPU verteilt dann die Konfiguration an die entsprechenden entfernten Module, die in der Konfiguration enthalten sind.

- ***Sichere Ein- und Ausgangsmodule***
  Sichere Ein- und Ausgangsmodule wie z. B. CSDI 161 oder CSTO 081 werden von der Safety-CPU konfiguriert. Mit dem SafetyDesigner oder der Standard-SPS kann nur lesend auf die Sicherheitsmodule zugegriffen werden.

- ***S-DIAS-Sicherheitsmodule***
  Die Safety-CPU SCP 010 kann mit max. zwei Eingangskarten SDI 100, einer Ausgangskarte STO 040 und zwei Relaiskarten SRO 020 verwendet werden.
  Die Safety-CPUs SCP 011, SCP 111 und SCP 111-S können max. 16 Karten unterstützen (Eingangskarte SDI 101, Ausgangskarte STO 081, Relaiskarte SRO 021, Geberkarte SSI 021, SNC-Inkrementalgeber SNC 021, Mischmodul SDM 081). Es können max. 8 Relaiskarten SRO 021 bzw. SRO 022 angesteckt werden (Relaiskarten belegen 2 Plätze).
  Bei den S-DIAS Safety-CPUs können über eine Safety-Interface-Schnittstelle 8 weitere sichere Eingänge eingebunden werden. Auf der Safety-CPU wird die Konfiguration entweder über den LASAL-SafetyDesigner oder z. B. über eine SD-Karte übertragen. Die Safety-CPU verteilt dann die Konfiguration an die entsprechenden entfernten Module, die in der Konfiguration enthalten sind.

- ***Sicherer Drive***
  Der Drive MDD2000 verfügt über integrierte Sicherheitsfunktionen (z.B. STO) und kann im Standalone-Betrieb sowie im Zusammenwirken mit einer sicheren CPU betrieben werden.

2.3.3 Sicherer Zustand

Der sichere Zustand entspricht immer dem Low-Pegel. Befindet sich das System nicht im Betriebszustand Operational bzw. Temporary Operational, so sind die sicheren Ausgänge immer ausgeschaltet, d. h. der Ausgang liegt auf dem Massepotential. Dies ist auch im Fehlerzustand der Fall.

2.3.4 Handbediengerät

Auf den S-DIAS-Sicherheitsmodulen SCP 010, SCP 011 und SCP 111 ist eine Safety-Interface-Bus-Schnittstelle implementiert, an die, wie in Bild **7** dargestellt, ein Handbediengerät zur Visualisierung von Prozessen sowie zur Bedienung und Beobachtung von Abläufen angeschlossen werden kann. Dieses Handbediengerät ist gemäß EN 60204-1, Abschnitt 10.7.1, in der Lage, die Sicherheitsfunktion Not-Halt zu unterstützen.

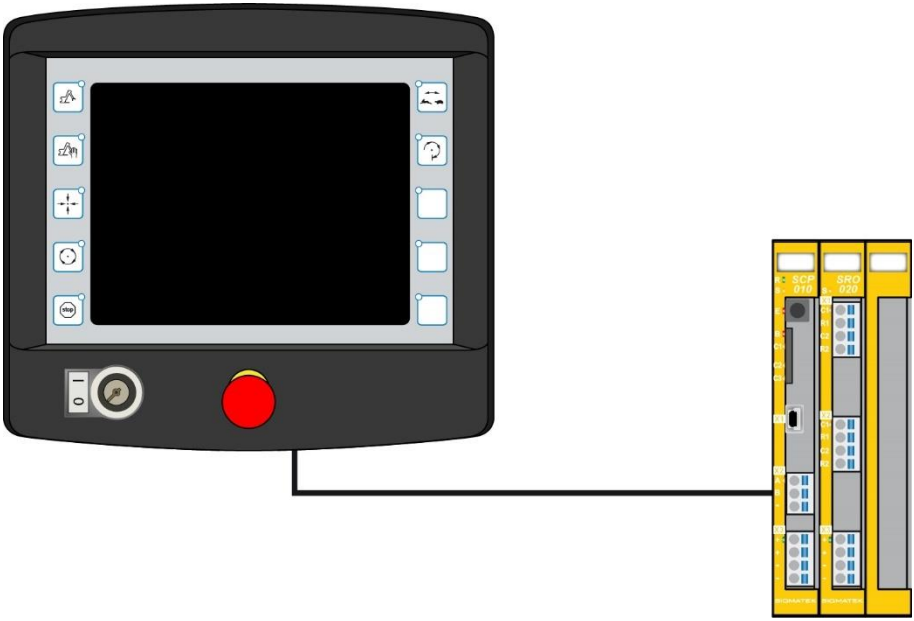


Bild 7 Anschluss eines Handbediengerätes

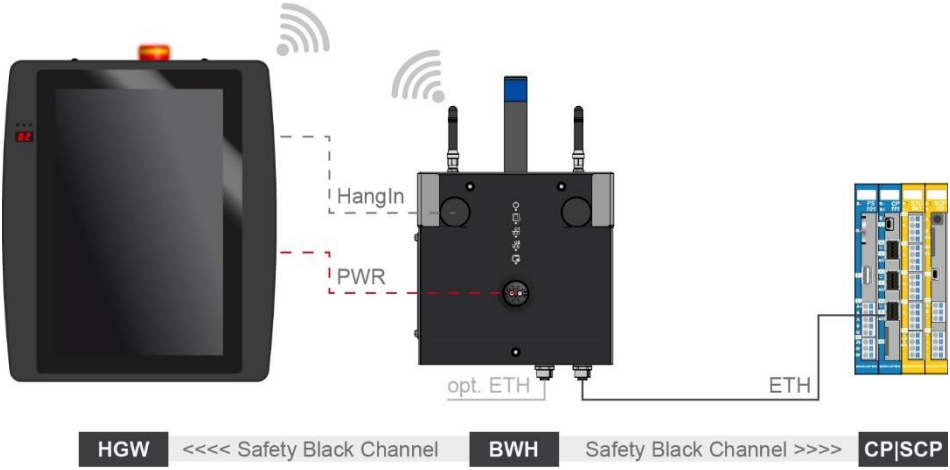


Bild 8 Anschluss eines HGW

Die Handbediengeräte (z.B. HBG 0811, HBG 0811-K, HGT 835, HGT 835-TF, HGT 1035, HGT 1035-H, HGT 1035-B, HBG 1011, HBG 1011-1, HBG 1011-H, HBG 1011-K, RBG 151, HGT 1051) dürfen ausschließlich mit den Sicherheitsmodulen SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211 betrieben werden!
Die Handbediengeräte HGW 0831-I, HGW 1033-3 und HGW 1033-32 dürfen ausschließlich mit der SCP 111, SCP 111-S und SCP 211 betrieben werden.

Nach EN ISO 13850, Abschnitt 4.1, sowie EN 60204-1 Abschnitt 10.7.1 muss dafür gesorgt sein, dass keine Verwechslung zwischen einem wirksamen und einem nicht wirksamen Handbediengerät vorkommen kann.

2.3.5 Safety-Interface

Das Safety-Interface der SCP010, SCP011 und SCP111 ist weitestgehend mit CAN kompatibel. Das Interface wird mit einer Baudrate von 500 k betrieben.
Folgende IDs werden von den Safety-CPUs verwendet:

Id	Verwendung	Anmerkung
0x55A	Power-On Selbsttest	
0x100	Zyklisch sendend	Ab Safetydesigner BuildNr 2320 bei SCP011 ab FWV377 und bei SCP111 ab FWV458 ist es möglich die Nutzung dieser ID zu unterdrücken. Wenn die Nutzung dieser IDs unterdrückt ist, ist keine Verwendung von Handbediengeräten oder SIB061 am Safety-Interface möglich.
0x740	Zyklisch sendend	

0x200	Empfangend	

2.4 Kommunikation im Safety-System

Mit dem SafetyDesigner können auf alle Sicherheitsmodule Lesezugriffe durchgeführt werden. Schreibzugriffe sind nur auf die Safety-CPU möglich um z. B. die Konfiguration darauf zu übertragen. Die zur Konfiguration gehörenden entfernten Sicherheitsmodule werden direkt über die Safety-CPU konfiguriert. Alternativ kann die Konfiguration auch von einer SD-Karte auf die Safety-CPU übertragen werden.

Der SafetyDesigner kann bei den S-DIAS Safety-Modulen nur auf die Safety-CPU lesend und schreibend zugreifen. Eine Kommunikation mit den Ansteckkarten (SDI 100, STO 040, SRO 020, SDI 101, STO 081, SRO 021, SRO 022, SSI 021, SNC 021, SAI 041 und SDM 081) erfolgt nicht.

2.5 Systemmerkmale

2.5.1 Konfigurationsmerkmale

Bei der Erstellung der Konfiguration gibt es bestimmte Einschränkungen; so darf ein sicheres Eingangs- oder Ausgangsmodul nur von einem Projekt angesprochen werden. Wird ein zweites Projekt generiert, das auf die in einem anderen Projekt verwendeten Sicherheitsmodule zugreift, so werden die Sicherheitsmodule mit der zuletzt übertragenen Konfiguration überschrieben.

Im selben Projekt gibt es die Einschränkung, dass ein sicherer Ausgang - gleichgültig ob von einem entfernten Sicherheitsmodul oder von der Safety-CPU selbst - nur von einem Objekt gesetzt werden darf. Sichere Eingänge können dagegen von mehreren Objekten im selben Projekt benutzt werden.

Die sicheren Ausgänge können zudem zurückgelesen und wiederverwendet werden. Dies wird im LASAL SafetyDesigner beschrieben.

In einem Projekt können maximal 128 Sicherheitsmodule verwendet werden.

Tausch und Vertauschung von Sicherheitsmodulen

Ein Modultausch darf nur im abgeschalteten Zustand vorgenommen werden. Der Tausch eines Sicherheitsmoduls wird erkannt. Beim Tausch mehrerer Sicherheitsmodule wird eine Fehlermeldung ausgegeben und das System muss neu konfiguriert werden. Werden mehrere Module vertauscht, so muss das System neu konfiguriert und validiert werden.

Beim Tausch von optionalen Modulen muss das System immer neu konfiguriert und validiert werden. Dies kann entweder mit Hilfe des SafetyDesigners oder der SD-Karte erfolgen.
Erfolgt diese erneute Validierung nicht, verliert die SCP ihre Konfiguration und wechselt in einen Fehlerzustand (ERRVAL 222 / 1222 Temporary Operation Time – siehe Kap. 2.6.4). Dies ist eine Sicherheitsmaßnahme für unautorisierte Module in unserem Safety-System.

Beim Tausch von SNC müssen Inkrementalgeber neu geteacht werden, siehe Produktdokumentation.

2.5.2 Konfiguration des Systems

2.5.2.1 Konfiguration des Systems über den SafetyDesigner

Die Konfiguration des Systems erfolgt über das Softwaretool „LASAL SafetyDesigner“. Im SafetyDesigner wird die sichere Applikation erzeugt. Dabei stehen Standardfunktionsblöcke wie z. B. UND-Gatter zur Verfügung. Zudem stehen komplexe Funktionsblöcke zur Verfügung, die dem PLC-Open-Standard entsprechen.

Die sichere Applikation wird aus den zur Verfügung stehenden Funktionsblöcken zusammengesetzt. Dabei werden die sicheren Ein- und Ausgänge entsprechend verknüpft. Die sicheren Safebool Ein- und Ausgänge besitzen ein spezielles Format, das drei Zustände erlaubt:

- Safebool_True
- Safebool_False
- Safebool_Error

Die Signale von der Standard-SPS können die zwei logischen Zustände True und False einnehmen. Soll z. B. ein Signal von der Standard-SPS auf ein sicheres UND-Gatter verknüpft werden, so muss dieses zuerst mit einem entsprechenden Funktionsblock auf ein sicheres Signalformat umgewandelt werden.

Über den SafetyDesigner können Signale von der Standard-SPS eingelesen und in der sicheren Applikation verwendet werden.

Ein von der sicheren Applikation berechneter Ausgang kann mit Hilfe eines Freigabesignals aus der nicht sicheren SPS abgeschaltet werden. Bei der Konfiguration der Hardwareklassen ist bei Verwendung eines unsicheren Freigabesignals dieses mit dem jeweiligen Pin „Unsafe Output“ des entsprechenden sicheren Ausgangs zu verknüpfen. Der umgekehrte Fall, dass ein unsicheres Freigabesignal einen von der sicheren Applikation ausgeschalteten Ausgang einschalten kann, ist jedoch nicht möglich.

Die erstellte Konfiguration kann mit dem SafetyDesigner auf eine Safety-CPU übertragen werden. Die Safety-CPU verteilt danach die Daten an die benötigten entfernten Sicherheitsmodule. Um mögliche Fehler zu vermeiden, muss beim Konfigurationsdownload unter anderem die Modulsicherheitsnummer der Safety-CPU bestätigt werden, auf die die Konfiguration übertragen wird. Die zu übertragenden Daten werden vom SafetyDesigner CRC-gesichert auf die Safety-CPU übertragen. Die übertragenen Daten werden danach über eine anders berechnete CRC vom SafetyDesigner wieder rückgelesen. Der Anwender kann somit überprüfen, ob Download- und Uploaddaten einander entsprechen. Näheres dazu ist in der Beschreibung des LASAL-SafetyDesigners zu finden.

2.5.2.2 Konfiguration des Systems über die SD-Karte

Die Konfiguration kann auch über eine SD-Karte verteilt werden. Dazu ist es notwendig, im ersten Schritt die SD-Karte zu beschreiben. Dazu muss die Safety-CPU in den Service Mode wechseln. Befindet sich die Safety-CPU im Service Mode, so kann die SD-Karte eingesteckt und über den SafetyDesigner (Befehl „Write SD-Card“) beschrieben werden. Nach dem Beschreiben der SD-Karte kann diese in eine andere Safety-CPU eingesteckt werden. Die entsprechende Safety-CPU muss jedoch im stromlosen Zustand sein. Befindet sich keine Konfiguration auf der Safety-CPU, so übernimmt die Safe CPU beim Hochfahren die Konfiguration der SD-Karte. Eine ausführliche Beschreibung der Konfiguration des Systems über die SD-Karte ist im Kapitel 4.3 zu finden.

2.5.3 Änderungen am System

Änderungen am System können aus einer Änderung der sicheren Applikation oder der Konfiguration bestehen, wenn ein Sicherheitsmodul entfernt, zusätzliches hinzugefügt oder ausgetauscht wird. Der Tausch eines Sicherheitsmoduls wird dabei vom System unterstützt, der gleichzeitige Tausch oder die Vertauschung mehrere Sicherheitsmodule dagegen nicht. Eine ausführliche Beschreibung hierzu ist in Kapitel 6 zu finden.

2.5.4 Reaktionszeit und Abschaltzeit

Die Reaktionszeit von einem sicheren Eingang bis hin zum sicheren Ausgang der Sicherheits-SPS wird bei der Erstellung der sicheren Applikation vom SafetyDesigner abgeschätzt. Die Reaktionszeiten des Sensors, der am Eingang angeschlossen ist bzw. die Ausgangsbeschaltung ist nicht in der Reaktionszeitabschätzung durch den SafetyDesigners enthalten. Bei den Modulen SRO 021 und SRO 022 (Modul mit Relais) wird die Reaktionszeit des eigenen Relais miteinberechnet.

Der SafetyDesigner schätzt dabei eine Worst-Case-Reaktionszeit ab. Nähere Einzelheiten hierzu werden in Kapitel 4.8 anhand von Bespielen beschrieben.

2.5.5 LEDs der Sicherheitsmodule

Um den Zustand eines Sicherheitsmoduls während des Betriebs überprüfen zu können, verfügen die Sicherheitsmodule über LED-Anzeigen, mit deren Hilfe folgende Informationen vermittelt werden:

LED	LED	Funktion
DC	GRÜN	Signalisiert, ob die +24 V-Versorgung für Ausgänge und Taktausgänge innerhalb der definierten Grenzen liegt.
RN	GRÜN	Run signalisiert den zeitlich begrenzten (LED „ST“ eingeschaltet) bzw. den zeitlich unbegrenzten (LED „ST“ ausgeschaltet) Operational Mode
ST	GELB	Status permanentes Leuchten: das Modul befindet sich im Service-Modus langsame Blinkfrequenz: das Modul befindet sich im Idle bzw. im Check Configuration-Modus (Verteilung der Konfiguration)
E	ROT	Error permanentes Leuchten: das Modul befindet sich im Error-Modus langsame Blinkfrequenz: bei entferntem Eingang ist das maximale Alter überschritten (lässt sich mit SafetyDesigner auslesen) schnelle Blinkfrequenz: schwerwiegender Fehler; mit dem Modul kann nicht mehr kommuniziert werden (lässt sich NICHT mit SafetyDesigner auslesen)

Tabelle 4 LED-Beschreibung

Verfügt ein Sicherheitsmodul über sichere Ein- bzw. Ausgänge, so ist für jeden von ihnen eine LED-Anzeige implementiert. Die Position dieser LEDs kann den entsprechenden Datenblättern der Sicherheitsmodule entnommen werden. Generell können diese LEDs drei Zustände anzeigen:

LED Zustand	Funktion
Ausgeschaltet	Ist die LED ausgeschaltet, so liegt am sicheren Eingang eine logische „0“ an bzw. der sichere Ausgang ist ausgeschaltet.
Leuchten	Bei leuchtender LED wird am sicheren Eingang eine logische “1” eingelesen, bzw. der sichere Ausgang ist eingeschaltet.
Blinken	Blinkt die LED, so wurde ein Fehler festgestellt. Die möglichen Fehler sind in Kapitel 5.3 beschrieben.

Tabelle 5 Ein- und Ausgangs-LEDs

Handelt es sich bei dem Sicherheitsmodul um eine Safety-CPU, so sind noch vier weitere LED-Anzeigen zur Bedienung des Validierungstasters vorgesehen:

LED	LED	Funktion
B	ROT	Signalisiert, ob der Validierungstaster betätigt wurde Leuchtet: Gültige Sequenz wurde bzw. wird eingegeben Blinkt schnell: Ungültige Sequenz wurde eingegeben. Dies hat zur Folge, dass die ungültig eingegebene Sequenz verworfen wird. Langsames blinken (1x, 2x bzw. 3x) zur Bestätigung, dass das eingegebene Kommando ausgeführt wurde
C1	GELB	Bestätigung der Eingabe für Kommando 1, nachdem eine gültige Startsequenz abgegeben wurde
C2	GELB	Bestätigung der Eingabe für Kommando 2, nachdem eine gültige Startsequenz abgegeben wurde
C3	GELB	Bestätigung der Eingabe für Kommando 3, nachdem eine gültige Startsequenz abgegeben wurde

Tabelle 6 Validierungstaster LEDs

2.5.6 Diagnose

Im C-DIAS und S-DIAS Safety-System gibt es im Fehlerfall zwei verschiedene Diagnosemöglichkeiten.

- Über die LED-Anzeigen der Sicherheitsmodule.

- Über den SafetyDesigner. Hierbei muss eine Onlineverbindung mit der entsprechenden sicheren Steuerung bestehen und das entsprechende Projekt auf der Safety-CPU geöffnet sein. Die entsprechenden Fehler in den Sicherheitsmodulen können dann ausgelesen werden. Näheres dazu wird in Kapitel 5.3 erläutert.

2.6 Betriebszustände

Eine Safety-CPU Modul nimmt jeden der in
Bild **9** dargestellten Betriebszustände ein. Safe Output und Safe Input Module hingegen nehmen nicht zwangsläufig jeden Betriebszustand ein. Die Betriebszustände einer Safety-CPU sind:

- Post (Power On Self Test)
- Idle
- Check Configuration
- Temporary Operational
- Operational
- Service
- Error

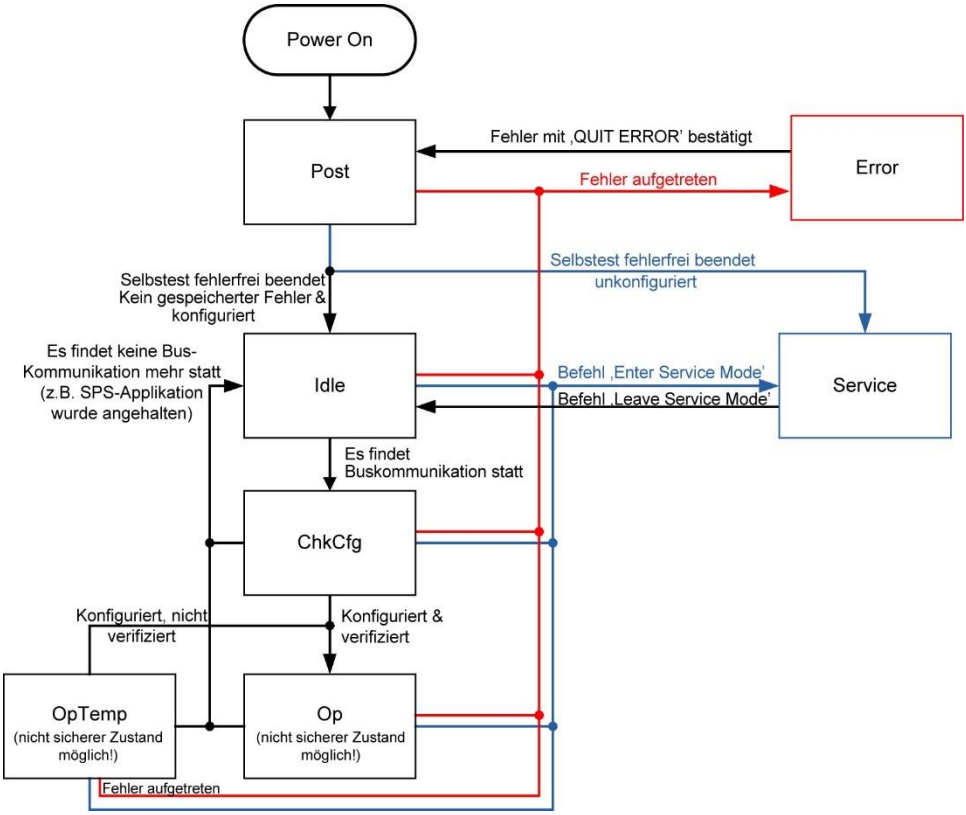


Bild 9: Zustände eines Moduls

Die Zustandsübergänge zur Laufzeit sind in den folgenden Unterabschnitten beschrieben.

2.6.1 Post – Power On Self Test

Nach dem Einschalten bzw. beim Wiederanlauf führt das Safety-CPU Modul einen Selbsttest durch. Dabei prüft es auch den Konfigurationszustand (konfiguriert/unkonfiguriert) und verzweigt abhängig vom Ergebnis dieser Prüfungen in einen der Zustände Idle, Service oder Error (vgl.
Bild **10**).

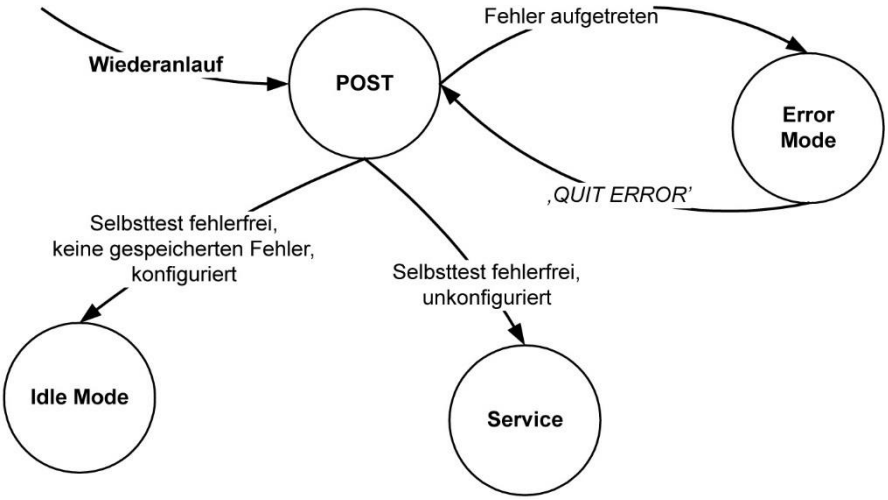


Bild 10: Zustand POST

Verzweigung nach	Genau dann, wenn
IDLE	Selbsttest fehlerfrei Keine gespeicherten Fehler Konfigurationszustand: „konfiguriert“
SERVICE	Selbsttest fehlerfrei Konfigurationszustand: „unkonfiguriert“
ERROR	Fehler im POST aufgetreten

Tabelle 7 Mögliche Zustandswechsel von POST

Außer beim Einschalten (Wiederanlauf) wird ein Zustandswechsel nach POST auch ausgelöst, wenn ein bestehender Fehler durch „QUIT ERROR“ bestätigt wird. Dieser Befehl kann mit Hilfe des SafetyDesigners sowie auch über den Validierungstaster auf dem Safety-CPU-Modul ausgelöst werden. Die sicheren Ein-/Ausgänge der jeweiligen Module befinden sich im POST im „sicheren Zustand“!

Keine LED leuchtet

Bild 11 Safety-CPU im POST

2.6.2 Idle

Das Modul ist bereit für den Übergang in den Check-Configuration (ChkCfg) Zustand. Das Modul befindet sich in diesem Zustand, wenn die SPS-Applikation steht - d.h., wenn keine Kommunikation mit der SPS-Applikation erfolgt. Um den Idle-Mode zu verlassen, ist sicherzustellen, dass die Standard-SPS sich nicht im Fehlerzustand befindet. Im Idle-Zustand befinden sich die sicheren Ein-/Ausgänge der jeweiligen Module immer im „sicheren Zustand“.

LED ST langsam blinkend

Bild 12 Safety-CPU im Idle Mode

2.6.3 ChkCfg – Check Configuration

Das Modul überprüft die Konfiguration. Eine Safety-CPU überprüft die Konfigurationen der angeschlossenen sicheren Ein-/Ausgangsmodule und aktualisiert diese gegebenenfalls. Die sicheren Ein-/Ausgangsmodule verweilen in diesem Zustand, falls eine Modul-Sicherheitsnummer eines entfernten Moduls ermittelt werden muss. Die sicheren Ein-/Ausgänge der jeweiligen Module befinden sich hier immer im „sicheren Zustand“. Tritt ein Fehler während der Check Configuration-Phase auf, so wechselt das Modul nach einem Timeout in den Fehlerzustand (Error-LED leuchtet). Der Fehler kann dann über den SafetyDesigner ausgelesen werden (siehe Diagnosekapitel). Wird die Check Configuration-Phase erfolgreich durchlaufen, so wechselt das Modul in den OpTemp oder Operational Mode.

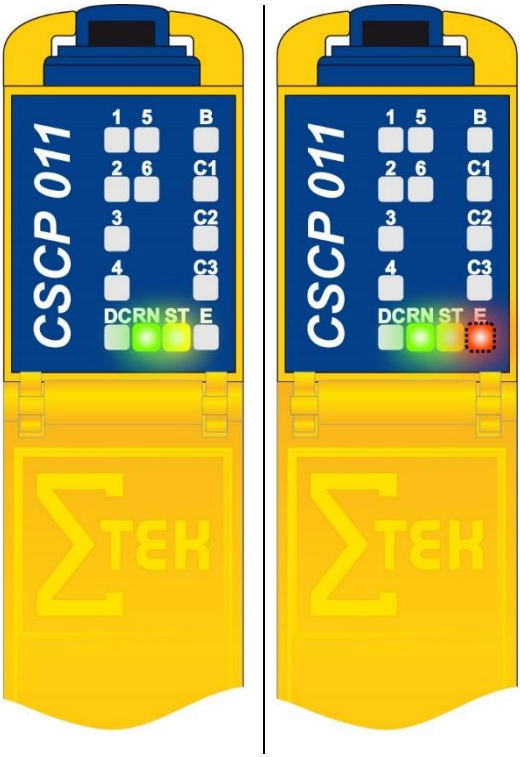
LED ST langsam blinkend

Bild 13 Safety-CPU im Check Configuration Mode

2.6.4 OpTemp – zeitlich begrenzter Operational Zustand

Das Modul befindet sich im zeitlich begrenzten Betrieb. In diesem Zustand muss die Validierung des Sicherheitssystems durchgeführt werden. Dies bedeutet, dass jetzt die korrekte Funktionalität der konfigurierten Sicherheitssteuerung überprüft werden muss. Solange das Modul nicht verifiziert ist, kann nicht in den Op-Zustand gewechselt werden. Wenn innerhalb einer gewissen Zeit (Temporary Operation Time) keine Verifizierung erfolgt, wird in den Fehlerzustand gewechselt (mit Errorcode 222 bzw. 1222 siehe Dokumentation SafetyDesigner). Nach Absetzen eines „Quit Error“ Befehls wird in den Service-Mode zurückgekehrt. Das Projekt muss neu geladen werden.

Die Temporary Operation Time muss über den SafetyDesigner konfiguriert werden und kann zwischen minimal 300 Sekunden und maximal 28800 Sekunden eingestellt werden. Die sicheren Ein-/Ausgänge der jeweiligen Module werden hier Applikationsbedingt ein-/ausgeschalten.



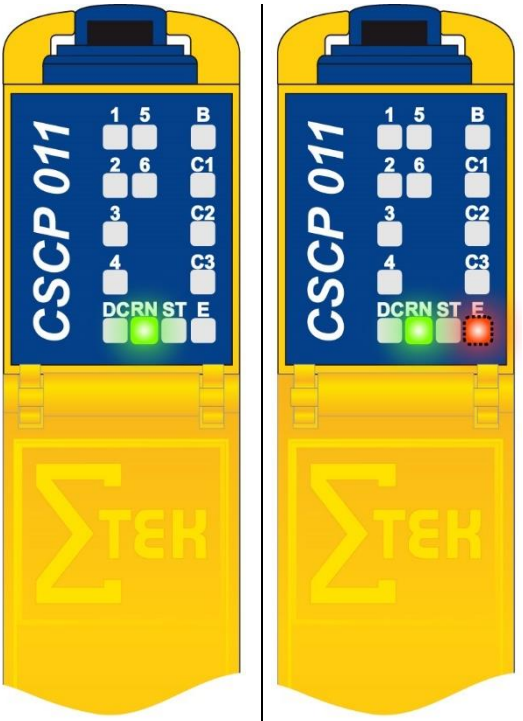
LED RN&ST leuchten

Bei fehlerhaft entfernten Eingängen, E blinkt langsam

Bild 14 Safety-CPU im temporary Operational Mode

2.6.5 Op – Operational

Das Modul ist zeitlich unbegrenzt betriebsbereit. Die sicheren Ein-/Ausgänge der jeweiligen Module werden hier entsprechend der Applikation geschaltet.



LED RN leuchtet

Bei fehlerhaft entfernten Eingängen, E blinkt langsam

Bild 15 Safety-CPU im Operational Mode

2.6.6 Service – Service Mode

Im Service Mode werden die Sicherheitsmodule konfiguriert. Auslieferungszustand der Sicherheitsmodule ist der Service Mode. Um eine Konfiguration zu ändern, muss in den Service Mode gewechselt werden. Dazu ist ein Login auf Konfigurationsebene der Safety-CPU notwendig.

Bei neu ausgelieferten Sicherheitsmodulen muss bei der ersten Konfiguration ein Passwort vergeben werden (beschrieben im LASAL SafetyDesigner).

Der Service Mode bietet über den SafetyDesigner folgende Möglichkeiten:

- ***„Clear Program“***
  Mit diesem Befehl wird die Konfiguration auf der Safety-CPU gelöscht. Ist das Sicherheitsmodul nicht konfiguriert, so kann es nicht mehr in den Operational bzw. temporary Operational Mode zurückwechseln.

- ***„Download“***
  Über das Download-Kommando wird die im SafetyDesigner entworfene oder geänderte Konfiguration auf die Safety-CPU(s) im Projekt übertragen.

- ***„Write SD Card“***
  Wird z. B. während des Service-Modes eine SD-Karte in die Safety-CPU eingesteckt, so kann diese über den Befehl „Write SD Card“ beschrieben werden. Dabei wird das im SafetyDesigner geöffnete Projekt auf die SD-Karte geschrieben.

- ***„Set Verified“***
  Nachdem die Konfiguration übertragen wurde und das System im temporary Operational Mode läuft, kann nach der erfolgreichen Validierung des Systems der „Set Verified“-Befehl ausgeführt werden. Nach Ausführen dieses Befehls kann in den zeitlich unbegrenzten Operational Mode gewechselt werden (siehe „Start“-Kommando)

- ***„Start“***
  Mit dem Start-Button kann vom Service-Mode in den Operational bzw. temporary Operational Mode gewechselt werden. Nach dem Download der Konfiguration vom SafetyDesigner auf die entsprechende Safety-CPU wird mit Betätigen des „Start“-Buttons die Verteilung der Konfiguration auf die entfernten Sicherheitsmodule gestartet. Nach dem erfolgreichen Verteilen der Konfiguration wechselt das System in den temporary Operational Zustand. Wird nach dem erfolgreich ausgeführten „Set Verified“ Kommando der „Start“ Button gedrückt, so wird in den Operational Mode gewechselt.

- ***„Quit Error“***
  Dieses Kommando kann auch im Service Mode abgesetzt werden. Durch Ausführen des Quit Errors wird der Login zurückgesetzt, d. h. um wieder in den Service Mode zu gelangen, ist ein neuerliches Login notwendig. Ein absetzen eines Quit Errors im Service Mode ist z. B. sinnvoll, wenn entfernte Sicherheitsmodule im Fehler stehen und diese konfiguriert werden sollen.

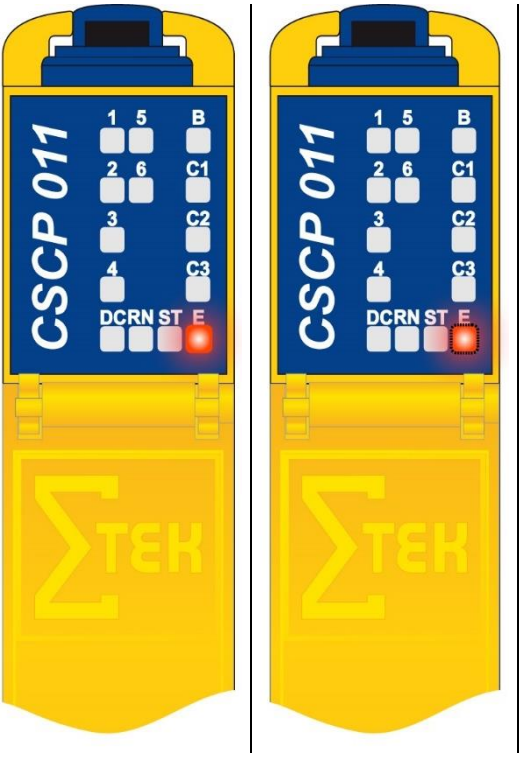
Die sicheren Ein-/Ausgänge der jeweiligen Module befinden sich dabei im „sicheren Zustand“.

LED ST leuchtet

Bild 16 Safety-CPU im Service Mode

2.6.7 Error – Fehlerzustand

In diesem Modus verbleibt das Modul im Fehlerfall so lange, bis ein „Quit Error“ Kommando ausgeführt wird. Es wird dann in den Post Zustand gewechselt, damit der Selbsttest noch einmal durchlaufen wird. Die sicheren Ein-/Ausgänge der jeweiligen Module befinden sich dabei im „sicheren Zustand“.



LED E leuchtet

Bei HW-Defekt (LED E blinkt schnell)

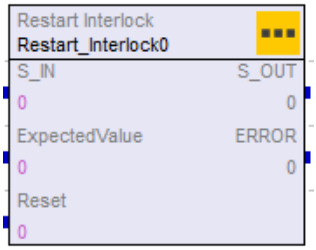
Bild 17 Safety-CPU im Error-Mode

2.6.8 SAI 041 – Auto-Quit

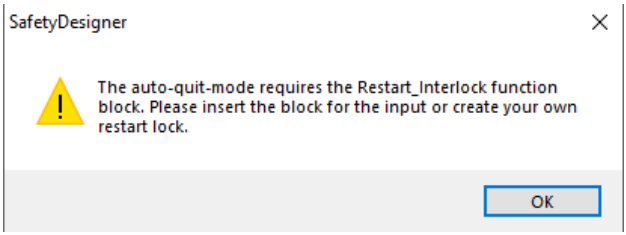
2.6.8.1 Verwendung des Auto-Quit-Modes

Die zusätzliche Eigenschaft („**AutoQuit**“) eines SAI041 Eingangkanals wird zur Verfügung gestellt, um bei jedem Eingangskanal die interne Wiederanlaufsperre deaktivieren zu können, d. h. nach Fehlersituationen am Modul und/oder am Netzwerk nehmen die zugehörigen Kanaldaten selbstständig wieder den korrekten Zustand ein.

Das Inaktivsetzen der Wiederanlaufsperre ist nur im Zusammenhang mit einem Erwartungswert in der Safety Applikation anzuwenden. Bei einer Diskrepanz muss der sichere Zustand eingeleitet werden und die Safety CPU stoppt die Applikation. Es liegt in der Verantwortung des Anwenders, die Kanaldaten der sicheren Eingangskanäle korrekt zu verschalten und mit einer Wiederanlaufsperre zu versehen. Hierzu können beispielsweise die Wiederanlaufsperre des Funktionsbausteins Restart_Interlock verwendet werden.



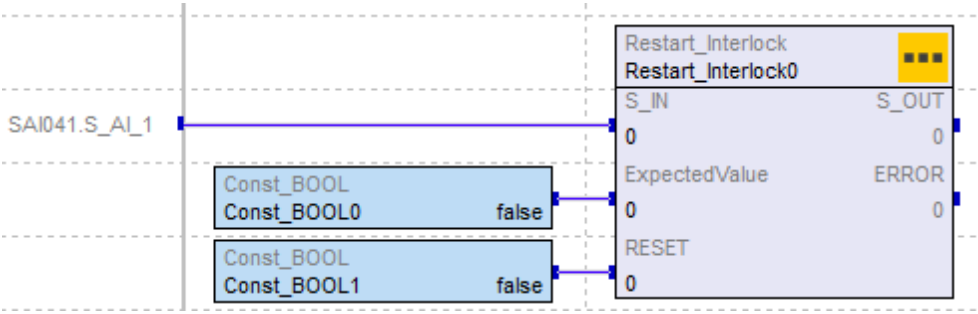
Der Anwender wird darauf hingewiesen den Funktionsblock zu verwenden bzw. eine eigene Wiederanlaufsperre anzulegen.



Die Anwendung von Eingangskanälen ohne korrekt verschaltete Wiederanlaufsperre kann einen automatischen Wiederanlauf zur Folge haben.

Beispiele für die Verwendung von Wiederanlaufsperren:

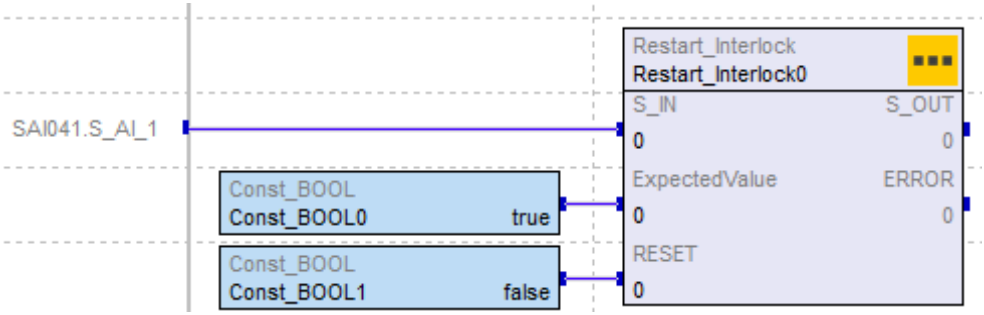
Beispiel 1: Fehler am Eingang der SAI041, Erwartungswert = FALSE:



Der Erwartungswert = FALSE, d.h., es wird kein Messwert erwartet, da dieser Eingangskanal in der Safety Applikationslogik deaktiviert ist.

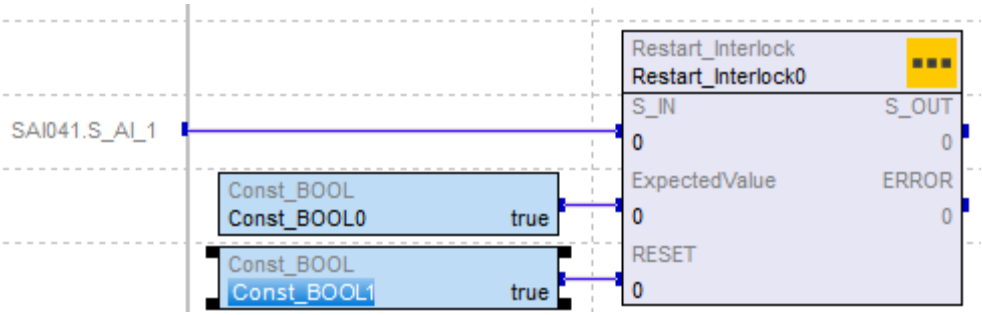
Es wird am Ausgang S_OUT ein der Eingang S_IN ausgegeben. Der ERROR-Ausgang steht auf FALSE

Beispiel 2: Messwert am Eingang der SAI041, Erwartungswert = TRUE:



Der Erwartungswert = TRUE, d.h., es wird ein Messwert erwartet, da dieser Eingangskanal in der Safety Applikationslogik aktiviert ist (Wiederanlaufsperre deaktiviert).
Der Messwert am Eingang SAI041.S_AI_1 wird am Ausgang S_OUT angezeigt. Der ERROR-Ausgang steht auf FALSE.

Beispiel 3: Fehler am Eingang der SAI041, Erwartungswert = TRUE:



Der Erwartungswert = TRUE, d.h., es wird ein Messwert erwartet, da dieser Eingangskanal in der Safety Applikationslogik aktiviert ist (Wiederanlaufsperre deaktiviert).

Liegt ein Fehler am Eingang SAI041.S_AI_1 an, wird der Fehler am Ausgang S_OUT angezeigt, da es in diesem Fall zu einem unerwarteten Fehler, wie z.B. Kabelbruch, gekommen ist. Der ERROR-Ausgang steht auf TRUE. Der Fehler wird dauerhaft an den Ausgang durchgereicht. Der ERROR-Ausgang steht auf TRUE. Der Fehler muss expilziert über den RESET-Eingang bestätigt werden. Danach wird wieder der Eingang SAI041.S_AI_1 am Ausgang S_OUT angezeigt. Der ERROR-Ausgang steht auf FALSE.

3 Installation und Montage

3.1 Montage eines Sicherheitsmoduls

Die C-DIAS Sicherheitsmodule sind auf einem C-DIAS-Modulträger zu installieren. Dabei muss die Versorgungsspannung auf dem Modulträger ausgeschaltet sein. S-DIAS-Module sind über eine VARAN-Kommunikation (z.B. Modul VI 020) anzubinden. Dabei muss die Versorgungsspannung ausgeschaltet sein.

Nähere Einzelheiten zur Installation sind in den Betriebsanleitungen der Sicherheitsmodule beschrieben.

3.2 Verdrahtung

Bitte beachten Sie bei der Verdrahtung zusätzlich folgende Hinweise:

- Sicherheitsgerichtete Eingänge unterliegen dem Ruhestromprinzip.
- Stellen Sie im Anwenderprogramm sicher, dass ein "0"-Signal der Baugruppe immer zum Abschalten der relevanten Ausgänge führt.
- Benachbarte Eingänge nicht mit demselben Testtakt belegen
- Bei Leitungslängen größer als 200 m und einem Leitungsquerschnitt von 1,5 mm² oder bei Leitungslängen größer als 300 m und einem Leitungsquerschnitt von 2,5 mm² bleibt ein Kurzschluss gegen Masse vom Betriebssystem unbemerkt.
- Bei Leitungslängen über 800 m können die Testtaktausgänge von Schaltvorgängen in 24 V-DC-Signalen gestört werden.
- Bei Leitungslängen größer als 500 m muss die Funktionsfähigkeit der Testtaktung durch Simulation von Kurzschlüssen zwischen den getakteten Eingängen getestet werden.
- Kurzschlüsse zwischen Testtaktausgang und zugehörigem Eingang müssen durch geeignete Leitungsführung ausgeschlossen werden.
- Als Leitermaterial soll Kupfer verwenden werden.
- Die Zuleitungen von kontaktbehafteten Sensoren sollen auf Quer- und Kurzschluss geprüft werden.
- Kommt die C-DIAS-Versorgungsspannung vom gleichen Netzteil wie die 24 V-Versorgungsspannung der Ein- bzw. Ausgänge, so kann ein Kurzschluss der externen Versorgungsspannung zu Masse das gesamte C-DIAS-System zum Ausfall bringen.

WICHTIG!

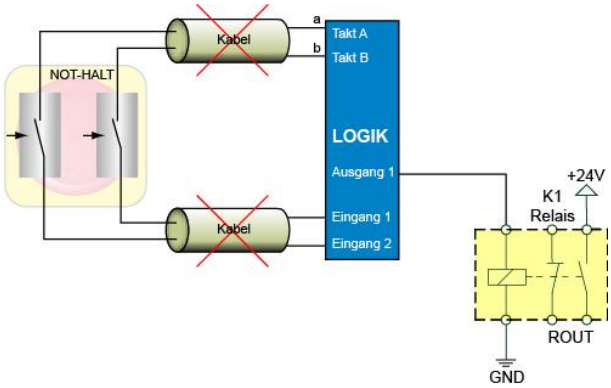
Unsachgemäße Verdrahtungen können zu Schäden an den Sicherheitsmodulen führen. Zudem kann nicht gewährleistet werden, dass die Sicherheitsfunktion bei unsachgemäßer Verdrahtung korrekt ausgeführt wird.

3.2.1 Verdrahtungsbeispiele und Beispiele der Konfigurationserstellung

3.2.1.1 Beispiel 1: Ansteuerung eines Relais

CPU Modulträger CMB 022

CPU



S -1 Testen der Konfiguration nach Installation

Nach der Installation aller Sicherheitsmodule oder nach dem Tausch eines Sicherheitsmoduls muss die Anlage durch sukzessives Testen der einzelnen Sicherheitsmodule verifiziert werden. Erst, wenn die Ansteuerung aller Sicherheitsmodule korrekt ist und die Verdrahtung der Sicherheitsmodule durch diesen Test verifiziert ist, kann die Anlage für den Betrieb freigegeben werden.

S -2 Verdrahtung der Taktsignale

Beim Anschluss der Taktsignale soll darauf geachtet werden, dass die Verbindungsleitungen von Takt A und Takt B nicht in einem gemeinsamen mehradrigen Kabel geführt werden.

Sehen Sie für jede Taktleitung ein separates Kabel mit ausreichend starkem Isolationsmantel vor.

Stellen Sie sicher, dass die Kabel querschlussfrei sind.

3.2.1.2 Beispiel 2: Bearbeitungsmaschine

Beschreibung des Beispiels

In einer Bearbeitungsmaschine wird das Werkstück durch Spannen der Klemmbacken gehalten. Werden die Klemmbacken entspannt, kann das Werkstück entnommen werden. Der Eingriffsbereich zum Werkstückwechsel wird durch eine Schutztür gesichert.
Beim Öffnen der Schutztür muss der Antriebsstrang der Bearbeitungsmaschine innerhalb von 50 ms abgeschaltet werden. Auf diese Weise wird ein Zugriff bei laufendem Werkzeug ausgeschlossen. Die Überwachung der Schutztür erfolgt mit 2 voneinander unabhängigen Endschaltern S3 und S4. Nach dem Ansprechen eines Endschalters muss der zweite Endschalter innerhalb von 500 ms ansprechen.
Beim Auslösen des Not-Halt-Schalters S2 muss die Bearbeitungsmaschine innerhalb von 50 ms gestoppt werden.
Der Antriebsstrang der Bearbeitungsmaschine wird über 2 in Serie geschaltete Relaiskontakte aktiviert. Mit den beiden Hilfskontakten der beiden Relais K1 und K2 wird der Status der Relais zurückgelesen. Das Ansprechen der Relais K1 und K2 wird mit einem Zeitfenster von 50 ms überwacht.
Die Signalleuchte P1 soll bei aktivem Antriebsstrang der Bearbeitungsmaschine aufleuchten.
Die Anlage kann nur manuell durch den Starttaster S1 gestartet werden bzw. nach einem Fehlerfall wieder gestartet werden.

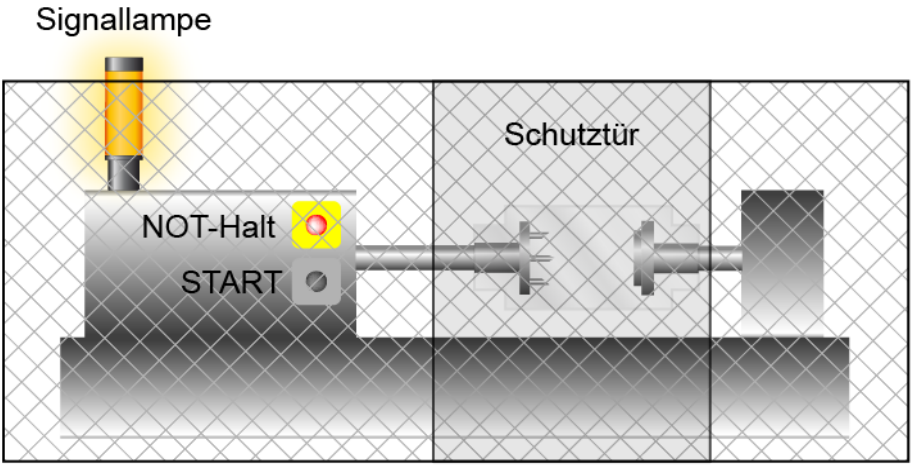


Bild 18 Schematischer Aufbau der Bearbeitungsmaschine

Verdrahtung

Die Schließerkontakte des Start-Tasters S1 werden 2-kanalig an die Taktausgänge A/B angeschlossen und auf 2 sichere Eingänge zurückgeführt.
Die Öffnerkontakte des Not-Halt Schalters S2 werden 2-kanalig an die Taktausgänge A/B angeschlossen und auf 2 sichere Eingänge zurückgeführt.
Die Schließerkontakte der beiden Endschalter S3 und S4 für die Schutztür werden 2-kanalig an die Taktausgänge A/B angeschlossen und auf 4 sichere Eingänge zurückgeführt.

Die beiden Spulen von Relais K1 und K2 werden über 2 sichere Ausgänge angesteuert. Die beiden Hilfskontakte (Öffner) der Relais K1 und K2 werden zum Rücklesen der Relaiskontakte verwendet. Die beiden Arbeitskontakte (Schließer) des Relais K1 und K2 werden in Serie geschaltet und bilden einen sicheren Relaisausgang für die Ansteuerung des Antriebsstrangs der Bearbeitungsmaschine.

Die Signalleuchte P1 wird über einen sicheren Ausgang angesteuert.

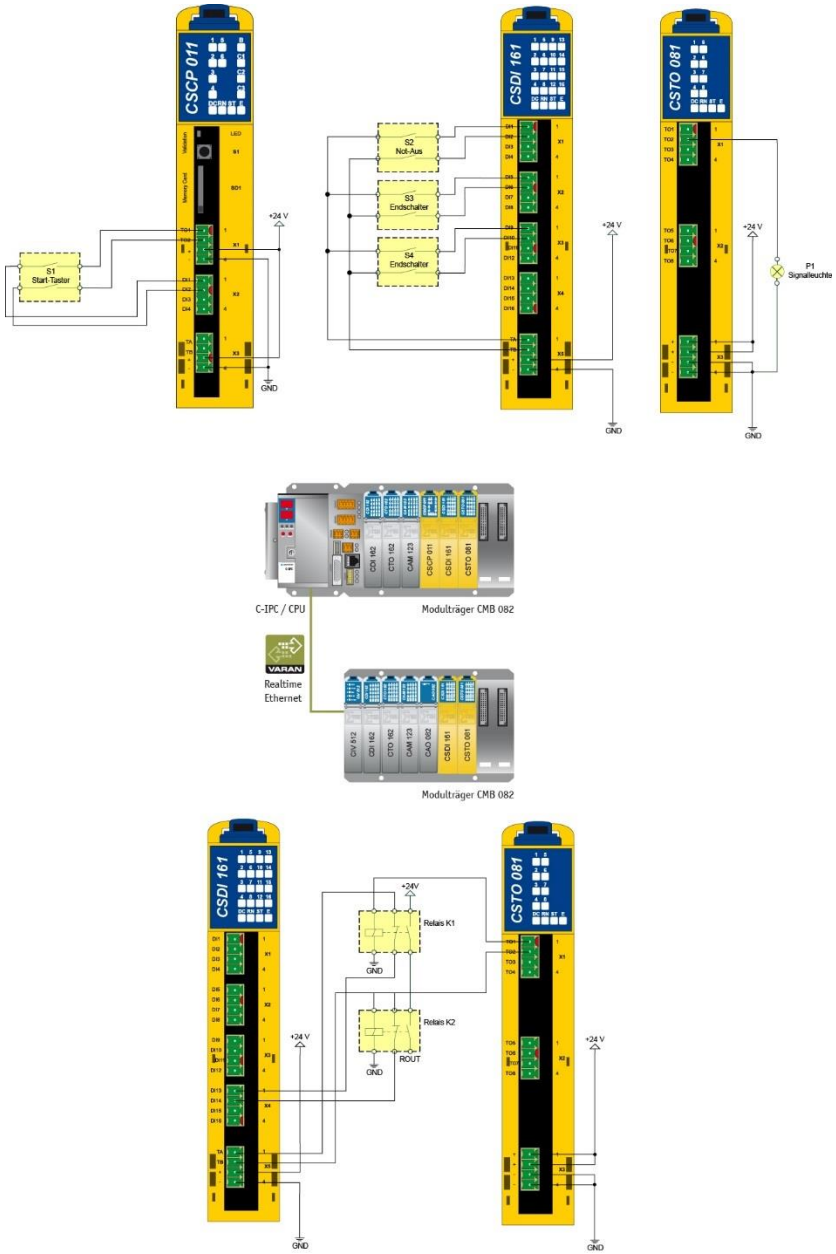


Bild 19 C-DIAS Hardwareaufbau

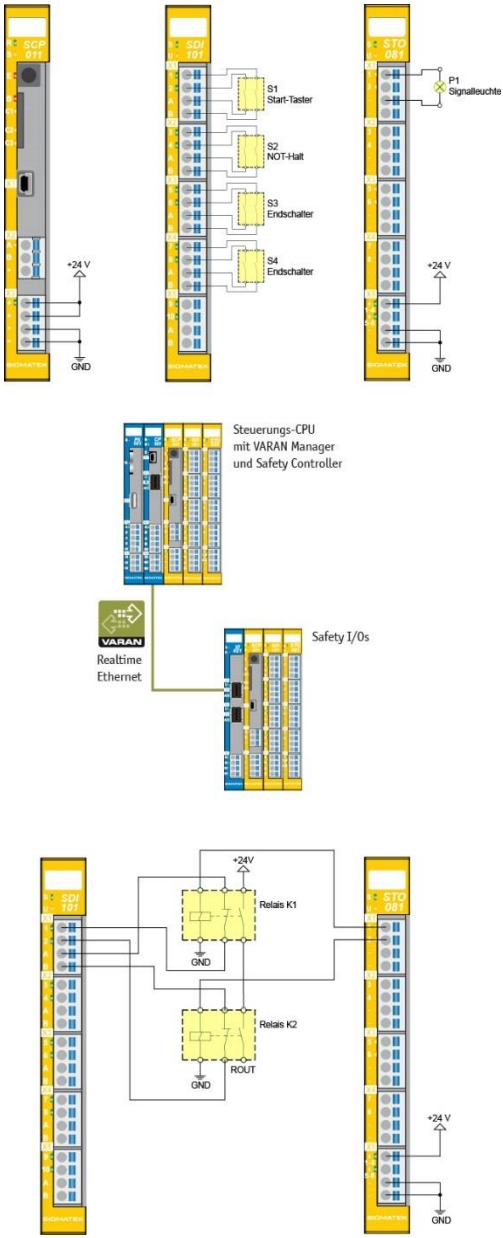


Bild 20 S-DIAS Hardwareaufbau

Verdrahtung zentraler Steuerungsaufbau	CSCP 011		CSDI 161		CSTO 081	
	Pin	**Anschluss**	**Pin**	**Anschluss**	**Pin**	**Anschluss**
	X1/1	n.c.	X1/1	Öffner Not-Halt S2 (A)	X1/1	Ansteuerung der Signalleuchte P1
	X1/2	n.c.	X1/2	Öffner Not-Halt S2 (B)	X1/2	n.c.
	X1/3	+24 V	X1/3	n.c.	X1/3	n.c.
	X1/4	GND	X1/4	n.c.	X1/4	n.c.
	X2/1	Schließer Starttaster S1 (A)	X2/1	Schließer Endschalter S3 (A)	X2/1	n.c.
	X2/2	Schließer Starttaster S1 (B)	X2/2	Schließer Endschalter S3 (B)	X2/2	n.c.
	X2/3	n.c.	X2/3	n.c.	X2/3	n.c.
	X2/4	n.c.	X2/4	n.c.	X2/4	n.c.
	X3/1	Taktausgang A	X3/1	Schließer Endschalter S4 (A)	X3/1	+24 V
	X3/2	Taktausgang B	X3/2	Schließer Endschalter S4 (B)	X3/2	+24 V
	X3/3	+24 V	X3/3	n.c.	X3/3	GND
	X3/4	GND	X3/4	n.c.	X3/4	GND
			X4/1	n.c.		
			X4/2	n.c.		
			X4/3	n.c.		
			X4/4	n.c.		
			X5/1	Taktausgang A		
			X5/2	Taktausgang B		
			X5/3	+24 V		
			X5/4	GND		

Tabelle 8 Beschaltung der zentralen Sicherheitsmodule

Verdrahtung dezentraler Steuerungsaufbau	CSDI 161		CSTO 081	
	Pin	**Anschluss**	**Pin**	**Anschluss**
	X1/1	n.c.	X1/1	n.c.
	X1/2	n.c.	X1/2	n.c.
	X1/3	n.c.	X1/3	n.c.
	X1/4	n.c.	X1/4	n.c.
	X2/1	n.c.	X2/1	Relaisansteuerung K1
	X2/2	n.c.	X2/2	Relaisansteuerung K2
	X2/3	n.c.	X2/3	n.c.
	X2/4	n.c.	X2/4	n.c.
	X3/1	n.c.	X3/1	+24 V
	X3/2	n.c.	X3/2	+24 V
	X3/3	n.c.	X3/3	GND
	X3/4	n.c.	X3/4	GND
	X4/1	Öffner Relais K1 (A)		
	X4/2	Öffner Relais K2 (B)		
	X4/3	n.c.		
	X4/4	n.c.		
	X5/1	Taktausgang A		
	X5/2	Taktausgang B		
	X5/3	+24 V		
	X5/4	GND		

Tabelle 9 Beschaltung der dezentralen Sicherheitsmodule

Konfiguration

Zuerst werden im SafetyDesigner die verwendeten Sicherheitsmodule im Hardwaretree platziert. Der entsprechende Hardwaretree dieses Beispielprojekts ist in
Bild **21** dargestellt.

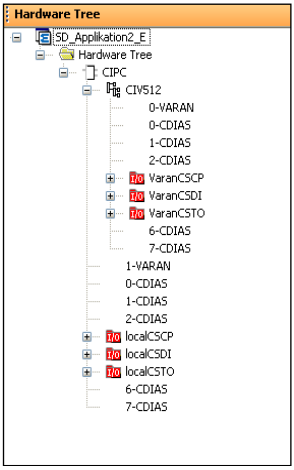


Bild 21 Hardwaretree des Beispielprojekts 2

Die Konfiguration wurde in diesem Beispielprojekt wie folgt umgesetzt:
Der Starttaster S1_A und S1_B, die an die Safety-CPU angeschlossen sind, werden über ein UND-Gatter miteinander verknüpft. Das Ergebnis wird in einer sicheren temporären Variable (StartSignal) vermerkt. Die Konfiguration des Starttasters S1_A ist in
Bild **22** abgebildet. Dabei wurde die Querschlusserkennung (Cross Circuit Detection auf A) aktiviert. Analog dazu ist der Starttaster S1_B mit Takt B konfiguriert.

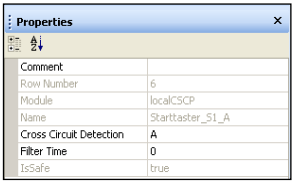


Bild 22 Konfiguration des Starttasters S1_A

Ebenso wie der Starttaster S1 werden auch die Schalter S2, S3 und S4 konfiguriert. Die Not-Halt-Funktionalität wurde mit dem Funktionsblock SF_EmergencyStop umgesetzt. Mit Hilfe des StartSignals, welches von einem sicheren Signal mit dem Funktionsblock Safebool to Bool in ein Boolsches Signal umgewandelt wird, wird der Reset des SF_EmergencyStop-

Funktionsblocks angesteuert. Die nichtverwendeten sicheren Eingänge diese Funktionsblocks werden über sichere Konstanten deaktiviert.

Mit dem Funktionsblock SF_GuardMonitoring wird die 500 ms Verzögerungszeit beim Schalten von S3 bzw. S4 des jeweiligen anderen Schalters realisiert. Dazu wird der Eingang Discrepancy mit einer Konstanten von 500 ms beschaltet. Die Resetfunktionalität wird wie vorher mit dem StartSignal sichergestellt. Die Ergebnisse der zwei komplexen Funktionsblöcke werden in den zwei temporären Variablen Emergency und GuardLockingState gemerkt und anschließend mit einem UND-Gatter verknüpft. Das Ergebnis dieses UND-Verknüpfung wird auf den sicheren Ausgang des lokalen Ausgangsmoduls auf die angeschlossene Signalleuchte geführt.

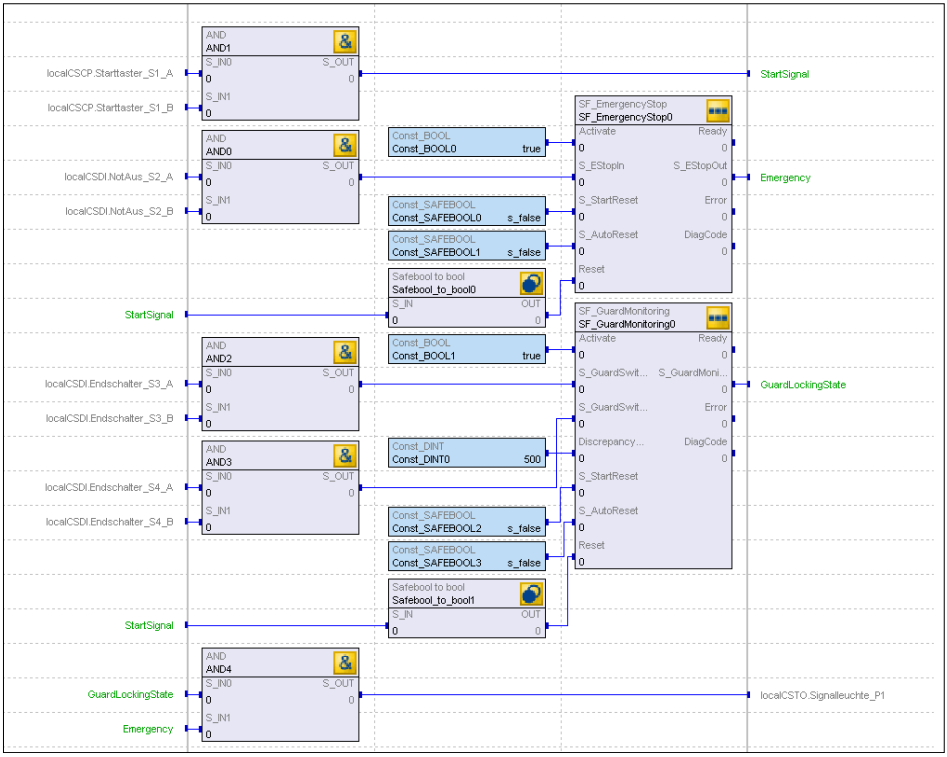


Bild 23 Lokales Netzwerk SafeCPU

Der Ausgang Signalleuchte_P1 wird von einem zweiten Netzwerk wieder zurückgelesen und steuert den komplexen Funktionsblock SF_EDM an. Die beiden in Serie geschalteten Relaiskontakte werden auf die sicheren Eingänge S_EDM1 und S_EDM2 zurückgelesen und in einem 50 ms Zeitfenster überwacht. Dies wird mit einer Konstanten, die mit dem Wert von 50 ms konfiguriert werden muss, realisiert.

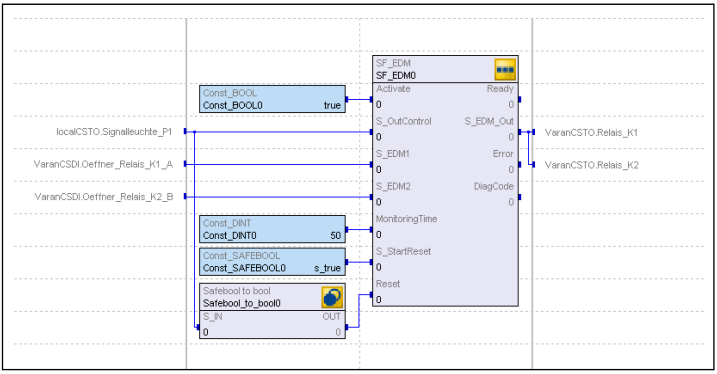


Bild 24 Netzwerk 2

3.2.1.3 Beispiel 3: Zweihandtaster

In diesem Beispiel wird eine dezentrale Verdrahtung dargestellt. An den sicheren Eingängen DI1 & DI2 des sicheren Eingangsmoduls CSDI 161 wird ein Zweihandschalter angeschlossen der über die Taktausgänge des Eingangsmoduls versorgt wird. So können u. a. Querschlüsse zwischen den sicheren Eingängen konfiguriert und somit erkannt werden. Über ein Bussystem z.B. C-DIAS und VARAN ist das sichere Eingangsmodul mit einer Safety-CPU verbunden. In der Safety-CPU wird die Sicherheitsapplikation abgearbeitet, d.h. die Eingänge vom sicheren Eingangsmodul werden eingelesen und an die sichere CPU weitergeleitet. Die Verarbeitung der sicheren Eingänge erfolgt in der Safety-CPU. Das Ergebnis der sicheren Applikation wird in diesem Beispiel an ein entferntes Ausgangsmodul weitergeleitet. Dieses schaltet dann einen Aktor, z.B. eine Signallampe ein bzw. aus.

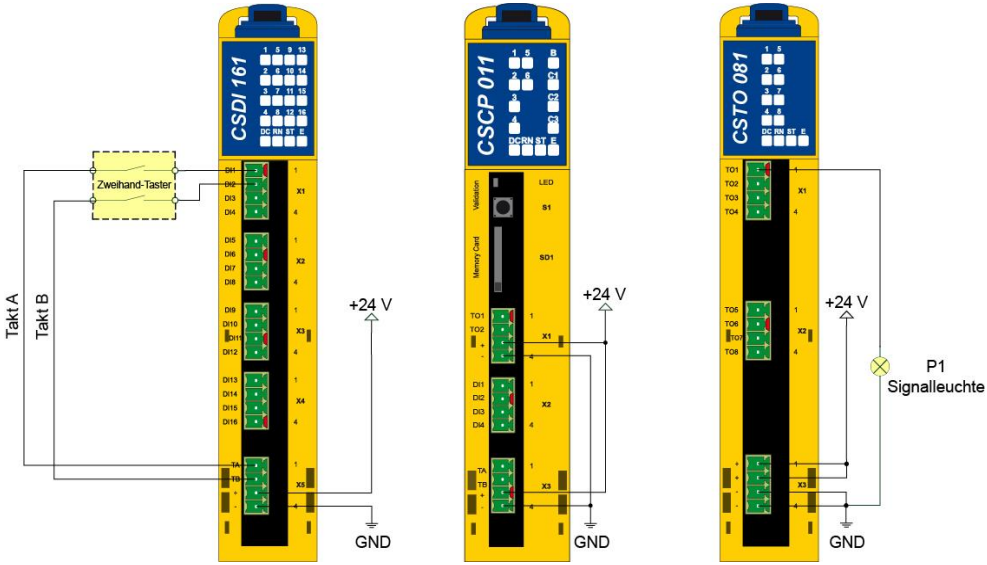


Bild 25 C-DIAS Hardwareaufbau des Beispiels 3

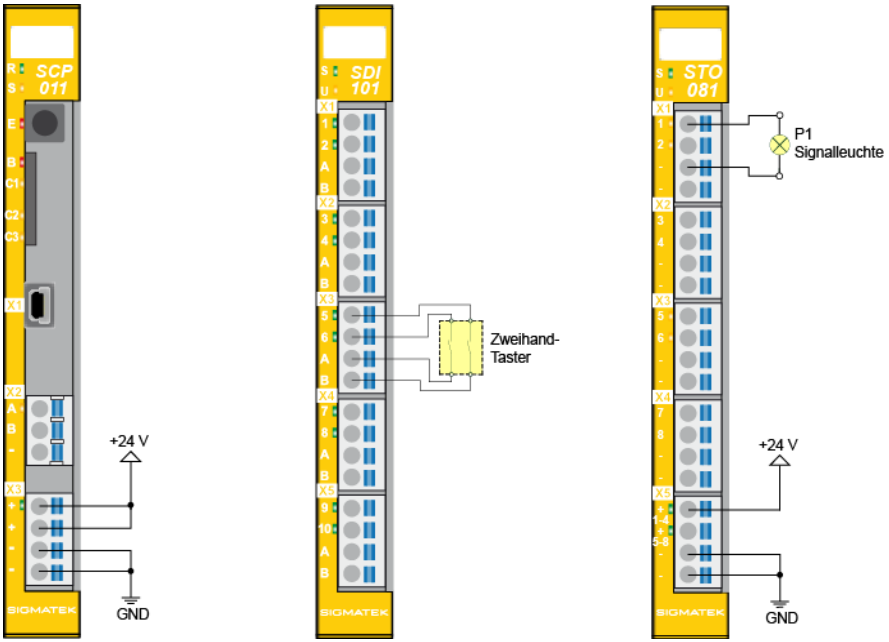


Bild 26 S-DIAS Hardwareaufbau des Beispiels 3

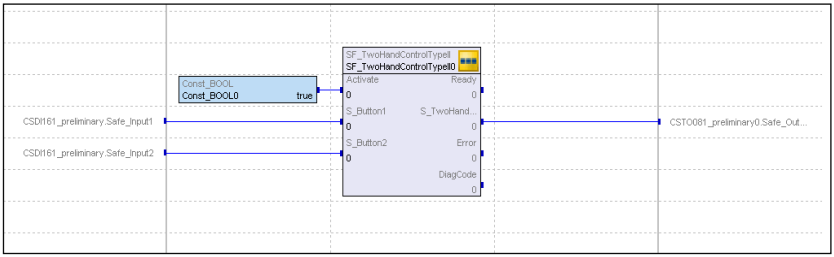


Bild 27 Mögliche Sicherheitsapplikation

3.2.1.4 Beispiel 4: Mutinglampe

Mit einem sicheren Ausgang eines Sicherheitsmoduls, z.B. einer Safety-CPU kann eine Mutinglampe angesteuert werden.

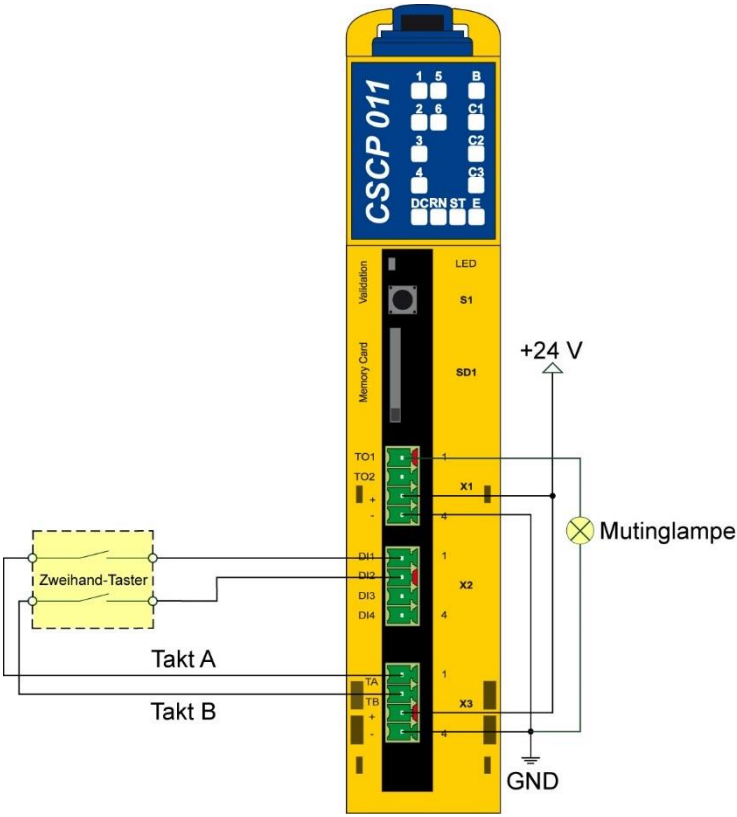


Bild 28 C-DIAS Ansteuerung einer Muting-Lampe

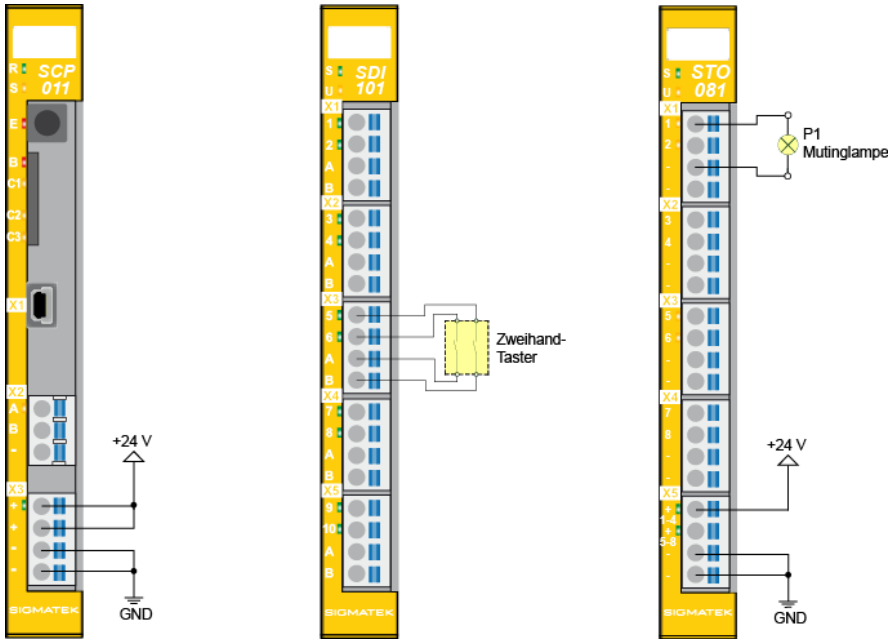


Bild 29 S-DIAS Ansteuerung einer Muting-Lampe

3.2.1.5 Beispiel 5: Optionale Module (ab Revision 2)

In diesem Beispiel wird die Verwendung eines optionalen Moduls beschrieben. Ein sicherer Eingang eines optionalen Eingangsmoduls CSDI 162 wird von einer Safety-CPU CSCP 012 verwendet.

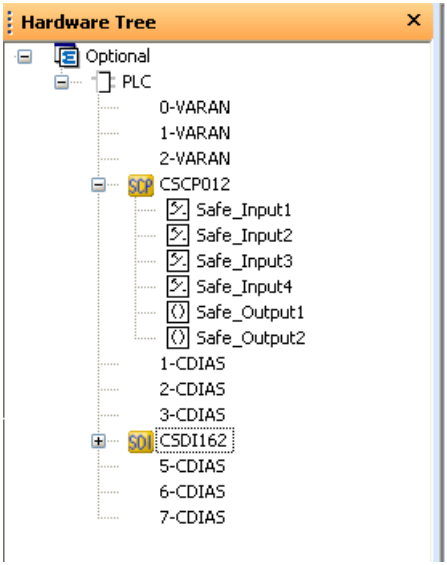


Bild 30 Möglicher Hardwareaufbau

In der Safety-CPU wird die Sicherheitsapplikation abgearbeitet, d.h. der Eingang des Eingangsmoduls wird ausgelesen und an die Safety-CPU weitergeleitet. Die Verarbeitung der sicheren Eingänge erfolgt in der Safety-CPU.

Da das Eingangsmodul optional ist, muss das Modul nicht vorhanden sein, d.h. es müssen keine Eingänge an die Safety-CPU weitergeleitet werden. In der Sicherheitsapplikation der Safety-CPU muss über die Funktionsblöcke SF_Optional_Pwd und SF_Optional_Switch die Abarbeitung des optionalen Eingangs gesteuert werden. Im Funktionsblock SF_Optional_Pwd wird passwortgeschützt eingestellt, ob ein optionaler Eingang eines Moduls verwendet wird. Im Funktionsblock SF_Optional_Switch wird entweder der Wert des Eingangs oder ein vom Anwender eingestellter Defaultwert weitergeschalten. Die Weiterschaltung erfolgt in Abhängigkeit vom Passwort-Funktionsblock.

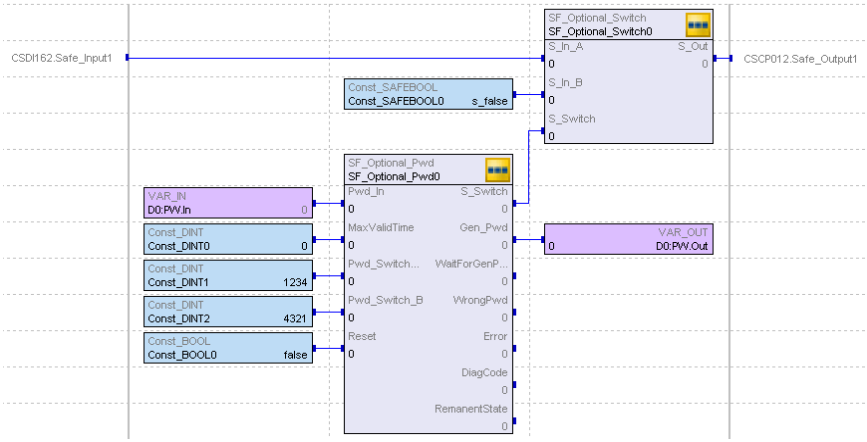


Bild 31 Mögliche Sicherheitsapplikation

3.2.1.6 Beispiel 6: Interfaces (ab Revision 2)

In diesem Beispiel wird die Verwendung von schreibenden und lesenden Interfaces beschrieben. Interfaces sind Variablen über die projektübergreifend zwischen Safety CPUs kommuniziert wird (Safety CPUs sind in verschiedenen Safety-Projekten). Dies bedeutet, dass eine Safety-CPU die Daten schreibend zur Verfügung stellt und eine andere Safety CPU diese Daten lesend verarbeitet. Ein schreibendes Interface wird von einer Safety-CPU CSCP 012_1 im VARAN-System 1 zur Verfügung gestellt. Dieses Interface wird von einer zweiten Safety CPU CSCP 012_2 im VARAN-System 2 als lesendes Interface verwendet. Die beiden Safety-CPUs sitzen am Bus-Master und sind in zwei unabhängigen VARAN-Systemen platziert. Die VARAN-Systeme sind über ein Interface Modul VBC 021 miteinander verbunden. Das schreibende Interface wird im Safety-Projekt des VARAN-Systems 1 erstellt und beim Netzwerk der Safety-CPU CSCP 012_1 als Ausgang gesetzt. In der SPS-Applikation des VARAN-Systems 1 wird das Interface in das VBC 021-Modul geschrieben. In der SPS-Applikation des VARAN-Systems 2 wird das Interface aus dem VBC 021-Modul gelesen.

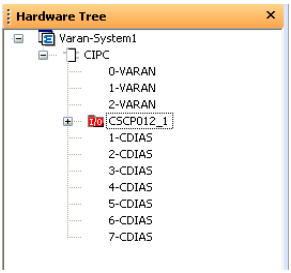


Bild 32 Möglicher Hardwareaufbau VARAN-System 1

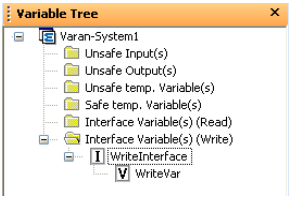


Bild 33 Mögliches Interface (Write)

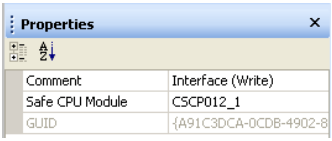


Bild 34 Mögliche Einstellungen

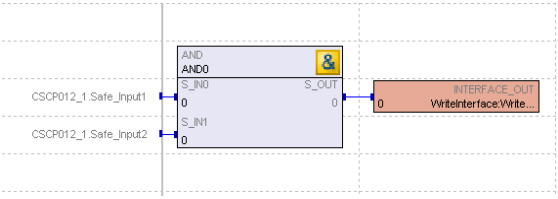


Bild 35 Mögliche Sicherheitsapplikation VARAN-System 1

Das exportierte, schreibende Interface wird im Safety-Projekt des VARAN-Systems 2 importiert und als lesendes Interface im Netzwerk der Safety-CPU CSCP 012_2 verwendet.

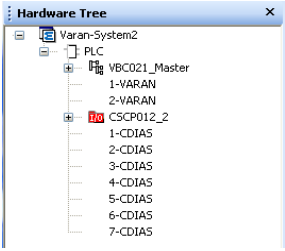


Bild 36 Möglicher Hardwareaufbau VARAN-System 2

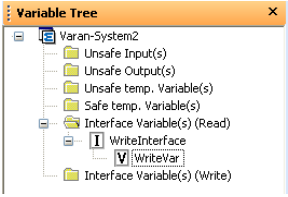


Bild 37 Mögliches Interface (Read)

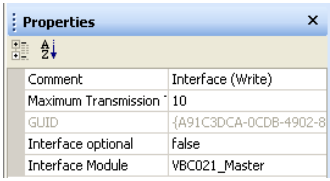


Bild 38 Mögliche Einstellungen

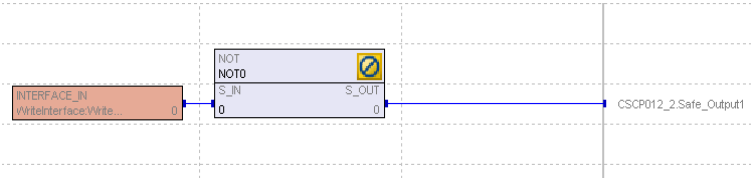


Bild 39 Mögliche Sicherheitsapplikation VARAN-System 2

Das Interface Module VBC 021 muss in beiden LASAL Class 2-Projekten platziert sein. Für die Übertragung der Interfaces müssen bei den Instanzen der Interface-Module Speicherbereiche reserviert werden (siehe Beschreibung Hardwareklassen in LASAL Class 2).

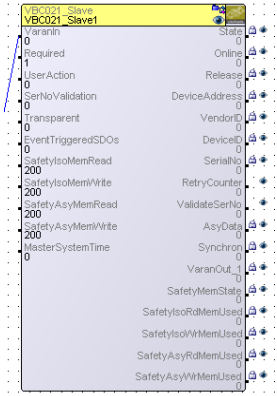


Bild 40 Mögliche Einstellung Speicherbereiche (VARAN-System 1)

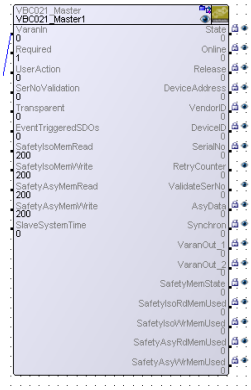


Bild 41 Mögliche Einstellung Speicherbereiche (VARAN-System 2)

3.2.1.7 Beispiel 7: Kontakterweiterung

Mit der sicheren Kontakterweiterung ist es dem Anwender möglich, aus einem sicheren elektronischen Ausgang mehrere potentialfreie Kontakte zu realisieren. Die Kontakterweiterung kommt überall dort zum Einsatz, wo potentialfrei geschaltet werden muss oder der Strom des elektronischen sicheren Ausgangs nicht ausreicht.

Einfacher fehlersicherer Ausgang

Bild 42 zeigt das Beispiel einer Kontakterweiterung durch zwei redundante Relais bei massebezogener (Ext. GND) Ansteuerung durch einen sicheren Ausgang TO1. Das Relais muss über zwangsgeführte Kontakte verfügen (beispielsweise 3 Schließer, 1 Öffner), von welchen der Öffner für die Rücklesung des Schaltzustandes (Querschlusserkennung) vorgesehen ist; der Öffner wird auf der einen Seite an den Takt TA angeschlossen, der auf der anderen Seite über einen sicheren Eingang DI1 eingelesen wird. Wenn die Kontakterweiterung in einem Schaltschrank untergebracht wird oder/und wenn die Verbindungsleitungen geschützt verlegt sind, ist ein Fehlerausschluss hinsichtlich Fremdeinspeisung möglich, so dass die Anforderungen von Kategorie 3/4 und PL d/e gemäß EN ISO 13849-1 und von SIL 2/3 gemäß EN 62061 erfüllt werden können.

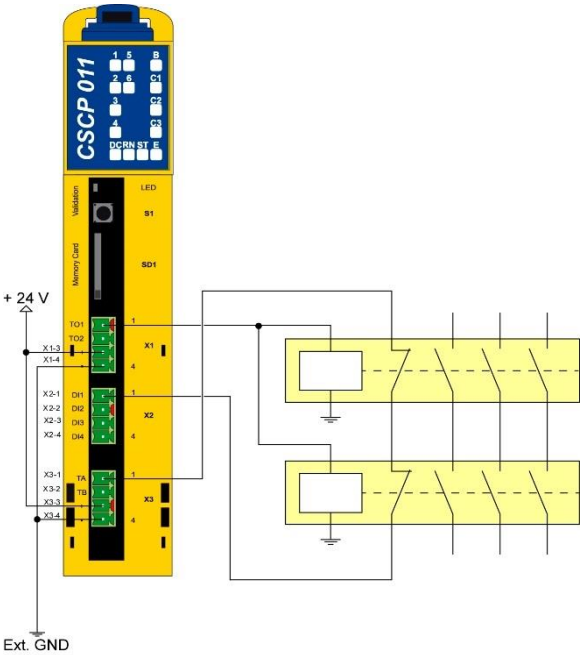


Bild 42 Einfacher fehlersicherer Ausgang

Zweikanaliger Ausgang

Im Gegensatz dazu zeigt Bild 43 das Beispiel einer zweikanaligen Kontakterweiterung mit der die Anforderungen nach Kategorie 4 und PL e gemäß EN ISO 13849-1 und von SIL 3 gemäß EN 62061 erfüllt werden können. Jedes Relais wird jeweils an einen sicheren Ausgang TO1 und TO2 angeschlossen und verfügt über einen eigenen Rücklesekreis mittels der Takte TA und TB, die über zwei sichere Eingänge DI1 und DI2 eingelesen werden (Querschlusserkennung). Die Relais müssen auch hier über zwangsgeführte Kontakte verfügen.

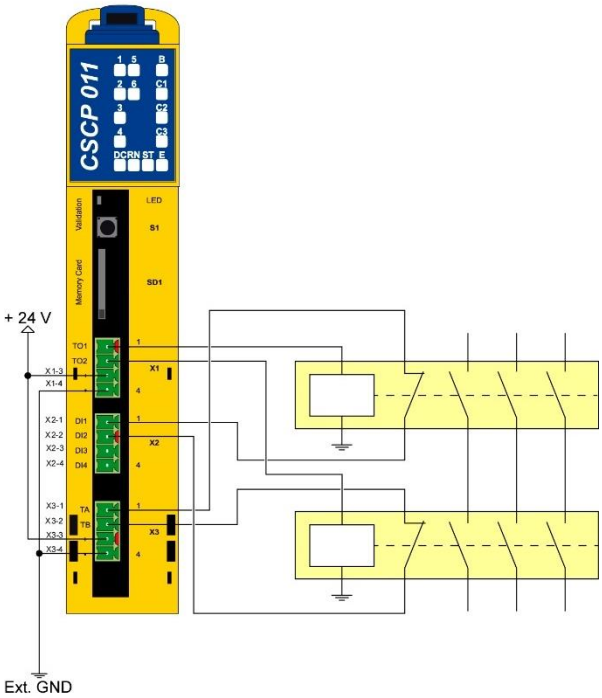


Bild 43 Zweikanaliger Ausgang

4 Inbetriebnahme und Konfiguration

4.1 Erstellen des Standard-Steuerungsprojekts

Die Safety-Komponenten werden wie die C-DIAS Standardkomponenten in ein LASAL-Projekt eingesetzt. Dabei steht für jedes Sicherheitsmodul eine Hardwareklasse zur Verfügung. Jedes Sicherheitsmodul mit sicheren Ausgängen besitzt dabei für jeden sicheren Ausgang eine Variable „Unsafe Output“. Diese Variable kann von der Standard-SPS angesteuert werden. Wird diese Variable verwendet, so ist sie im SafetyDesigner zu konfigurieren. Die unsichere Freigabevariable ist somit mit dem entsprechenden sicheren Ausgang UND-verknüpft; d.h. wenn die sichere Applikation den sicheren Ausgang setzt, so kann dieser Ausgang von der Standard-SPS trotzdem abgeschaltet werden. Diese Variable kann jedoch keinen ausgeschalteten sicheren Ausgang einschalten.

Nachdem die Sicherheitsmodule in der LASAL-Umgebung eingesetzt und dementsprechend verdrahtet worden sind, ist die Standardapplikation zu validieren; d.h. zu prüfen, ob beim Online gehen mit der Standard-SPS alle Module gefunden werden.

4.2 Erstellen der sicheren Applikation über den SafetyDesigner

4.2.1 Erstellen der Konfiguration

Beim Erstellen der Konfiguration kann entweder der Hardwaretree online eingelesen bzw. manuell im SafetyDesigner aufgebaut werden oder über eine, in LASAL Class 2 erstellte Datei, eingelesen werden. Zum Online gehen wird die IP-Adresse der Standard-SPS benötigt. Zum Online gehen auf ein S-DIAS Safety-Modul im Standalone-Betrieb wird die COM-Schnittstelle, an welcher das Modul hängt, benötigt. Zum Aufbau der sicheren Applikation stehen Standardlogikblöcke und komplexe PLC-Open-ähnliche Funktionsblöcke zur Verfügung. Die Erstellung der Konfiguration ist im LASAL SafetyDesigner beschrieben.

Beim Erstellen der Konfiguration sind folgende Punkte zu beachten:

- Ein sicherer Ausgang kann jeweils nur durch ein Signal gesetzt werden.
- Ein sicherer Eingang kann mehrfach verwendet werden.
- Die Sicherheitsmodule, die von einem Projekt verwendet werden, können nicht gleichzeitig von einem anderen Projekt verwendet werden. Werden in der Konfiguration Sicherheitsmodule von einem anderen Projekt verwendet, so wird beim Verteilen der Konfiguration das entsprechende Sicherheitsmodul neu konfiguriert.
- Die Verdrahtung ist insbesondere bei den sicheren Eingängen und deren Konfiguration zu beachten (Zweikanaligkeit, Querschlusserkennung, usw.).

4.2.2 Konfiguration des Systems

Nach dem Erstellen der Konfiguration muss mit dem SafetyDesigner online gegangen werden, um die Konfiguration auf die entsprechende Safety-CPU(s) übertragen zu können. Dazu ist ein Wechsel in den Service Mode der Safety-CPU vorzunehmen. Für diesen Wechsel ist es notwendig, sich mit dem entsprechenden Passwort anzumelden. Ist noch kein Passwort vergeben worden, muss ein solches zuerst angelegt werden.

☞	**WICHTIG!** Bei der ersten Inbetriebnahme ist für die Safety-CPU noch kein Passwort vergeben (Auslieferungszustand der Safety-CPU ohne Passwort). Der Anwender muss ein Passwort auf der Safety-CPU setzen. Dazu ist im Online Mode der „Change Password Button“ zu drücken. Mit dem Change Password Dialog kann nun das neue Passwort auf der Safety-CPU gesetzt werden. Das Eingabefeld des alten Passwortes bleibt leer, die Eingabefelder für das neue Passwort und für die Bestätigung des neuen Passwortes müssen ausgefüllt werden (Länge des Passwortes 6-8 Zeichen).

Ist der Wechsel in den Service Mode erfolgt, kann mit dem Button „Download“ die Konfiguration auf die Safety-CPU übertragen werden. Wird die Onlineverbindung während des Downloads zum SafetyDesigner getrennt, befindet sich eine ungültige Konfiguration auf der Safety-CPU und die sicheren Ausgänge verbleiben im sicheren Zustand. Der Download muss nach Wiederherstellen der Onlineverbindung wiederholt werden.

Nach dem Download ist der „Start“ Button zu betätigen. Nun wird die Konfiguration auf die entfernten Sicherheitsmodule, falls vorhandenen, verteilt (Betriebszustand Check Config). Nachdem die Konfiguration verteilt wurde, wechselt das System in den zeitlich begrenzten Laufzeitzustand. Die maximale Zeit, in der in diesem Zustand verharrt wird, kann konfiguriert werden und beträgt 8 Stunden. Wird diese Zeitdauer überschritten, wechselt das System in den Fehlerzustand und die sicheren Ausgänge werden abgeschaltet.

Der Sinn des zeitlich begrenzten Laufzeitzustandes besteht darin, dem Anwender die Möglichkeit zu geben, die Validierung des Sicherheitssystems vorzunehmen. Bei der Validierung ist zu prüfen, ob sich das Sicherheitssystem wie erwartet verhält. Die Validierung umfasst unter anderem folgende Punkte:

- ***Überprüfung der Verdrahtung***
  Hierbei muss geprüft werden, ob alle Ein- und Ausgänge wie konfiguriert verdrahtet sind. Bei den sicheren Eingängen ist insbesondere darauf zu achten, dass die Eingänge korrekt mit den Takten versorgt werden.

- ***Funktionstests***
  Auf jeden Schaltvorgang der sicheren Eingänge ist die Reaktion zu überprüfen. So muss beispielsweise bei Betätigung eines Not-Halt am Eingang ein bestimmter Ausgang innerhalb der konfigurierten Reaktionszeit abschaltet werden. Alle Schaltvorgänge im Sicherheitssystem und deren Reaktionen müssen in dieser Weise simuliert und nachgeprüft werden.

Wurde die Validierung erfolgreich durchgeführt, kann mit dem Befehl „Set Verified“ im Service Mode in den zeitlich unbegrenzten Laufzeitzustand gewechselt werden.

WICHTIG!
Bei der Validierung des Sicherheitssystems müssen alle Sicherheitsfunktionen auf ihre korrekte Ausführung überprüft werden.

Beim Tausch oder nachträglichen Hinzufügen optionaler Safety Module muss das System immer neu konfiguriert und validiert werden. Dies kann entweder mit Hilfe des SafetyDesigners oder der SD-Karte erfolgen.
Erfolgt diese erneute Validierung nicht, verliert die SCP ihre Konfiguration und wechselt in einen Fehlerzustand (ERRVAL 222 / 1222 Temporary Operation Time – siehe Kap. 2.6.4). Dies ist eine Sicherheitsmaßnahme für unautorisierte Module in unserem Safety-System.

4.3 Konfiguration über die SD-Karte

4.3.1 Beschreiben der SD-Karte

Beim Beschreiben der SD-Karte wird das jeweils geöffnete SafetyDesigner-Projekt auf die SD-Karte gespeichert. Dies kann nur mit Hilfe des SafetyDesigners vorgenommen werden. Um die SD-Karte zu beschreiben, ist folgendermaßen vorzugehen:

4.3.1.1 Wechsel in den Service Mode

Nachdem mit Hilfe des SafetyDesigners in den Service Mode gewechselt worden ist, kann die SD-Karte in die Safety-CPU eingesteckt werden.

☞	**WICHTIG!** Die SD-Karte darf nicht während des normalen Betriebs (Operational bzw. temporary Operational Betriebsmodus) in die Safety-CPU eingesteckt werden. Geschieht dies dennoch, so wechselt die Safety-CPU in den Fehlerzustand (Fehlermeldung 88 bzw. 1088). Tritt dieser Fehler auf, ist die SD-Karte zu entnehmen und ein „Quit Error“-Befehl abzusetzen. Nach Behebung des Fehlers kann in den Service Mode gewechselt und die SD-Karte eingesteckt werden.

4.3.1.2 Beschreiben der SD-Karte

Im Service-Mode wird im SafetyDesigner der Befehl „Write SD-Card“ freigeschaltet. Mit diesem Befehl kann nun das geöffnete Projekt im SafetyDesigner auf die Safety-CPU übertragen werden.

4.3.1.3 Rückkehr zum normalen Betriebsmodus

Nach dem Beschreiben der SD-Karte kann diese aus der Safe CPU entnommen und anschließend in den Operational bzw. temporary Operational-Modus zurückgewechselt werden.

☞	**WICHTIG!** Ist die Konfiguration auf der SD-Karte die gleiche wie im Flash der entsprechenden Safety-CPU, so kann auch mit eingesteckter SD-Karte in den Operational Mode zurückgewechselt werden. Unterscheidet sich die Konfiguration auf der SD-Karte und die im Flash der Safety-CPU, so wechselt das System anstatt in den Operational Mode in den Fehlerzustand (Fehlermeldung 87 bzw. 1087). Tritt der Fehler auf, muss die SD-Karte entnommen und ein „Quit Error“ Befehl abgesetzt werden.

4.3.2 Konfigurieren einer Safety-CPU über die SD-Karte

Um die auf einer SD-Karte gespeicherte Konfiguration in den Flash-Speicher einer Safety-CPU zu übernehmen ist wie folgt vorzugehen:

4.3.2.1 Konfiguration im Flash-Speicher der Safety-CPU löschen

Um die Konfiguration von der SD-Karte übernehmen zu können, muss zunächst die Konfiguration auf der Safety-CPU gelöscht werden. Dies kann entweder mit dem SafetyDesigner (Einloggen in den Service Mode und den Befehl „Clear“ ausführen) oder über den Validierungstaster an der Safety-CPU durchgeführt werden. Nachdem die Konfiguration auf der Safety-CPU gelöscht ist, kann die Safety-CPU nicht mehr in den Operational bzw. temporary Operational Laufzeitzustand zurückwechseln. Die Safety-CPU verharrt im Service Mode.

4.3.2.2 System abschalten und SD-Karte einstecken

Im nächsten Schritt ist das System herunterzufahren. Danach muss die SD-Karte mit der gültigen Konfiguration in die Safety-CPU eingesteckt werden.

4.3.2.3 System einschalten mit SD-Karte

Beim Wiederanlauf des Systems wird die Konfiguration von der SD-Karte in den Flash-Speicher der Safety-CPU übertragen. Dies ist jedoch nur möglich, wenn sich auf der SD-Karte eine gültige Konfiguration befindet.

☞	**WICHTIG!** Besitzt die SD-Karte ein falsches Format (Fehlermeldung 86 bzw. 1086) oder ist der Flash-Speicher der Safety-CPU nicht gelöscht (Fehlermeldung 87 bzw. 1087), so wird dies erkannt und die Safety-CPU wechselt in den Fehlerzustand. In diesen Fällen muss die SD-Karte neu beschrieben werden. Der Fehler kann durch Entnahme der SD-Karte und anschließende Quittierung des Fehlers mit Hilfe eines „Quit Error“ Befehls aufgehoben werden. Stimmt die Konfiguration mit den real vorhandenen Modulen nicht überein, so schlägt der Verteilungsvorgang der Konfiguration fehl (Fehlermeldung 9 bzw. 1009) und die Safety-CPU wechselt gleichfalls in den sicheren Zustand. In diesem Fall ist die Konfiguration zu überprüfen, d.h. es muss kontrolliert werden, ob alle benötigten Sicherheitsmodule auch vorhanden sind, diese sich nicht im Fehlerzustand befinden und die Standardkommunikation zu diesen Sicherheitsmodulen intakt ist.

4.4 Konfiguration eines sicheren Eingangs

4.4.1 Aufbau eines sicheren digitalen Eingangs

Bild **44** zeigt die Struktur der sicheren Eingangsschaltung:

Der Eingang ist nach IEC 61131-2, Typ 1, ausgelegt, gegen Überspannung geschützt und besitzt eine feste Eingangsverzögerungszeit.

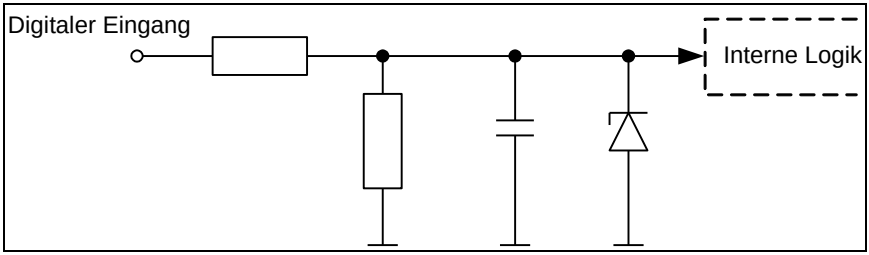


Bild 44 Aufbau eines digitalen Eingangs

Das digitale Eingangssignal wird durch einen Spannungsteiler auf ein niedrigeres Potential gebracht. Spannungsteiler und Kondensator verursachen eine Verzögerung des Eingangssignals, die bei der Berechnung der Reaktionszeit berücksichtigt werden muss. Die Zener-Diode schützt die interne Logik vor Überspannungen.

Die Zeitverzögerung, mit der ein Wechsel des Eingangssignals detektiert werden kann, beträgt maximal 2,5 ms. Eine zusätzliche Filterzeit kann mit Hilfe des SafetyDesigners hinzugefügt werden.

4.4.2 Konfiguration eines sicheren Eingangs

Ein jeder sichere Eingang besitzt die folgenden Konfigurationseigenschaften:

- Maximum Transmission Time (nicht Revision 4)
- Filter Time (Revision 1 und ab Revision 3)
- Cross Circuit Detection

Diese Eigenschaften können mit Hilfe des LASAL-SafetyDesigners eingestellt werden. Durch Anklicken eines Eingangs können diese Eigenschaften im Feld „Properties“ des SafetyDesigners zugewiesen werden. Diese Größen sind wie folgt definiert:

4.4.2.1 Maximum Transmission Time

Hierbei handelt es sich um die Zeit, innerhalb der ein eingelesener Eingang aktualisiert werden muss. Diese Zeit wird vor allem von der eingestellten Taktfrequenz des Busses bestimmt. Standardmäßig ist im SafetyDesigner eine Maximum Transmission Time von 10 ms (Revision 1) angegeben. Ab Revision 2 wird beim Einfügen des Moduls die Zeit ermittelt und eingetragen. Dabei wird davon ausgegangen, dass der Standardbus im Millisekundenraster arbeitet. Die Maximum Transmission Time kann zwischen 1 ms und 100 ms eingestellt werden.

4.4.2.2 Maximum Transmission Time (Output as Input)

Hierbei handelt es sich um die Zeit, innerhalb der ein rücklesender Ausgang aktualisiert werden muss. Diese Zeit wird vor allem von der eingestellten Taktfrequenz des Busses bestimmt. Standardmäßig ist im SafetyDesigner eine Maximum Transmission Time von 10 ms (Revision 1) angegeben. Ab Revision 2 wird beim Einfügen des Moduls die Zeit ermittelt und eingetragen. Dabei wird davon ausgegangen, dass der Standardbus im Millisekundenraster arbeitet. Die Maximum Transmission Time der rücklesenden Ausgänge kann zwischen 1 ms und 100 ms eingestellt werden.

4.4.2.3 Filter Time (Revision 1 und ab Revision 3)

Hierbei handelt es sich um den Softwarefilter, der ebenfalls zwischen 1 ms und 100 ms eingestellt werden kann. Der Softwarefilter ist vor allem hilfreich, um Störimpulse am Eingangssignals besser unterdrücken zu können.

4.4.2.4 Cross Circuit Detection

Sollen Querschlüsse erkannt werden, müssen die sicheren Eingänge mit den Signalen der Taktausgänge des jeweiligen Sicherheitsmoduls versorgt werden. Dabei ist der eine Eingang mit Takt A und der zweite mit Takt B zu verbinden und im SafetyDesigner zusätzlich zur Verdrahtung noch gesondert im Feld „Cross Circuit Detection“ zu konfigurieren. Ist die Querschlusserkennung aktiviert, so verändern sich die Reaktionszeiten.

☞	**WICHTIG!** Die Einstellungen der Maximum Transmission Time, der Filter Time und der Cross Circuit Detection haben direkt Einfluss auf die Reaktionszeit des Systems (siehe Kapitel 4.8)

4.4.3 Beschaltungsbeispiele eines sicheren Eingangs

4.4.3.1 Einkanaliges Einlesen mit Taktversorgung und Querschlusserkennung

Das C-DIAS und S-DIAS Safety-System unterstützt ein einkanaliges Einlesen eines Sensors. Dabei ist ein Anschluss des Sensors an die Taktversorgung von Takt A oder Takt B des entsprechenden Sicherheitsmoduls anzuschließen. Der Ausgang des Sensors, der mit dem Taktausgang A oder B versorgt wird und auf einen sicheren Eingang zu verdrahten ist, muss auf dem entsprechenden Sicherheitsmodul konfiguriert werden. Dies ist über den LASAL-SafetyDesigner einzustellen. Dabei muss der Eingang 1 - im folgenden Beispiel im Feld Cross Circuit Detection - mit Takt A konfiguriert werden. Nähere Informationen dazu sind in der Beschreibung zum LASAL SafetyDesigner zu finden.

Die Taktausgänge werden alle 26 Sekunden für maximal 4 ms abgeschaltet.

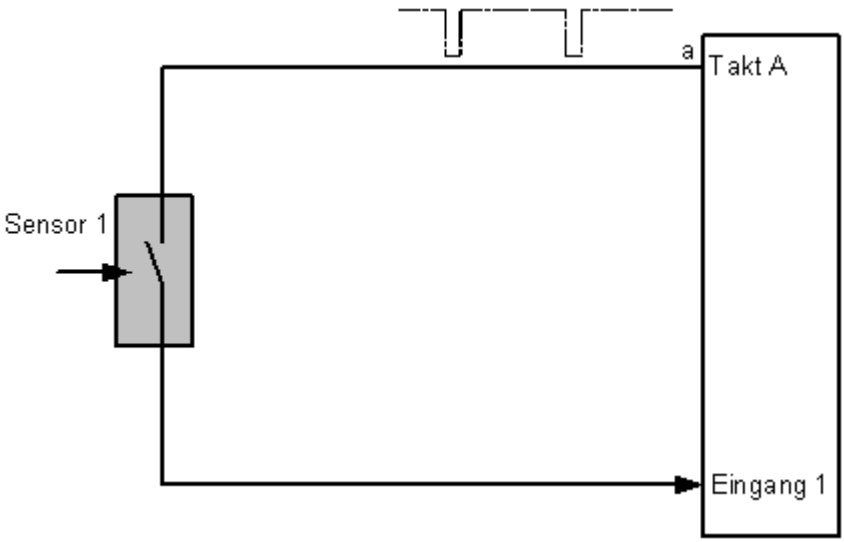
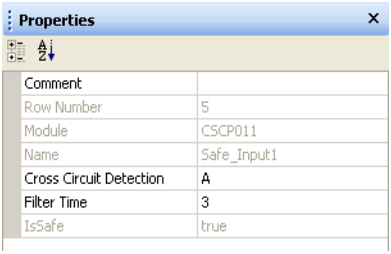


Bild 45 Einkanaliges Einlesen eines Eingangs

Im SafetyDesigner ist dieses Beispiel wie folgt aufgebaut:

Bild 46 Netzwerk einer einkanaligen Ansteuerung

Die Eingänge sind dabei wie folgt konfiguriert:



Properties

Comment	
Row Number	5
Module	CSCP011
Name	Safe_Input1
Cross Circuit Detection	A
Filter Time	3
IsSafe	true

Bild 47 Konfiguration der sicheren Eingänge

Wird eine einkanalige Verdrahtung verwendet, so können folgende Fehler detektiert werden:

- Taktimpuls konnte nicht erkannt werden – Fehlercode 102 bzw. 1102
  Ist der zu testende sichere Eingang so beschalten, dass er auf „High“ ist, und kann der Taktimpuls nicht detektiert werden, so besteht möglicherweise ein Querschluss mit der Versorgung oder der Taktausgang ist defekt. In diesem Fall ist die Verdrahtung durch den Anwender zu überprüfen. Ist die Verdrahtung korrekt, ist der entsprechende Taktausgang nachzumessen.

- Falscher Takt wird erkannt – Fehlercode 103 bzw. 1103
  Wird beim Durchführen des externen Eingangstests der falsche Takt an einem sicheren Eingang erkannt, so wird dies festgestellt. Mögliche Ursachen sind hierbei Querschlüsse oder eine falsche Verdrahtung.

	WICHTIG! Werden die Taktausgänge zur Verdrahtung verwendet, dann muss die sichere Applikation dementsprechend konfiguriert werden!

	WICHTIG! Ist der Taktausgang defekt, so dass er immer nur den Low-Zustand ausgibt, kann dies nicht detektiert werden! Kann dagegen der High-Zustand nicht mehr ausgeschalten werden, so wird dies über Taktimpulse erkannt!

In diesem Beispiel ist außerdem darauf zu achten, dass sich die Reaktionszeit um den Test der Querschlusserkennung verlängert. Die Verlängerung der Reaktionszeit beträgt 6 ms.

4.4.3.2 Einkanaliges einlesen ohne Taktversorgung und Querschlusserkennung

Wird ein Sensor einkanalig an einen sicheren Eingang angeschlossen, so muss bei der Konfiguration folgendes beachtet werden:

	WICHTIG! • Der Sensor darf nicht mit einem der Taktsignale versorgt werden, da ansonsten die Taktimpulse Auswirkungen auf die sichere Applikation haben können. • Im SafetyDesigner muss die Querschlusserkennung (Cross Circuit Detection) des einkanalig angeschlossenen Eingangs auf „0“ gesetzt sein.

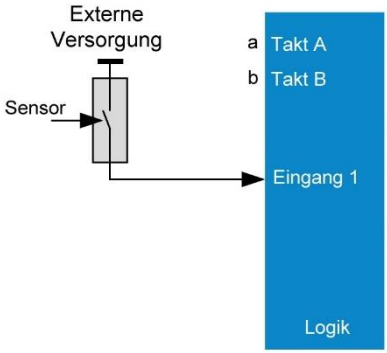


Bild 48 Einkanaliges einlesen eines Eingangs

4.4.3.3 Zweikanaliges Einlesen mit Taktversorgung und Querschlusserkennung

Das C-DIAS und S-DIAS Safety-System unterstützt ein zweikanaliges Einlesen eines Sensors, z. B. eines zweikanaligen Not-Halt-Tasters. Dabei ist ein Anschluss des Sensors an die Taktversorgung von Takt A und der andere auf die Taktversorgung von Takt B des entsprechenden Sicherheitsmoduls anzuschließen. Der Ausgang des Sensors, der mit dem Taktausgang A versorgt wird und auf einen sicheren Eingang zu verdrahten ist, muss auf dem entsprechenden Sicherheitsmodul konfiguriert werden. Dies ist über den LASAL-SafetyDesigner einzustellen. Dabei muss der Eingang 1 - im folgenden Beispiel im Feld Cross Circuit Detection - mit Takt A und der Eingang 2 mit Takt B konfiguriert werden. Auf diese Weise wird automatisch überprüft, ob die Ausgänge untereinander kurzgeschlossen sind. Nähere Informationen dazu sind in der Beschreibung zum LASAL SafetyDesigner zu finden.

Die zwei Taktausgänge werden zu verschiedenen Zeitpunkten alle 26 Sekunden für maximal 4 ms abgeschaltet.

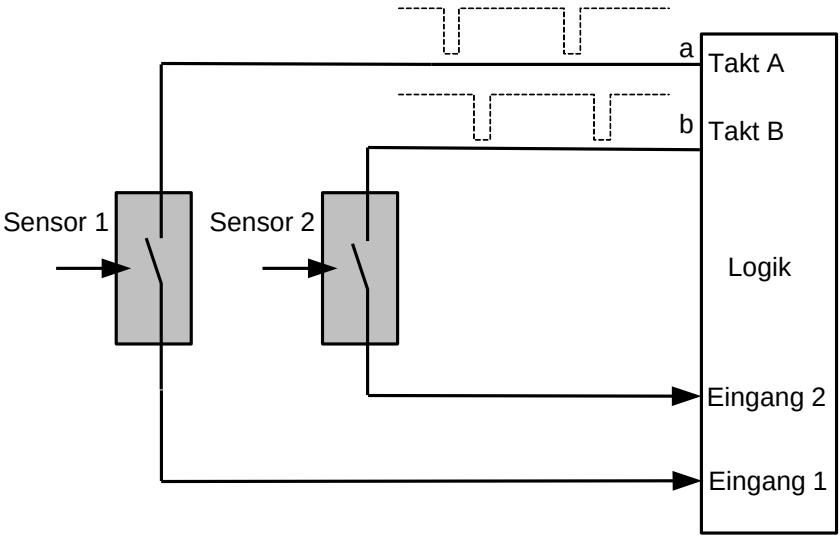


Bild 49 Zweikanaliges Einlesen eines Eingangs

Im SafetyDesigner ist dieses Beispiel wie folgt aufgebaut:

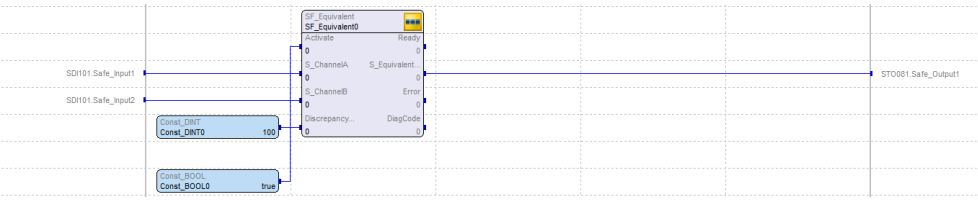
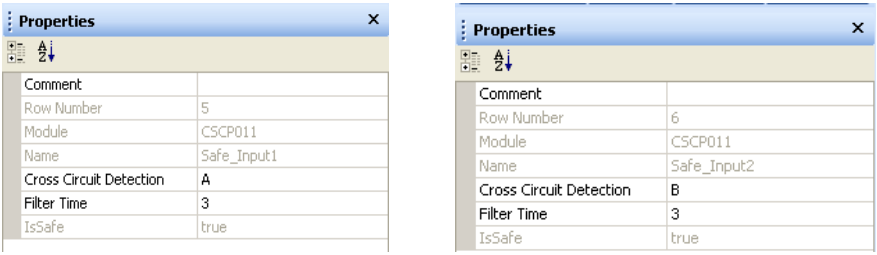


Bild 50 Netzwerk einer zweikanaligen Ansteuerung

Die Eingänge sind dabei wie folgt konfiguriert:



Properties

Comment	
Row Number	5
Module	CSCP011
Name	Safe_Input1
Cross Circuit Detection	A
Filter Time	3
IsSafe	true

Properties

Comment	
Row Number	6
Module	CSCP011
Name	Safe_Input2
Cross Circuit Detection	B
Filter Time	3
IsSafe	true

Bild 51 Konfiguration der sicheren Eingänge

Wird eine zweikanalige Verdrahtung verwendet, so können folgende Fehler detektiert werden:

- Taktimpuls konnte nicht erkannt werden – Fehlercode 102 bzw. 1102
  Ist der zu testende sichere Eingang so beschalten, dass er auf „High“ ist, und kann der Taktimpuls nicht detektiert werden, so besteht möglicherweise ein Querschluss oder der Taktausgang ist defekt. In diesem Fall ist die Verdrahtung durch den Anwender zu überprüfen. Ist die Verdrahtung korrekt, ist der entsprechende Taktausgang nachzumessen.

- Falscher Takt wird erkannt – Fehlercode 103 bzw. 1103
  Wird beim Durchführen des externen Eingangstests der falsche Takt an einem sicheren Eingang erkannt, so wird dies festgestellt. Mögliche Ursachen sind hierbei Querschlüsse oder eine falsche Verdrahtung.

	WICHTIG! Werden die Taktausgänge zur Verdrahtung verwendet, dann muss die sichere Applikation dementsprechend konfiguriert werden!

	WICHTIG! Ist der Taktausgang defekt, so dass er immer nur den Low-Zustand ausgibt, kann dies nicht detektiert werden! Kann dagegen der High-Zustand nicht mehr ausgeschalten werden, so wird dies über Taktimpulse erkannt!

In diesem Beispiel ist außerdem darauf zu achten, dass sich die Reaktionszeit um den Test der Querschlusserkennung verlängert. Die Verlängerung der Reaktionszeit beträgt 6 ms.

4.4.3.4 Zweikanaliges Einlesen

Es kann auch ein zweikanaliges Einlesen mit Querschlusserkennung realisiert werden, ohne dass sich die Reaktionszeit um die Zeit des Eingangstests verlängert. In diesem Fall sind die jeweiligen sicheren Eingänge lokal mit Äquivalenz zu verknüpfen. Das aus der Äquivalenz-Verknüpfung entstandene Signal ist im SafetyDesigner neu zu konfigurieren, d.h. die Parameter

- Cross Circuit Detection
- Maximum Transmission Time
- Filter Time (Revision 1 und ab Revision 3)

des Signals sind festzulegen.

☞	**WICHTIG!** Die Maximum Transmission Time muss für das neue Signal, das aus der Äquivalenz-Verknüpfung entsteht, erneut konfiguriert werden!

4.4.3.5 Überwachung kontaktbehafteter Sensoren am Beispiel Not-Halt

Bei der Überwachung kontaktbehafteter zweikanaliger Sensoren (vgl. Zweikanaliges Einlesen mit Taktversorgung und Querschlusserkennung), wie beispielsweise eines Not-Halts, entsteht das Problem, dass auch die Kontakte des Sensors auf einen Fehler hin geprüft werden müssen.
Bild **52** zeigt am Beispiel eines Not-Halts, wie dies erreicht werden kann.

Die beiden sicherheitsgerichteten Eingänge des Not-Halts werden mit einer Äquivalenzfunktion (SF_Equivalent) verbunden, deren Ausgang den Funktionsblock für den Not-Halt (SF_EmergencyStop) ansteuert. Mit Hilfe der Äquivalenzfunktion wird sichergestellt, dass ein defekter Sensor erkannt wird. Für nähere Details zu den Funktionsblöcken wird auf den SafetyDesigner verwiesen.

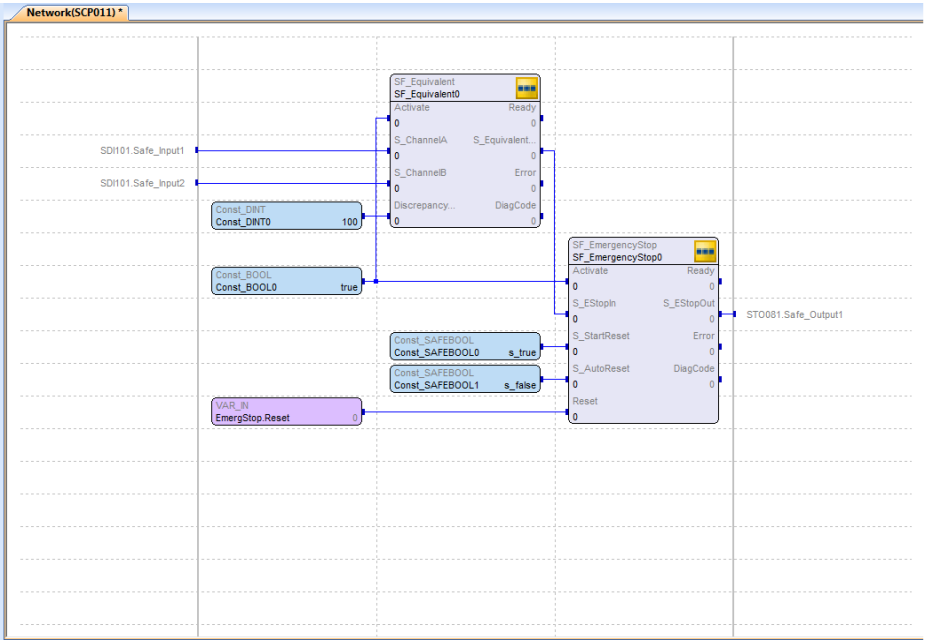


Bild 52 Schaltung einer Not-Halt-Funktion

4.4.3.6 OSSD-Signale an SIGMATEK-Safety-SPS-Eingängen

Geräte mit OSSD Ausgängen (z.B. Lichtgitter), die eigene Testimpulse für ihre Ausgänge haben, funktionieren je nach Testimpulsdauer nur in Verbindung mit Modulen mit einem konfigurierbaren SW Eingangsfilter. Dieser kann im Safety Designer konfiguriert werden.

OSSD Ausgänge verursachen Testimpulse, die zum Abfallen der Eingänge führen können und somit ohne SW-Eingangsfilter und bei aktivierter Cross Circuit Detection zum Auslösen eines Safety Error führen.
Die Cross Circuit Detection ist zu deaktivieren da in diesem Fall die Taktausgänge A/B nicht verwendet werden. Mit dem SW Eingangsfilter können die extern generierten OSSD Ausgangstestimpulse unterdrückt werden, sodass die Eingangssignale richtig ausgewertet werden.

- CSCP011 & CSDI161
  - ➢ Diese haben einen SW Eingangsfilter, der auch für den Kunden konfigurierbar ist

- Daraus entstand die: CSCP012 & CSDI162
  - ➢ Diese haben keinen SW Eingangsfilter, der konfiguriert werden kann

- Auch die SCP010 & SDI100 wurden ohne SW Eingangsfilter entwickelt
  - ➢ Diese haben keinen SW Eingangsfilter, der konfiguriert werden kann

- SCP011 und SCP111 mit SDI101 und SDM081: diese haben einen SW Eingangsfilter

Beispiel:

Ein Sicherheitsschalter mit zweikanaligem OSSD Ausgang mit Testpulsen von 500 µs wird verwendet. Das SDI101 hat eine HW-seitige Eingangsverzögerung von max. 500µs und diese kann bis zu 20% variieren. Dadurch kann nicht gewährleistet werden, dass die Testimpulse gefiltert werden. Somit muss ein zusätzlicher SW Eingangsfilter verwendet werden. Da es sich um ein zweikanalig angeschlossenes Gerät handelt, muss die Querschlusserkennung im Safety-Designer abgeschaltet werden.

Achtung: Taktausgang A/B werden in dieser Anschlussvariante nicht genutzt. Verdrahtungsfehler können somit nicht erkannt werden. Vom Anwender sind geeignete Maßnahmen zum Erkennen von Verdrahtungsfehlern zu treffen.

Achtung: Je nach Einstellung des SW Eingangsfilters, kann auch eine Anpassung der Discrepancy Zeit erforderlich sein.

4.5 Konfiguration eines sicheren Ausgangs

4.5.1 Aufbau eines sicheren digitalen Ausgangs

Nachfolgendes Bild zeigt die Struktur der sicheren Ausgangsschaltung:

Der Ausgang ist nach IEC 61131-2 ausgelegt, gegen Überspannung geschützt und besitzt eine feste Ausgangsverzögerungszeit (kleiner 1 ms). Beim Start des Systems oder im Fehlerfall sind die sicheren Ausgänge immer abgeschaltet. Kommt es zur Zerstörung eines der beiden Ausgangstreiber, so kann der Ausgang über den jeweils anderen Ausgangstreiber in jedem Fall abgeschaltet werden. Um eine sichere Abschaltung garantieren zu können, wird bei einem eingeschalteten Ausgang getestet, ob dieser sich abschalten lässt (Abschaltdauer siehe Hardwaredokumentation). Bei der Verkabelung ist hier keine Zweikanaligkeit nötig, da diese im Modul realisiert ist.

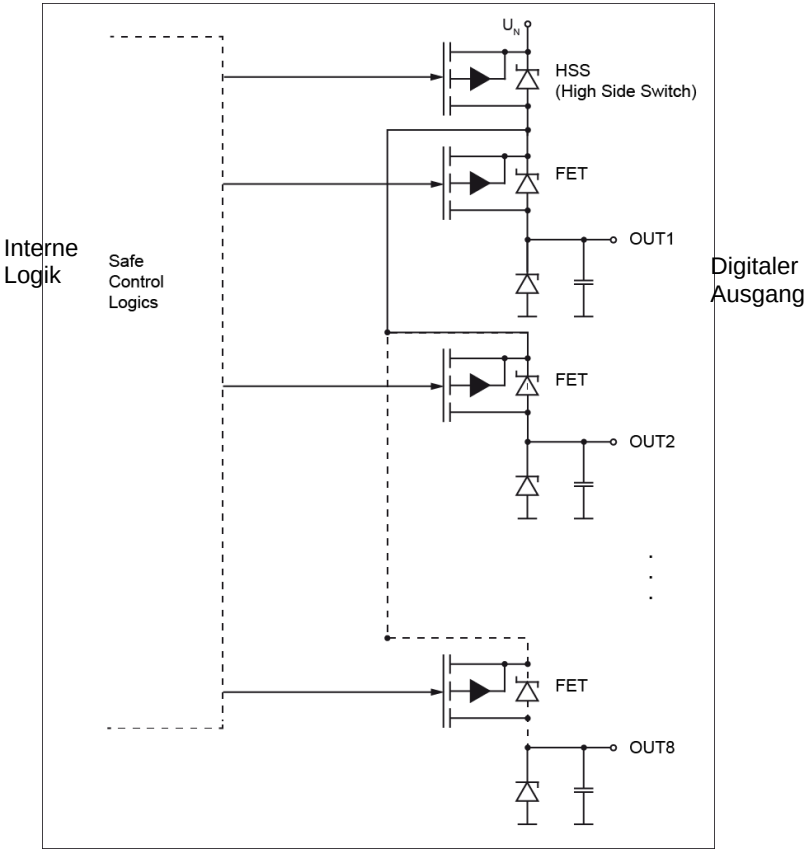


Bild 53 Schematische Ausgangsschaltung

4.5.2 Konfiguration eines sicheren Ausgangs

Bei einem sicheren Ausgang kann ein „Enable signal used“ von standardmäßig „false“ auf „true“ verändert werden. Dies bedeutet, dass über ein unsicheres Signal von der Standardsteuerung der sichere Ausgang deaktiviert werden kann, unabhängig vom Ergebnis der sicheren Applikation. Ein Einschalten des sicheren Ausgangs über das unsichere Freigabesignal ist nur möglich, wenn die sichere Applikation den Ausgang auch eingeschaltet hat.

Handelt es sich um einen sicheren Ausgang eines Ausgangsmoduls, so ist hier analog zu den sicheren Eingängen eine Maximum Transmission Time anzugeben. Die Maximum Transmission Time beschreibt in diesem Fall die maximale Übertragungszeit von einer Safety-CPU zu dem entsprechenden Ausgang. Diese Kenngröße hängt vor allem wieder vom Bussystem und dessen Taktrate ab.

Ein sicherer Ausgang kann nur im temporary Operational bzw. im Operational Mode eingeschalten werden. In allen anderen Betriebszuständen sind die Ausgänge immer abgeschaltet und somit im sicheren Zustand.

4.5.3 Verwendung unsicherer Freigabesignale

Die Verwendung unsicherer Freigabesignale wird in Bild **54** näher erläutert.

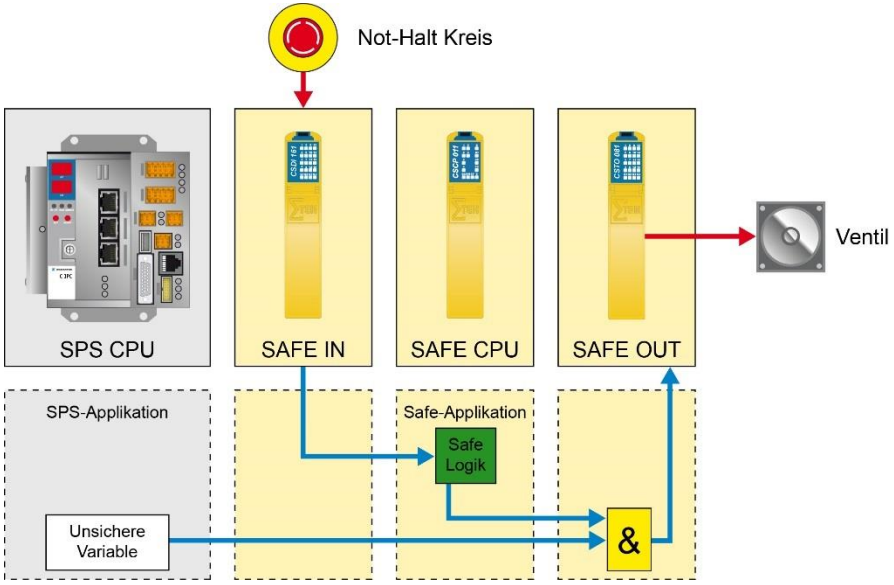
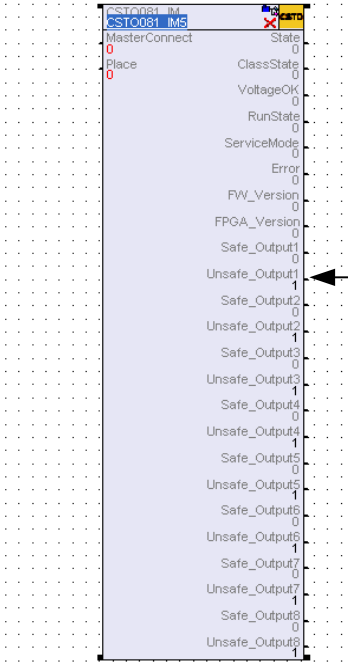


Bild 54 Verwendung unsicherer Freigabesignale

Die unsichere Freigabevariable muss in den Hardwareklassen initialisiert werden. Dazu ist in den Hardwareklassen das entsprechende „Unsafe Output“ Signal anzusteuern.

Soll zum Beispiel bei einem sicheren Ausgangsmodul der Ausgang 1 mit einem unsicheren Freigabesignal verschalten werden, so ist in der Hardwareklasse dem Signal „Unsafe Output“ eine „1“ zuzuweisen. Zudem muss im SafetyDesigner die Variable „Enable signal used“ von standardmäßig false auf true gesetzt werden.



Dieses Signal muss von der Standard- SPS angesteuert werden

Bild 55 Hardwareklasse eines sicheren Ausgangsmoduls

4.6 Konfiguration einer Safety-CPU

Über die Safety-CPU erfolgt die Konfiguration des Sicherheitssystems. Dabei ist die Safety-CPU das einzige Sicherheitsmodul, auf das der SafetyDesigner schreibend zugreifen kann. In der Safety-CPU wird zudem die sichere Applikation abgearbeitet. Für die sichere Applikation steht der Safety-CPU jeweils ein bestimmter Bereich des Flash- und Ram-Speichers der Mikrokontroller zur Verfügung, der nicht überschritten werden kann.

Die Verteilung der Konfiguration an eventuell vorhandene entfernte Sicherheitsmodule wird während der Check-Configurationphase beim Hochlauf des Systems, beim Quit Error und beim Hochlauf nach einer Änderung der Konfiguration durchgeführt. Findet die Safety-CPU die entfernten Sicherheitsmodule nicht, so wird über den SafetyDesigner der Fehler (meist Fehlercode 9 bzw. 1009) angezeigt. Dies kann der Fall sein, wenn z. B. die Standardkommunikation nicht läuft, wenn ein entferntes Sicherheitsmodul im Fehler steht, oder wenn ein Sicherheitsmodul nicht vorhanden ist.

Hinsichtlich der Konfiguration kann ein Modul verschiedene Zustände annehmen:

Zustand	Beschreibung
Unkonfiguriert	Das Modul enthält keine Parametrierungsdaten. (Auslieferungszustand)
Ungültig	Parametrierungsdaten des Moduls sind ungültig.
Konfiguriert, nicht verifiziert	Das Modul enthält Parametrierungsdaten, ist aber noch nicht verifiziert und somit nur zeitlich begrenzt lauffähig.
Verifiziert	Das Modul ist verifiziert und somit ohne zeitliche Begrenzung lauffähig.

Tabelle 10 Modulzustände bezüglich der Konfiguration

Der Konfigurationszustand der Safety-CPU(s) wird im SafetyDesigner dargestellt.

Die maximal zur Verfügung stehende Zykluszeit der Safety-CPU für die Abarbeitung der sicheren Applikation kann in einem Bereich von 1 ms bis 50 ms eingestellt werden. Wird eine zu kleine Zykluszeit gewählt, so wechselt das System in den Fehlerzustand (Errorcode 1). In diesem Fall kann die Zykluszeit im SafetyDesigner neu konfiguriert werden, so dass sichergestellt ist, dass die sichere Applikation innerhalb der konfigurierten Zykluszeit abgearbeitet werden kann. Die maximale Zykluszeit der Safety-CPU wird vom SafetyDesigner abgeschätzt und dient als Richtwert.

4.7 Berechnung der Monitoring Settings (ab Revision 2)

Nach dem Erstellen einer Konfiguration kann über den SafetyDesigner-Button „Monitored Settings“ die max. benötigte Zykluszeit einer Safety-CPU sowie die Maximum Transmission Time der einzelnen Module berechnet werden. Der Anwender muss für die korrekte Berechnung die Zykluszeit des Bussystems (C-DIAS oder VARAN) in [ms] einstellen. Der voreingestellte Wert ist 1 ms. Zusätzlich müssen vom Anwender die übertragenen PDOs pro Buszyklus eingestellt werden. Der voreingestellte Wert ist 1 PDO pro Zyklus. In der Revision 4 kann die Anzahl der PDOs pro Zyklus nicht eingestellt werden; bei der FSoE-Kommunikation werden alle Daten in einem Frame übertragen. Mit Hilfe dieser Einstellungen und der erstellten Applikation (Aufbau des Hardwarebaums und Verschaltung in den Netzwerken) können die Werte für die Zykluszeit und die max. Übertragungszeiten ermittelt werden. Die berechneten Werte können vom Anwender in das Projekt übernommen werden.

☞	Der Anwender muss die vom SafetyDesigner vorgeschlagenen Werte im laufenden System auf Richtigkeit überprüfen.

4.8 Reaktionszeit

Nach dem Erstellen einer Konfiguration wird über den SafetyDesigner Button „Check Resources“ die Reaktionszeit der verwendeten sicheren Ausgänge dargestellt. Dabei wird immer die maximal überwachte Reaktionszeit abgeschätzt. Haben zudem z. B. bei einem sicheren Ausgangsmodul alle Ausgänge dieselbe Reaktionszeit, so wird diese nur für einen sicheren Ausgang angezeigt.

☞	**WICHTIG!** Bei den hier berechneten Reaktionszeiten sind Reaktionszeiten von Sensoren an den Eingängen und Aktoren an den Ausgängen nicht miteingerechnet. Schaltverzögerungen von Relais sind nicht miteingerechnet. Bei den Modulen SRO 021 und SRO 022 sind die Zeiten der eigenen Relais miteingerechnet.

☞	Der Anwender muss die vom SafetyDesigner vorgeschlagenen Werte im laufenden System auf Richtigkeit überprüfen (z.B. durch wiederholte Messungen der Reaktionszeiten im laufenden System).

Im folgenden Abschnitt wird die Bestimmung der Reaktionszeit anhand einiger konkreter Beispiele erläutert.

4.8.1 Reaktionszeitbestimmung an einer Safety-CPU mit lokalen Ein- und Ausgängen

4.8.1.1 Einkanalige Beschaltung

In diesem Beispiel wird der Eingang 1 (DI 1) einer Safety-CPU auf den Ausgang 1 (TO 1) derselben Safety-CPU verknüpft. Der Eingangssensor darf dabei nicht mit einem Taktausgang versorgt werden, da ansonsten ein Testpuls der Eingangtests die sichere Applikation beeinflussen kann.

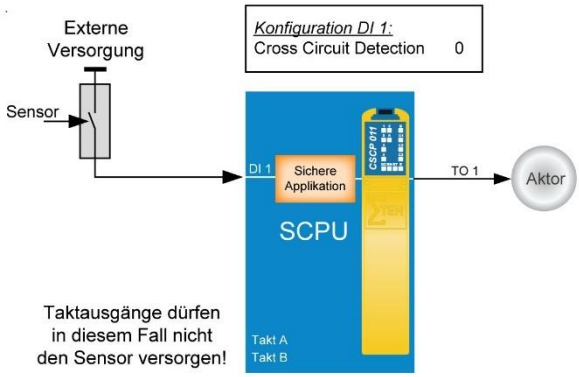


Bild 56 lokaler Eingang - Safety-CPU - lokaler Ausgang

Die Reaktionszeit eines solchen Systems lässt sich wie folgt ermitteln:

$$T_{Reaktionszeit} = T_{IN} + T_{SW\text{-}Filter} + 2*T_{SCPU,cycle}$$ (Revision 1)

$$T_{Reaktionszeit} = T_{IN} + 2*T_{SCPU,cycle}$$ (ab Revision 2)

Bedeutung der Parameter

Parameter	Beschreibung	Konfigurierbar
T_{IN}	maximale Hardwarefilterzeit; beträgt im ungünstigsten Fall 2,5 ms	nein
$T_{SW\text{-}Filter}$	zusätzliche Filterzeit	ja
$T_{SCPU,cycle}$	Zykluszeit der Safety-CPU	ja

Tabelle 11 Konfigurationsparameter einer einkanaligen Beschaltung

4.8.1.2 Zweikanaliger Eingang mit Querschlusserkennung

In diesem Beispiel wird der Eingang 1 (DI 1) und der Eingang 2 (DI 2) einer Safety-CPU auf den Ausgang 1 (TO 1) derselben Safety-CPU verknüpft. Die sicheren Eingänge stammen von zwei verschiedenen Sensoren. Die Eingangssensoren werden dabei mit jeweils einem Taktausgang versorgt. Die entsprechenden Eingänge müssen zudem mit jeweiligen Takten konfiguriert werden.

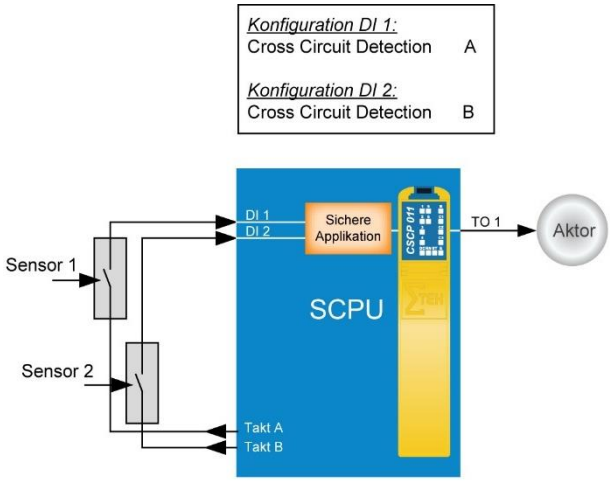


Bild 57 lokaler Eingang - Safety-CPU - lokaler Ausgang

Die Reaktionszeit eines solchen Systems lässt sich wie folgt ermitteln:

$$T_{Reaktionszeit} = T_{IN} + T_{Inputtest} + T_{SW\text{-}Filter} + 2*T_{SCPU,cycle}$$ (Revision 1)

$$T_{Reaktionszeit} = T_{IN} + T_{Inputtest} + 2*T_{SCPU,cycle}$$ (ab Revision 2)

Bedeutung der Parameter

Parameter	Beschreibung	Konfigurierbar
T_{IN}	maximale Hardwarefilterzeit; beträgt im ungünstigsten Fall 2,5 ms	nein
$T_{SW\text{-}Filter}$	zusätzliche Filterzeit	ja
$T_{SCPU,cycle}$	Zykluszeit der Safety-CPU	ja
$T_{Inputtest}$	Dauer des Eingangstests im ungünstigsten Fall 6 ms	nein

Tabelle 12 Konfigurationsparameter einer zweikanaligen Beschaltung

4.8.1.3 Zweikanaliger Anschluss eines Sensors mit Querschlusserkennung und lokaler UND-Verknüpfung

Hierbei handelt es sich um ein zweikanalig angeschlossenes System, bei dem die beiden Eingangssignale vom selben Sensor kommen und mit einem lokalen UND verknüpft sind. Wird die Querschlusserkennung aktiviert, so berechnet der SafetyDesigner die maximale Reaktionszeit ohne die Inputtestzeit $T_{Inputtest}$. Dies liegt darin begründet, dass beide Eingangssignale vom selben Sensor stammen und der Eingangstest nicht gleichzeitig an beiden Eingangssignalen durchgeführt wird. Somit kann während der Durchführung des Eingangstests des Eingangs, der mit dem Takt A verbunden ist, der andere mit Takt B verbundene Eingang, wenn nötig, den sicheren Zustand einleiten oder umgekehrt.

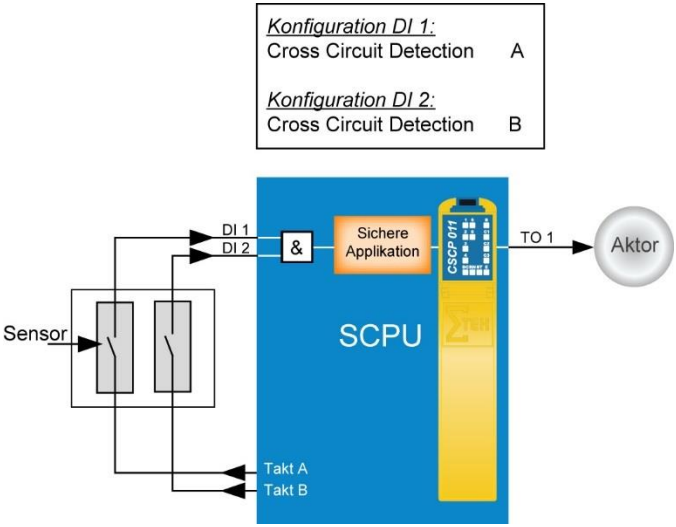


Bild 58 Zweikanalig angeschlossene Sensoren

Die Reaktionszeit eines solchen Systems lässt sich wie folgt ermitteln:

$$T_{REAKTIONSZEIT} = T_{IN} + T_{SW\text{-}FILTER} + 2*T_{SCPU,CYCLE\ (VOR\ REVISION\ 1)}$$

$$T_{REAKTIONSZEIT} = T_{IN} + 2*T_{SCPU,CYCLE\ (AB\ REVISION\ 2)}$$

4.8.2 Bestimmung der Reaktionszeit bei einer Safety-CPU mit entfernten Ein- und Ausgängen bei Querschlusserkennung

Bei diesem System handelt es um z. B. einen Not-Halt, der an ein SafeInput-Modul angeschlossen ist. Das Safe-Input Modul ist über ein Kommunikationssystem, z. B. C-DIAS mit einer Safety-CPU verbunden. Die Safety-CPU verarbeitet den lokalen Eingang und gibt das Ergebnis über das Bussystem an ein entferntes Ausgangsmodul weiter.

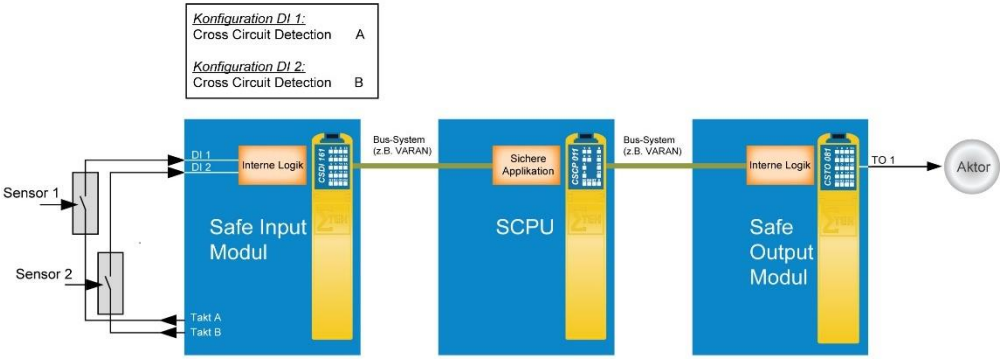


Bild 59 SIN: lokaler Eingang - Bus - Safety-CPU - Bus - SOUT: lokaler Ausgang

Die Reaktionszeit eines solchen dezentralen Systems kann wie folgt angegeben werden:

$$T_{Reaktionszeit} = T_{IN} + T_{Inputtest} + T_{SW\text{-}Filter} + 2 * T_{SIN,cycle} + \text{Maximum Transmission Time (Input)} + 2 * T_{SCPU,cycle} + \text{Maximum Transmission Time (Output)} + 2 * T_{SOUT,cycle} + T_{Drift}$$

(Revision 1)

$$T_{Reaktionszeit} = T_{IN} + T_{Inputtest} + T_{SIN,cycle} + T_{bus} + \text{Maximum Transmission Time (Input)} - T_{bus} + 2 * T_{SCPU,cycle} + \text{Maximum Transmission Time (Output)} + T_{SOUT,cycle} + T_{bus}$$

(ab Revision 2)

Bedeutung der Parameter

Parameter	Beschreibung	Konfigurierbar
T_{IN}	maximale Hardwarefilterzeit; beträgt im ungünstigsten Fall 2,5 ms	nein
$T_{Inputtest}$	Dauer des Eingangstests im ungünstigsten Fall 6 ms (indirekt über Querschlusserkennung)	nein
$T_{SW\text{-}Filter}$	zusätzliche Filterzeit	ja
$T_{SIN,cycle}$	Verarbeitungszeit des sicheren Eingangsmoduls	nein
Maximum Transmission Time (Input)	die maximal erlaubte Verzögerung zwischen einem entfernten Eingang und der verarbeitenden Safety-CPU	ja
Maximum Transmission Time (Output)	die maximal erlaubte Verzögerung zwischen einer Safety-CPU und dem dazugehörigen entfernten Ausgang	ja
$T_{SCPU,cycle}$	Zykluszeit der Safety-CPU	ja
$T_{SOUT,cycle}$	Verarbeitungszeit des sicheren Ausgangsmoduls	nein
T_{Drift}	maximale Zeitdrift zwischen zwei Sicherheitsmodulen (im ungünstigsten Fall 6 ms).	nein
T_{bus}	Buszyklus des Systems (C-DIAS oder VARAN)	ja

Tabelle 13 Konfigurationsparameter einer einkanaligen Beschaltung mit entfernten Sicherheitsmodulen

Der Eingang wird diesmal vom sicheren Eingangsmodul eingelesen. Wenn die Querschlusserkennung gewählt wird, muss die Zeit T_{Input} zur Reaktionszeit hinzuaddiert werden. Zusätzlich zu den vorangegangenen Beispielen muss hier auch die Verarbeitungszeit des sicheren Eingangsmoduls ($T_{SIN,cycle}$) und die des sicheren Ausgangsmoduls ($T_{SOUT,cycle}$) berücksichtigt werden.

Darüber hinaus sind vom Anwender die maximal erlaubten Übertragungszeiten zwischen der Safety-CPU und den entfernten Sicherheitsmodulen zu berücksichtigen. Dabei ist bei einem sicheren Eingang die Maximum Transmission Time die maximal erlaubte Zeitverzögerung zwischen einem entfernten Eingang und der verarbeitenden Safety-CPU. Analog dazu ist bei einem sicheren Ausgang die Maximum Transmission Time die maximal erlaubte Zeitverzögerung zwischen einer Safety-CPU und dem dazugehörigen entfernten Ausgang.

Da jedes Sicherheitsmodul seine eigene Zeitbasis besitzt, und die Synchronisation zwischen den Sicherheitsmodulen nur zu bestimmten Zeitpunkten stattfindet, können zwei Sicherheitsmodule im ungünstigsten Fall bis zu 6 ms auseinanderdriften. Diese Drift (T_{Drift}) ist in einem System mit entfernten Sicherheitsmodulen zu berücksichtigen.

4.8.3 Bestimmung der Reaktionszeit mit FSoE-Kommunikation

Bei diesem System handelt es sich z. B. um einen Not-Halt, der am Eingangsmodul einer SCP 111 angeschlossen ist. Die SCP 111 verarbeitet den lokalen Eingang und gibt das Ergebnis über das Bussystem an eine entfernte Safety CPU (ebenfalls eine SCP 111) mit Ausgangsmodul weiter.

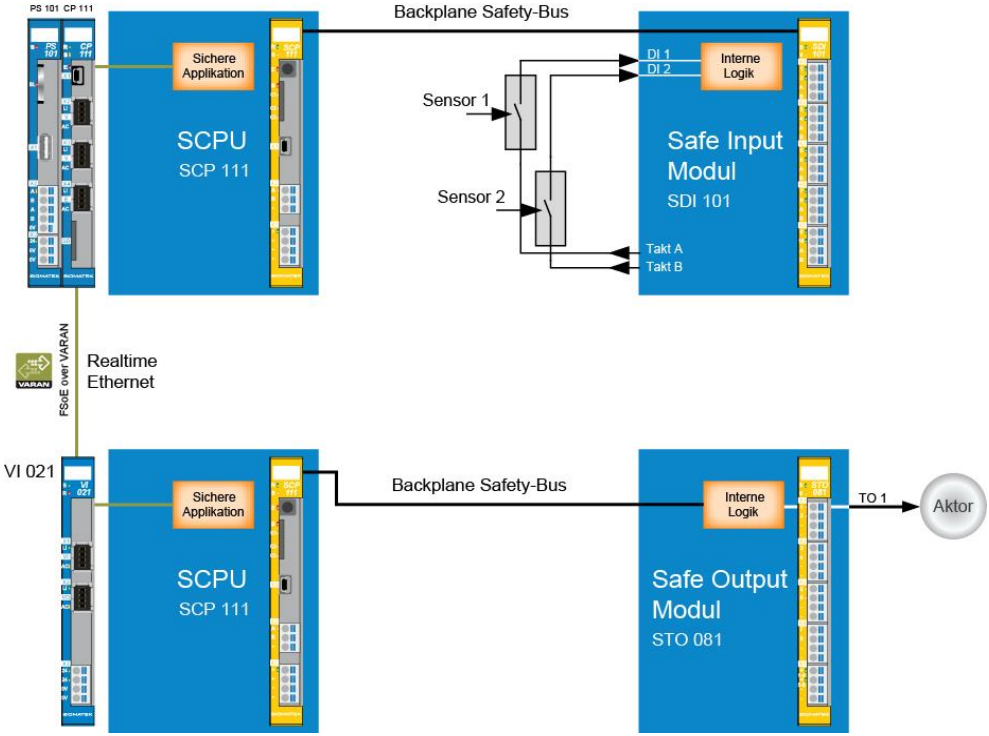


Bild 60 FSoE-Kommunikation

$$T_{Reaktionszeit} = T_{IN} + T_{Inputtest} + T_{SW\text{-}Filter} + 2 * T_{SCPU,cycle} \text{ (FSoE Master)} + 2 * \text{Transmission Time (eingestellte Zeit der FSoE-Verbindung)} + 2 * T_{SCPU,cycle} \text{ (FSoE Slave)}$$

(Revision 4)

Bedeutung der Parameter

Parameter	Beschreibung	konfigurierbar
T_{IN}	maximale Hardwarefilterzeit; beträgt im ungünstigsten Fall 2,5 ms	nein
$T_{Inputtest}$	Dauer des Eingangstests im ungünstigsten Fall 6 ms (indirekt über Querschlusserkennung)	nein
$T_{SW\text{-}Filter}$	zusätzliche Filterzeit	ja
Transmission Time	maximale Übertragungszeit zwischen FSoE-Master und FSoE-Slave	ja
$T_{SCPU,cycle}$	Zykluszeit der Safety-CPU	ja

Tabelle 14 Konfigurationsparameter einer einkanaligen Beschaltung mit entfernten Sicherheitsmodulen

4.8.4 Fixe Zeitparameter, die Einfluss auf die Reaktionszeit haben

In folgender
Tabelle **15** sind die unveränderlichen, durch das System vorgegebenen Parameter noch einmal zusammenfassend dargestellt. Diese Parameter stellen die Worst Case Bedingung dar.

Abkürzung	Max. Zeitwert	Erklärung
T_{IN}	2,5 ms	maximale Eingangsverzögerung
$T_{SIN,cycle}$ (Revision 1)	2,5 ms	interner Zyklus des Eingangsmoduls
$T_{SIN,cycle}$ (ab Revision 2)	1,0 ms	interner Zyklus des Eingangsmoduls
$T_{SOUT,cycle}$ (Revision 1)	3,5 ms	interner Zyklus des Ausgangsmoduls
$T_{SOUT,cycle}$ (ab Revision 2)	1,0 ms	interner Zyklus des Ausgangsmoduls
T_{Drift}	6 ms	maximale Zeitdrift zwischen zwei Sicherheitsmodulen
$T_{Inputtest}$	6 ms	maximale Zeit des bei der Querschlusserkennung aktivierten Eingangstests

Tabelle 15 Fixe Zeitparameter

4.8.5 Konfigurierbare Zeitparameter, die Einfluss auf die Reaktionszeit haben

Die folgende
Tabelle **16** gibt die zu konfigurierenden Zeitparameter wieder.

Abkürzung	Min	Max	Default	Erklärung
$T_{SW\text{-}Filter}$	0 ms	100 ms	0 ms	konfigurierbarer Eingangsfilter um eventuelle Störungen des externen Eingangssignals herauszufiltern.
SCPU, cycle (Revision 1)	1 ms	50 ms	6 ms	entspricht max. Cycle Time; siehe Kapitel 4.6
SCPU, cycle (ab Revision 2)	1 ms	50 ms	3 ms	entspricht max. Cycle Time; siehe Kapitel 4.6
Maximum Transmission Time (Input) (Revision 1)	1 ms	100 ms	10 ms	Maximum Transmission Time, die für jeden sicheren digitalen Eingang konfiguriert werden muss.
Maximum Transmission Time (Output) (Revision 1)	1 ms	100 ms	10 ms	Maximum Transmission Time, die für jeden sicheren digitalen Ausgang konfiguriert werden muss.
Maximum Transmission Time (ab Revision 2)	1 ms	100 ms	Wert wird berechnet	Maximum Transmission Time, die für jeden sicheren digitalen Eingang/Ausgang konfiguriert werden muss.
Maximum Transmission Time für HGW und Interfaces IP-Adressen (ab Revision 4)	1 ms	5000 ms	300 ms	Maximum Transmission Time für HGW und WLAN-Verbindungen

Tabelle 16 Einstellbare Zeitparameter

Neben den Zeitparametern von
Tabelle **16** muss noch festgelegt werden, ob das System zweikanalig oder einkanalig verdrahtet ist. Liegt eine Zweikanaligkeit vor und wird die Querschlusserkennung gewünscht, so ist jeweils ein Eingang mit Takt A und der andere mit Takt B zu versorgen und auch zu konfigurieren.

WICHTIG!
Die eingestellte VARAN-Zykluszeit hat direkt Einfluss auf die Maximum Transmission Time. Um sicherzustellen, dass die sichere Kommunikation ständig verfügbar ist, muss die Maximum Transmission Time mindestens fünfmal der eingestellten VARAN-Zykluszeit entsprechen (Revision 1).

5 Betrieb

5.1 Abarbeiten der sicheren Applikation

Nach der erfolgreichen Konfiguration der Sicherheitsmodule (siehe Kapitel 4) geht das Sicherheitssystem in den Operational Mode über.

WICHTIG!
Im Betriebszustand des Operational Mode muss der SafetyDesigner von der Steuerung getrennt werden.

5.2 Bedienung des Validierungstasters

Unabhängig vom SafetyDesigner kann das Sicherheitssystem auch mit Hilfe des Validierungstasters gesteuert werden. Der Validierungstaster ist, wie die SD-Karte auch, nur auf der Safety-CPU implementiert. Da sich das System im zeitlich unbegrenztem Betrieb befindet, ist nur eine sinnvolle Untermenge der Befehle des SafetyDesigners möglich: diese sind:

- ***Quit Error***
  Mit diesem Befehl kann ein Fehler zurückgesetzt werden. Bleibt der Fehler auch nach dem „Quit Error“-Kommando bestehen, handelt es sich entweder um einen „permanenten Fehler“ oder aber der Fehler wurde erneut festgestellt z. B. auf Grund einer fehlerhaften Verdrahtung o.ä.

- ***Clear Config***
  Mit diesem Befehl wird der Flash-Speicher der Safety-CPU gelöscht, wenn beispielsweise eine neue Applikation über die SD-Karte eingespielt werden soll. Die Funktionalität dieses Befehls entspricht der des Befehls „Clear“ beim SafetyDesigner.

- ***Set Verified***
  Mit diesem Kommando wird das Set Verified-Flag gesetzt, d.h. es findet ein Zustandsübergang vom zeitlich begrenzten Laufzeitzustand in den zeitlich unbegrenzten statt.

Wird ein falsches Kommando eingegeben, so wird dies erkannt. Die LED des Validierungstasters beginnt daraufhin zeitweise zu blinken. Das System ändert seinen Laufzeitzustand nicht. 8520_up_9510

Die Eingabe eines Kommandos mittels Validierungstaster setzt sich aus 3 Teilsequenzen zusammen, der Start- und Ende-Sequenz sowie der Sequenz zur Selektion des Kommandos (siehe folgendes Diagramm).

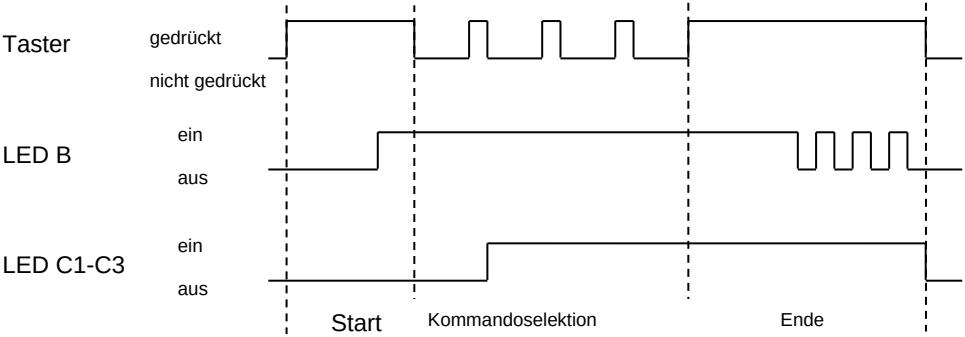


Bild 61 Kommandoeingabe über den Validierungstaster

5.2.1 Erklärung der einzelnen Sequenzen

5.2.1.1 Start-Sequenz

Der Taster ist solange zu betätigen, bis die LED B leuchtet (nach ca. 3 Sekunden). Wird der Taster zu lange betätigt (länger als ca. 10 Sekunden), wird eine Fehler-Sequenz ausgegeben (siehe „Fehler-Sequenz“). Das gleiche gilt, wenn der Taster zu früh freigegeben wird (also bevor sich LED B einschaltet), oder der Taster nach der Freigabe sofort wieder betätigt wird (Zeit zwischen 2 Tasterbestätigungen kürzer als ca. 200 ms).

5.2.1.2 Sequenz zur Kommandoselektion

Nach der eingegebenen Startsequenz erfolgt die Selektion des gewünschten Kommandos. Dies geschieht mittels Tasterbetätigungen mit folgenden zeitlichen Vorgaben: Betätigungsdauer mind. 200 ms, max. ca. 3 Sekunden, Pause zwischen den einzelnen Tasterbetätigungen mind. 200 ms, max. 10 Sekunden. Nach jeder korrekten Tasterbetätigung (inkl. der Mindestpause von ca. 200 ms) wird das aktuell selektierte Kommando durch die LED C1 – C3 angezeigt. Wird ein ungültiges Kommando selektiert (siehe „Gültige Kommandos“), wird die Fehler-Sequenz ausgegeben, ebenso bei Nichteinhaltung der o.a. zeitlichen Vorgaben. Die LED B leuchtet während dieser Sequenz durchgehend.

5.2.1.3 Ende-Sequenz

Diese Sequenz dient zur Quittierung des selektierten Kommandos. Hierfür ist der Taster solange zu betätigen, bis LED B zu blinken beginnt (nach ca. 3 Sekunden, blinkt im langsamen Abstand). Die Anzahl der Leuchtimpulse der LED B hängt dabei vom zuvor selektierten Kommando ab (siehe „Gültige Kommandos“).

Wenn die LED B erlischt, muss der Taster freigegeben werden. Nach der Mindestpause von ca. 200 ms, in der der Taster nicht erneut betätigt werden darf, wird in den Service-Mode gewechselt und das Kommando ausgeführt.

Wird der Taster nach Beendigung der Blink-Phase noch länger als ca. 3 Sekunden betätigt, so wird das selektierte Kommando nicht akzeptiert und die Fehler-Sequenz angezeigt. Dasselbe gilt, wenn der Taster zu früh freigegeben oder die Mindestpause von ca. 200 ms nicht eingehalten wurde. Nach Ausführung des Kommandos wird je nach Kommando in den entsprechenden Modus gewechselt (siehe „Gültige Kommandos“).

Führt die Ausführung des Kommandos zu einem Fehler (weil z. B. SET_VERIFIED ausgeführt werden soll, obwohl keine gültigen Konfigurationsdaten auf der Safety-CPU vorhanden sind), so erfolgt anschließend die Ausgabe der Fehlersequenz.

5.2.1.4 Fehler-Sequenz

Erfolgt eine ungültige Tasterbetätigung, wie in den o.a. Sequenzen beschrieben, so wird in die Fehler-Sequenz gewechselt. Diese Sequenz wird durch schnelles Blinken von LED B visualisiert. Das Blinken des LED B dauert mindestens ca. 3 Sekunden an.

Ist der Taster nach Ablauf der 3 Sekunden noch immer betätigt, so wird das Blinken der LED B solange fortgeführt, bis der Taster freigegeben und eine Mindestpause von ca. 200 ms eingehalten wird. Erst nachdem LED B erlischt, kann die Startsequenz erneut eingegeben werden.

Nach Beendigung der Fehler-Sequenz erfolgt ein Modus-Wechsel gemäß „Übersicht der Modulzustände“. Eventuell eingeschaltete LEDs C1 – C3 werden nach Beendigung der Fehlersequenz ausgeschaltet.

5.2.1.5 Übersicht über die Kommandos

Die Anzahl der Tasterbetätigungen entspricht der Anzahl der Leuchtimpulse der LED B während der Ende-Sequenz.

Kommandos	Anzahl Tasterbetätigungen	LED C1	LED C2	LED C3
QUIT_ERROR	1	X		
CLR_CFG	2	X	X	
SET_VERIFIED	3	X	X	X

Tabelle 17 Validierungstaster-Befehle

5.2.1.6 Übersicht Modulzustände und Kommandos

Nachfolgende Tabellen zeigen eine Darstellung der Zustände, in denen sich das System befinden kann und die Kommandos, die in diesen Zuständen jeweils wirksam werden können und ihre Wirkungen.

	Kommando		
Zustand des Systems	***QUIT_ERROR***	***CLR_CFG***	***SET_VERIFIED***
Check-Configuration		**X**	
Zeitlich begrenzter Operational Mode		**X**	**X**
Operational Mode		**X**	
Service Mode		**X**	
Error	**X**		

Tabelle 18 Modulzustände und Kommandos

Ausgeführtes Kommando	Wirkung des Kommandos	Zustand nach Ausführung des Kommandos
QUIT_ERROR	Es wird bei der Safety-CPU und allen von der Safety-CPU benötigten Safe-IO-Modulen ein eventuell vorhandener Fehler quittiert und der Fehlerzustand verlassen.	SW-RESET [(1)]
CLR_CFG	Die Konfiguration auf der Safety-CPU wird gelöscht. Nach Ausführung des Befehls befindet sich die Safe CPU im Service Mode.	Service Mode
SET_VERIFIED	Der Konfigurations-Zustand wird auf „verifiziert“ gesetzt.	Operational Mode

[(1)] Es wird ein SW-RESET durchgeführt. Ist der Fehler danach noch vorhanden, verbleibt die Safety-CPU im Fehlermodus, andernfalls läuft die Safety-CPU korrekt an.

Allgemeine Anmerkung: Wurde ein Kommando fehlerhaft eingegeben, führt die Safety-CPU die Fehler-Sequenz aus (siehe oben). Nach Beendigung der Fehler-Sequenz kann das Kommando erneut eingegeben werden.

Tabelle 19 Validierungstasterkommandos

INFO

Steht die Safety-CPU selbst im Fehlerzustand, so wird beim Absetzen eines „Quit Error“ Kommandos über den Validierungstaster der Fehler in der Safety-CPU zurückgesetzt. Gehören zu der auf der Safety-CPU befindendlichen Konfiguration noch entfernte Sicherheitsmodule, die ihrerseits im Fehlerzustand stehen, so wird dort der Fehlerzustand nicht aufgehoben. Um diesen aufzuheben, ist ein erneutes „Quit Error“ Kommando notwendig.

5.3 Diagnose im Fehlerfall

5.3.1 Diagnose über die LEDs

Anhand der LEDs der Sicherheitsmodule kann zwischen verschiedenen Fehlerarten unterschieden werden:

5.3.1.1 Modul selbst steht im Fehler

Wenn das Sicherheitsmodul während seiner Selbsttests bei sich einen Fehler feststellt, so wechselt dieses in den Fehlerzustand. Dies ist anhand des dauerhaften Aufleuchtens der Error-LED (siehe Kapitel 2.5.5) zu erkennen. Der aufgetretene Fehler kann über die LEDs nicht näher bestimmt werden. Um ihn zu identifizieren, ist eine Diagnose über den SafetyDesigner notwendig. Wenn die DCOK-LED ausgeschaltet ist, liegt dies in der Regel an einer falschen Versorgungsspannung. In diesem Fall ist die externe Spannungsversorgung der Taktausgänge bzw. der sicheren Ausgänge zu überprüfen.

5.3.1.2 Entferntes Modul steht im Fehler

Hat ein Sicherheitsmodul, z. B. ein Safety-Output Modul eine Erwartungshaltung von einem anderen entfernten Sicherheitsmodul, z. B. einer Safety-CPU, und steht das entfernte Sicherheitsmodul im Fehlerzustand, so empfängt die Safety-CPU nur Fehlerdaten. Daraufhin schaltet das sichere Ausgangsmodul die Ausgänge in den sicheren Zustand und die Error-LED beginnt zu blinken. Um den Fehler zu beheben, muss der aufgetretene Fehler des entfernten Sicherheitsmoduls mit Hilfe des SafetyDesigners diagnostiziert werden, um ihn beheben zu können.

Das gleiche Verhalten ist gegeben, wenn die Safety-CPU des obigen Beispiels zwar korrekt arbeitet, die sicheren Daten aber, die das Safe-Output Modul empfängt, veraltet sind. Ist dies der Fall, so muss eventuell die Konfiguration betrachtet und das dort einstellbare maximale Alter angepasst werden. Ist dies jedoch nicht der Fall, so ist möglicherweise die sichere Kommunikation zwischen den beiden sicheren Modulen unterbrochen und das Ausgangsmodul empfängt deshalb keine gültigen Daten.

5.3.1.3 Interner Fehler

Tritt bei einem Sicherheitsmodul ein interner Fehler (Hardwarefehler) auf, so wird dieser über die internen Selbsttests detektiert. Das Modul geht daraufhin in den Fehlerzustand. Über den SafetyDesigner kann dieser Fehler identifiziert werden. Kann der Fehler nicht mit dem Quit Error Befehl zurückgesetzt werden, so muss sich der Anwender mit dem Hersteller in Verbindung setzen.

5.3.1.4 Sicher Ein- bzw. Ausgang ist im Fehlerzustand

Auch falsche Verdrahtungen eines sicheren Ein- oder Ausgangs können zum Teil detektiert werden. In einem solchen Fall muss die Verdrahtung des Sicherheitsmoduls überprüft werden.

Die detektierbaren Fehler hängen maßgeblich von der Konfiguration ab; so kann der Querschlusstest beispielsweise nur bei einer zweikanaligen Verdrahtung auch wirklich Querschlüsse detektieren. Dies muss am SafetyDesigner explizit eingestellt werden. Schaltungsbeispiele hierzu werden in den Kapiteln zur Bestimmung der Reaktionszeit dargestellt.

Ob ein Fehler überhaupt detektiert werden kann, hängt auch vom elektrischen Zustand des sicheren Ein- oder Ausgangs ab. Beispielsweise kann ein ausgeschalteter Ausgang naturgemäß nicht daraufhin getestet werden, ob er noch abgeschaltet werden kann. Ebenso wenig kann bei einem abgeschalteten Eingangssignal getestet werden, ob der Eingang noch abgeschaltet werden kann.

5.3.2 Diagnose über den SafetyDesigner

Der Anwender kann, gleichgültig welcher Fehler aufgetreten ist, jederzeit mit dem SafetyDesigner online gehen um den Fehler auszulesen. Steht ein sicheres Modul im Fehlerzustand, so kann dieser mit dem Servicebefehl „Get Module State“ abgefragt werden. Für eine Safety-CPU wird der Fehlerzustand automatisch im Konsolenfenster des SafetyDesigners ausgegeben.

Steht nicht das Sicherheitsmodul im Fehlerzustand, sondern wurde ein sicherer Ein- oder Ausgang als fehlerhaft detektiert, so wird dies im Fenster „Error of Channels“ des SafetyDesigners angezeigt.

5.3.3 Fehlerbehandlung

Tritt ein Fehler beispielsweise infolge einer fehlerhaften Verdrahtung auf, so kann dieser nach der Korrektur der Verdrahtung quittiert werden. Wird dagegen ein Fehler diagnostiziert, der durch einen Hardwaredefekt ausgelöst wurde, so kann dieser nicht quittiert werden. In diesem Fall liegt ein „permanenter Fehler“ vor. Beispiele solcher Fehler sind:

Fehlerart	Fehlermeldung
RAM-Fehler	E_RA_MARCH; E_RA_GALPAT
ROM-Fehler	E_ROMTEST_VECTORS, E_ROMTEST_BOOTSECTOR, E_ROMTEST_OSIMAGE
Interne Taktfehler	E_REFCLOCK_MIN, E_REFCLOCK_MAX
Defekter Ausgangshalbleiter	E_WD_TEST E_SO_TEST_FET3 E_SOTEST_HSS1
Zu großer Drift der Module	E_CYCLIC_TIME_DRIFT

Tabelle 20 Permanente Fehler

Tritt einer dieser permanenten Fehler auf, so muss das betroffene Sicherheitsmodul gegen ein funktionsfähiges Sicherheitsmodul ausgetauscht werden. Das defekte Sicherheitsmodul ist an SIGMATEK GmbH & CO KG zur Reparatur einzusenden.

Lässt sich z. B. ein sicherer Ausgang nicht mehr abschalten und tritt dieser Fehler während des Operational Modes auf, so geht der entsprechende Ausgang in den Fehlerzustand (Ausgangs-LED blinkt). Im SafetyDesigner kann nun im Feld „Error of Channels“ der Fehler konkret abgelesen werden. Wird nun ein „Quit Error“ abgesetzt und der Fehler wurde nicht beseitigt, so bleibt der Fehlerzustand erhalten. Wurde der Fehler dagegen behoben, so wechselt das System nach einem „Quit Error“ wieder in den Operational-Zustand.

5.3.4 Fehler an sicheren Eingängen

Die hier aufgelisteten Fehler werden nur bei Systemen erkannt, bei denen die Querschlusserkennung aktiviert wurde.

5.3.4.1 Taktsignal konnte nicht erkannt werden

Ist die Querschlusserkennung aktiviert und der einzulesende sichere Eingang auf High, so muss der Eingangssensor mit der entsprechenden Taktversorgung des Sicherheitsmoduls versorgt werden. Diese Taktversorgung wird in regelmäßigen Abständen kurz abgeschaltet. Dadurch wird geprüft, ob ein Querschluss zwischen zwei mit unterschiedlichen Takten versorgten Eingängen besteht bzw. ob sich der Eingang noch abschalten lässt. Ist der Eingang auf High und wird der Taktimpuls nicht detektiert so wird ein Fehler festgestellt. Mögliche Ursachen sind eine falsche Verdrahtung bzw. ein Defekt des Taktausgangs. Nach Beseitigung des Querschlusses kann über einen Quit Error bzw. über einen Neustart des Systems der Fehler behoben werden.

5.3.4.2 Es wurde ein falsches Taktsignal erkannt

In diesem Fall liegt vermutlich ein Querschluss zwischen den Eingängen oder eine falsche Verdrahtung vor und im Fenster „Error of Channels“ des SafetyDesigners wird der Fehlercode 103 angezeigt; die LED des entsprechenden fehlerhaften Eingangs blinkt[2]. Nach Beseitigung des Fehlers kann mit einem Quit Error bzw. durch einen Neustart des Systems der Fehler aufgehoben werden.

5.3.5 Fehler an sicheren Ausgängen

5.3.5.1 Rückgelesene und erwartete Ausgangswerte stimmen nicht überein

Stimmen die vom Sicherheitsmodul zurückgelesen Werte der Ausgangssignale nicht mit den von der Applikation berechneten überein, so wird im Fenster „Error of Channels“ des SafetyDesigners der Fehler 137 bzw. 1137 angezeigt. Die entsprechende Ausgangs-LED blinkt und die sicheren Ausgänge des Moduls werden abgeschaltet. Ursache dieses Fehlers kann entweder ein Hardwaredefekt oder eine falsche Beschaltung des Ausgangs (zu hohe kapazitive Last) sein. Die Beschaltung ist zu überprüfen. Wurde der Fehler beseitigt, kann er mit einem „Quit Error“ Befehl bzw. durch einen Neustart des Systems aufgehoben werden.

[2] Das Blinken der LED gilt nur für das C-Dias System.

5.3.5.2 Ausgänge lassen sich nicht abschalten

Können die sicheren Ausgänge nicht abgeschaltet werden, so wird dies innerhalb des internen Testsintervalls (alle 26 Sekunden) erkannt. Bei dem entsprechenden Sicherheitsmodul blinkt dann der betroffene Ausgang und wird abgeschaltet. Im SafetyDesigner wird in „Error of Channels“ der entsprechende fehlerhafte Ausgang mit dem Fehlercode 143 bzw. 1143 oder 144 bzw. 1144 angezeigt. Der Fehler kann folgende Ursachen haben:

- Sicherer Ausgang ist durch einen Verdrahtungsfehler auf 24 V geklemmt
- Es hängt eine zu große kapazitive Last am sicheren Ausgang (siehe Datenblätter der entsprechenden Sicherheitsmodule)
- Es handelt sich um einen Defekt am sicheren Ausgang.

Nach Beheben des Fehlers (mit Ausnahme des Defekts, der nicht behoben werden kann) muss der Fehler quittiert werden. Besteht der Fehlerzustand nach dem Quit Error immer noch (z. B. bei einem Defekt), so bleibt der Ausgang weiterhin abgeschaltet. Wird das System neu gestartet oder wird der Quit Error über den Validierungstaster abgesetzt, so wird dieser Defekt im POST detektiert. Das Sicherheitsmodul wechselt daraufhin in den Fehlerzustand.

5.3.5.3 Querschluss zwischen den Ausgängen

Besteht ein Querschluss zwischen sicheren Ausgängen, so werden diese abgeschaltet und die Error-LEDs dieser Ausgänge blinken. Im SafetyDesigner wird in „Error of Channels“ der Fehler 144 bzw. 1144 für den entsprechenden Ausgang angezeigt. Während des Betriebs kann dieser Fehler nur detektiert werden, wenn die sicheren Ausgänge gesetzt sind. Tritt dieser Fehler auf, so muss die Verdrahtung der sicheren Ausgänge überprüft werden. Ist der Fehler behoben, so kann er mit absetzten eines Quit Errors zurückgesetzt werden.

5.3.6 Fehler beim Verteilen der Konfiguration

Wurde auf ein Sicherheitssystem, bestehend aus einer Safety-CPU und entfernten Sicherheitsmodulen, erfolgreich eine Konfiguration übertragen und der Verteilungsvorgang der Konfiguration initiiert, so kann dieser Prozess unter bestimmten Bedingungen fehlschlagen. Gleiches gilt auch für die Verteilung der Konfiguration beim Wiederanlauf eines solchen Systems. In einem solchen Fall wird im SafetyDesigner jeweils der Fehler 9 bzw. 1009 mit einem speziellen Identifier ausgegeben. Die möglichen Identifier sind:

- ***Identifier 0:***
  Wird dieser Errorcode ausgegeben, so fehlt mehr als ein sicheres Modul in der Hardwaretopologie, dass aber von der Konfiguration benötigt wird. Tritt dieser Fehler auf, so ist zu überprüfen, ob alle Sicherheitsmodule auch wirklich vorhanden sind. Zudem muss die Kommunikation zu jedem Sicherheitsmodul intakt sein. Dies kann z. B. anhand der Hardwareklassen im Standard-SPS Projekt überprüft werden. Werden alle Hardwareklassen der Sicherheitsmodule gefunden, so funktioniert die Kommunikation. Nach Beheben des Fehlers kann dieser mit einem „Quit Error“ Kommando behoben werden.

- ***Identifier 1:***
  Dieser Fehler tritt z. B. auf, wenn mehr als ein Sicherheitsmodul getauscht wurden. In diesem Fall muss die Konfiguration neu verteilt werden.

- ***Identifier 2:***
  In diesen Fall kann eine in der Konfiguration enthaltene Safety-CPU nicht identifiziert werden. Es ist daher zu überprüfen, ob alle in der Konfiguration enthaltenen Safety-CPUs auch tatsächlich vorhanden sind und ob eine korrekte Kommunikation mit ihnen besteht.

- ***Identifier 3:***
  Tritt dieser Fehler auf, so konnte die Konfiguration nicht verteilt werden. In diesem Fall ist zu überprüfen, ob alle Sicherheitsmodule vorhanden sind und eine Kommunikationsverbindung zu diesen besteht. Zudem ist zu überprüfen, ob die Hardwareklassen der Sicherheitsmodule im Standard-SPS-Projekt richtig platziert sind. Der Fehler kann mit Hilfe eines „Quit Error“ Befehls bzw. eines Neustarts des Systems behoben werden.

- ***Identifier 4:***
  Dieser Identifier weist darauf hin, dass ein entferntes Modul im Fehler steht. Dieses muss identifiziert und der Fehler muss korrigiert werden. Danach kann mit Hilfe eines „Quit Error“ Befehls bzw. beim Neustarts der Fehler behoben werden.

- ***Identifier 5 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass mind. ein lokales SDI-Modul bei einer S-DIAS-CPU fehlt. Das fehlende Modul muss eingefügt werden. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 6 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass ein lokales Safety-Interface-Modul bei einer S-DIAS-CPU fehlt. Das fehlende Modul muss eingefügt werden. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustarts der Fehler behoben werden.

- ***Identifier 7 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass mind. ein lokales STO-Modul bei einer S-DIAS-CPU fehlt. Das fehlende Modul muss eingefügt werden. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 8 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass mind. ein lokales SRO-Modul bei einer S-DIAS-CPU fehlt. Das fehlende Modul muss eingefügt werden. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 9 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass eine S-DIAS-CPU (Modul ist im Master Modus) versucht hat die Konfiguration zu beschreiben. Die eigene Konfiguration ist auf den Master Modus eingestellt. Die Konfiguration des eigenen Moduls muss gelöscht werden. Danach kann ein erneutes Verteilen der Konfiguration erfolgen.

- ***Identifier 10 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass ein Slave-Modul festgestellt hat, das das entfernte Module nicht richtig konfiguriert sind. Entfernte Module müssen konfiguriert werden. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 11 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass ein Eingangsmodul am falschen Platz steckt. Modul am richtigen Platz einfügen. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 12 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass ein Ausgangsmodul am falschen Platz steckt. Modul am richtigen Platz einfügen. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 13 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass ein SafeDint-Eingangsmodul am falschen Platz steckt. Modul am richtigen Platz einfügen. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 14 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass die Anzahl der lokalen Eingänge falsch ist. Anzahl durch Entfernen oder Einfügen von Eingangsmodulen richtigstellen. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 15 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass die Anzahl der lokalen Ausgänge falsch ist. Anzahl durch Entfernen oder Einfügen von Ausgangsmodulen richtigstellen. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 16 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass versucht wurde ein fehlendes Modul anzusprechen. Modul an der entsprechenden Stelle einfügen. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 17 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass ein Erweiterungsmodul nicht konfiguriert werden konnte. Versuchen erneut zu konfigurieren. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 18 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass zu viele Erweiterungsmodule vorhanden sind. Überzählige Module entfernen. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 19 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass zu wenige Erweiterungsmodule vorhanden sind. Fehlende Erweiterungsmodule einfügen. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

- ***Identifier 20 (S-DIAS Module):***
  Dieser Identifier weist darauf hin, dass ein falsches Safety-Interface-Modul angesteckt ist. Richtiges Safety-Interface-Modul anstecken. Danach kann mit Hilfe eines „Quit Error“-Befehls bzw. beim Neustart der Fehler behoben werden.

6 Änderungen am System

6.1 Update von Sicherheitsmodulen

Das Firmware-Update eines Sicherheitsmoduls kann nicht vom Kunden durchgeführt werden. Für ein Firmware-Update muss das Sicherheitsmodul an den Hersteller SIGMATEK GMBH & CO KG eingesandt werden.

6.2 Änderung der Konfiguration

Eine Änderung der Konfiguration muss mit Hilfe des SafetyDesigners vorgenommen werden. Die Konfigurationsdatei kann nur geändert werden, wenn der SafetyDesigner vom Zielsystem getrennt ist, also keine Onlineverbindung zwischen beiden besteht.

Nach der Änderung der Konfigurationsdatei muss diese mit Hilfe des SafetyDesigners auf das entsprechende Zielsystem übertragen werden. Nach dem erfolgreichen Download wechselt das System in den zeitlich begrenzten Laufzeitzustand. Anschließend muss die Validierung des Zielsystems durchgeführt werden. Nach eingehender Prüfung aller Funktionen auf Korrektheit kann daraufhin in den zeitlich unbegrenzten Laufzeitzustand gewechselt werden.

Beim Tausch oder nachträglichen Hinzufügen optionaler Safety Module muss das System immer neu konfiguriert und validiert werden. Dies kann entweder mit Hilfe des SafetyDesigners oder der SD-Karte erfolgen.
Erfolgt diese erneute Validierung nicht, verliert die SCP ihre Konfiguration und wechselt in einen Fehlerzustand (ERRVAL 222 / 1222 Temporary Operation Time – siehe Kap. 2.6.4). Dies ist eine Sicherheitsmaßnahme für unautorisierte Module in unserem Safety-System.

6.3 Modultausch

Beim Austausch eines Sicherheitsmoduls muss zwischen dem Austausch einer Safety-CPU und dem eines entfernten sicheren Eingangs- bzw. Ausgangsmoduls unterschieden werden.

GEFAHR!
Beim Austausch eines Sicherheitsmoduls muss unbedingt darauf geachtet werden, dass zuvor das System von der Versorgungsspannung getrennt wird.

	INFO! Beim Tausch optionaler Safety-Module muss das System immer neu konfiguriert und validiert werden. Dies kann entweder mit Hilfe des SafetyDesigners oder der SD-Karte erfolgen. Erfolgt diese erneute Validierung nicht, verliert die SCP ihre Konfiguration und wechselt in einen Fehlerzustand (ERRVAL 222 / 1222 Temporary Operation Time – siehe Kap. 2.6.4). Dies ist eine Sicherheitsmaßnahme für unautorisierte Module in unserem Safety-System.

6.3.1 Tausch einer Safety-CPU

Die im Austausch neu eingeführte Safety-CPU muss zunächst neu konfiguriert werden. Dies kann entweder mit Hilfe des SafetyDesigners oder der SD-Karte erfolgen.

6.3.2 Tausch eines sicheren Eingangs- bzw. Ausgangsmoduls

Der Tausch eines Sicherheitsmoduls wird vom System unterstützt. Nach dem Abschalten der Spannungsversorgung kann das Sicherheitsmodul gegen ein neues ausgetauscht werden. Anschließend kann das System wieder hochgefahren werden. Befand sich das sichere System vor dem Tausch des Sicherheitsmoduls im Operational Mode, so wechselt es beim Wiederanlauf in den temporary Operational Mode. Um in den zeitlich unbegrenzten Operational Mode zu gelangen, muss das System neu validiert werden.

6.3.3 Tausch mehrerer sicherer Eingangs- bzw. Ausgangsmodule

Wird mehr als ein Sicherheitsmodul getauscht, so wechselt das sichere System beim Wiederanlauf in den Fehlerzustand. Es wird der Fehlercode 9 bzw. 1009 ausgegeben. In diesem Fall muss das gesamte System neu zu konfiguriert werden.

6.3.4 Tausch sicherer Eingangs- bzw. Ausgangsmodule bei den Safety-Modulen SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211

Bei den Modulen SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211 können mehrere der zugehörigen Ansteckkarten getauscht werden. Nach dem Abschalten der Spannungsversorgung können die Sicherheitsmodule gegen neue ausgetauscht werden. Anschließend kann das System wieder hochgefahren werden. Befand sich das sichere System vor dem Tausch des Sicherheitsmoduls im Operational Mode, dann bleibt dieser erhalten.

6.4 Hinzufügen eines Sicherheitsmoduls

Befindet sich das sichere System im Operational Mode und wird ein weiteres Sicherheitsmodul hinzugefügt, das nicht zur Konfiguration gehört, so hat dies keine Auswirkung auf das sichere System.

Ist das hinzugefügte Sicherheitsmodul bereits konfiguriert, so ist es möglich, dass die Error-LED dieses Sicherheitsmoduls blinkt, z.B. wenn ein sicheres Ausgangsmodul hinzugefügt wurde, das bereits konfiguriert ist und Daten von einer nicht vorhandenen Safety-CPU erwartet. Dies hat jedoch keine Auswirkungen auf das sichere System.

Beim Hinzufügen eines bereits konfigurierten sicheren Eingangsmoduls ist es möglich, dass dieses ganz normal in den Operational Mode wechselt. Dieses Modul versendet dann zwar sichere Daten, die jedoch keinen Abnehmer finden. Somit hat dieses Modul keine Auswirkung auf das sichere System.

6.5 Entfernen eines Sicherheitsmoduls

Wird ein Sicherheitsmodul entfernt, das in einem sicheren System verwendet wird, so sind folgende Fälle zu unterscheiden:

6.5.1 Sicheres Eingangsmodul wird entfernt

Wird ein sicheres Eingangsmodul während des Betriebs entfernt (z.B. durch den Ausfall der Buskommunikation zu diesem Modul), so beginnt die Error-LED der vom entfernten Eingangsmodul abhängigen Safety-CPU zu blinken. Die von dem Eingangsmodul abhängigen sicheren Ausgänge wechseln in den sicheren Zustand. Im SafetyDesigner wird der Fehler 199 (Überschreitung des maximalen Alters) für die entsprechenden sicheren Ausgänge angegeben. Kehrt das ausgefallene Sicherheitsmodul während des Betriebs (z.B. durch Wiederkehr der Kommunikation) zurück, so bleiben die entsprechenden sicheren Ausgänge im sicheren Zustand. Der Fehler muss mit Hilfe eines Quit Error Befehls oder alternativ durch einen Neustart des Systems behoben werden.

6.5.2 Sichere CPU wird entfernt

Fällt die sichere Safety-CPU aus, so wird dies auf Grund der Erwartungshaltung vom abhängigen sicheren Ausgangsmodul festgestellt. Die Error-LED dieses Ausgangsmoduls blinkt und die abhängigen sicheren Ausgänge gehen in den sicheren Zustand. Wird mit dem SafetyDesigner online auf die sichere Steuerung zugegriffen, so kann die Safety-CPU nicht mehr aufgefunden werden. Ein von der entfernten Safety-CPU abhängiges sicheres Eingangsmodul bemerkt den Ausfall der Safety-CPU hingegen nicht, da das sichere Eingangsmodul keine Erwartungshaltung gegenüber der Safety-CPU hat. Kehrt die Safety-CPU wieder ins System zurück, so verharren die entsprechenden sicheren Ausgänge weiterhin im sicheren Zustand. Zur Behebung des Fehlerzustandes ist ein „Quit Errors“ Befehl bzw. ein Neustart des Systems erforderlich.

6.5.3 Sicheres Ausgangsmodul wird entfernt

Beim Ausfall eines sicheren Ausgangsmoduls gehen die von diesem Ausgangsmodul abhängigen sicheren Ausgänge anderer Module in den sicheren Zustand. Die Safety-CPU bemerkt den Ausfall des sicheren Ausgangsmoduls nur, wenn in der Konfiguration der Safety-CPU ein sicherer Ausgang des ausgefallenen Sicherheitsmoduls zurückgelesen wird (beispielsweise verknüpft auf die Ausgänge andere Module). Ist dies der Fall, so beginnt das Error-LED der Safety-CPU zu blinken und die davon abhängigen sicheren Ausgänge wechseln in den sicheren Zustand. Wird in der Konfiguration kein sicherer Ausgang des ausgefallenen Ausgangsmoduls zurückgelesen, so wird dies von der Safety-CPU nicht registriert. Bei der Wiederkehr des sicheren Ausgangsmoduls bleibt der zuvor ausgelöste Fehler erhalten. Es ist entweder ein Neustart des Systems oder ein Absetzen eines Quit Error Befehls notwendig.

7 Besonderheiten im System

7.1 Verwendung optionaler Module (ab Revision 2)

Im SafetyDesigner können Safety-Module oder lesende Interfaces über den Property Browser auf „optional“ geschalten werden. Dies bedeutet, dass einzelne Module oder Interfaces für die Abarbeitung der Konfiguration auf der Safety-CPU nicht vorhanden sein müssen. Für die Daten dieser Module oder Interfaces kann ein vom Anwender voreingestellter Wert verwendet werden. Die Verwendung von optionalen Modulen oder Interfaces ist an Voraussetzungen geknüpft.

In der Sicherheitsapplikation werden nach den Eingängen des optionalen Moduls/Interfaces und der restlichen Logik spezielle Funktionsblöcke (SF_Optional_Pwd/SF_Optional_PwdII und SF_Optional_Switch) platziert, die im Falle eines fehlenden Moduls/Interfaces definierte Werte (auch solche, die dem nicht sicheren Zustand entsprechen) an die dahinterliegende Logik weiterreichen.

Ist das Feststellen der Erreichbarkeit von optionalen Modulen für die Anwendung erforderlich, kann im Interface eine SafeBool mit Konstant „True“ angelegt werden. Dadurch kann in der

Anwendung festgestellt werden ob es sich um einen Wert aus dem optionalen Modul handelt oder es ein vordefinierter Wert der Fehlerbehandlung ist.

GEFAHR!

Es ist hier zu beachten, dass eine gefährliche Situation eintreten könnte, wenn der Zustand dieser Funktionsblöcke (bezüglich des Vorhandenseins eines optionalen Moduls/Interfaces) nicht mit der Realität übereinstimmt.

WICHTIG!

Das System ist nach jedem Wechsel zwischen optional und nicht optional vom Anwender auf Richtigkeit zu prüfen.

WICHTIG!

Das Programm der SPS ist nach jedem Wechsel zwischen optional und nicht optional neu zu starten.
Ab Safety-Firmware V245 besteht die Möglichkeit, auch ohne Neustart des Programms in der SPS ein optionales Modul anzustecken und zu verwenden. Dazu muss im Programm der Server QuitCommError der HW-Klasse SCP 010 beschrieben werden. Das Beschreiben dieses Servers bewirkt ein Löschen von Kommunikationsfehlern. Dadurch kann ein (möglicherweise unerwarteter) Wiederanlauf der Maschine stattfinden. Daher ist es erforderlich, den Benutzer vor dem Löschen eines solchen Fehlers auf diese Gefahr aufmerksam zu machen und ihm die Möglichkeit zu geben, den Vorgang abzubrechen (z.B. durch ein Fenster auf der Benutzeroberfläche mit einem entsprechenden Hinweistext und Schaltflächen zum Abbrechen und Fortsetzen).
Beim Tausch oder nachträglichen Hinzufügen optionaler Safety Module muss das System immer neu konfiguriert und validiert werden. Dies kann entweder mit Hilfe des SafetyDesigners oder der SD-Karte erfolgen.
Erfolgt diese erneute Validierung nicht, verliert die SCP ihre Konfiguration und wechselt in einen Fehlerzustand (ERRVAL 222 / 1222 Temporary Operation Time – siehe Kap. 2.6.4). Dies ist eine Sicherheitsmaßnahme für unautorisierte Module in unserem Safety-System.

WICHTIG!

Der Wechsel des Systems (zwischen optional und nicht optional) **darf nur von geschultem Fachpersonal durchgeführt werden**!

WICHTIG!

Der Funktionsblock SF_Optional_PwdII darf in den Safety-CPUs CSCP 011 und CSCP 012 nicht verwendet werden!

7.2 Sicherheitsmaßnahmen und -hinweise

Durch die Verwendung des Funktionsblocks „SF_OPTIONAL_PWDII“ werden grundsätzlich alle Sicherheitsfunktionen betroffen; daher sind unbedingt die nachfolgenden Maßnahmen und Gefahrenhinweise zu berücksichtigen. Die Nichtbeachtung dieser Warnhinweise kann zu schweren Körperverletzungen oder zum Tod führen.

Der Anwender der Maschine muss im Hinblick auf die möglichen Gefahren, die von der Verwendung des Funktionsblock „SF_OPTIONAL_PWDII“ ausgehen können, und unter Berücksichtigung der für die spezifische Anwendung geltenden normativen Anforderungen (beispielsweise hydraulische Gesenkbiegepressen) eine Risikoanalyse erstellen und die erforderlichen Maßnahmen der Risikominderung treffen.

Die Gültigkeitsdauer des von der Sicherheits-CPU errechneten Codes (Anmeldezeit) muss in jedem Fall so kurz wie möglich sein; insbesondere muss sichergestellt werden, dass sie nicht schichtübergreifend wirksam ist.

Es muss gewährleistet sein, dass Passworteingabe und Bestätigung des automatisch errechneten Codes von ein und demselben autorisierten Einrichter vorgenommen wird.

Die Maschine muss während der Gültigkeitsdauer des automatisch errechneten Codes permanent im Blickfeld des Einrichters der Maschine sein.

Außer dem Einrichter der Maschine dürfen sich innerhalb der Grenzen der Maschine gemäß EN 12100 keine weiteren Personen aufhalten. Insbesondere muss der freie Zugang zur Maschine durch geeignete Maßnahmen verhindert werden.

Befehlsgeräte ohne Not-Halt-Funktion sind so zu installieren, dass von jeder Position aus in Handreichweite jederzeit ein Not-Halt ausgelöst werden kann.

7.3 Verwendung von Interface-Variablen (ab Revision 2)

Durch Interface-Variablen kann projektübergreifend zwischen Safety-CPUs kommuniziert werden (Safety-CPUs sind in verschiedenen Safety-Projekten konfiguriert und müssen am Bus-Master sitzen). Dies bedeutet, dass eine Safety-CPU die Daten schreibend zur Verfügung stellt und eine andere Safety-CPU diese Daten lesend verarbeitet. Näheres zu den Interface-Variablen ist in der Beschreibung des LASAL-SafetyDesigners zu finden.

7.4 Master- und Slave-Mechanismus beim Modul SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211

Im SafetyDesigner können Safety-Module vom Typ SCP 010/SCP 011/SCP 111/SCP 111-S/SCP 211 über den Property Browser auf Master- und Slave-Modus geschalten werden. Es muss mindestens eine Safety-CPU im Master-Modus betrieben werden. Die Module im Slave-Modus sind den eingestellten Modulen im Master-Modus zugeordnet.

Vorteile für den Anwender:

- Download der Konfiguration nur noch bei den Master-Modulen nötig
- Download der Konfiguration auf eine SD-Karte nur noch bei den Master-Modulen nötig
- Einloggen nur noch bei den Master-Modulen nötig
- Keine Passwort-Einstellung bei den Slave-Modulen nötig
- Quit Error und Start der Slave-Module über das zugeordnete Master-Modul
- Slave-Module müssen nicht verifiziert werden

Näheres zum Master-Slave-Mechanismus ist in der Beschreibung des LASAL-SafetyDesigners zu finden.

☞	Module im Slave-Modus können nicht ohne ihr zugehöriges Master-Modul betrieben werden. Ein Slave-Modul kann nur dann im Operational Modus laufen, wenn auch das Master-Modul im Operational/temp. Operational Modus läuft.

☞	Soll ein Modul im Slave-Modus betrieben werden, muss zuvor geprüft werden, ob dieses Modul nicht als Master konfiguriert ist. Ist das Modul als Master konfiguriert, muss die Konfiguration auf dem Modul gelöscht werden.

☞	Es wird empfohlen, dass verschiedene Mastersysteme nur über die Master-Module miteinander kommunizieren. Ein Mastersystem besteht aus einem Master-Modul und seinen zugehörigen Slave-Modulen. Es sollte kein Slave-Modul eines Mastersystems mit einem anderen Mastersystem kommunizieren. Bei dieser direkten Kommunikation wäre es sonst eventuell nötig das System mehrfach zu starten.

7.5 Verwendung der Module SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211 im Standalone-Betrieb

Die S-DIAS-Module SCP 010, SCP 011, SCP 111, SCP 111-S und SCP 211 können als Standalone-Variante verwendet werden. Dies bedeutet, dass das Modul nicht in einem Standard-SPS-Projekt eingebunden werden muss. Die Konfiguration des Moduls erfolgt direkt und nicht über eine Standard-SPS (Ausnahme: SSI). Näheres zur Verwendung im Standalone-Betrieb ist in der Beschreibung des LASAL-SafetyDesigners zu finden.

7.6 Kommunikation über FSoE (Revison 4)

7.6.1 Was ist eine FSoE-Kommunikation

Unter einer FSoE-Kommunikation versteht man den Austausch der sicheren Daten zwischen zwei Safety-Modulen über das FSoE-Protokoll.

Fail Safe over EtherCAT (FSoE) ist ein Protokoll zur Übertragung von sicherheitsrelevanten Daten unter Verwendung eines FSoE-Masters und FSoE-Slaves. In jedem FSoE-Zyklus sendet der FSoE-Master Daten an den FSoE-Slave und startet zugleich einen Watchdog-Timer. Der FSoE-Slave verarbeitet die Daten und generiert eine Rückübermittlung an den FSoE-Master. Der FSoE-Slave startet ebenfalls eine Laufzeitüberwachung. Der FSoE-Master empfängt die Daten und hält den Watchdog-Timer an. Erst nach vollständiger Ausführung dieses Zyklus generiert der FSoE-Master neue Daten für die Übertragung. Jeder FSoE-Slave besitzt eine, im jeweiligen System eindeutige, FSoE-Slave-Adresse. Der Aufbau einer Verbindung erfolgt über diese Slave-Adresse. Zusätzlich wird jeder Verbindung eine, im jeweiligen System eindeutige, Connection ID zugewiesen.

7.6.2 Erstellung einer FSoE-Verbindung zwischen zwei Modulen

Die Slave-Adressen und Connection IDs werden durch den Safety Designer automatisch vergeben. Die Festlegung, welches Modul der FSoE-Master bzw. FSoE-Slave einer FSoE-Verbindung ist, wird ebenfalls durch den Safety Designer automatisch festgelegt. Die Vergabe erfolgt beim Platzieren von sicheren Eingängen, sicheren Ausgängen und Interfaces im Netzwerk einer Safety-CPU (die Safety-CPU sitzt am Bus-Master). Es wird dabei zwischen zwei Safety-Modulen eine FSoE-Verbindung aufgebaut. Die Slave-Adresse und die Connection ID werden durch den Safety Designer festgelegt. Die erlaubten Werte werden durch die eingestellten Grenzen der Slave-Adressen und Connection IDs beim Projekt vorgegeben. Die Grenzen können vom Anwender zwischen 1 und 65335 eingestellt werden (Defaultwert: 1-65335). Bei der Benutzung von schreibenden Interfaces in einer FSoE-Verbindung muss beim Interface die max. Anzahl der Verwendungen als lesendes Interface eingestellt werden. Der Defaultwert beträgt 10 Verwendungen. Der maximale Wert ist 150 Verwendungen. Dies ist nötig, da für jede Verwendung eine eigene FSoE-Verbindung aufgebaut werden muss. Schreibende Interfaces werden immer als FSoE-Slave einer Verbindung angesehen.

Für die schreibenden Interfaces kann keine Connection ID vergeben werden; die Connection ID wird erst beim FSoE-Master (lesendes Interface) festgelegt. Beim Export von schreibenden Interfaces wird die eingestellte Slave-Adresse, sowie die eingestellten Grenzen der Slave-Adressen und Connection IDs mit exportiert.

Diese exportierten Daten werden im Projekt der lesenden Interfaces entsprechend geladen. Die exportierte Slave-Adresse wird beim lesenden Interface (fungiert immer als FSoE-Master) als Slave-Adresse für die Verbindung zum FSoE-Slave verwendet. Die exportierten Grenzwerte ermöglichen eine Prüfung für die Eindeutigkeit der Slave-Adressen und Connection IDs in den beiden Projekten.

Für jede FSoE-Verbindung muss die maximale Transmission Time (Übertragungszeit am Bus) eingestellt werden; der Safety Designer berechnet diese Zeit und trägt sie bei der Verbindungserstellung automatisch ein.

Der Anwender muss darauf achten, dass die Slave-Adressen und die Connection IDs im kompletten System eindeutig sind. Der Safety Designer kann die Eindeutigkeit nur innerhalb des Projekts prüfen.

Bei lesenden Interfaces besteht die Möglichkeit als Slave-Adresse 0 zu vergeben; in diesem Fall ermittelt die Safety-CPU über den eingestellten Hardwarepfad zum schreibenden Interface die dort gespeicherte Slave-Adresse.

Es besteht auch die Möglichkeit als Connection ID 0 zu vergeben; in diesem Fall werden am Modul gespeicherte Connection IDs verwendet. Die Zahl 0 als Connection ID darf nur verwendet werden, wenn am Modul entsprechende Connection IDs vordefiniert sind.

Bei schreibenden Interfaces besteht die Möglichkeit als Slave-Adresse 0 zu vergeben, in diesem Fall werden am Modul gespeicherte Slave-Adressen verwendet. Die Zahl 0 als Slave Adresse darf nur verwendet werden, wenn am Modul entsprechende Slave-Adressen vordefiniert sind.

7.6.3 Änderung der Werte

Der Anwender kann die eingestellten Werte in einem Dialog kontrollieren und gegebenenfalls ändern. Der Aufruf des Dialogs erfolgt über das Kontextmenü des Projekts.

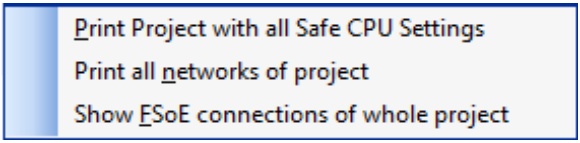


Bild 62 FSoE Menü

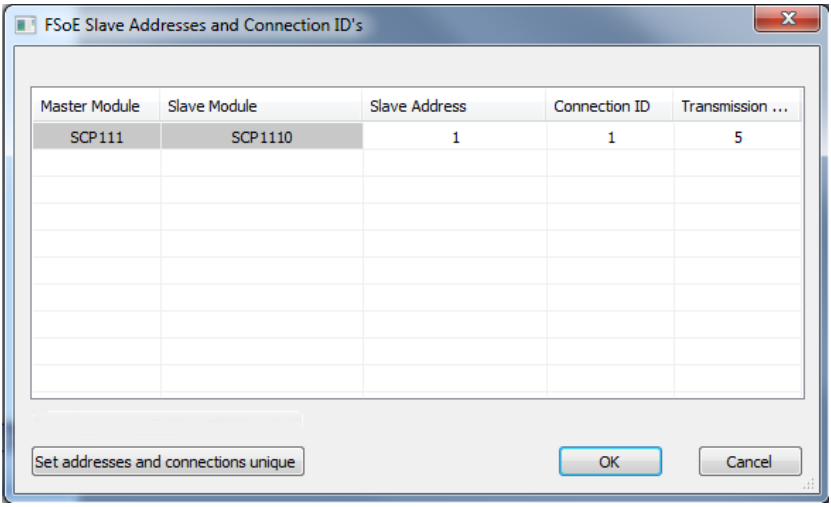


Bild 63 FSoE-Verbindung

Der Dialog zeigt die einzelnen FSoE-Verbindungen mit den Einstellungen an. Grau hinterlegte Zellen können nicht geändert werden. In der Spalte „Master Module“ steht der FSoE-Master einer Verbindung. Schreibende Interfaces besitzen keinen FSoE-Master, es wird eine leere Zelle angezeigt. In der Spalte „Slave Module“ steht entweder der FSoE-Slave einer Verbindung oder ein lesendes/schreibendes Interface. Die lesenden und schreibenden Interfaces sind durch Texte entsprechend gekennzeichnet. In der Spalte „Slave Address“ steht die Adresse eines FSoE-Slaves. Die Adresse kann vom Anwender geändert werden und muss im System eindeutig sein. In der Spalte „Connection ID“ steht die ID einer Verbindung. Die ID kann vom Anwender geändert werden und muss im gesamten System eindeutig sein. Schreibende Interfaces besitzen keine Connection ID, es wird eine leere Zelle angezeigt. In der Spalte „Transmission Time“ steht die Zeit, welche zur Übertragung von einem Modul zum anderen Modul benötigt wird. Die Zeit kann vom Anwender geändert werden. Alle Werte, welche vom Anwender geändert werden können, werden auf Gültigkeit geprüft. Ungültige Werte können nicht übernommen werden.

Erlaubte Werte der Slave-Adresse: 1-65335 (in Abhängigkeit der eingestellten Grenzwerte)

Bei Interfaces kann 0 vergeben werden (dies bedeutet bei lesenden Interfaces eine Ermittlung der Slave-Adresse aus dem Hardwarepfad des Kopplermoduls; bei schreibenden Interfaces wird eine am Modul gespeicherte Slave-Adresse verwendet). Bei lesenden Interfaces werden die Grenzen des Projekts für das schreibende Interface verwendet (Daten werden aus der importierten XML-Datei entnommen).

Erlaubte Werte Connection ID: 1-65335 (in Abhängigkeit der eingestellten Grenzwerte)

Erlaubte Werte Transmission Time: 1-5000 [ms]

Über die Schaltfläche „Set addresses and connections unique“ können die Slave-Adressen und die Connection ID auf im Projekt eindeutigen Werte gesetzt werden. Es werden alle eingestellten Werte gelöscht und die neuen Werte über die eingestellten Grenzwerte gesetzt (Beginn mit dem kleinstmöglichen Wert).

Mit OK werden die geänderten Daten ins Projekt übernommen.

7.6.4 Watchdog-Zeit

Die maximal überwachte Watchdog-Zeit, ist die Zeit, welche vom Verschicken eines FSoE-Frames bis zum Eintreffen der Antwort vergeht. Diese Zeit muss vom Anwender nicht eingestellt werden, sondern wird vom Safety Designer über die vom Anwender eingestellte Transmission-Time und die Zykluszeiten der Module ermittelt. Die vom Anwender eingestellte Transmission-Time enthält die Übertragungszeit am Bus und einen Buszyklusversatz (Safety CPUs laufen nicht bussynchron).

Berechnung der Watchdog-Zeit durch den Safety Designer:

Zeit = 2 * Zykluszeit FSoE-Master
+ 2 * Zykluszeit FSoE-Slave
+ 2 * Transmission-Time

Bei der Berechnung der Watchdog-Zeit für Interfaces kann die Zykluszeit für schreibende Interfaces nicht ermittelt werden; es ist daher nötig, dass der Anwender diese Zeit aus dem Projekt der schreibenden Interfaces ermittelt und bei der Transmission-Time der lesenden Interfaces addiert. Die Daten des schreibenden Interfaces können aus dem Monitoring Settings Dialog des anderen Projekts entnommen werden.

Ermittlung Transmission-Time der lesenden Interfaces:

Zeit = Zykluszeit FSoE-Slave (Zykluszeit beim schreibenden Interface)
+ Transmission-Time (beim schreibenden Interface)
+ Transmission-Time (beim lesenden Interface)

7.7 Erstellung einer FSoE Verbindung über eine IP-Adresse

Die Funktionalität ist auf Safety-CPUs mit FSoE-Kommunikation beschränkt (SCP111, SCP 111-S und SCP 211). Die Kommunikation über IP-Adressen funktioniert nur bei der Verwendung von Interfaces; es muss dazu beim lesenden Interface die IP-Adresse für die Seite des schreibenden Interfaces eingestellt werden.

IP-Adressen können nur bei einer FSoE-Kommunikation verwendet werden.

Das schreibende Interface fungiert in der FSoE-Verbindung als FSoE-Slave; das lesende Interface als FSoE-Master. Um eine eindeutige FSoE-Kommunikation zu gewährleisten, müssen die Connection IDs und die FSoE-Slaveadressen eindeutig sein. Die Connection ID wird im Normalfall vom FSoE-Master (lesendes Interface) festgelegt und dem FSoE-Slave mitgeteilt. Bei der Verwendung der IP-Adressen besteht nun zusätzlich die Möglichkeit die Connection IDs auf Seite der schreibenden Interfaces (FSoE-Slave) festzulegen.
Das lesende Interface kann bei ausgewähltem Vergabeservice für den Aufbau einer FSoE-Verbindung die Connection ID vom schreibenden Interface anfordern. Das schreibende Interface liefert eine Connection ID aus dem eingestellten Bereich für die Connection IDs; sind bereits alle IDs vergeben, kann keine Verbindung aufgebaut werden.

7.7.1 Einstellungen für die Verwendung der IP-Adresse und des Vergabeservices

Bei der Verwendung des Vergabeservices für die Connection IDs muss auf der Seite der schreibenden Interfaces der Connection ID Service *(„Using connection ID service“)* aktiviert werden; die Aktivierung erfolgt im PropertyBrowser. Als Defaultwert ist false eingestellt; ist dieses Flag auf true gestellt, wird vom SafetyDesigner automatisch ein Bereich für die erlaubten Connection IDs berechnet und angezeigt *(„Range of connection IDs“)*.

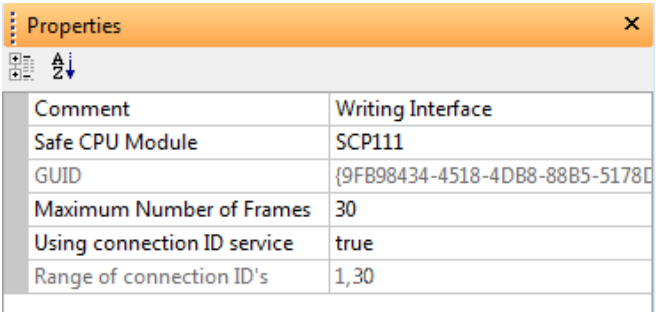


Bild 64 PropertyBrowser

Der Bereich der Connection IDs berechnet sich aus der Anzahl der Verwendungen und aus dem erlaubten Bereich für die Connection IDs des Projekts. Der Bereich wird vom SafetyDesigner automatisch berechnet und kann nicht verändert werden.

Beim Export der schreibenden Interfaces wird zusätzlich zu den bereits bestehenden Daten, das Flag für die Verwendung des Vergabeservices mitgeschrieben.

Das Flag für den Vergabeservice wird auf der Seite der lesenden Interfaces eingelesen und automatisch berücksichtigt. Die Einstellung wird im PropertyBrowser angezeigt *(„Using connection ID service“)* und kann vom Anwender nicht verändert werden.

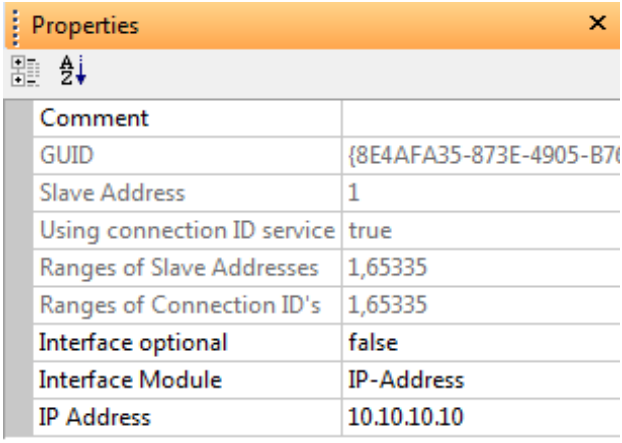


Bild 65 PropertyBrowser

Im PropertyBrowser des lesenden Interfaces kann als Interface Modul die Kommunikation über eine IP-Adresse mittels einer Combobox eingestellt werden. Bisher waren als Interface-Module nur PLCs oder Kopplermodule (z.B. VBC) erlaubt; ist als Interface Module die IP-Adresse eingestellt, wird automatisch ein Property für die IP-Adresse (*„IP-Address“*) angezeigt.

7.7.2 FSoE-Dialog für schreibende Interfaces

Im FSoE Connections Dialog wird für schreibende Interfaces der Bereich der Connection IDs dargestellt, die vom Vergabeservice verwendet werden können. Die Slave Adresse wird vom SafetyDesigner automatisch vergeben, kann aber vom Anwender verändert werden.

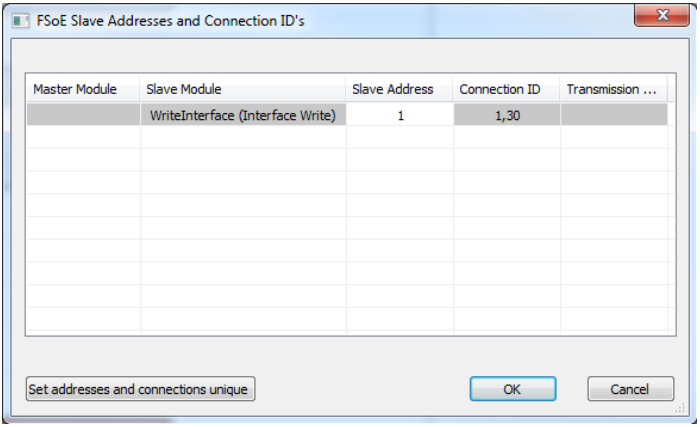


Bild 66 FSoE-Verbindung für schreibendes Interface

7.7.3 FSoE-Dialog für lesende Interfaces

Bei der Verwendung des Vergabeservice kann beim lesenden Interface keine Connection ID mehr eingestellt werden. Die Transmission Time kann vom Anwender eingestellt werden; es ist hier eine maximale Zeit von 5000 ms erlaubt.

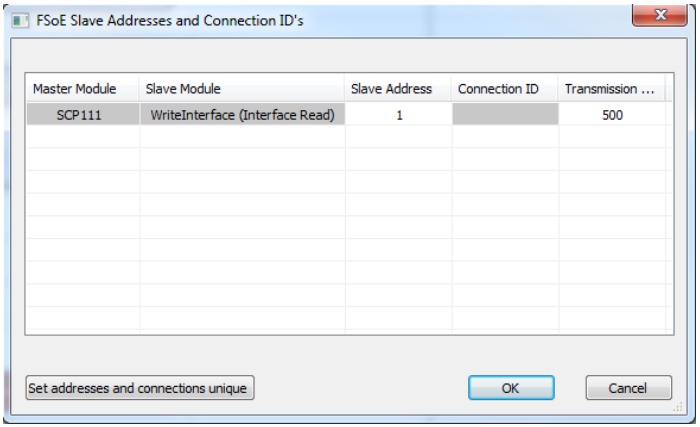


Bild 67 FSoE-Verbindung für lesendes Interface

Monitoring Settings für lesende Interfaces

Es ist bei der Kommunikation über IP-Adressen nicht mehr möglich eine Transmission Time für die lesenden Interfaces zu berechnen. Der Anwender muss die Zeit selbstständig ermitteln und dann eintragen.

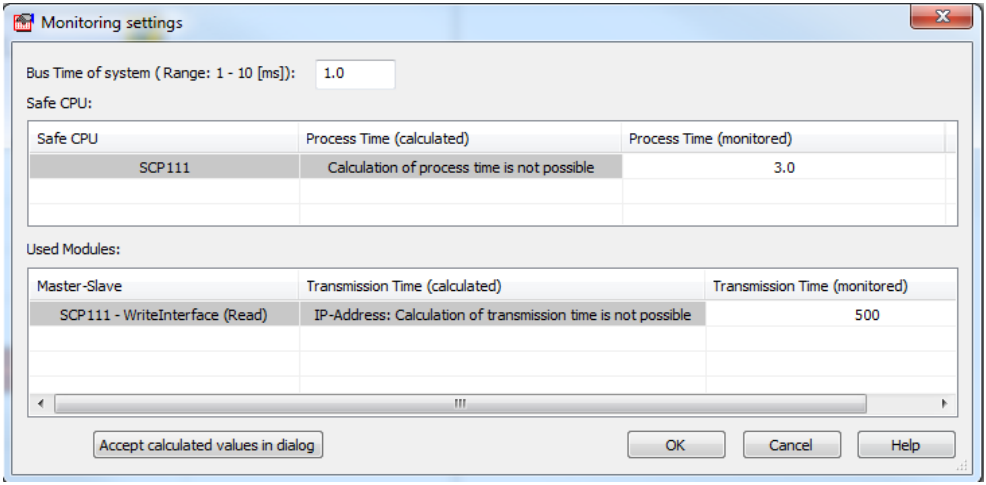


Bild 68 Monitoring settings für lesendes Interface

Das maximale Alter bei lesenden Interfaces kann bis zu 5000 ms betragen; da sich über W-LAN große Zeiten ergeben können.

7.7.4 Ermittlung der maximalen Transmission Time

Es muss bei den lesenden Interfaces eine maximale Transmission Time zwischen den Modulen eingestellt werden. Die automatische Berechnung durch den SafetyDesigner ist nicht möglich. Nachfolgend wird erklärt, wie die Zeit durch den Anwender ermittelt werden kann.

Formel zur Ermittlung der Transmission Time:

Zeit = Zykluszeit FSoE-Slave (Zykluszeit beim schreibenden Interface)
+ Bus-Übertragungszeit beim schreibenden Interface
+ Zeit für Anzahl der Verwendungen des schreibenden Interfaces
+ Zeit für Anzahl der lesenden Interfaces
+ Zusatzzeit aufgrund Black-Channel (Netzqualität, Netzauslastung, Einfluss Roaming, Auslastung Standard-CPU, ...)

Die Zykluszeit des FSoE-Slaves, die Bus-Übertragungszeit des schreibenden Interfaces und die Anzahl der Verwendungen des schreibenden Interfaces können aus dem Projekt des schreibenden Interfaces entnommen werden. Die Zusatzzeit aufgrund von Black-Channel muss anhand des verwendeten Mediums und dessen Qualität vom Anwender festgelegt werden.

Formel zur Ermittlung der Zeit für die Anzahl der Verwendungen des schreibenden Interfaces:

Zeit = Anzahl der Verwendungen des schreibenden Interfaces
x 10 ms (Zeitdifferenz zwischen dem Versenden von zwei UDP-Paketen) (aber mindestens 300 ms)

Die Zeit für Anzahl der Verwendungen des schreibenden Interfaces muss mindestens 300 ms betragen, sollte die ermittelte Zeit kleiner sein, muss mit 300 ms gerechnet werden. Der Wert von 300 ms ergibt sich daraus, dass bei der Übertragung über W-LAN/Ethernet einzelne Pakete ausfallen können und somit mehrfach versendet werden müssen. Es gibt maximal 2 Wiederholungen. Die Zeitdifferenz zwischen den Wiederholungen beträgt 100 ms.

Formel zur Ermittlung der Zeit für die Anzahl der lesenden Interfaces:

Zeit = die Anzahl von lesenden Interfaces in diesem Projekt
x 10 ms (Zeitdifferenz zwischen dem Versenden von zwei UDP-Paketen)

Die Zeitdifferenz zwischen dem Versenden von zwei UDP-Paketen wird von der eingestellten Cyclic-Time am HW-Control-Objekt (Objekt im LASAL Class 2 Projekt) beeinflusst. Die Zeit beträgt mindestens 10 ms, kann je nach Einstellung aber darüber hinausgehen.

7.7.4.1 Beispiele zur Ermittlung der Transmission Time

Angenommene Zeiten, welche für alle Beispiele verwendet werden.
Zykluszeit FSoE-Slave = 1 ms
Bus-Übertragungszeit beim schreibenden Interfaces = 3 ms
Black-Channel = 500 ms
Es wird in den Beispielen jeweils die Transmission-Time für ein lesendes Interface beim Projekt R1 berechnet.

7.7.4.2 Beispiele 1

Ein schreibendes Interface wird an drei Projekte mit je einem lesenden Interface verteilt.

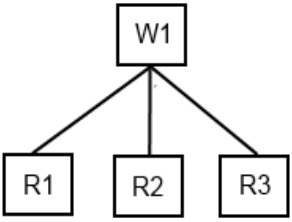


Bild 69 Schreibendes Interface an 3 Projekten

Ermittlung der Zeit:

Zeit = 1 ms (Zykluszeit FSoE-Slave)
+ 3 ms (Bus-Übertragungszeit beim schreibenden Interface)
+ 300 ms (Zeit für Anzahl schreibender Interfaces)
+ 10 ms (Zeit für Anzahl lesender Interfaces)
+ 500 ms (Black-Channel)

Transmission-Time = Summe aller Zeiten = 814 ms

7.7.4.3 Beispiele 2

3 schreibende Interfaces werden an ein Projekt mit drei lesenden Interfaces verteilt.

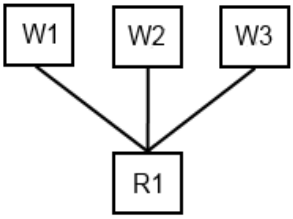


Bild 70 3 schreibende Interfaces an einem Projekt

Ermittlung der Zeit:

Zeit =		1 ms (Zykluszeit FSoE-Slave)
	+	3 ms (Bus-Übertragungszeit beim schreibenden Interface)
	+	300 ms (Zeit für Anzahl schreibender Interfaces)
	+	30 ms (Zeit für Anzahl lesender Interfaces)
	+	500 ms (Black-Channel)

Transmission-Time = Summe aller Zeiten = 834 ms

7.7.4.4 Beispiele 3

Zwei schreibende Interfaces werden an zwei Projekte mit je zwei lesenden Interfaces verteilt.

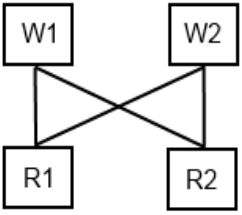


Bild 71 2 schreibende Interfaces an 2 Projekten

Ermittlung der Zeit:

Zeit =		1 ms (Zykluszeit FSoE-Slave)
	+	3 ms (Bus-Übertragungszeit beim schreibenden Interface)
	+	300 ms (Zeit für Anzahl schreibender Interfaces)
	+	20 ms (Zeit für Anzahl lesender Interfaces)
	+	500 ms (Black-Channel)

Transmission-Time = Summe aller Zeiten = 824 ms

7.7.4.5 Beispiele 4

Ein schreibendes Interface wird an 50 Projekte mit je einem lesenden Interface verteilt.

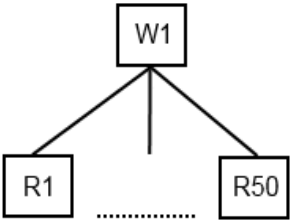


Bild 72 Schreibendes Interface an 50 Projekten

Ermittlung der Zeit:

Zeit =		1 ms (Zykluszeit FSoE-Slave)
	+	3 ms (Bus-Übertragungszeit beim schreibenden Interface)
	+	500 ms (Zeit für Anzahl schreibender Interfaces)
	+	10 ms (Zeit für Anzahl lesender Interfaces)
	+	500 ms (Black-Channel)

Transmission-Time = Summe aller Zeiten = 1014 ms

7.7.5 Vorteile des Vergabeservices

Die Verwendung des Vergabeservice hat den Vorteil, dass alle Safety-Applikationen auf der Seite der lesenden Interfaces identisch sein können, da die Connection IDs auf der Seite der schreibenden Interfaces vergeben werden.

Wird kein Vergabeservice verwendet, müssen die Safety-Applikationen auf der Seite der lesenden Interfaces verschieden sein. Es ist in jeder Safety-Applikation eine im System eindeutige Connection ID für den Aufbau der FSoE-Verbindung zum schreibenden Interface einzutragen. Diese Connection ID wird vom SafetyDesigner automatisch vergeben (innerhalb des im Projekt eingestellten Bereichs für die Connection IDs). Die Prüfung der Eindeutigkeit kann vom SafetyDesigner nur innerhalb eines Projekts übernommen werden. Die Eindeutigkeit innerhalb aller Safety-Applikationen muss vom Anwender geprüft werden.

Vorteile des Connection ID Vergabeservice:

- Beim Vergabeservice braucht sich der Anwender nicht um die Eindeutigkeit der Connection IDs zu kümmern (wird vom Vergabeservice übernommen).

- Beim Vergabeservice können auf der lesenden Seite identische Applikationen verwendet werden, da keine eindeutige Connection ID eingestellt werden muss. Beispiel für einen solchen Aufbau, siehe folgendes Bild:

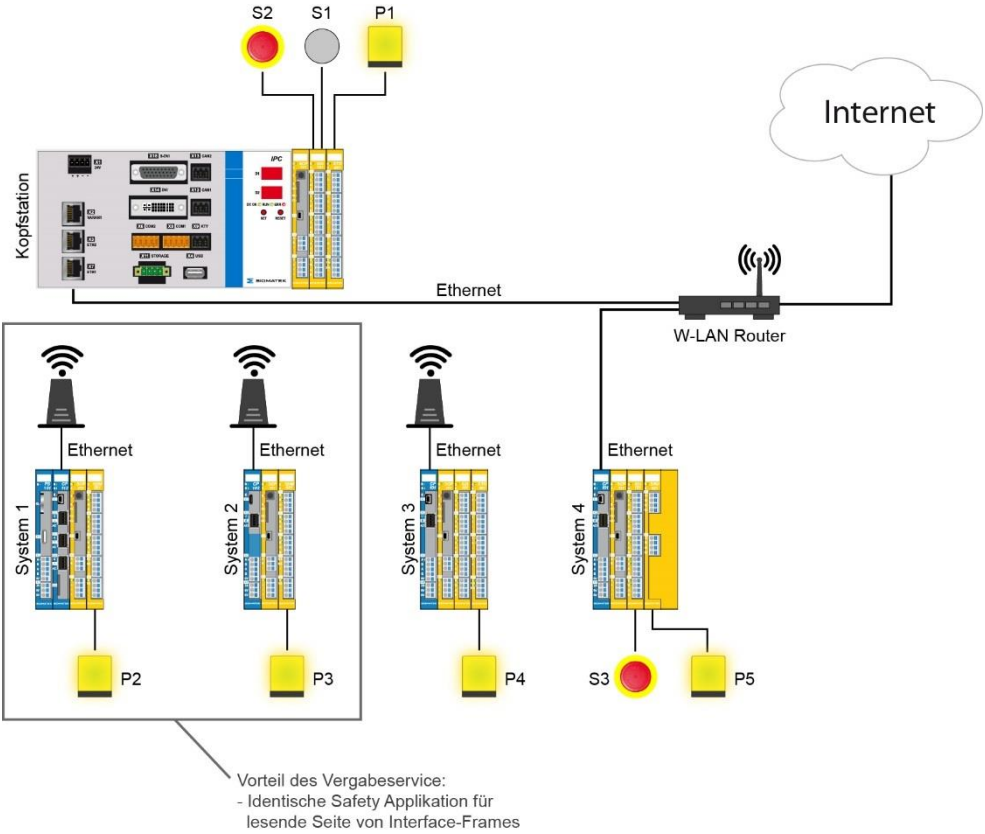


Bild 73 Connection ID Vergabeservice

7.8 Kompatibilität der S-DIAS-Sicherheitsmodule

Nachfolgende Tabelle zeigt den Zusammenhang, der zwischen der jeweiligen Software- und Firmware-Version und den einzelnen Sicherheitsmodulen bestehen muss, damit diese lauffähig sind (beispielsweise ist das Mischmodul SDM 081 unter Version V334 nicht, wohl aber unter V340, lauffähig).

SCP 211 FW Version	**SCP 111 FW-Version**	**SCP 011 FW-Version**	**Module**											**Safety-Designer Build**
			SDI 101	SDM 081	SRO 021	STO 081	SSI 021*	SIB 061	SNC 021	SCP 011	SCP 111**	SRO 022	SAI 041	
		V334												ab 1156
		V340												ab 1187
		V344												ab 1239
		V346												ab 1239
		V352												ab 1446
		V355												ab 1446
		V360												ab 1446
		V367												ab 1446
		V368												ab 1724
		V369												ab 1748
		V370												ab 1767
		V371												ab 1827
		V372												ab 2058
		V374												ab 2058
		V377												ab 2320
	V423													ab 1353
	V429													ab 1353
	V431													ab 1502
	V435													ab 1584
	V443													ab 1616
	V444													ab 1658
	V445													ab 1724
	V446													ab 1748
	V447													ab 1767
	V448													ab 1827
	V449													ab 2058
	V453													ab 2231
	V458													ab 2320
V505	V465													xxxx

Tabelle 21: Kompatibilität der S-DIAS-Sicherheitsbauteile

***SSI 021 erst ab V344 voll kompatibel**

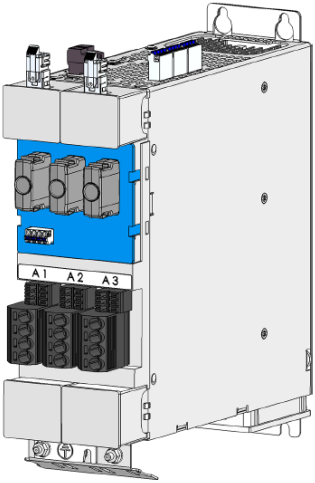
SSI 021 bis V344: kompatibel mit folgenden Einschränkungen:
Im SSI-Absolutwertgeber-Modul SSI 021 entstehen sichere analoge Werte (Variablen vom Typ SAFEDINT). Üblicherweise werden diese SAFEDINT-Werte lokal an jener Safety-CPU verarbeitet, an der das SSI 021-Modul angeschlossen ist. Wenn sichere analoge Werte (Variablen vom Typ SAFEDINT) an eine andere Safety-CPU transferiert und dort weiterverarbeitet werden, muss ZWINGEND eine SCP 011 ab Firmwarestand V344 eingesetzt werden. Die Übertragung von SAFEDINT-Variablen findet statt, wenn bei zwei oder mehreren Safety-CPUs in einem Projekt SAFEDINT-Werte in Netzwerken der entfernten Safety-CPU platziert werden, oder aber bei Verwendung von SAFEDINT-Werten in Interface-Frames (Sichere Variablen).

****Bei der SCP 111 werden die sicheren Prozessdaten mit einem eigenen Sicherheitsprotokoll übertragen (FSoE), daher können die SCP 111, SCP 111-S und SCP 211 nicht zusammen mit einer CSCP 011/012, SCP 010/011 in einem Safety-Projekt verwendet werden.**

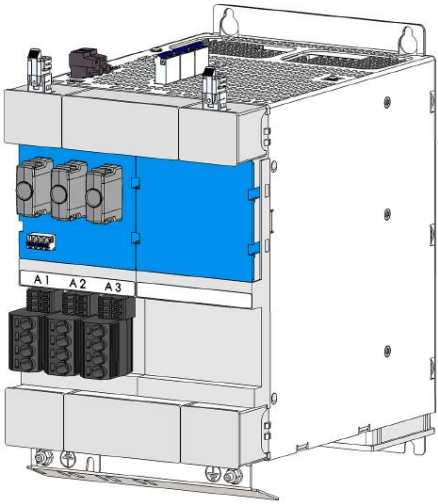
8 MDD 2000 (DIAS DRIVE 2000)

Allgemeine Beschreibung

Die DIAS- Drive 2000 Serie beinhaltet Netz- /Achsmodule und Achsmodule für eine Netzeingangsspannung von 400/480 V AC. Das System ist derzeit in 2 verschiedenen Baugrößen erhältlich. Im nachfolgenden Dokument werden die Geräte der MDP/MDD 21XX Serie als „Baugröße 1“, Geräte der MDP/MDD 22XX Serie als „Baugröße 2“ bezeichnet. In den Netz-/Achsmodulen (MDP) sowie in den Achsmodulen (MDD) sind bis zu 3 Servoverstärker integriert. Mit einem Netz-/Achsmodul können mehrere Achsmodule versorgt werden.
Das DIAS-Drive 2000 ist ein komplettes Servoantriebssystem, kleiner bis mittlerer Leistung, welches auch für Anwendungen mit hoher Regelgüte eingesetzt werden kann. Es ist vollständig in die Entwicklungsumgebung LASAL integriert. Das Netz- /Achsmodul und die Achsmodule werden direkt an der Schaltschrankwand montiert. Es ist keine Montageplatte erforderlich.
Die Strom-, Drehzahl- und Positionsregelung arbeitet mit einer Zykluszeit von 62,5 µs. DIAS-Drive 2000 hat eine hohe Flexibilität bei der Anbindung an verschiedene Rückführungssysteme. VARAN verbindet das Antriebssystem mit der Maschinensteuerung.



Baugröße 1



Baugröße 2

8.2.1 Bestimmungsgemäße Verwendung

Die Power Drive Systeme (PDS) der Serie DIAS-Drive 2000 sind ausschließlich für den Einsatz im Schaltschrank mit den Netz-/Achsmodulen derselben Serie bestimmt. Zusammen werden sie als Komponenten in elektrische Anlagen und Maschinen eingebaut und dürfen nur dort betrieben werden. Die Sicherheitsfunktionen sind für den Einsatz in sicherheitsgerichteten Anwendungen (Funktionale Sicherheit) bestimmt und erfüllen alle notwendigen Anforderungen für einen sicheren Betrieb gemäß EN 62061, EN ISO 13849-1/2 und EN 61800-5-2. Die erreichten Sicherheitsintegritätslevel (SIL), Performancelevel (PL) unterscheiden sich je nach Typ der verwendeten Geber, Verwendung der sicheren Eingänge mit/ohne Taktausgang zur Querschlusserkennung, einkanalig oder zweikanalig, usw.
Bitte beachten Sie dazu die jeweilige EG-Baumusterprüfbescheinigungen (TÜV-Zertifikat).

8.2.2 Systemvoraussetzungen

Die Verwendung des MDD2000 benötigt mindestens folgende Systemvoraussetzungen:
Salamander OS: 09.01.140 oder höher
Hardwareklassenversion: 1.0 oder höher
Motion-Version: 1.0 oder höher
SafetyDesigner-Version: 01.01.070 oder höher

Der DIAS-Drive 2000 kann nur mit einer funktionalen SPS (z.B. CP 112) mit einem Betriebssystem Salamander betrieben werden.

8.2.3 Geber

Als sicher Geber werden Hiperface DSL Safety Geber (z.B. EKS36, EKM36) unterstützt. Die Auflösung der Geber ist maximal 32 Bit Singleturn und maximal 32 Bit Multiturn.
Die Sicherheitsfunktionen sind nur in Kombination mit Hiperface DSL Safety Gebern verfügbar.

8.2.4 Sicherheitsfunktionen

Der MDD2000 verfügt über folgende Sicherheitsfunktionen.

Stopp-Funktionen	
STO	Safe Torque Off
SS1	Safe Stop 1
SS2	Safe Stop 2
SOS	Safe Operating Stop
SBC	Safe Brake Control
SBT	Safe Break Test
Begrenzungsfunktionen	
SLS	Safely-limited Speed
SLP	Safely-limited Position
SLA	Safely-limited Acceleration
SLI	Safely-limited Increment
SDI	Safe Direction
Überwachungsfunktionen	
SMS	Safe Maximum Speed
SMA	Safe Maximum Acceleration
SSM	Safe Speed Monitor
SCA	Safe CAM
Restart & Error Acknowledge	
Restart Acknowledge	Starten des Drives nach Stoppfunktion
Error Acknowledge	Quittieren eines Fehlers

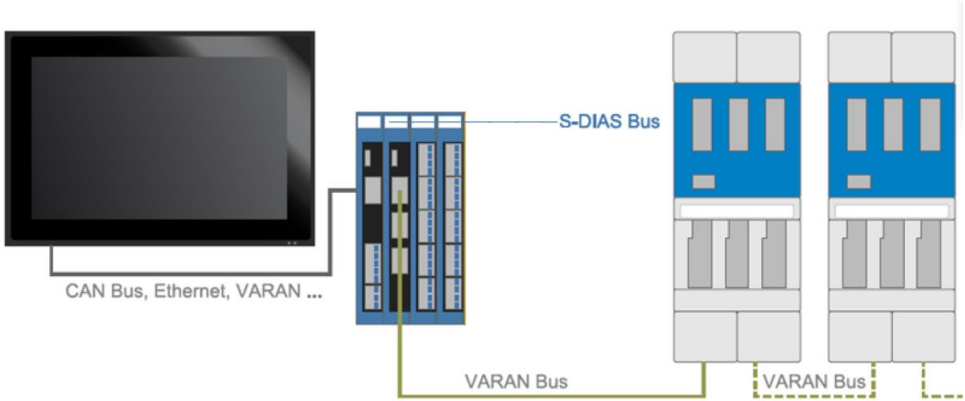
Die Parametrierung der Sicherheitsfunktionen erfolgt im SafetyDesigner. Die Beschreibung der Sicherheitsfunktionen sowie der einzelnen Parameter der Sicherheitsfunktion ist in der Hilfe des SafetyDesigner zu finden.

8.2.5 Funktionsgerichtete Regelung des Drives

Die funktionsgerichtete Regelung des Drives und der Achsen erfolgt über eine LasalClass2 Applikation. Der Anwender kann die Applikation im LasalClass2 erstellen. Die Firma Sigmatek unterstützt den Anwender durch bereits vorgefertigte Hardwareklassen und Libraries (z.B. Motion Library). Die Grundeinstellungen des Drives sind ebenfalls in der Entwicklungsumgebung LasalClass2 integriert. Der Bereich DiasDrive in LasalClass2 beschäftigt sich mit der Konfiguration und Abstimmung von Drive-Hardwaremodulen, die mittels VARAN-Bus in ein Steuerungssystem eingebunden sind, bis hin zur Einbindung von Drive-Informationen in eine LasalClass2– Applikation. Die Beschreibung zur Erstellung einer Applikation sind in der Dokumentation der Entwicklungsumgebung LasalClass2 zu finden, sowie in den Dokumentationen der Hardwareklassen und Libraries.

8.2.6 Standalone Betrieb

Der MDD2000 kann im Standalone-Betrieb verwendet werden.



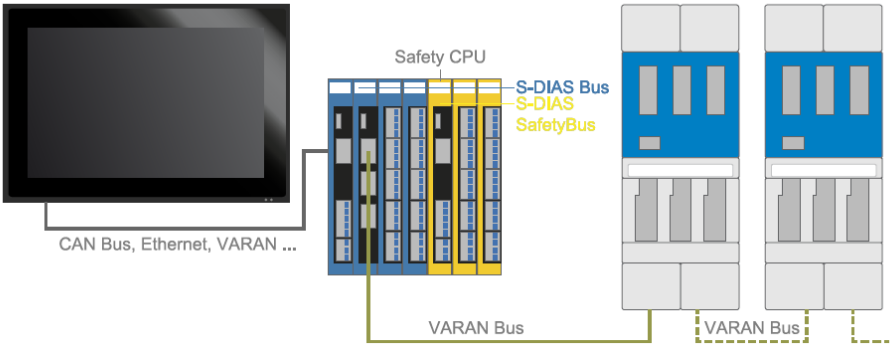
Beispiel Standalone

Die Sicherheitsfunktionen des Drives werden hier über die 4 sicheren Eingänge des Drives aktiviert. Die Einstellung des Mappings können entweder einkanalig oder zweikanalig erfolgen. Die Einstellung des Mappings wird über den SafetyDesigner vorgenommen. Die Parametrierung der Sicherheitsfunktionen erfolgt ebenfalls im SafetyDesigner. Die erstellte Konfiguration kann über eine SPS (z.B. CP112) durch den SafetyDesigner auf den Drive gespielt werden. Die Beschreibung ist in der Hilfe des SafetyDesigner zu finden.

Einkanaliges und zweikanaliges Input-Mapping darf und kann nicht gemeinsam verwendet werden.
Alle Achsen eines MDD2000 können nur mit der gleichen Art des Input-Mappings betrieben werden.

8.2.7 Betrieb mit einer Safety-CPU

Der MDD 2000 kann zusammen mit einer Safety-CPU (z.B. SCP111) verwendet werden.



Beispiel Gesamtübersicht

Die Kommunikation zwischen Drive und Safety-CPU erfolgt mittels FSoE. Die Sicherheitsfunktionen des Drives werden hier über sichere Ausgänge der Achsen aktiviert. Die Ausgänge (z.B. Safe_Funktion1 bei den Achsen) werden mittels FSoE-Kommunikation an den Drive übertragen. Die Einstellung des Mappings wird über den SafetyDesigner vorgenommen. Die Parametrierung der Sicherheitsfunktionen erfolgt ebenfalls im SafetyDesigner. Die erstellte Konfiguration wird über die Safety-CPU auf den Drive übertragen. Der SafetyDesigner spielt dazu die Konfiguration auf die verwendete Safety-CPU. Die Beschreibung ist in der Hilfe des SafetyDesigner zu finden.

Eine Mischung der Aktivierung der Sicherheitsfunktionen zwischen sicheren Eingängen und der Verwendung einer Safety-CPU ist nicht möglich.

8.2.8 Verifizierung der Geber

Es ist nötig die Geber auf den 3 Achsen zu verifizieren. Bis zum Abschluss der Verifizierung läuft der Drive nur in einem temporären Operational Mode. Diese Einstellung ist zeitlich begrenzt. Die Zeit kann im SafetyDesigner eingestellt werden (5min-480min). Die Einstellung wird im PropertyBrowser bei „Temporary Operation Time in Minutes“ vorgenommen.

Properties

Name	DriveStandalone
Comment	
Filename	D:\Temp\2023\0727\DriveStandalone\Driv
Temporary Operation Time in Minutes	60
Ranges of Slave Address	1,1000
Ranges of Connection ID's	1,1000
Easy Instance	false
Revision Documentation	0.0
Save in XML-File	false
Write additional CRC	true

Nach dem Ablauf der eingestellten Zeit fällt der Drive in einen Fehler und muss neu gestartet werden.

Während des temporären Operational Mode kann der Drive nur mit einer eingeschränkten Geschwindigkeit betrieben werden. Die Geschwindigkeit muss bei den Achsen des Drives eingestellt werden.

⊟ General Settings	
Max. Position Age	1
Max. Speed in Temp. Mode	0
Velocity Filter Time	5

Während des temporären Operational Mode werden die Monitoring Funktionen (z.B. SMS) nicht ausgeführt.

.

Ablauf der Verifizierung

Die Verifizierung wird aus der funktionalen Applikation angestoßen. Die Firma Sigmatek stellt hierfür bereits vorgefertigte Bausteine (z.B. Klasse MDD2000_Axis) zur Verfügung. Der vorgegebene Ablauf muss eingehalten werden. Genaueres siehe Dokumentation der Klassen und Motion-Library.

Baustein zum Verifizieren der Achsen

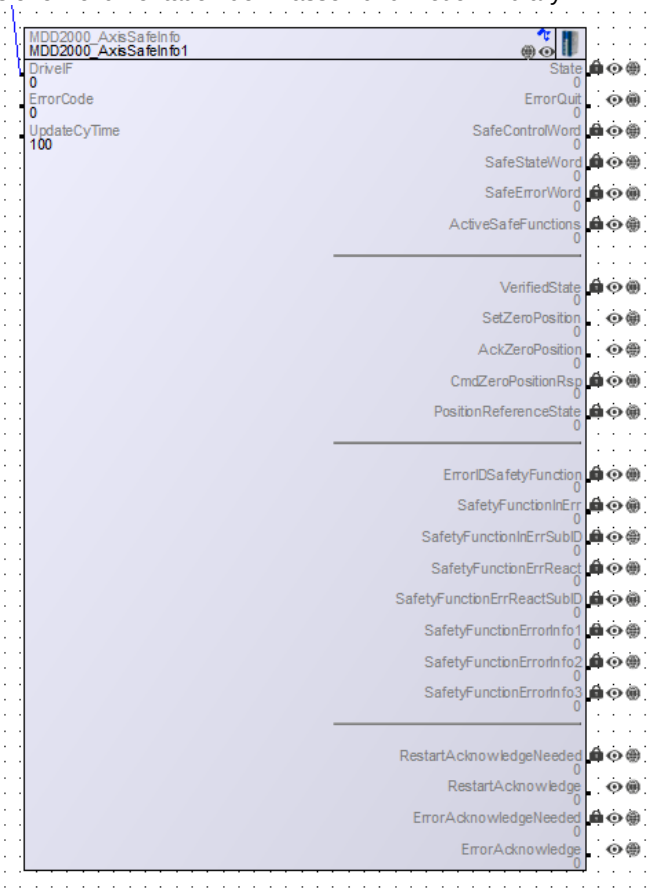
Ablauf:

- Drive läuft im Temporären Operational Mode
- Reset der Verifizierung (falls ein Geber bereits validiert ist)
- Verifizierung Achse 1
- Verifizierung Achse 2
- Verifizierung Achse 3
- Drive in den SERVICE-MODE setzten
- Finalisierung der Verifizierung
- Drive Starten
- Drive läuft im Operational Mode

Der Drive speichert nach der Verifizierung die Seriennummer der einzelnen Geber. Zusätzlich wird im Geber eine ID hinterlegt. Der Drive prüft die Seriennummer und die ID regelmäßig, um einen Tausch der Geber zu erkennen.

8.2.9 Referenzierung der Absolut-Position

Für die Sicherheitsfunktion SLP (Safe Limited Position) wird eine Absolut-Positon der Geber benötigt. Zur Bestimmung der Absolut-Position muss eine Referenzfahrt der Motoren durchgeführt werden. Die Referenzierung wird aus der funktionalen Applikation angestoßen. Die Firma SIGMATEK stellt hierfür bereits vorgefertigte Bausteine (z.B. Klasse MDD2000_AxisSafeInfo) zur Verfügung. Der vorgegebene Ablauf muss eingehalten werden. Genaueres siehe Dokumentation der Klassen und Motion-Library.



Baustein zur Referenzierung der Achse

Im SafetyDesigner müssen zusätzlich Parameter bei den Achsen eingestellt werden, die Vorgaben für die Referenzierung liefern.

⊟ Position Reference	
Min. Position Change	0
Position tolerance	0

Ablauf der Referenzierung:

- Anfahren der Nullposition
- Setzen der Nullposition
- Verfahren der Achse um den eingestellten Wert (Min. Position Change)
- Anfahren der Nullposition, Wert muss im eingestellten Toleranzfenster sein (Position tolerance)
- Finalisieren der Referenzierung
- Starten des Drives

Eine nicht durchgeführte Referenzierung bzw. eine falsch durchgeführte Referenzierung kann zu Schäden an der Maschine führen

8.2.10 Ablauf der Inbetriebnahme eines Drives im Standalone-Betrieb (ohne Safety-CPU)

Bei der Inbetriebnahme des Drives mit Sicherheitsfunktionalität sind bestimmte Abläufe zu befolgen.
Der Drive muss sowohl funktional als auch safety-technisch konfiguriert werden. Die funktionale Konfiguration erfolgt über die Entwicklungsumgebung LaslClass2. Die Sicherheitskonfiguration erfolgt über den SafetyDesigner. Nach der Konfiguration des Drives müssen die Geber, die Konfigurationen und die Maschine auf Funktion getestet werden. Nach diesem Ablauf kann die Verifizierung der Geber und Drives durchgeführt werden. Die Schritte sind zu dokumentieren. Im Protokoll sollen mindestens der Name des Ausführenden, das Datum und die durchgeführten Schritte, aufgelistet sein.

Arbeitsschritte funktionsgerichtet

- Erstellen der Applikation für den Drive in LasalClass2
- Erstellen der Drivekonfiguration (z.B. Reglerparamter) in LasalClass2
- Einspielen der Daten über das Tool LasalClass2 auf die Steuerung

Arbeitsschritte Safety
- Erstellen der Konfiguration im SafetyDesigner
- Einspielen der Daten auf den Drive (über SafetyDesigner)

Inbetriebnahme

- Starten des Drives (läuft im temporären Operational Mode)
- Testen der Geber auf Funktionsfähigkeit
- Referenzierung der Absolut-Position (wenn nötig)
- Testen der funktionsgerichteten Applikation
- Testen der sicherheitsgerichteten Applikation und Maschine
- Verifizieren der Geber
- Drive läuft im Operational Mode

8.2.11 Ablauf der Inbetriebnahme eines Drives mit einer Safety-CPU

Bei der Inbetriebnahme des Drives mit Sicherheitsfunktionalität sind bestimmte Abläufe zu befolgen.
Der Drive muss sowohl funktional als auch safety-technisch konfiguriert werden. Die funktionale Konfiguration erfolgt über die Entwicklungsumgebung LaslClass2. Die Sicherheitskonfiguration erfolgt über den SafetyDesigner. Nach der Konfiguration des Drives müssen die Geber, die Konfigurationen, die Safety-CPU und die Maschine auf Funktion getestet werden. Nach diesem Ablauf kann die Verifizierung der Geber, des Drives und der Safety-CPU durchgeführt werden. Die Schritte sind zu dokumentieren. Im Protokoll sollen mindestens der Name des Ausführenden, das Datum und die durchgeführten Schritte, aufgelistet sein.
Die Inbetriebnahme der Sicherheitsseite ist in zwei Schritten zu sehen. Zuerst wird die Safety-CPU bespielt. Die Konfiguration der Safety-CPU enthält die Daten für den Drive. Der Mechanismus ist der gleiche wie bei zwei Safety-CPUs. Die Safety-CPU fungiert als „Sigmatek-Master“ und der Drive als „Sigmatek Slave“. Die Safety-CPU baut nach dem Start eine Verbindung zum Drive auf. Die Safety-CPU sendet die Konfiguration zum Drive. Danach ist der Drive als konfiguriert zu sehen und kann verifiziert und referenziert werden (Auslösung aus Applikation über den funktionalen FW-Teil, definierte Vorgehensweise). Der Drive läuft bis zum Abschluss der Verifikation/Referenzierung im temp. OP-Mode. Nach der Verifikation/Referenzierung läuft der Drive im OP-Mode.

Die Safety-CPU baut eine FSoE-Verbindung zum Drive auf und läuft ab diesem Moment im temp. OP-Mode. Die Daten können ausgetauscht werden. Die Safety-CPU muss durch den Anwender validiert werden und läuft danach im OP-Mode. Dies darf erst erfolgen, nachdem der Drive verifiziert wurde.

Arbeitsschritte funktionsgerichtet

- Erstellen der Applikation für den Drive in LasalClass2
- Erstellen der Drivekonfiguration (z.B. Reglerparamter) in LasalClass2
- Einspielen der Daten über das Tool LasalClass2 auf die Steuerung

Arbeitsschritte Safety

- Erstellen der Konfiguration mit einem Drive und einer Safety-CPU im SafetyDesigner
- Einspielen der Daten auf die Safety-CPU (über SafetyDesigner)

Inbetriebnahme

- Starten des Systems (Lasal Applikation muss korrekt laufen, Safety-CPU starten)
- Aufbau der Verbindung zwischen Safety-CPU und Drive
- Safety-CPU prüft CRC der Konfiguration am Drive
- Verteilen der Konfiguration auf den Drive, wenn CRC auf Drive und Safety-CPU nicht zusammenpassen
- Starten des Drives (läuft im temporären Operational Mode)
- Testen der Geber auf Funktionsfähigkeit
- Referenzierung der Absolut-Position (wenn nötig)
- Testen der funktionalen Applikation
- Testen der Sicherheits-Applikation
- Testen der Maschine
- Verifizieren der Geber
- Verifizieren der Safety-CPU

8.2.12 Ablauf Gebertausch

Beim Tausch des Gebers muss der Drive in den SERVICE-Mode gesetzt werden, wird dies nicht gemacht generiert der Drive einen Fehler beim Abstecken eines Gebers.

Der Safety-Teil des Drives erkennt den Gebertausch (wenn Geber-ID/Seriennummer am Drive nicht stimmen). Es wird hier die Seriennummer des Gebers geprüft und ein Hinweis an den Anwender gegeben.

Fall mit Safety-CPU

Der Gebertausch wird von der Safety-CPU nicht erkannt, somit kann die Safety-CPU nicht reagieren. Es wird von der Safety-CPU erkannt, dass die Verbindung zum Drive abbricht, da der Drive im SERVICE-Mode ist. Der FSoE-Watchdog ist abgelaufen. Bei optionalen Drives wird in der Safety-CPU ein Errors of channels generiert, sonst ein Fehler. Die SCP bleibt immer im Operational-Mode. Die Safety-CPU generiert eine Meldung, wenn die FSoE-Verbindung ausfällt.

Der Drive muss nach dem Gebertausch neu in Betrieb genommen werden. Es müssen alle Geber neu verifiziert werden. Der Anwender ist hier verpflichtet den Drive neu zu verifizieren. War der getauschte Geber referenziert, muss dies wieder durchgeführt werden. Diese Schritte sind zu dokumentieren. Im Protokoll sollen mindestens der Name des Ausführenden, das Datum und die durchgeführten Schritte, aufgelistet sein.

Ablauf

- Drive in den SERVICE-Mode setzten
- Geber austauschen
- Reset der Verifizierung der Geber durchführen
- Starten des Drives (läuft im temporären Operational Mode)
- Testen des Gebers auf Funktionsfähigkeit
- Referenzierung der Absolut-Position (wenn nötig)
- Testen der funktionalen Applikation
- Testen der Sicherheits-Applikation
- Testen der Maschine
- Verifizierung der Geber

8.2.13 Ablauf Tausch eines Drives

Beim Tausch des Drives, muss zwischen der Verwendung als Standalone und der Verwendung mit eine Safety-CPU unterschieden werden.
Bei der Verwendung im Standalone-Betrieb ist eine komplette Inbetriebnahme wie in Kapitel 8.2.11 durchzuführen.
Bei der Verwendung mit einer Safety-CPU ist der Ablauf anders als bei der Erstinbetriebnahme.
Die Safety-CPU kann beim Starten feststellen, dass der Drive mit der Sicherheitsnummer nicht mehr im System vorhanden ist (Sicherheitsnummer in Safety-CPU gespeichert). Die Safety-CPU generiert eine Fehlermeldung, bzw. wenn der Drive optional ist, läuft die Safety-CPU weiter im Operational Mode und generiert einen Error of Channels. Im SafetyDesigner kann der Fehler ausgelesen werden. Der Anwender muss nun einen RESCAN am System auslösen (Befehl aus SafetyDesigner), damit die Safety-CPU die Sicherheitsnummer des neuen Drives auslesen kann. Die Safety-CPU fällt in den temp. Operational Mode zurück.

Es muss der Ablauf der Inbetriebnahme erneut durchgeführt werden (Drive verifizieren und referenzieren; Safety-CPU validieren)

Der Anwender ist verpflichtet den Drive neu zu verifizieren. Dies muss in einem Protokoll festgehalten werden.

Die Safety-CPU muss validiert werden. Dies darf erst erfolgen, nachdem der Drive verifiziert wurde.

Ablauf:

- Safety-CPU stellt anderen Drive fest (über Sicherheitsnummer des Drives)
- Safety-CPU generiert einen Fehler bzw, einen Error of Channels
- RESCAN-Befehl an der Safety-CPU auslösen (z.B. über SafetyDesigner)
- Safety-CPU erkennt neuen Drive und verteilt die Konfiguration
- Starten des Drives (läuft im temporären Operational Mode)
- Testen der Geber auf Funktionsfähigkeit
- Referenzierung der Absolut-Position (wenn nötig)
- Testen der funktionsgerichteten Applikation
- Testen der sicherheitsgerichteten Applikation und Maschine
- Verifizieren der Geber
- Validieren der Safety-CPU

8.2.14 Ablauf Tausch einer Safety-CPU

Der Ablauf auf der Safety-CPU ist wie bei einer Erstinbetriebnahme zu sehen.

Die Safety-CPU prüft die CRC der Konfiguration am Drive und überträgt bei Unterschieden die Konfiguration zum Drive.

Der Drive muss bei geänderter Konfiguration neu verifiziert /referenziert werden, sonst nicht. Dies muss in einem Protokoll festgehalten werden.

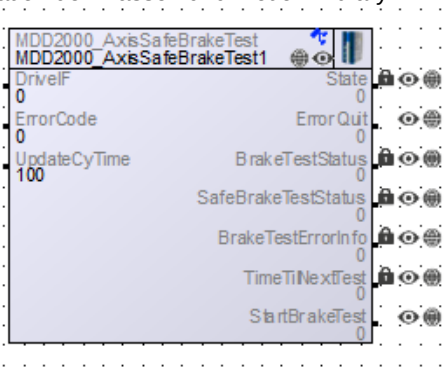
Die Safety-CPU muss validiert werden.

Ablauf

- Einspielen der Daten auf die Safety-CPU (über SafetyDesigner)
- Aufbau der Verbindung zwischen Safety-CPU und Drive
- Safety-CPU prüft CRC der Konfiguration am Drive
- Verteilen der Konfiguration auf den Drive, wenn CRC auf Drive und Safety-CPU nicht zusammenpassen
- Starten des Drives (läuft im temporären Operational Mode, wenn Drive neu konfiguriert wurde)
- Testen der Geber auf Funktionsfähigkeit
- Referenzierung der Absolut-Position (wenn neu konfiguriert wurde)
- Testen der funktionalen Applikation
- Testen der Sicherheits-Applikation
- Testen der Maschine
- Verifizieren der Geber (wenn neu konfiguriert wurde)
- Validieren der Safety-CPU

8.2.15 Bremsentest

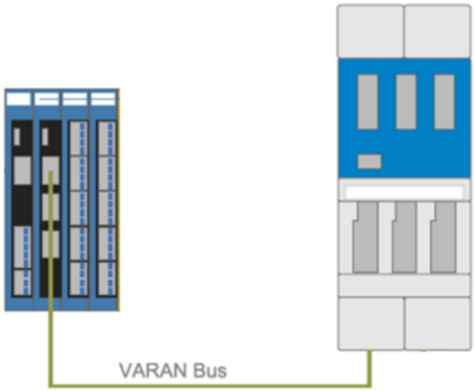
Bei der Verwendung einer Bremse ist diese regelmäßig zu testen.
Es gibt dazu die Funktion SBT (Safe Brake Test). Die Funktion kann nicht als reine Sicherheitsfunktion gesehen werden. Die Funktion kann im SafetyDesigner parametriert werden. Siehe dazu Dokumentation im SafetyDesigner.
Der Test der Bremse wird aus der funktionalen Applikation aufgerufen. Die Firma SIGMATEK stellt hierfür bereits vorgefertigte Bausteine (z.B. Klasse MDD2000_AxisSafeBrakeTest) zur Verfügung. Der vorgegebene Ablauf muss eingehalten werden. Genaueres siehe Dokumentation der Klassen und Motion-Library.



Baustein für Bremsentest

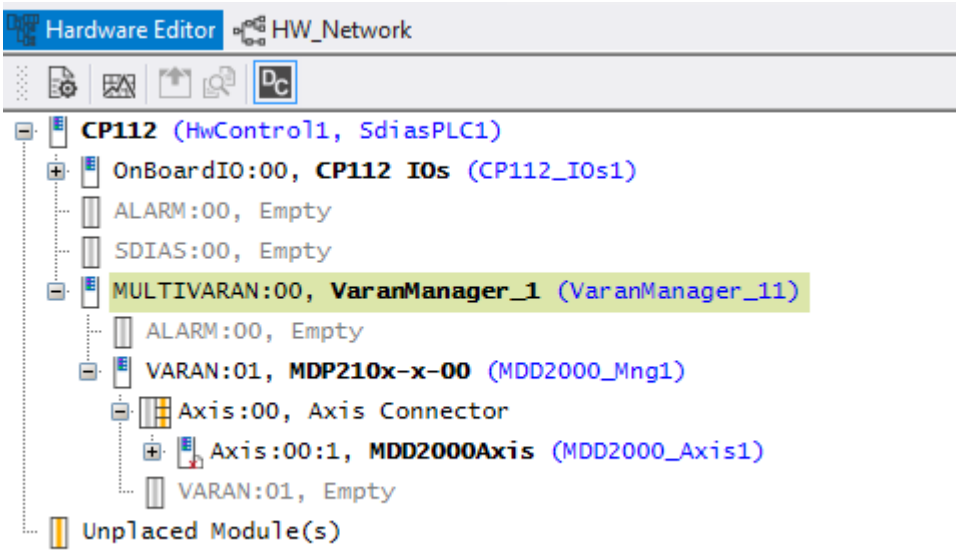
8.2.16 Beispiel zur Erstellung einer Konfiguration im Standalone-Betrieb

Als Beispiel wir ein einfacher Aufbau mit einer CPU und einem Drive erklärt.

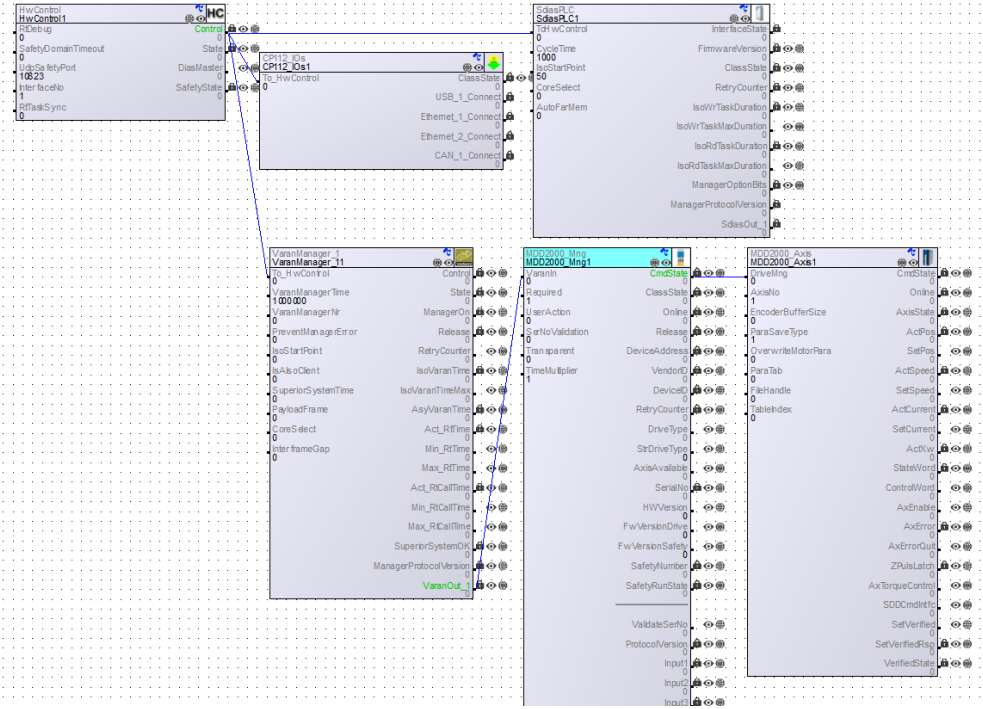


Es wird hierfür eine Applikation in der Einwicklungsumgebung LasalClass2 erstellt. Die Applikation enthält den Hardwareaufbau und die vom Anwender benötigte Funktionalität zum Bedienen des funktionalen Bereichs des Drives.

Aufbau des HW-Trees:

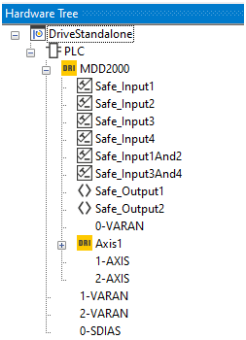


Aufbau des Hardware-Netzwerkes:



Im SafetyDesigner muss die Konfiguration des Drives aus Safety-Sicht erstellt werden. Hierzu muss ein Projekt mit dem entsprechend Hardware-Baum und der Parametrierung der Achsen mit den Sicherheitsfunktionen erfolgen.

Aufbau des HW-Trees:



Nach der Erstellung des Hardware-Aufbaus kann mit der Parametrierung der Achsen begonnen werden. Hier müssen zuerst die allg. Einstellungen für den Geber durchgeführt werden. Dies sind zum Beispiel, welcher Geber-Typ wird verwendet, welche Auflösungen hat der Geber, und welche Geschwindigkeit ist, im temp. Operational Mode, maximal erlaubt.

Allgemeine Einstellungen

⊟ Axis Configuration	
Encoder Type	HIPERFACE DSL
Material Number	0
⊟ Encoder Configuration	
Encoder Resolution1	18
Encoder Resolution2	9
Rotations	1
Position Difference	2
⊟ General Settings	
Max. Position Age	1
Max. Speed in Temp. Mode	20
Velocity Filter Time	5
⊞ Position Reference	
⊞ Position Conversion	

Zusätzlich kann festgelegt werden welche Einheiten verwendet werden sollen.

Einheiten:

⊟ UNIT	
Time unit	ms
Position unit	inc
Velocity unit	rev/min
Acceleration unit	Velocity_unit/s
Current unit	mA

Nach den allgemeinen Einstellungen können die Sicherheitsfunktionen parametriert werden. Dies kann entweder im Property Browser oder View durchgeführt werden.

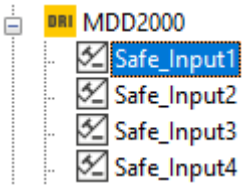
Selected Axis: 0: Axis1 Selected Function: Safely-limited Speed

STO SS1 SS2 SOS SBC SBT SLS SLP SLA SLI SDI SMS SMP SMA SSM SCA Mapping

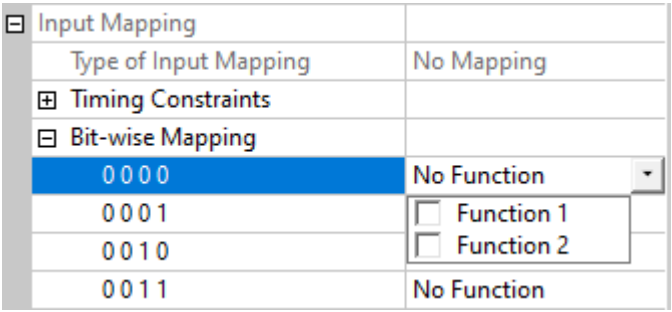
	SLS_1	SLS_2	SLS_3	SLS_4	SLS_5	SLS_6	SLS_7	SLS_8	Units
Time Velocity	25	0	0	0	0	0	0	0	ms
Upper Limit	0	0	0	0	0	0	0	0	rev/min
Lower Limit	0	0	0	0	0	0	0	0	rev/min
Time Velocity Limit	0	0	0	0	0	0	0	0	ms
Time Deceleration	0	0	0	0	0	0	0	0	ms
Deceleration Limit	0	0	0	0	0	0	0	0	rev/min/s
Error Reaction	STO	STO	STO	STO	STO	STO	STO	STO	
Function Mapping									
Status Word									

SLS time for velocity monitoring

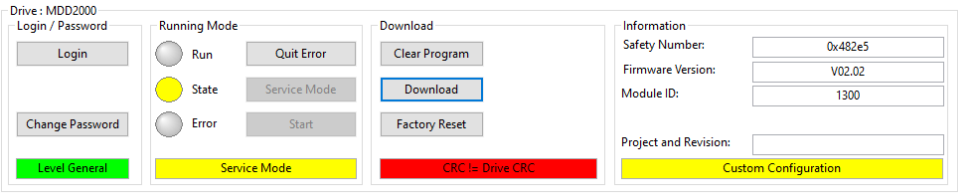
Es können hier für die einzelnen Funktionen die Parameter eingestellt werden. Es wird für jeden Parameter ein kurzer Hilfetext angezeigt. Die eingegebenen Werte werden automatisch auf Gültigkeit geprüft.
Es stehen am Drive pro Achse 16 Funktionen für die Abarbeitung zu Verfügung. Die Sicherheitsfunktionen können diesen 16 Funktionen (Function Mapping) zugeordnet werden.
Diese 16 Funktionen können über die 4 sicheren Eingänge des Drives ausgelöst werden.

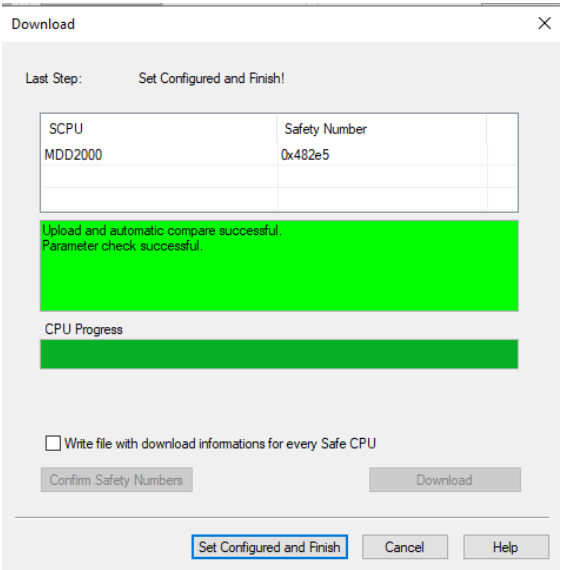


Die Funktionen können entweder einkanalig oder zweikanalig den Eingängen zugeordnet werden. Die Einstellungen können im Property Browser vorgenommen werden.

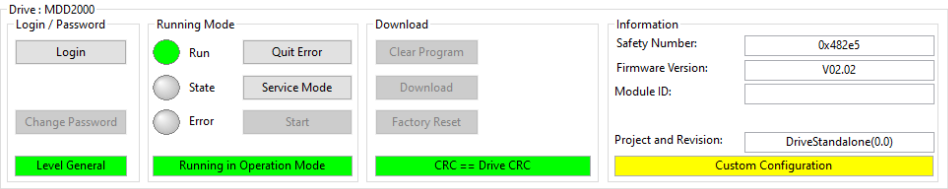


Nach dem Abschluss der Parametrierung kann die Applikation über den Safety-Designer auf den Drive gespielt werden. Die Vorgehensweise ist ähnlich zu einer Safety-CPU. Es erfolgt ein Anmelden am Drive mit einem nachfolgenden Download der Applikation.

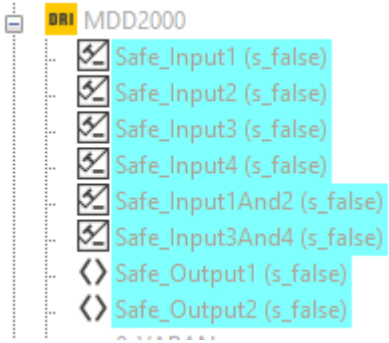




Nach erfolgreichem Download kann der Drive gestartet werden.



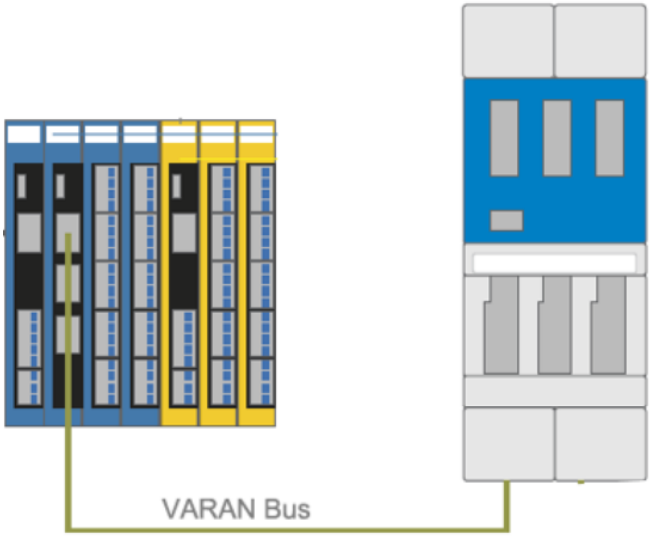
Im Hardware-Baum können nun die Werte der Eingänge angezeigt werden.



Die Geber können nun aus der funktionalen Applikation heraus verifiziert und referenziert werden.
Die Verifizierung der Geber erfolgt über die Instanz der Klasse MDD200_Axis in der funktionsgerichteten Applikation. Der Server 'SetVerified' muss dazu auf 1 gesetzt werden. Am Server 'VerifiedState' ist zu erkennen, ob der Geber verifziert ist.
Die Referenzierung der Absolut-Position erfolgt über die Instanz der Klasse MDD2000_AxisSafeInfo in der funktionsgerichteten Applikation.

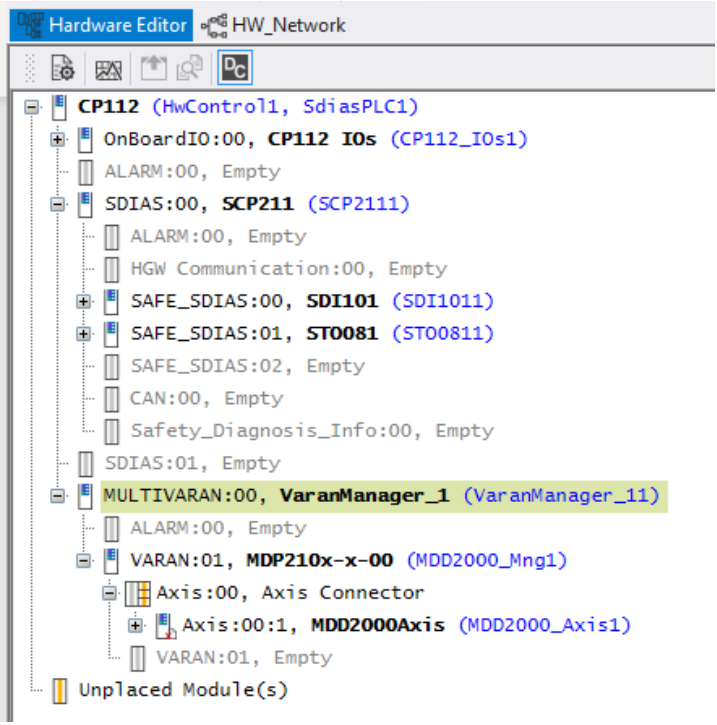
8.2.17 Beispiel zur Erstellung einer Konfiguration zusammen mit einer Safety-CPU

Als Beispiel wir ein einfacher Aufbau mit einer CPU, einer Safety-CPU und einem Drive erklärt.

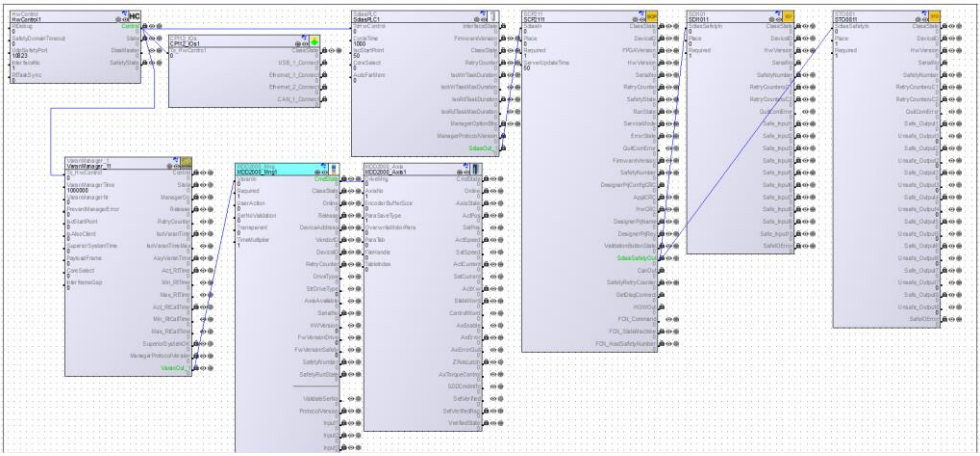


Es wird hierfür eine Applikation in der Einwicklungsumgebung LasalClass2 erstellt. Die Applikation enthält den Hardwareaufbau und die vom Anwender benötigte Funktionalität zum Bedienen des funktionalen Bereichs des Drives.

Aufbau des HW-Trees:

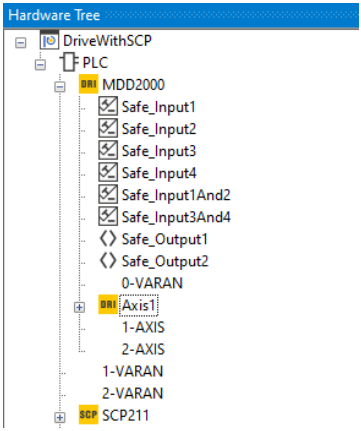

Hardware Editor
HW_Network
CP112 (HwControl1, SdiasPLC1)
OnBoardIO:00, CP112 IOs (CP112_IOs1)
ALARM:00, Empty
SDIAS:00, SCP211 (SCP2111)
ALARM:00, Empty
HGW Communication:00, Empty
SAFE_SDIAS:00, SDI101 (SDI1011)
SAFE_SDIAS:01, STO081 (STO0811)
SAFE_SDIAS:02, Empty
CAN:00, Empty
Safety_Diagnosis_Info:00, Empty
SDIAS:01, Empty
MULTIVARAN:00, VaranManager_1 (VaranManager_11)
ALARM:00, Empty
VARAN:01, MDP210x-x-00 (MDD2000_Mng1)
Axis:00, Axis Connector
Axis:00:1, MDD2000Axis (MDD2000_Axis1)
VARAN:01, Empty
Unplaced Module(s)

Aufbau des Hardware-Netzwerkes:



Im SafetyDesigner muss die Konfiguration des Drives aus Safety-Sicht erstellt werden. Hierzu muss ein Projekt mit dem entsprechend Hardware-Baum und der Parametrierung der Achsen mit den Sicherheitsfunktionen erfolgen.

Aufbau des HW-Trees:



Nach der Erstellung des Hardware-Aufbaus kann mit der Parametrierung der Achsen begonnen werden. Hier müssen zuerst die allg. Einstellungen für den Geber durchgeführt werden. Dies sind zum Beispiel, welcher Geber-Typ wird verwendet, welche Auflösungen hat der Geber, und welche Geschwindigkeit ist, im temp. Operational Mode, maximal erlaubt.
Allgemeine Einstellungen

⊟ Axis Configuration	
Encoder Type	HIPERFACE DSL
Material Number	0
⊟ Encoder Configuration	
Encoder Resolution1	18
Encoder Resolution2	9
Rotations	1
Position Difference	2
⊟ General Settings	
Max. Position Age	1
Max. Speed in Temp. Mode	20
Velocity Filter Time	5
⊞ Position Reference	
⊞ Position Conversion	

Zusätzlich kann festgelegt werden welche Einheiten verwendet werden sollen.

Einheiten:

⊟ UNIT	
Time unit	ms
Position unit	inc
Velocity unit	rev/min
Acceleration unit	Velocity_unit/s
Current unit	mA

Nach den allgemeinen Einstellungen können die Sicherheitsfunktionen parametriert werden. Dies kann entweder im Property Browser oder View durchgeführt werden.

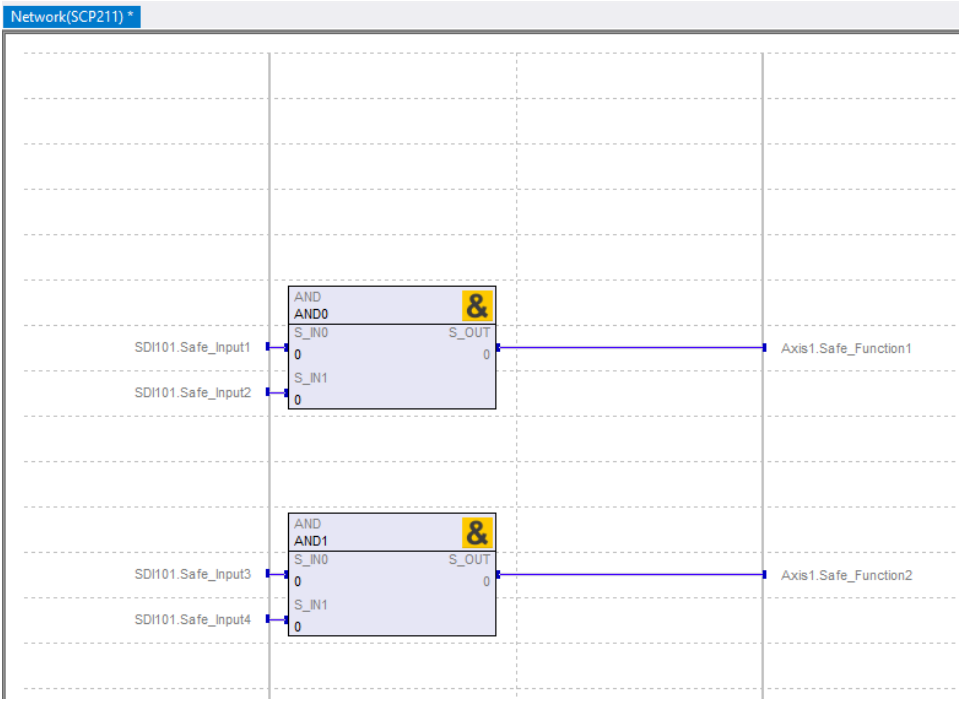
Selected Axis: 0: Axis1 Selected Function: Safely-limited Speed

STO | SS1 | SS2 | SOS | SBC | SBT | SLS | SLP | SLA | SLI | SDI | SMS | SMP | SMA | SSM | SCA | Mapping

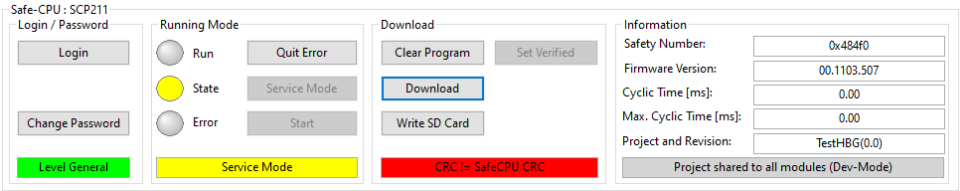
	SLS_1	SLS_2	SLS_3	SLS_4	SLS_5	SLS_6	SLS_7	SLS_8	Units
Time Velocity	25	0	0	0	0	0	0	0	ms
Upper Limit	0	0	0	0	0	0	0	0	rev/min
Lower Limit	0	0	0	0	0	0	0	0	rev/min
Time Velocity Limit	0	0	0	0	0	0	0	0	ms
Time Deceleration	0	0	0	0	0	0	0	0	ms
Deceleration Limit	0	0	0	0	0	0	0	0	rev/min/s
Error Reaction	STO	STO	STO	STO	STO	STO	STO	STO	
Function Mapping									
Status Word									

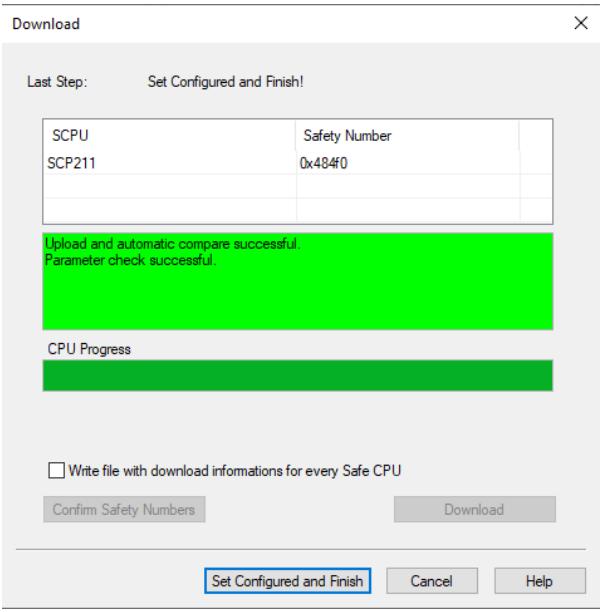
SLS time for velocity monitoring

Es können hier für die einzelnen Funktionen die Parameter eingestellt werden. Es wird für jeden Parameter ein kurzer Hilfetext angezeigt. Die eingegebenen Werte werden automatisch auf Gültigkeit geprüft.
Es stehen am Drive pro Achse 16 Funktionen für die Abarbeitung zu Verfügung. Die Sicherheitsfunktionen können diesen 16 Funktionen (Function Mapping) zugeordnet werden.
Diese 16 Funktionen werden durch Ausgänge bei den Achsen repräsentiert und können in der Safety-CPU aktiviert werden. Die Aktivierung erfolgt über das Platzieren der Ausgänge in einem Netzwerk der Safety-CPU. Die Informationen werden über eine FSoE-Verbindung von der Safety-CPU an den Drive übermittelt.



Nach dem Abschluss der Parametrierung kann die Applikation über den Safety-Designer auf die Safety-CPU gespielt werden. Es erfolgt ein Anmelden an der Safety-CPU mit einem nachfolgenden Download der Applikation





Nach erfolgreichem Download kann die Safety-CPU gestartet werden. Die Applikation wird an den Drive übermittelt. Der Drive kann danach gestartet werden.
Die Geber können nun aus der funktionalen Applikation heraus verifiziert und referenziert werden.
Die Verifizierung der Geber erfolgt über die Instanz der Klasse MDD200_Axis in der funktionsgerichteten Applikation. Der Server 'SetVerified' muss dazu auf 1 gesetzt werden. Am Server 'VerifiedState' ist zu erkennen, ob der Geber verifziert ist.
Die Referenzierung der Absolut-Position erfolgt über die Instanz der Klasse MDD2000_AxisSafeInfo in der funktionsgerichteten Applikation.

9 Wartung und Außerbetriebnahme

9.1 Allgemeines

WICHTIG!
Eine Fernwartung muss auf den Diagnosemodus beschränkt werden.
Das Forcen oder gar der Applikationsdownload ist nur mit organisatorischen Maßnahmen vor Ort erlaubt. Der Anlagenbetreiber muss für diesen Fall die Verbindung von extern explizit über die Firewall (VPN, etc.) erlauben.

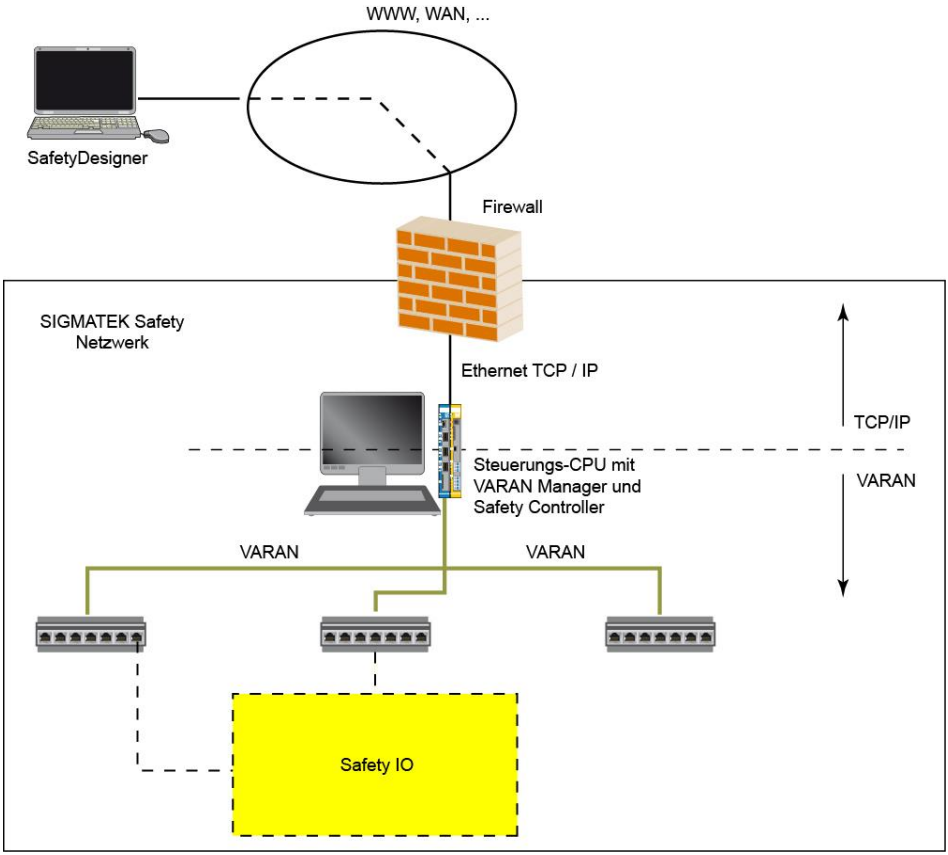


Bild 74: Konzept bei Fernwartung

Da ein technisches Security-Konzept (IT-Sicherheit) immer in der Verantwortung des Netzwerkplaners und Betreibers liegt, wird hierfür nur eine organisatorische Vorgehensweise beschrieben.

9.2 Voraussetzungen

WICHTIG!

1. Die Parametrierung und Programmierung sowie das Debuggen und Forcen ist nur mit dem SafetyDesigner der Firma SIGMATEK erlaubt.
2. Die Kommunikation darf nur über eine Standard-CPU als Gateway zu den Sicherheitskomponenten erfolgen (Ausnahme: SCP 010/SCP 011/SCP 111/SCP 111-S/SCP 211 im Standalone-Betrieb).
3. Ein Netzwerk muss mit einer Firewall, die den zu erwartenden Bedrohungen standhält, geschützt sein.

9.3 Anforderungen an den Netzwerkbetreiber

GEFAHR!

1. Der Netzwerkbetreiber muss sicherstellen, dass von außen keine Kommunikation mit einem parametrierfähigen Werkzeug (z. B. via SafetyDesigner und PC) zu seinem internen Netzwerk möglich ist. Dieses wird in der Regel durch die Firewall gewährleistet.
2. Eine Verbindung darf nur dann aufgebaut werden, wenn der Netzwerkadministrator explizit eine bestimmte IP-Adresse (für das gewünschten Konfigurationstool) freischaltet. Eine Freischaltung setzt einen zusätzlichen direkten Kontakt (z. B. Telefon) zwischen einer Serviceperson vor Ort und dem Telearbeitsplatz voraus.
3. Die Serviceperson vor Ort muss alle Handlungen überwachen und ist für die Anlage verantwortlich.
4. Nach Beenden der Aktivitäten von außen ist die Firewall für Außenstehende wieder zu sperren.

Adäquate Methoden, die den Stand der Technik und ein entsprechendes Security-Niveau gewährleisten, sind ebenfalls zulässig.

10 Konformitätserklärung

SIGMATEK

EU-Konformitätserklärung
EU Declaration of Conformity

Hersteller (Manufacturer):	Sigmatek GmbH & Co KG
Anschrift (Address):	Sigmatekstraße 1 A- 5112 Lamprechtshausen Austria
Produktgruppe (Productfamily):	**S-Dias Safety**
Produktbezeichnung (Product name):	**SCP111**
Benannte Stelle: (Notified Body of EC-Type-Examination Certificate):	**TÜV AUSTRIA Deutschland GMBH**
Kennnummer der Benannten Stelle: (Notified Body Number):	**0408**
Nummer der EG-Baumusterbescheinigung: (EC-Type-Examination Certificate Number):	**TÜV-A-MHF/MG/13-06962**

Das (Die) bezeichnete(n) Produkt(e) stimmt (stimmen) mit den Vorschriften folgender Europäischer Richtlinien überein. Die Ausgabe der verwendeten Normen entspricht der zum Zeitpunkt der Erstellung dieses Dokumentes geltenden Fassung:
The indicated product(s) is (are) in conformance with the regulations of the following European Directives. The edition of the Standards used comply with those valid at the time this document was created.

2014/30/EU — Richtlinie des Rates zur Harmonisierung der Rechtsvorschriften der Mitgliedsstaaten über die elektromagnetische Verträglichkeit (EMV-Richtlinie)
2014/30/EU — Council Directive on the harmonization of the laws of the member states relating to electromagnetic compatibility (EMC Directive)

Harmonisierte Europäische Norm (Harmonized European Standard):

EN 61000-6-2
EN 61000-6-4
EN 61326-3-1

2014/35/EU — Richtlinie zur Harmonisierung der Rechtsvorschriften der Mitgliedsstaaten über die Bereitstellung elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen (Niederspannungs-Richtlinie)
2014/35/EU — Directive relating to electrical equipment designed for use within certain voltage limits (Low Voltage Directive).

Harmonisierte Europäische Norm (Harmonized European Standard):

EN 61131-2

CECON1179

Page 1/2

SIGMATEK GmbH & Co KG | Sigmatekstraße 1, A-5112 Lamprechtshausen | Tel.: +43 62 74/43 21-0, Fax: +43 62 74/43 21-18 | office@sigmatek.at, www.sigmatek-automation.com | UID-Nummer: ATU 34970403

SIGMATEK

SIGMATEK

EU-Konformitätserklärung
EU Declaration of Conformity

2006/42/EG 2006/42/EC	Richtlinie des Europäischen Parlaments und des Rates über Maschinen (Maschinenrichtlinie). Machinery Directive

Harmonisierte Europäische Norm (Harmonized European Standard):

EN ISO 13849
EN 62061

2011/65/EU	Richtline des Europäischen Rates Europäischen Parlaments und des Rates zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten (RoHS-Richtlinie).
2011/65/EU	Directive of the European Parlament and the council on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Lamprechtshausen, den 13.06.2018
Ort und Datum
Place and date

Andreas Melkus
Name und Unterschrift Geschäftsführer
Name and Signature of Managing Director

CECON1179

Page 2/2

SIGMATEK GmbH & Co KG
Sigmatekstraße 1
A-5112 Lamprechtshausen
Tel.: +43 62 74/43 21-0
Fax: +43 62 74/43 21-18
office@sigmatek.at
www.sigmatek-automation.com
UID-Nummer:
ATU 34970403

Hinweis:
Aktuelle EU-Konformitätserklärungen zu allen SIGMATEK Produkten finden Sie auf der Homepage www.sigmatek-automation.com

11 Zertifikat S-DIAS I/O System mit internem Bus

ZERTIFIKAT | CERTIFICATE | CERTIFICAT | CERTIFICADO | СЕРТИФИКАТ | شهادة | 证书 | 인증서

EG-Baumusterprüfbescheinigung
Certificate of EC type examination

Nr.: TÜV-A-MHF/MG13-06962A

gemäß Richtlinie 2006/42/EG (Maschinen)
according to the Directive 2006/42/EC (Machinery)

TÜV AUSTRIA

Akkreditierung Austria A 0274 ISO/IEC 17020

Auftraggeber: *Applicant:*	Sigmatek GmbH & Co. KG Sigmatekstraße 1 5112 Lamprechtshausen Österreich/Austria	**Hersteller:** *Manufacturer:*	Sigmatek GmbH & Co. KG Sigmatekstraße 1 5112 Lamprechtshausen Österreich/Austria
Produkt: *Product:*	‚S-DIAS I/O System mit internem Bus' *‚S-DIAS I/O System with internal Bus'*	**Zubehör:** *Accessories:*	Gemäß Anhang *According to annex*
Typ: *Type:*	Logikeinheiten für Sicherheitsfunktionen *Logic units to ensure safety functions*		
Beschreibung: *Description:*	Sicherheitsbezogenes Programmierbares I/O-System *Safety related programmable I/O-system*		
Prüfgrundlagen: *Tested according to:*	Richtlinie 2006/42/EG idgF. und Normen: EN ISO 13849, EN / IEC 62061 *Directive 2006/42/EC in current version and standards EN ISO 13849, EN / IEC 62061* (Anwendung gemäß Risikobeurteilung / *application according to risk assessment)*		
Bemerkungen: *Remarks:*	Produkte und Sicherheitskennwerte gemäß Anhang. *Products and safety parameters according to annex.*		

Hiermit bestätigt die TÜV AUSTRIA SERVICES GMBH als Benannte Stelle (ID-Nr. 0408), dass das oben angeführte Produkt den grundlegenden Sicherheits-Anforderungen der Richtlinie 2006/42/EG entspricht. Grundlage dieser Bescheinigung ist das zur Prüfung vorgelegte Prüfmuster und die technische Dokumentation.
Gemäß Artikel 5 und Anhang III ist am Produkt die CE-Kennzeichnung vorgesehen.

Hereby TÜV AUSTRIA SERVICES GMBH certifies as Notified Body (ID-No 0408), that the above mentioned product meets the essential safety requirements of the Directive 2006/42/EC. The certificate is based on the test specimen and the technical documentation subjected to the test.
According to Article 5 and annex III the CE mark is foreseen to be affixed on the product.

Prüfbericht: 13-00055A MFO SIGMATEK SDIAS_int_Bus PB
Test report: 13-00055A MFO SIGMATEK SDIAS_int_Bus PB

TÜV AUSTRIA SERVICES GMBH TÜV AUSTRIA

14.12.2018 **Datum** *Date*	**Dipl.-Ing. (FH) Matthias Forkl** **Benannte Stelle 0408** *Notified Body 0408*	**30.11.2023** **Gültig bis** *Valid till*

Auszugsweise Vervielfältigung nur mit Genehmigung der TÜV AUSTRIA SERVICES GMBH gestattet.
Duplication of this document in parts is subject to the approval by TÜV AUSTRIA SERVICES GMBH.

FM-INE-AS-MRL-0100b
Revision 02 vom 12.01.2017
MG13-06962A MFO SIGMATEK_SDIAS_intBus_BB.docx

TÜV AUSTRIA SERVICES GMBH
Industry and Energy
Anlagen- und Maschinensicherheit

Deutschstraße 10
A-1230 Wien
Tel.: +43 / 5 0454-6202
http://www.tuv.at

005408-17-4

Hinweis:
EG-Baumusterprüfbescheinigungen (TÜV-Zertifikate) zu weiteren SIGMATEK Sicherheits (Safety)Produkten finden Sie auf der Homepage www.sigmatek-automation.com

12 Anhang A: Fehlerbehandlung

Sollte keine der angeführten Maßnahmen Abhilfe schaffen, wenden Sie sich bitte an SIGMATEK GmbH & Co KG.

Error Variable	Beschreibung	Reason-Code 0	Reason-Code 1	Maßnahme	LED-Anzeige
ERRVAL(0)	Kein Fehler			Normaler Betrieb	
ERRVAL(1)	Die zyklische Verarbeitung ist innerhalb der erlaubten Zeit nicht fertig geworden. Mögliche Ursache(n): • Fehlerhafte Applikation	aktuelle Zykluszeit in Mikrosekunden (Maximum aus den beiden Werten von Controller 1 und 2)	Limit der Zykluszeit in Mikrosekunden	Zykluszeit bei der Safety-CPU erhöhen, Fehlerbehebung durch Quit Error	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(2)	Bei einem Funktionsaufruf wurde ein Buffer als Parameter übergeben. Die Größe des Buffers ist allerdings zu klein. Mögliche Ursache(n): • Programmfehler	tatsächliche Buffer-Größe	benötigte Buffer-Größe	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(3)	Es wurde festgestellt, dass eine globale Variable überschrieben wurde. Mögliche Ursache(n): • Programmfehler oder defektes RAM	betroffene Variable, die überschrieben wurde mögliche Werte: 0 aktueller Fehlercode	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(4)	Es wird ein Programmcode ausgeführt, der laut Programmlogik nie ausgeführt werden dürfte. Mögliche Ursache(n): • Programmfehler, defekte CPU	Code-Stelle, die ausgeführt wurde mögliche Werte: 0 bis 41	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(5)	Beim Zugriff auf ein Array liegt der Index außerhalb der Array-grenzen. Mögliche Ursache(n): • Programmfehler	Ursache des Fehlers mögliche Werte: 0 bis 20	maximal möglicher Array-Index	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(6)	Ungültiger Parameterwert bei einem Funktionsaufruf (NULL-Pointer). Mögliche Ursache(n): • Programmfehler	Ursache des Fehlers mögliche Werte: 0 bis 7	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(7)	Beim RAM-Test, Algorithmus March C-wurde ein Lesefehler oder CRC-32-Fehler festgestellt. Mögliche Ursache(n): • Hardwarefehler • RAM, Flash, Adress-, Datenleitung Programmfehler • RAM-Test wird bei nicht gesperrten Interrupts durchgeführt	betreffender Test-Schritt	betroffener Bereich im RAMt	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(8)	Beim RAM-Test, Algorithmus Galpat wurde ein Lesefehler oder CRC-32-Fehler festgestellt. Mögliche Ursache(n): • Hardwarefehler • RAM, Flash, Adress-, Datenleitung Programmfehler • RAM-Test wird bei nicht gesperrten Interrupts durchgeführt	betreffender Test-Schritt	betroffene Bereiche im RAM (CRC32-Prüfung und GalPat-Prüfung)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(9)	Die Konfiguration der benötigten Module stimmt nicht. Mögliche Ursache(n): • Tausch mehrerer Module • Module falsch konfiguriert • inkompatibler Interface Frame (falsche CRC)	0 es fehlt mehr als 1 Modul	wenn Reason-Code 0 = zwischen 0 und 1: immer 0	- Wenn mehr als ein Modul getauscht wurde, muss die Applikation neu runtergespielt werden. - Bei falscher Konfiguration muss die Applikation neu runtergespielt werden. - Überprüfung, ob der Hardwardware-Aufbau mit der Applikation übereinstimmt; Applikation entsprechend umbauen. - Bei falscher Interface CRC muss das schreibende Interface neu exportiert werden und auf der lesenden Seite importiert werden. Apliaktion muss neu runtergespielt werden. -Fehlerbehebung durch Quit Error	Error-LED des Sicherheitsmoduls leuchtet rot
		1 es fehlt ein Modul, und es hat zuvor schon ein Modul-Update stattgefunden			
		2 an das fehlende Modul kann nichts verteilt werden (S-CPU)	wenn Reason-Code 0 = 2: Sicherheitsnummer des entfernten Moduls		
		3 maximal Anzahl der Wiederholungsversuche der Konfigurationsverteilung oder Konfigurationsprüfung ist überschritten worden	wenn Reason-Code 0 = 3: Anzahl der Wiederholungsversuche		
		4 beim Versuch die Konfiguration zu versenden wurde festgestellt, dass das Zielmodul im Fehlerzustand ist	wenn Reason-Code 0 = 4: Fehlercode des entfernten Moduls		

ERRVAL(10)	Der RAM Speicher, der für Datenstrukturen mit einer konfigurationsabhängigen Größe verwendet wird, ist zu klein. Mögliche Ursache(n): • zu viele Module • zu große Applikation	immer 0	immer 0	-Größe der Applikation prüfen und entsprechend verkleinern, Applikation erneut runterspielen, Fehlerbehebung durch Quit Error. -Anzahl der Module prüfen, und entsprechend Module entfernen, Fehlerbehebung durch Quit Error	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(11)	Beim Verteilen der Konfigurationsdaten an ein entferntes Modul ist die max. Anzahl von Fehlern überschritten worden. Mögliche Ursache(n): • Übertragungsfehler • anderes Modul defekt	Fehler-Code des letzten Verteilungsversuchs	Returncode des zuletzt ausgeführten SSDO Befehls	-Die Verteilung mehrmals anstoßen; falls dies nicht ausreicht bei SIGMATEK nachfragen. -Falls defekte Module, bei SIGMATEK nachfragen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(12)	Beim Exception-Handling ist ein Fehler aufgetreten. Mögliche Ursache(n): • Softwarefehler	0 maximale Anzahl der verschachtelten TRY-CATCH-ETRY-Blöcke wurde überschritten 1 Ende eines TRY-CATCH-ETRY-Blocks ohne beginnendem TRY erreicht 2 Exception nicht im normalen Programm-Mode geworfen 3 kein TRY-Block zum Abfangen der Exception vorhanden	Anzahl der offenen TRY-CATCH-ETRY-Blöcke	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(13)	Nach dem Verteilen der Konfigurationsdaten an ein entferntes Modul wurde beim Rücklesen ein Unterschied festgestellt.	immer 0	immer 0	Applikation nochmals runterspielen und starten Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(14)	Der Interpretercode in den Konfigurationsdaten wurde nicht gefunden. Mögliche Ursache(n): • Fehlerhafte Konfiguration • Softwarefehler	immer 0	immer 0	Applikation nochmals runterspielen und starten Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(15)	In der Interpreterliste der Konfiguration wird ein FSB angegeben, zu dem kein FSB-Code existiert. Mögliche Ursache(n): • es wurde eine fehlerhafte Konfiguration eingespielt • Flash defekt	FB-ID des nicht gefundenen FB-Codes	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(16)	Beim ROM-Test in einem unveränderlichen Flash Bereich wurde ein Fehler festgestellt. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Flash defekt	Ursache des Fehlers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(17)	Der aufgerufene FSB hat einen Fehlercode zurückgegeben.	Ist-Fehlercode des FB (ist immer ungleich 0)	Soll-Fehlercode des FB (ist immer 0 = kein Fehler)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot.
ERRVAL(18)	Der entfernte sichere Eingang eines fehlenden optionalen Moduls hat das max. Alter überschritten	immer 0	immer 0	Es ist zu überprüfen, ob die Standardkommunikation zu dem benötigten Sicherheitsmodul intakt ist. Zudem ist sicherzustellen, dass sich das benötigte Sicherheitsmodul nicht im Fehlerzustand befindet. Außerdem kann es sein, dass die Maximum Transmission Time zu niedrig konfiguriert wurde. Diese Punkte sind zu überprüfen. Wurde der Fehler behoben, so kann mit einem Quit Error bzw. einem Neustart des Systems der Fehler aufgehoben werden.	Error-LED des Sicherheitsmoduls blinkt
ERRVAL(19)	Nach dem Aufruf des FSB wurde im Applikationsspeicher ein unerlaubter Wert festgestellt. Mögliche Ursache(n): • fehlerhafter FSB	tatsächliches Muster am Ende des Objektspeichers	Soll-Muster am Ende des Objektspeichers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(20)	Der aufgerufene FSB hat die Zählervariable nicht inkrementiert. Mögliche Ursache(n): • fehlerhafter FSB	tatsächlicher Wert der Zählervariable	Soll-Wert der Zählervariable	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(21)	Bei der Verwaltung des RAM-Speichers für Datenstrukturen mit einer konfigurationsabhängigen Größe wurde ein Fehler festgestellt. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(22)	Die Antwort auf einen SSDO Request liegt noch nicht vor. Mögliche Ursache(n): • Laufzeit über den Bus • Verarbeitungszeit im Zielmodul zu groß	immer 0	immer 0	Zeit am Bus erhöhen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(23)	In einer SSDO Antwort wurde im Returncode-Feld ein Fehler angezeigt. Mögliche Ursache(n): • Fehler im entfernten Modul	immer 0	immer 0	Entfernte Module auf Fehler überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(24)	In einer SSDO-Antwort sind weniger Daten enthalten als erwartet. Mögliche Ursache(n): • Fehler im entfernten Modul	tatsächliche Länge der Daten in der SSDO Antwort	Soll-Länge der Daten in der SSDO Antwort	Entfernte Module auf Fehler überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(25)	Beim Test der Prüfsummen über die konstanten Elemente der Konfigurationstabellen im RAM wurde ein Fehler entdeckt. Mögliche Ursache(n): • Softwarefehler, RAM defekt	Identifizierung der Tabelle mögliche Werte: 0 bis 5	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(26)	Der Zugriff auf den Applikationsspeicher war nicht möglich. Mögliche Ursache(n): • Softwarefehler • fehlerhafte Anfrage vom SafetyDesigner	0	in den beiden niederwertigen Bytes ist der ermittelte ungültige Zellen-Index enthalten, in den beiden höherwertigen Bytes steht die Anzahl vorhandener Zellen	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
		1	ungültiger Zellen-Index		
		2	ungültiger Address-Offset		
		3	in den beiden niederwertigen Bytes ist Address-Offset enthalten, in den beiden höherwertigen Bytes steht die Länge		
		4	ungültige Länge (nicht durch 4 teilbar)		
ERRVAL(27)	Bei einem Speicherbereich im Flash wurde ein ungültiger Blockheader erkannt. Mögliche Ursache(n): • Hardwarefehler (Flash defekt) • Programmiervorgang wurde unterbrochen	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(28)	Bei einem Anmeldeversuch wurde ein ungültiges Passwort angegeben. Mögliche Ursache(n): • Tippfehler • Hackerangriff	immer 0	immer 1	Fehler wird im SafetyDesigner im Konsolenfenster angezeigt. Das Passwort muss erneut eingegeben werden.	Weiterhin normaler Betrieb
ERRVAL(29)	In einem SSDO Frame ist ein ungültiger Parameter vorhanden. Mögliche Ursache(n): • Softwarefehler	Identifizierung der Fehlerursache mögliche Werte:		Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
		0	immer 0		
		1	immer 0		
		2	immer 0		
		3	immer 0		
		4	bei Reason-Code 0 = 4: die niederwertigen 2 Bytes enthalten die Größe des übergebenen Buffers, die höherwertigen 2 Bytes die max. Größe		
ERRVAL(30)	In einem SSDO Frame fehlt ein Parameter. Mögliche Ursache(n): • Softwarefehler	wird nur in der Firmware für den Hardwaretest verwendet		Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(31)	Interner Fehler bei der Verarbeitung der SSDOs. Mögliche Ursache(n): • Softwarefehler	Länge des zu schreibenden SSDO	maximale Länge eines SSDO	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(32)	Das SSDO Paket enthält ein ungültiges Befehlsbyte. Mögliche Ursache(n): • Softwarefehler	ungültiges Kommando	Anzahl vorhandener Kommandos	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(33)	Bei dem Versuch zur Passwortänderung wurde ein ungültiges neues Passwort angegeben. Mögliche Ursache(n): • Benutzerfehler	immer 0	immer 0	Wird ein falsches Passwort eingegeben, so kommt im SafetyDesigner eine Warnung. Kommt der Fehler 33: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(34)	Das SSDO Paket enthält eine ungültige virtuelle Adresse. Mögliche Ursache(n): • Softwarefehler	Identifizierung der Fehlerursache mögliche Werte: 0 bis 1	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(35)	Bei der Verarbeitung der SSDOs wurde festgestellt, dass ein interner Buffer zu klein für die angeforderte Datenmenge ist. Mögliche Ursache(n): • Softwarefehler • fehlerhaftes Safety-Tool	Identifizierung der Fehlerursache mögliche Werte: 0 bis 1	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(36)	Der ADC funktioniert nicht richtig. Mögliche Ursache(n): • Hardwarefehler	Nummer des fehlerhaften ADC-Kanals	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(37)	Der gemessene ADC Wert der externen Referenz-Spannung ist zu klein. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	unteres Limit	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(38)	Der gemessene ADC Wert der externen Referenz-Spannung ist zu groß. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	oberes Limit	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(39)	Der gemessene ADC Wert einer Versorgungsspannung ist zu klein. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	unteres Limit	Das Sicherheitsmodul wird mit einer falschen externen Spannung versorgt. Es ist zu überprüfen, dass die Spannung zwischen 18 V und 30 V liegt (nominal 24 V). Danach kann mit Quit Error der Fehler behoben werden.	Error-LED des Sicherheitsmoduls leuchtet rot DCOK-LED leuchtet nicht
ERRVAL(40)	Der gemessene ADC Wert einer Versorgungsspannung ist zu groß. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	oberes Limit	Das Sicherheitsmodul wird mit einer falschen externen Spannung versorgt. Es ist zu überprüfen, dass die Spannung zwischen 18 V und 30 V liegt (nominal 24 V). Danach kann mit Quit Error der Fehler behoben werden.	Error-LED des Sicherheitsmoduls leuchtet rot DCOK-LED leuchtet nicht

ERRVAL(41)	Der gemessene ADC Wert einer Versorgungsspannung ist zu klein. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	unteres Limit	Spannungsversorgung überprüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(42)	Der gemessene ADC Wert einer Versorgungsspannung ist zu groß. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	oberes Limit	Spannungsversorgung überprüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(43)	Der gemessene ADC Wert einer Versorgungsspannung ist zu klein. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	unteres Limit	Spannungsversorgung überprüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(44)	Der gemessene ADC Wert einer Versorgungsspannung ist zu groß. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	oberes Limit	Spannungsversorgung überprüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(45)	Der gemessene ADC Wert einer Versorgungsspannung ist zu klein. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	unteres Limit	Spannungsversorgung überprüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(46)	Der gemessene ADC Wert einer Versorgungsspannung ist zu groß. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	oberes Limit	Spannungsversorgung überprüfen	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(47)	Der gemessene ADC Wert einer Versorgungsspannung ist zu klein. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	unteres Limit	Spannungsversorgung überprüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(48)	Der gemessene ADC Wert einer Versorgungsspannung ist zu groß. Mögliche Ursache(n): • Hardwarefehler	gemessener Wert	oberes Limit	Spannungsversorgung überprüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(49)	Bei der Prüfung des LOG-Speichers im POST wurde festgestellt, dass beide Sektoren voll sind. Mögliche Ursache(n): • Hardwarefehler • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(50)	Bei der Prüfung des LOG-Speichers im POST wurde festgestellt, dass beide Sektoren Daten enthalten aber nicht voll sind. Mögliche Ursache(n): • Hardwarefehler • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(51)	Die Meldungen sind nicht zusammenhängend (Löcher im Log- Speicher). Mögliche Ursache(n): • Programmfehler	Startadresse des ersten gefundenen leeren Eintrags im Log-Speicher	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(52)	Die Information über die gespeicherten Sicherheitsnummern der entfernten Module ist inkonsistent. Mögliche Ursache(n): • Programmfehler	tatsächliche Anzahl der gespeicherten entfernten Module	nicht erlaubte Anzahl der gespeicherten entfernten Modulen	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(53)	Der SSDO Befehl kann im aktuellen Zustand nicht ausgeführt werden. Mögliche Ursache(n): • Modul führt den Bootcode aus	immer 0	immer 0	Neu starten Falls der Fehler immer noch auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(54)	Es wurde versucht auf einen Speicherbereich zuzugreifen (Flash oder SD-Karte) auf dem kein Zugriff möglich oder erlaubt ist. Mögliche Ursache(n): • Programmfehler • Fehler im Safety-Tool	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(55)-ERRVAL(59)	Beim Flash programmieren ist ein Timeout aufgetreten. Mögliche Ursache(n): • Hardwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(60)-ERRVAL(61)	Beim Programmieren des Flash wurde versucht, eine gesperrte Page zu programmieren. Mögliche Ursache(n): • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(62)-ERRVAL(66)	Beim Programmieren des Flash ist ein Fehler aufgetreten. Mögliche Ursache(n): • Programmfehler • Hardwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(67)	Es wurde versucht einen Flashbereich zu löschen, der nicht zu den Sektorgrenzen im Flash passt. Mögliche Ursache(n): • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(68)	Ungültiger Parameterwert bei einem Funktionsaufruf. Mögliche Ursache(n): • Programmfehler	Identifizierung der Fehlerursache mögliche Werte: 0 bis 54	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(69)	Der Platz im SPDO für die zu übertragenden Sicherheitswerte ist zu klein. Mögliche Ursache(n): • Softwarefehler	Index des höchstwertigen Bytes der zu übertragenden Sicherheitswerte	maximale Größe der zu übertragenden Sicherheitswerte	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(70)	Kreuzkommunikation funktioniert nicht (Übertragungsfehler). Mögliche Ursache(n): • Hardwarefehler	1 Fehler beim Selbsttest im Post 2 Fehler im U_ART erkannt 3 FPGA Fifo Sendebuffer ist voll	Fehlerflags	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(71)	Kreuzkommunikation funktioniert nicht (Übertragungsfehler). Mögliche Ursache(n): • Hardwarefehler	bei E_CC1: 1 Fehler beim Selbsttest im Post 2 Fehler im U_ART erkannt bei ECC2: Fehlerflags	Fehlerflags	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(72)	Es wurde versucht, eine Division durch 0 auszuführen. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(73)	Kreuzkommunikation funktioniert nicht (Übertragungsfehler). Mögliche Ursache(n): • Hardwarefehler	über die Kreuzkommunikation empfangener Wert	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(74)	Die logische Programmlaufüberwachung hat festgestellt, dass ein im Op/OpTemp Modus auszuführender Programmteil nicht ausgeführt wurde. Mögliche Ursache(n): • Softwarefehler	ID des Programmteils	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(75)	Die in den beiden Controllern eingelesenen Werte für die lokalen Eingänge weisen für eine unzulässig lange Zeit unterschiedliche Werte auf. Mögliche Ursache(n): • Hardwarefehler • Eingangsschaltung	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(76)	Kreuzkommunikation funktioniert nicht (Timeout). Mögliche Ursache(n): • Hardwarefehler • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(77)	Der Inhalt einer STDO Antwort ist in beiden Controllern unterschiedlich. Mögliche Ursache(n): • Softwarefehler	0 oder 1 je nach Art des Fehlers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(78)	Die Laufzeitüberwachung wurde unerlaubterweise in einem Operational-Laufzeitzustand deaktiviert. Mögliche Ursache(n): • Softwarefehler	ID des Aufrufers, von dem die Laufzeitüberwachung deaktiviert wurde	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(79)-ERRVAL(81)	Kreuzkommunikation funktioniert nicht (unerwarteter Wert empfangen). Mögliche Ursache(n): • Hardwarefehler • Softwarefehler	über die Kreuzkommunikation empfangener Wert	erwarteter Wert (= Soll-Wert)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(82)	Das berechnete Ausgangsabbild ist in den beiden Controllern unterschiedlich. Mögliche Ursache(n): • Softwarefehler • Hardwarefehler	Index der Zelle im Applikationsspeicher, deren Inhalt nicht mit der des anderen Controller übereinstimmt	Inhalt der im Reason-Code 0 angeführten Zelle	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(83)	Der andere Controller ist bei der Kreuzkommunikation nicht mehr synchron. Es handelt sich hier noch um keinen Fehler, der den sicheren Zustand herbeiführt. Als Reaktion auf diesen Fehler synchronisieren sich die Controller neu, tauschen Informationen aus und erst dann wird entschieden, ob der sichere Zustand herbeigeführt wird. Mögliche Ursache(n): • ein Controller hat einen Fehler festgestellt, der andere (noch) nicht	immer 0	immer 0	Fehler quittieren, System ev. neu starten Falls Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls blinkt schnell
ERRVAL(84)	Der Inhalt der SD-Karte konnte nicht geladen werden, weil die Konfiguration im Flash nicht vorhanden und auch nicht gelöscht ist. Mögliche Ursache(n): • Anwenderfehler	immer 0	immer 0	Speicher der Safety-CPU löschen und nochmals versuchen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(85)	Die SD-Karte konnte nicht initialisiert werden. Mögliche Ursache(n): • Hardwarefehler	immer 0	immer 0	SD-Karte nochmals bespielen, andere SD Karte verwenden Falls Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(86)	Der Inhalt auf der SD-Karte entspricht nicht dem erwarteten Format. Mögliche Ursache(n): • Hardwarefehler • Softwarefehler • Anwenderfehler	immer 0	immer 0	SD-Karte nochmals bespielen Falls Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(87)	Die Konfigurationsdaten auf der SD-Karte stimmen nicht mit denen im Flash überein. Mögliche Ursache(n): • Anwenderfehler	CRC der Konfigurationsdaten auf der SD-Karte	CRC der Konfigurationsdaten im Flash	Prüfen, ob die richtige SD-Karte eingesteckt ist. Wenn die richtige SD-Karte eingesteckt ist, dann Speicher der Safety-CPU löschen und nochmals versuchen. Entweder ist die Konfiguration im Flash zu löschen, falls die Konfiguration der SD-Karte übernommen werden soll. Soll jedoch die Konfiguration von der SD-Karte übernommen werden, so ist die Konfiguration auf dem Flash zu löschen und das System bei eingesteckter SD-Karte neu zu starten.	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(88)	Die SD-Karte wurde eingesteckt, während das Modul eingeschaltet war und sich nicht im Service Mode befand. Mögliche Ursache(n): • Anwenderfehler	immer 0	immer 0	SD-Karte wieder entnehmen, Fehler quittieren und in den Service Mode wechseln, dann SD-Karte einstecken.	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(89)	Interner Fehler in einer Ablauftabelle.	Identifizierung der Fehlerursache mögliche Werte: 0 bis 1	ungültiger Status bzw. Index	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(90)	Der gemessene Wert des Referenzclocks vom FPGA (REFCLK) ist zu klein. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Hardwarefehler • CPU • FPGA	Anzahl gemessener Flanken	minimale Anzahl der zu messenden Flanken	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(91)	Der gemessene Wert des Referenzclocks vom FPGA (REFCLK) ist zu groß. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Hardwarefehler • CPU • FPGA	Anzahl gemessener Flanken	maximale Anzahl der zu messenden Flanken	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(92)	Beim Warten auf die SSDO Response ist eine Zeitüberschreitung aufgetreten. Mögliche Ursache(n): • Laufzeit über den Bus • Verarbeitungszeit im Zielmodul	immer 0	immer 0	Laufzeiten verringern	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(93)	Der andere Controller hat einen Fehler festgestellt. Mögliche Ursache(n): • Ursache gemäß Fehlercode des anderen Controllers	Fehlercode des anderen Controllers	immer 0	Fehlercode des anderen Controllers prüfen.	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(94)	Der Konfigurationszustand des anderen Controllers stimmt mit dem eigenen nicht überein. Mögliche Ursache(n): • Modul wurde während des Konfigurierens abgeschaltet	Konfigurationsstatus des eigenen Controllers	Konfigurationsstatus des anderen Controllers	Modul neu konfigurieren	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(95)	Eine Konstante im Applikationsspeicher wurde verändert und stimmt nicht mehr mit dem im Flash gespeicherten Wert überein. Mögliche Ursache(n): • Hardwarefehler (defektes Flash, defektes RAM) • Softwarefehler	Index der Speicherzelle der fehlerhaften Konstante im Applikationsspeicher	Index der Konstante im Flash	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(96)	Die Versorgungsspannungen sind nach dem Power-On nicht innerhalb eines Zeitlimits auf den richtigen Wert gegangen. Mögliche Ursache(n): • Hardwarefehler	immer 0	immer 0	Versorgungsspannung überprüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(97)	Bei der Bearbeitung der digitalen Eingänge kam es zu einem internen Fehler. Mögliche Ursache(n): • Softwarefehler	Index des ersten Rohwertes der digitalen Eingänge	Index des letzten Rohwertes der digitalen Eingänge	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(98)	Die Reaktion auf den internen Test konnte nicht ermittelt werden. Mögliche Ursache(n): • Softwarefehler	Bit-Maske der digitalen Eingänge	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(99)	Beim Eingangstest (interner Test) ist ein Fehler festgestellt worden. Mögliche Ursache(n): • Hardwarefehler	Zustände der digitalen Eingänge	Bit-Maske der digitalen Eingänge	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(100)	Während des externen Tests ist ein interner Test aktiv. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(101)	Die Reaktion auf den externen Test konnte nicht ermittelt werden. Mögliche Ursache(n): • Softwarefehler	Bit-Maske der digitalen Eingänge	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(102)	Externer Test: Bei einem am Takt angeschlossenen Eingang ist der Taktimpuls nicht erkannt worden. Mögliche Ursache(n): • Querschluss	immer 0	immer 0	Verdrahtung des Querschlusses mit der Applikation vergleichen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(103)	Externer Test: Bei einem am Takt angeschlossenen Eingang ist der Taktimpuls des anderen Taktausgangs erkannt worden. Mögliche Ursache(n): • Querschluss	immer 0	immer 0	Verdrahtung des Querschlusses mit der Applikation vergleichen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(104)	Der Lo-Resolution Timer arbeitet nicht richtig (gemessene Werte sind zu klein). Mögliche Ursache(n): • Hardwarefehler	gemessener Wert des Lo-Resolution Timers	unteres Limit für die Messung	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(105)	Der Lo-Resolution Timer arbeitet nicht richtig (gemessene Werte sind zu groß). Mögliche Ursache(n): • Hardwarefehler	gemessener Wert des Lo-Resolution Timers	oberes Limit für die Messung	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(106)	Der Millisekunden-Timer arbeitet nicht richtig (gemessene Werte sind zu klein). Mögliche Ursache(n): • Hardwarefehler • Softwarefehler	gemessener Wert des Millisekunden-Timers	unteres Limit für die Messung	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(107)	Der Millisekunden-Timer arbeitet nicht richtig (gemessene Werte sind zu groß). Mögliche Ursache(n): • Hardwarefehler • Softwarefehler	gemessener Wert des Millisekunden-Timers	oberes Limit für die Messung	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(108)	Beim Startup ist während des Wartens auf den FPGA eine Zeitüberschreitung aufgetreten. Mögliche Ursache(n): • Hardwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(109)	Das Format des Info-Sektors im Flash stimmt nicht. Mögliche Ursache(n): • Modul wurde noch nie initialisiert (mit dem Clear-All Befehl) • HW-Fehler im Flash	immer 0	immer 0	Modul konfigurieren Falls Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(110)-ERRVAL(128)	Das Format der Konfigurationsdaten im Flash stimmt nicht. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • HW-Fehler im Flash	Detailinformation zur Fehlerursache	Detailinformation zur Fehlerursache	Modul konfigurieren Falls Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(129)	Nicht verwendet.				
ERRVAL(130)	Bei einem Funktionsaufruf wurde ein Buffer als Parameter übergeben. Die Größe des Buffers ist allerdings zu groß. Mögliche Ursache(n): • Programmfehler	tatsächliche Größe des Buffers	maximale Größe des Buffers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(131)	Für den SSDO Befehl wurde ein falscher Frametyp verwendet. Mögliche Ursache(n): • Fehler im Safety-Tool	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(132)	Bei den Modul-Sicherheitsnummern der entfernten Module ist ein Wert doppelt vorhanden. Mögliche Ursache(n): • beim Ermitteln der Modul-Sicherheitsnummer anhand des Topologiepfads ist ein Fehler aufgetreten	Index des Moduls in der Tabelle der entfernten Module	doppelt vorhandene Modul-Sicherheitsnummer	- Applikation nochmals starten - Alle Sicherheitsnummern auf Eindeutigkeit prüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(133)	Der Microcontroller befindet sich nicht im korrekten Prozessor-Modus. Entweder sind die Flags für den Prozessor-Modus oder für die Aktivierung der Interrupts im Programm Status-Register nicht korrekt gesetzt, oder es wird der falsche Stack verwendet. Mögliche Ursache(n): • der Wechsel des Prozessor-Modus funktioniert nicht korrekt (aufgrund Hardware- oder Software-Fehler)	gesetzte Flags im Programm Status-Register oder der Wert des Stack-Pointers	Soll-Wert für die Flags im Programm Status-Register oder untere bzw. obere Grenze des zu verwendenden Stack-Bereichs	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(134)	Das berechnete Ausgangsabbild ist in den beiden Controllern unterschiedlich.	Zustände der lokalen Ausgänge des eigenen Controllers	Zustände der lokalen Ausgänge des anderen Controllers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(135)	Die Leitung 24 V1 DCOK signalisiert, dass die Spannung nicht in Ordnung ist. Mögliche Ursache(n): • externe Spannungsversorgung nicht angeschlossen • Hardwarefehler	immer 0	immer 0	Es ist sicherzustellen, dass die externe Spannungsversorgung der Taktausgänge bei Sicherheitsmodulen mit digitalen Eingängen und die Versorgungsspannung der Ausgänge für Sicherheitsmodule mit digitalen Ausgängen korrekt ist. Nach Anlegen der richtigen Spannung kann der Fehler mit „Quit Error“ beziehungsweise durch einen Wiederanlauf behoben werden.	Error-LED des Sicherheitsmoduls leuchtet rot DCOK-LED leuchtet nicht
ERRVAL(136)	Die boolsche Darstellung eines Ausgangs hat einen ungültigen Wert. Mögliche Ursache(n): • Softwarefehler (Speicher wurde an unerlaubter Stelle überschrieben) • Hardwarefehler (RAM defekt)	Index der Zelle im Applikationsspeicher mit dem ungültigen Wert, 0xFFFFFFFF bedeutet, dass der Fehler beim Kodieren des SAFEBOOL-Wertes für den SPDO-Frame entdeckt wurde	ungültiger Wert	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(137)	Die Werte der zurückgelesenen Ausgänge stimmen mit den Werten der Sollwerte der Ausgänge nicht überein. Mögliche Ursache(n): • Hardwarefehler (z.B. Ausgangstransistor defekt) • externer Fehler (z.B. Kurzschluss, Versorgungsspannung der Ausgänge fehlt) • Softwarefehler	Sollwerte (Bit 0 = 1. Ausgang)	Istwerte (Bit 0 = 1. Ausgang)	Spannungsversorgung prüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	LED des sicheren Ausgangs blinkt
ERRVAL(138)	Beim Watchdog-Test ist ein Fehler aufgetreten. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Hardwarefehler	Bit-Maske zur Identifizierung der Testschritte, bei denen der Fehler entdeckt wurde	aktueller Testschritt	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(139)-ERRVAL(141)	In der Konfiguration sind beim COPY Befehl ungültige Parameter angegeben. Mögliche Ursache(n): • es wurde eine fehlerhafte Konfiguration eingespielt • Flash defekt	Index der Quelle bzw. des Ziels	maximale Anzahl vorhandener Zellen bzw. unteres oder oberes Index-Limit	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(142)	Nach dem Einschalten der oberen Ausgangshalbleiter (HSS) ist mind. ein Ausgang auf 1 gegangen, obwohl keiner der unteren Ausgangshalbleiter (FET) eingeschaltet war. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Ausgangshalbleiter (FET) defekt	Sollwert (Bit 0 = 1. Ausgang) immer 0	Istwert, betroffener Ausgänge (Bit 0 = 1. Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(143)	Nach dem Abschalten des HSS Ausgangshalbleiters ist keiner der zuvor gesetzten Ausgänge auf 0 gegangen. Mögliche Ursache(n): • Ausgangshalbleiter (HSS) defekt • unzulässig große kapazitive Last	Werte der Ausgänge nach dem Abschalten des HSS (Bit 0 = 1. Ausgang)	zuvor gesetzte Ausgänge (Bit 0 = 1. Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	LED des sicheren Ausgangs blinkt
ERRVAL(144)	Nach dem Abschalten des FET Ausgangshalbleiters ist der zugehörige Ausgang nicht auf 0 gegangen. Mögliche Ursache(n): • Ausgangshalbleiter (FET) defekt • unzulässig große kapazitive Last	betroffener Ausgang (Bit 0 = 1. Ausgang)	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	LED des sicheren Ausgangs blinkt

ERRVAL(145)	Nach dem Abschalten des FET Ausgangshalbleiters hat ein Ausgang der nicht über diesen FET angeschlossen ist, seinen Wert geändert. Mögliche Ursache(n): • Interner Querschluss im Ausgangskreis	Status der Ausgänge (Bit 0 = 1. Ausgang)	Soll-Status der Ausgänge (Bit 0 = 1. Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	LED des sicheren Ausgangs blinkt
ERRVAL(146)	Die zyklische Verarbeitung ist innerhalb der erlaubten Zeit nicht fertig geworden. Mögliche Ursache(n): • fehlerhafte Applikation	Caller-Id mit der zuletzt die Runtime-Triggerung erfolgte	Code-Adresse, an der nach Beendigung der Interrupt-Funktion fortgesetzt wird	Zykluszeit der SafetyCPU erhöhen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(147)	Die logische Programmlaufüberwachung hat festgestellt, dass ein Programmteil unzulässig lange nicht mehr aufgerufen wurde. Mögliche Ursache(n): • Softwarefehler	< 100 Index des Programmteils >=100 ID des Programmteils, wo der Fehler festgestellt wurde 100-107	RCO < 100 einzuhaltende Zeit des Programmteils	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(148)-ERRVAL(149)	Die logische Programmlaufüberwachung hat festgestellt, dass ein Programmteil unzulässig lange nicht mehr aufgerufen wurde. Mögliche Ursache(n): • Softwarefehler	< 100 Index des Programmteils >= 100 ID des Programmteils, wo der Fehler festgestellt wurde 100-107	RCO < 100 einzuhaltende Zeit des Programmteils	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(150)	Der Eingangswert ist unzulässig lange nicht mehr aktualisiert worden. Mögliche Ursache(n): • Fehler in der Eingangshardware • ständige Änderung des Eingangssignals	betroffener Eingang (Bit 0 = 1. Eingang)	maximales Alter	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(151)-ERRVAL(152)	Die reservierten Stackbereiche wurden überschrieben. Mögliche Ursache(n): • Softwarefehler • Stack-Reserve zu klein dimensioniert	ID des betroffenen Stackbereichs	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(153)	Das berechnete Ausgangsabbild ist in den beiden Controllern unterschiedlich.	CRC des Sende SPDO Frames und des App-Speichers des eigenen Controllers	CRC des Sende SPDO Frames und des App-Speichers des anderen Controllers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(154)	Die Information über die gespeicherten Sicherheitnummern der entfernten Module ist inkonsistent. Mögliche Ursache(n): • Programmfehler	Index des gesuchten Moduls	Anzahl der Elemente in der Tabelle der entfernten Module	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(155)-ERRVAL(197)	Der CPU-Test hat einen Fehler festgestellt. Mögliche Ursache(n): • CPU-Fehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(198)	Der interne Zähler für die Zykluszeit arbeitet falsch. Mögliche Ursache(n): • Softwarefehler	letzte Zeitdifferenz	maximale Zeitdifferenz	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(199)	Der entfernte sichere Eingangswert hat das maximale Alter überschritten. Mögliche Ursache(n): • Bus-Übertragungsfehler • Fehler in der Hardware des entfernten Moduls. • Softwarefehler im entfernten Modul	immer 0	immer 0	Es ist zu überprüfen, ob die Standardkommunikation zu jedem benötigten Sicherheitsmodul intakt ist. Zudem ist sicherzustellen, dass sich kein benötigtes Sicherheitsmodul im Fehlerzustand befindet. Außerdem kann es sein, dass die maximale Transmission Time zu niedrig konfiguriert wurde. Diese Punkte sind zu überprüfen. Wurde der Fehler behoben, so kann mit einem Quit Error bzw. einem Neustart des Systems der Fehler aufgehoben werden.	Error-LED des Sicherheitsmoduls blinkt
ERRVAL(200)	Der angeforderte IRQ-Registertest wurde im Interrupt nicht ausgeführt. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(201)-ERRVAL(205)	Es ist eine unerwartete Exception aufgetreten. Mögliche Ursache(n): • Softwarefehler	Adresse des unterbrochenen Codes	bei einer Exception außerhalb des FSB-Aufrufs: - immer 0 bei einer Exception während des FSB-Aufrufs: - FSB-ID in den unteren 2 Bytes - Objekt-Index in den oberen 2 Bytes	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(206)	Die Systemzeiten beider Controller haben eine zu große Abweichung. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Hardwarefehler	ermittelte Drift zwischen den beiden Controller-Systemzeiten	maximal zulässige Drift	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(207)	Die Modul-Art und Modul-Variante in der Firmware stimmt nicht mit den in den unveränderlichen Modulparametern gespeicherten Werten überein. Mögliche Ursache(n): • falsche Firmware	Modul-Art und -Variante der Firmware	Modul-Art und -Variante des Bootloaders	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(208)-ERRVAL(209)	Die unveränderlichen Modulparameter sind in den beiden Controllern unterschiedlich. Mögliche Ursache(n): • Hardwarefehler • Flash falsch programmiert	Modulparameter des eigenen Controllers	Modulparameter des anderen Controllers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(210)	Die Firmware Versionen sind in den beiden Controllern unterschiedlich. Mögliche Ursache(n): • falsche Firmware	Firmware-Version im eigenen Controller	Firmware-Version im anderen Controller	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(211)	Beim ROM-Test in einem unveränderlichen Flash Bereich wurde ein Fehler festgestellt. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Flash defekt	Informationen über die Ursache des Fehlers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(212)	Beim ROM-Test in einem unveränderlichen Flash Bereich wurde ein Fehler festgestellt. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Flash defekt	Informationen über die Ursache des Fehlers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(213)-ERRVAL(217)	Beim ROM-Test in einem änderbaren Flash Bereich wurde ein Fehler festgestellt. Mögliche Ursache(n): • Flash defekt • Modul wurde während des Flash Programmierens ausgeschaltet	Informationen über die Ursache des Fehlers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(218)	Nach dem Einschalten der unteren Ausgangshalbleiter (FET) ist mind. ein Ausgang auf 1 gegangen, obwohl keiner der oberen Ausgangshalbleiter (HSS) eingeschaltet war. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Ausgangshalbleiter (HSS) defekt	Sollwert (Bit 0 = erster Ausgang), immer 0	Istwert, betroffene Ausgänge (Bit 0 = erster Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(219)	Der Inhalt einer SSDO Antwort ist in beiden Controllern unterschiedlich. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(220)	Es wurde versucht, das Flash mit einer ungültigen Länge zu beschreiben. Mögliche Ursache(n): • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(221)	Es wurde versucht aus einem Datenbuffer zu lesen, wobei der Buffer weniger als die angeforderte Datenmenge enthält. Mögliche Ursache(n): • Softwarefehler • fehlerhaftes Safety-Tool (SSDO-Befehl)	Anzahl der Bytes, die aus dem Buffer gelesen werden sollten	Größe des Buffers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(222)	Die Zeit für den Testmodus oder die maximale Idle-Zeit ist abgelaufen.	0 Zeit für den Testmodus ist abgelaufen	immer 0	bei abgelaufenen Testmodus die Konfiguration erneut runterspielen und neu starten	Error-LED des Sicherheitsmoduls leuchtet rot
		1 Zeit für die maximale Idle-Zeit ist abgelaufen 2 Zeit für die maximale Check Config Zeit ist abgelaufen	immer 0	bei abgelaufener Idle-Zeit bzw. Check Config Zeit den Fehler quittieren und erneut starten.	
ERRVAL(223)	Der zeitliche Ablauf beim internen Test stimmt nicht. Es wurde versucht einen Test zu starten, während der vorherige Test noch nicht zu Ende ist. Mögliche Ursache(n): • Softwarefehler	Bit-Maske der Eingänge	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(224)	Der zeitliche Ablauf beim internen Test stimmt nicht. Es wurde versucht einen Test zu starten während der vorherige Test noch nicht zu Ende ist. Mögliche Ursache(n): • Softwarefehler	Taktausgang A (=1) oder B (=0)	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(225)	Der Konfigurations-Zustand kann nicht auf 'konfiguriert' gesetzt werden, da die CRCs der zur Konfiguration gehörenden Bereiche ungültig sind. Mögliche Ursache(n): • es wurde ein Firmware-Update durchgeführt; • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(226)	Der Konfigurations-Zustand kann nicht auf 'konfiguriert' gesetzt werden, da die vom Aufrufer übergebene CRC nicht mit der tatsächlichen übereinstimmt. Das Modul wechselt nicht in den Fehlerzustand. Es wird der Fehler im SafetyDesigner im Konsolenfenster angezeigt. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	immer 0	immer 0	Das Sicherheitsmodul muss erneut konfiguriert werden Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(227)	Das Format der Konfigurationsdaten im Flash stimmt nicht. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	tatsächlicher Konfigurationszustand	Soll-Konfigurationszustand	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(228)	Der Konfigurations-Zustand kann nicht auf 'konfiguriert' gesetzt werden, da die Konfiguration gelöscht ist. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(229)	Die Konfiguration ist nicht in dem Zustand, in dem das Verified-Flag gesetzt werden kann. Mögliche Ursache(n): • die Konfiguration ist noch nie verteilt worden • die Konfiguration ist im Developer-Mode in die Safety-CPU geschrieben worden	immer 0	immer 0	-Programm nicht im Developer Mode starten -Programm erneut starten und somit Verteilung auslösen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(230)	Der SSDO Befehl kann aufgrund fehlender Berechtigung nicht ausgeführt werden. Mögliche Ursache(n): • Fehler im SafetyDesigner	immer 0	immer 0	Mit dem SafetyDesigner erneut Online gehen und Befehle erneut ausführen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(231)	Beim Onlinegehen konnte keine Session geöffnet werden. Mögliche Ursache(n): • ein anderer SafetyDesigner ist bereits online	immer 0	immer 0	Prüfen, ob mehrere SafetyDesigner Online sind, es darf nur ein SafetyDesigner zugreifen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(232)	Die max. Anzahl der entfernten Module ist überschritten worden.	Anzahl der entfernten Module	maximale Anzahl möglicher entfernter Module	Anzahl der entfernten Module prüfen und entsprechend ändern	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(233)	Der in den CFG-Pins kodierte Modultyp passt nicht zur Firmware. Mögliche Ursache(n): • Falsche Firmware	CFG-Pins laut Hardware	CFG-Pins laut Firmware	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(234)	Der SSDO Befehl kann in diesem Laufzeit-Zustand nicht ausgeführt werden. Mögliche Ursache(n): • Fehler im SafetyDesigner	immer 0	immer 0	Mit dem SafetyDesigner erneut Online gehen und Befehle erneut ausführen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(235)	Die Parameter im Firmware-Header der neuen Firmware passen nicht zu diesem Modul. Mögliche Ursache(n): • Falsche Firmware	Parameter in der Firmware	Parameter im Bootcode	Es muss ein Modul verwendet werden, dass eine kompatible Firmware besitzt.	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(236)	Beim Zugriff auf die SD-Karte ist ein Fehler aufgetreten. Mögliche Ursache(n): • SD-Karte wurde entfernt • defekte oder inkompatible SD-Karte	Identifikation der Fehlerursache	zuletzt aufgetretener Fehler	Es ist zu überprüfen, ob die SD-Karte entfernt wurde. Wurde die SD-Karte nicht entfernt, so ist die SD-Karte auszutauschen. Der Fehler kann mit dem Herausnehmen der SD-Karte und mit einem „Quit Error“-Befehl zurückgesetzt werden.Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(237)	Schreib-/Lesefehler im Interpretercode der Konfiguration. Bei der Prüfung der Konfiguration wurde einer der folgenden Fehler festgestellt: a) Es wurde versucht eine Zelle zu beschreiben, die bereits von einer anderen Quelle beschrieben worden ist (z. B. wenn 2 COPY Befehle mit dem gleichen Ziel existieren, oder wenn ein COPY Befehl eine nicht beschreibbare Zelle als Ziel angibt). b) Es wurde versucht, von einer nicht lesbaren Zelle zu lesen. Eine Zelle ist nicht lesbar, wenn es keine zugehörige Quelle gibt, von der sie beschrieben wurde (nicht initialisiert), oder wenn sei nicht als Quelle eines COPY Befehls verwendet werden darf (z. B. der Header des Objektspeichers Mögliche Ursache(n): • Es wurde eine fehlerhafte Konfiguration eingespielt • Flash defekt	Index der fehlerhaften Zelle	0 bei einem Schreibfehler 1 bei einem Lesefehler	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(238)	Der POST (PowerOn Selbsttest) ist nicht vollständig abgearbeitet worden. Mögliche Ursache(n): • Softwarefehler	Bit-Maske mit den noch ausstehenden POST-Test-Schritten	immer 0	Während des Hochlauftests wurde ein Fehler festgestellt. Über den SafetyDesigner wird angezeigt, um welchen Fehler es sich handelt. Danach kann der Fehler behoben werden.	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(239)	Der auf die SD-Karte zu schreibende Sektorbuffer ist in beiden Controllern unterschiedlich. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(240)	Der Force-Modus wurde unzulässig beendet. Mögliche Ursache(n): • Auftreten eines Session-Timeout bzw. Login-Timeout, z. B. aufgrund einer Unterbrechung der Online-Kommunikation mit dem SafetyDesigner, • Wechsel des Login-Levels (z.B. Abmelden) • Schließen der Session im SafetyDesigner	immer 0	immer 0	Bei einer Unterbrechung der Kommunikation zwischen SafetyDesigner und Modul, den Fehler quittieren	

ERRVAL(241)	Das Format der Passwörter auf der SD-Karte stimmt nicht. Mögliche Ursache(n): • SD-Karte defekt • Inhalt wurde nachträglich geändert	immer 0	immer 0	SD-Karte neu bespielen, andere SD-Karte verwenden Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(242)	Interner Fehler bei der Verarbeitung der STDOs. Mögliche Ursache(n): • Softwarefehler	Länge des zu schreibenden STDO	maximale Länge eines STDO	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(243)	Die Information über eine Modul-Sicherheitsnummer eines entfernten Moduls wird benötigt, ist aber nicht vorhanden bzw. ungültig. Mögliche Ursache(n): • Softwarefehler	Wert der ungültigen Modul-Sicherheitsnummer (0 oder 0xFFFFffff)	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(244)	Im Interpretercode der Konfiguration ist eine FSB-ID angegeben, für die kein entsprechender Code existiert. Mögliche Ursache(n): • Fehler im Safety-Tool	FB-ID	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(245)	Ein in den Konfigurationsdaten angegebener Wert ist zu groß. Mögliche Ursache(n): • Eingabe eines zu großen Wertes im SafetyDesigner.	gibt an welcher Parameter zu groß ist 0 Testzeit im temporären Operational Zustand 1 Zykluszeit für die Laufzeitüberwachung 2 maximales Alter eines entfernten Eingangs 3 Filterzeit eines lokalen Eingangs	Limit	Wert entsprechend der max. Größe einstellen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(246)-ERRVAL(255)	Funktionsblock hat einen Fehlercode zurückgegeben. Die folgenden Fehlercodes werden von den Funktionsblöcken angeliefert und sind daher nicht in der Firmware enthalten. Mögliche Ursache(n): • Softwarefehler			Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1000)	Kein Fehler			Normaler Betrieb	
ERRVAL(1001)	Die zyklische Verarbeitung ist innerhalb der erlaubten Zeit nicht fertig geworden. Mögliche Ursache(n): • fehlerhafte Applikation	aktuelle Zykluszeit in Mikrosekunden (das Maximum aus den beiden Werten von Kontroller 1 und 2)	Limit der Zykluszeit in Mikrosekunden	Konfiguration muss geändert werden, z.B. Erhöhung der max. Cyclic Time bei der SafetyCPU Fehlerbehebung durch „Quit Error“.	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1002)	Bei einem Funktionsaufruf wurde ein Buffer als Parameter übergeben. Die Größe des Buffers ist allerdings zu klein. Mögliche Ursache(n): • Programmfehler	tatsächliche Buffer-Größe oder bei einem Wert >= 0x1000 Kennung der Programmstelle des Fehlers (mögliche Werte 0x1000-0x100B)	benötigte Buffer-Größe	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1003)	Es wurde festgestellt, dass eine globale Variable überschrieben wurde. Mögliche Ursache(n): • Programmfehler • defektes RAM	betroffene Variable, die überschrieben wurde mögliche Werte: 0 aktueller Fehlercode	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1004)	Es wird ein Programmcode ausgeführt, der laut Programmlogik nie ausgeführt werden dürfte. Mögliche Ursache(n): • Programmfehler • defekte CPU	dient zur Identifizierung der Code-Stelle, die ausgeführt wurde mögliche Werte: 0 bis 104	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1005)	Beim Zugriff auf ein Array liegt der Index außerhalb der Arraygrenzen. Mögliche Ursache(n): • Programmfehler	dient zur Identifizierung der Ursache des Fehlers mögliche Werte: 0 bis 57	beinhaltet den max. möglichen Array-Index	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1006)	Ungültiger Parameterwert bei einem Funktionsaufruf (NULL-Pointer). Mögliche Ursache(n): • Programmfehler	dient zur Identifizierung der Ursache des Fehlers mögliche Werte: 0 bis 30	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1007)	Beim RAM-Test, Algorithmus March C-wurde ein Lesefehler oder CRC-32-Fehler festgestellt. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Hardwarefehler • RAM, Flash, Adress-, Datenleitung Programmfehler • RAM-Test wird bei nicht gesperrten Interrupts durchgeführt	betreffender Test-Schritt	betroffener Bereich im RAM	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1008)	Beim RAM-Test, Algorithmus Galpat wurde ein Lesefehler oder CRC-32-Fehler festgestellt. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Hardwarefehler • RAM, Flash, Adress-, Datenleitung Programmfehler • RAM-Test wird bei nicht gesperrten Interrupts durchgeführt	betreffender Test-Schritt	betroffene Bereiche im RAM (CRC32-Prüfung und GalPat-Prüfung)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1009)	Die Konfiguration der benötigten Module stimmt nicht. Mögliche Ursache(n): • Tausch mehrerer Module • Module falsch konfiguriert	0 es fehlt mehr als ein Modul 1 es fehlt ein Modul, und es hat zuvor schon ein Modul-Update stattgefunden	wenn Reason-Code 0 zwischen 0 und 1 ist: immer 0	Wenn mehr als ein Modul getauscht wurde, muss die Applikation neu runtergespielt werden.	Error-LED des Sicherheitsmoduls leuchtet rot

	• inkompatibler Interface Frame (falsche CRC)	2 an das fehlende Modul kann nichts verteilt werden (S-CPU)	wenn Reason-Code 0 2 ist: Sicherheitsnummer des entfernten Moduls	- Bei falscher Konfiguration muss die Applikation neu runtergespielt werden. - Überprüfung, ob der Hardwareaufbau mit der Applikation übereinstimmt; Applikation entsprechend umbauen. - Bei falscher Interface CRC muss das schreibende Interface neu exportiert werden und auf der lesenden Seite importiert werden. Applikation muss neu runtergespielt werden. -Fehlerbehebung durch Quit Error	
		3 maximale Anzahl der Wiederholungsversuche der Konfigurationsverteilung oder Konfigurationsprüfung wurde überschritten	wenn Reason-Code 0 3 ist: Anzahl der Wiederholungsversuche		
		4 beim Versuch die Konfiguration zu versenden, wurde festgestellt, dass das Zielmodul im Fehlerzustand ist	wenn Reason-Code 0 4 ist Laufzeitzustand des entfernten Moduls		
		5 es fehlt mindestens ein lokales SDI-Modul 6 es fehlt mindestens ein lokales Safety-Interface-Modul 7 es fehlt mindestens ein lokales STO-Modul 8 es fehlt mindestens ein lokales SRO-Modul 9 ein Modul (Master-Modul) hat versucht, die Konfiguration zu beschreiben, während die eigene Konfiguration nicht gelöscht und auf Master eingestellt war 10 ein Slave Modul hat festgestellt, dass die entfernten Module nicht richtig konfiguriert sind	wenn Reason-Code 0 zwischen 5 und 10 ist: immer 0		

		11 lokales Eingangsmodul auf dem falschen Steckplatz (Zählung beginnt bei 1) 12 lokales Ausgangsmodul auf dem falschen Steckplatz (Zählung beginnt bei 1) 13 DINT-Eingangsmodul auf dem falschen Steckplatz (Zählung beginnt bei 1)	wenn Reason-Code 0 zwischen 11 und 13 ist: Steckplatznummer des Moduls		
		14 Anzahl lokaler Eingänge falsch 15 Anzahl lokaler Ausgänge falsch 16 es wurde versucht ein lokales Modul anzusprechen, welches fehlt			
		17 ein Erweiterungsmodul konnte nicht konfiguriert werden (Zählung beginnt bei 1)	wenn Reason-Code 0 17 ist: Steckplatznummer des Moduls		
		18 zu viele Erweiterungsmodule angesteckt 19 zu wenige Erweiterungsmodule angesteckt 20 falsches Safety-Interface Modul angesteckt			

ERRVAL(1010)	Der RAM Speicher, der für Datenstrukturen mit einer konfigurationsabhängigen Größe verwendet wird, ist zu klein. Mögliche Ursache(n): • zu viele Module • zu große Applikation	0 Daten für IO-Listen und entfernte Module 1 Status der FSoE-Verbindung 2 FSoE-Buffer	immer 0	-Größe der Applikation prüfen und entsprechend verkleinern Applikation erneut runterspielen, Fehlerbehebung durch Quit Error. -Anzahl der Module prüfen, und entsprechend Module entfernen, Fehlerbehebung durch Quit Error	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1011)	Beim Verteilen der Konfigurationsdaten an ein entferntes Modul ist die max. Anzahl von Fehlern überschritten worden. Mögliche Ursache(n): • Übertragungsfehler • anderes Modul defekt	Fehler-Code des letzten Verteilungsversuchs	Returncode des zuletzt ausgeführten SSDO-Befehls	Die Verteilung mehrmals anstoßen Falls defekte Module: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1012)	Beim Exception-Handling ist ein Fehler aufgetreten. Mögliche Ursache(n): • Softwarefehler	0 maximale Anzahl der verschachtelten TRY-CATCH-ETRY-Blöcke wurde überschritten 1 Ende eines TRY-CATCH-ETRY-Blocks ohne beginnendem TRY erreicht 2 Exception nicht im normalen Programm-Mode geworfen 3 kein TRY-Block zum Abfangen der Exception vorhanden	Anzahl der offenen TRY-CATCH-ETRY-Blöcke	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1013)	Nach dem Verteilen der Konfigurationsdaten an ein entferntes Modul wurde beim Rücklesen ein Unterschied festgestellt.	Modul-Index des betroffenen Moduls	immer 0	Applikation nochmals runterspielen und starten Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1014)	Der Interpretercode in den Konfigurationsdaten wurde nicht gefunden. Mögliche Ursache(n): • Fehlerhafte Konfiguration • Softwarefehler	immer 0	immer 0	Applikation nochmals runterspielen und starten Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1015)	In der Interpreterliste der Konfiguration wird ein FSB angegeben, zu dem kein FSB-Code existiert. Mögliche Ursache(n): • es wurde eine fehlerhafte Konfiguration eingespielt • Flash defekt	FSB-ID des nicht gefundenen FSB-Codes	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1016)	Beim ROM-Test in einem unveränderlichen Flash Bereich wurde ein Fehler festgestellt. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Flash defekt	Informationen über die Ursache des Fehlers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1017)	Der aufgerufene FSB hat einen Fehlercode zurückgegeben.	Fehlercode des FSB (immer ungleich 0)	FSB-ID und Objekt-Index des betroffenen FSB	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1018)	Der entfernte sichere Eingang eines fehlenden optionalen Moduls (entferntes Modul oder Safety-Interface-Modul) hat das maximale Alter überschritten.	immer 0	immer 0	Es ist zu überprüfen, ob die Standardkommunikation zu dem benötigten Sicherheitsmodul intakt ist. Zudem ist sicherzustellen, dass sich das benötigte Sicherheitsmodul nicht im Fehlerzustand befindet. Außerdem kann es sein, dass die Maximum Transmission Time zu niedrig konfiguriert wurde. Diese Punkte sind zu überprüfen. Wurde der Fehler behoben, so kann mit einem Quit Error bzw. einem Neustart des Systems der Fehler aufgehoben werden.	Error-LED des Sicherheitsmoduls blinkt

ERRVAL(1019)	Nach dem Aufruf des FSB wurde im Applikationsspeicher ein unerlaubter Wert festgestellt. Mögliche Ursache(n): • fehlerhafter FSB	tatsächliches Muster am Ende des Objektspeichers	Soll-Muster am Ende des Objektspeichers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1020)	Der aufgerufene FSB hat die Zählervariable nicht inkrementiert. Mögliche Ursache(n): • fehlerhafter FSB	tatsächlicher Wert der Zählervariable	Soll-Wert der Zählervariable	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1021)	Bei der Verwaltung des RAM-Speichers für Datenstrukturen mit einer konfigurationsabhängigen Größe wurde ein Fehler festgestellt. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1022)	Die Antwort auf einen SSDO Request liegt noch nicht vor. Mögliche Ursache(n): • Laufzeit über den Bus • Verarbeitungszeit im Zielmodul zu groß	immer 0	immer 0	Zeit am Bus erhöhen, falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1023)	In einer SSDO Antwort wurde im Returncode-Feld ein Fehler angezeigt. Mögliche Ursache(n): • Fehler im entfernten Modul	immer 0	immer 0	Entfernte Module auf Fehler überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1024)	In einer SSDO-Antwort sind weniger Daten enthalten als erwartet. Mögliche Ursache(n): • Fehler im entfernten Modul	tatsächliche Länge der Daten in der SSDO-Antwort	Soll-Länge der Daten in der SSDO-Antwort	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1025)	Beim Test der Prüfsummen über die konstanten Elemente der Konfigurationstabellen im RAM wurde ein Fehler entdeckt. Mögliche Ursache(n): • Softwarefehler • RAM defekt	Identifizierung der Tabelle mögliche Werte: 0 bis 11	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1026)	Der Zugriff auf den Applikationsspeicher war nicht möglich. Mögliche Ursache(n): • Softwarefehler • fehlerhafte Anfrage vom SafetyDesigner	0	bei Reason-Code 0 = 0: In den beiden niederwertigen Bytes ist der ermittelte ungültige Zellen-Index enthalten, in den beiden höherwertigen Bytes steht die Anzahl vorhandener Zellen	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
		1	bei Reason-Code 0 = 1: ungültiger Zellen-Index		
		2	bei Reason-Code 0 = 2: ungültiger Adress-Offset		

		3	bei Reason-Code 0 = 3: in den beiden niederwertigen Bytes ist Adress-Offset enthalten, in den beiden höherwertigen Bytes steht die Länge;		
		4	bei Reason-Code 0 = 4: ungültige Länge (nicht durch 4 teilbar)		
ERRVAL(1027)	Bei einem Speicherbereich im Flash wurde ein ungültiger Blockheader erkannt. Mögliche Ursache(n): • Hardwarefehler (Flash defekt) • Programmiervorgang wurde unterbrochen	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1028)	Bei einem Anmeldeversuch wurde ein ungültiges Passwort angegeben. Fehler wird im SafetyDesigner im Konsolenfenster angezeigt. Mögliche Ursache(n): • Tippfehler • Hackerangriff	immer 0	immer 1	Das Passwort muss erneut eingegeben werden.	Weiterhin normaler Betrieb
ERRVAL(1029)	In einem SSDO Frame ist ein ungültiger Parameter vorhanden. Mögliche Ursache(n):	0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
		1	immer 0		
		2	immer 0		
		3	immer 0		

	• Softwarefehler	4	bei Reason-Code 0 = 4: die niederwertigen 2 Bytes enthalten die Größe des übergebenen Buffers, die höherwertigen 2 Bytes die max. Größe		
ERRVAL(1030)	In einem SSDO Frame fehlt ein Parameter. Mögliche Ursache(n): • Softwarefehler	wird nur in der Firmware für den Hardwaretest verwendet		Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1031)	Interner Fehler bei der Verarbeitung der SSDOs. Mögliche Ursache(n): • Softwarefehler	Länge des zu schreibenden SSDOs	maximale Länge eines SSDOs	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1032)	Das SSDO Paket enthält ein ungültiges Befehlsbyte. Mögliche Ursache(n): • Softwarefehler	ungültiges Kommando	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1033)	Bei dem Versuch zur Passwortänderung wurde ein ungültiges neues Passwort angegeben. Mögliche Ursache(n): • Softwarefehler • Fehlerhafter SafetyDesigner	immer 0	immer 0	Wird ein falsches Passwort eingegeben, so kommt im SafetyDesigner eine Warnung. Kommt der Fehler 33, so handelt es sich um einen internen Fehler des Betriebssystems. Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1034)	Das SSDO Paket enthält eine ungültige virtuelle Adresse. Mögliche Ursache(n): • Softwarefehler	Identifizierung der Fehlerursache mögliche Werte: 0 bis 1	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1035)	Bei der Verarbeitung der SSDOs wurde festgestellt, dass ein interner Buffer zu klein für die angeforderte Datenmenge ist. Mögliche Ursache(n): • Softwarefehler • fehlerhafter SafetyDesigner	Identifizierung der Fehlerursache mögliche Werte: 0 bis 1	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1036)	Beim Selbsttest des Safety-Interface-Controllers wurde ein Fehler festgestellt. Mögliche Ursache(n): • Hardwarefehler	Identifizierung der Fehlerursache mögliche Werte: 0 Testnachricht konnte nicht versendet werden 1 es wurde keine Antwort auf die Testnachricht empfangen 2 Daten der empfangenen Testnachricht sind falsch	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1037)	Die remanenten Variablen sind inkonsistent. Mögliche Ursache(n): • Hardwarefehler • Softwarefehler	0 im POST wurde festgestellt, dass die Checksumme der remanenten Variablen im EEPROM nicht korrekt ist 1 Fehler in der Konsistenz der remanenten Variablen während der zyklischen Verarbeitung festgestellt	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1038)	Es ist ein Watchdog Fehler aufgetreten Mögliche Ursache(n): • Softwarefehler	Adresse des Codes	bei einer Exception außerhalb des FSB Aufrufs: - immer 0 bei einer Exception während des FSB Aufrufs: - FSB-ID in den unteren 2 Bytes - Objekt-Index in den oberen 2 Bytes	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1039)	Die Version des Bootloaders ist falsch Mögliche Ursache(n): • falsche Firmware	vorhandene Version des Bootloaders	minimal benötigte Version des Bootloaders	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1040)	Beim Zugriff auf den internen IO-Bus ist ein Fehler aufgetreten. Mögliche Ursache(n): • Hardwarefehler • Modul wurde abgesteckt	0 Fehler beim Lesezugriff eines Bytes 1 Fehler beim Lesezugriff eines 2 Byte Werts	bei Reason-Code 0 zwischen 0 und 1: Byte 0 und 1 sind die Adresse des Fehlers Byte 2 und 3 sind die Adresse des Moduls; teilt man diesen Wert durch 0x400 erhält man die Position des Moduls (beginnend bei 0)	Wenn ein Modul abgesteckt wurde, das Modul anstecken und neu starten Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
		2 Fehler beim Schreibzugriff eines Bytes 3 Fehler beim Schreibzugriff eines 2 Byte Werts	bei Reason-Code 0 zwischen 2 und 3: Byte 0 und 1 sind die Adresse des Fehlers Byte 2 und 3 ist der zu schreibende Wert		

		4 unterschiedliche Werte der Controller für die Modul-ID			
		5 Zeitfehler beim Warten auf das Grant des SPI-Masters 6 Zeitfehler beim Warten auf das Ready des SPI-Masters 7 falsche Länge des SPI-Flash 8 falsche CRC des SPI-Flash	bei Reason-Code 0 zwischen 5 und 8: Position des Moduls bei welchen der Fehler aufgetreten ist (beginnend bei 0)		
		9 unterschiedliche Sicherheitsnummer in beiden Kontrollern			
		10 keine eindeutigen Sicherheitsnummern in den Erweiterungsmodulen	bei Reason-Code 0 = 10: Wert der Sicherheitsnummer, welche doppelt ist		
		11 beim Ermitteln der Seriennummern liefern beide Kontroller unterschiedliche Werte	bei Reason-Code 0 = 11: Position des Moduls bei welchen der Fehler aufgetreten ist (beginnend bei 0)		
		12 unterschiedliche Anzahl von Erweiterungsmodulen in beiden Kontrollern	bei Reason-Code 0 = 12: Byte 0: Anzahl der erkannten IO-Module am Kontroller Byte 1: Anzahl der erkannten IO-Module am anderen Kontroller		

		13 fehlende Sicherheitsnummer in einem Erweiterungsmodul	bei Reason-Code 0 = 13: Position des Moduls bei welchen der Fehler aufgetreten ist (beginnend bei 0)		
ERRVAL(1041)	Die Werte der zurückgelesenen Ausgänge, welche bereits im Fehler sind, sind nicht auf 0. Mögliche Ursache(n): • Hardwarefehler (z.B. Ausgangstransistor defekt) • externer Fehler (z.B. Kurzschluss) • Softwarefehler	Ausgänge, welche nicht enabled sind (Bit 0 = 1. Ausgang)	Istwert (Bit 0 = 1. Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1042)	Beim Test des OUTRESET-Signals sind nicht alle Ausgänge auf 0 gegangen. Mögliche Ursache(n): • Hardwarefehler (z.B. Ausgangstransistor defekt) • externer Fehler (z.B. Kurzschluss) • Softwarefehler	getestete Ausgänge (Bit 0 = 1. Ausgang)	Istwert (Bit 0 = 1. Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1043)	Ein lokales Erweiterungsmodul ist im Fehlerzustand. Mögliche Ursache(n): • Fehler im Erweiterungsmodul	0 Fehler des Erweiterungsmoduls 1 0 basierende Position des Erweiterungsmoduls	Reason-Code 0 des Erweiterungsmoduls	Erweiterungsmodul tauschen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1044)	Bei einem lokalen Erweiterungsmodul ist in der Init-Phase ein Fehler aufgetreten. Mögliche Ursache(n): • Fehler im Erweiterungsmodul • Falsche Konfiguration	0 Stromwerte des SNC-Moduls können nicht aus dem Modul ausgelesen werden 1 Es sind keine Stromwerte verfügbar, die ins SNC-Modul geschrieben werden sollten 2 Es ist ein SNC-Modul auf einer Slave-Safety-CPU vorhanden. 3 Es ist ein SNC-Modul mit einer nicht unterstützten Versionsnummer vorhanden	0 basierende Position des Erweiterungsmoduls	Stromwerte prüfen, Safety-CPU auf den Master-Modus umstellen; SNC-Modul tauschen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1045)	Das zum Eingang oder Ausgang gehörende Erweiterungsmodul ist nicht vorhanden. Mögliche Ursache(n): • ein optionales Modul ist nicht angeschlossen	0 digitaler Ausgang 1 digitaler Eingang 2 SNC-Modul	immer 0	Optionale Module prüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1046)	Bei der Vergabe einer dynamischen FSoE Slave-Adressen wurde festgestellt, dass keine freien Adressen mehr verfügbar sind. Mögliche Ursache(n): • Konfiguration fehlerhaft	immer 0	immer 0	Konfiguration überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1047)-ERRVAL(1048)	Nicht verwendet				

ERRVAL(1049)	Bei der Prüfung des LOG-Speichers im POST wurde festgestellt, dass beide Sektoren voll sind. Mögliche Ursache(n): • Hardwarefehler • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1050)	Bei der Prüfung des LOG-Speichers im POST wurde festgestellt, dass beide Sektoren Daten enthalten aber nicht voll sind. Mögliche Ursache(n): • Hardwarefehler • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1051)	Die Meldungen im LOG-Speicher sind nicht zusammenhängend (Löcher im LOG-Speicher). Mögliche Ursache(n): • Programmfehler	Startadresse des ersten gefundenen leeren Eintrags im LOG-Speicher	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1052)	Die Information über die gespeicherten Sicherheitsnummern der entfernten Module ist inkonsistent. Mögliche Ursache(n): • Programmfehler	immer 0xFFFFFFFF	immer 0xFFFFFFFF	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1053)	Der SSDO Befehl kann im aktuellen Zustand nicht ausgeführt werden. Mögliche Ursache(n): • Modul führt den Bootcode aus	immer 0	immer 0	Neu starten Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1054)	Es wurde versucht auf einen Speicherbereich zuzugreifen (Flash oder SD-Karte) auf dem kein Zugriff möglich oder erlaubt ist. Mögliche Ursache(n): • Programmfehler • Fehler im SafetyDesigner	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1055)	Beim Flash programmieren ist ein Fehler aufgetreten. Mögliche Ursache(n): • Hardwarefehler	dient zur Identifizierung der Fehlerursache	dient zur Identifizierung der Fehlerursache	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1056)	Beim Status-Wechsel im STM Modul wurde festgestellt, dass bereits ein Wechsel aktiv ist. Mögliche Ursache(n): • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1057)	Beim Aktivieren des Timers im STM Modul wurde festgestellt, dass bereits ein Timer aktiv ist. Mögliche Ursache(n): • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1058)	Es sind bei einer Abfrage im STM Modul nicht alle benötigten Flags gesetzt. Mögliche Ursache(n): • Programmfehler	Flags die gesetzt sein sollten	Flags die aktuell gesetzt sind	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1059)	Der Diagnosecode bzw. der Login-Status am Funktionsblock HGW-Login hat einen falschen Wert Mögliche Ursache(n): • Fehler im Funktionsblock	dient zur Identifizierung der Fehlerursache 1 Diagnosecode hat einen ungültigen Wert angenommen 2 Login-Status hat einen ungültigen Wert angenommen	Wert vom Diagnose-Code bzw. Login-Status	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1060)	Es wurde versucht die zyklischen CAN-Nachrichten zu unterdrücken, während das nicht möglich ist. Mögliche Ursache(n): • Konfigurationsfehler	1 Es ist ein Modul projektiert, dass die CAN-Nachrichten benötigt (zb SIB oder HBG) 2 Es wurde ein Modul am CAN erkannt, dass die CAN-Nachrichten benötigt (zb SIB oder HBG)	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1061)-ERRVAL(1066)	Nicht verwendet				
ERRVAL(1067)	Die FSoE-Verbindung zwischen HGW Modul und Sicherheits-CPU ist unkontrolliert abgerissen. Mögliche Ursache(n): • Verbindung gestört • Entfernung zwischen den Modulen zu groß	immer 0	immer 0	Fehlerquittierung und erneute Anmeldung	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1068)	Ungültiger Parameterwert bei einem Funktionsaufruf. Mögliche Ursache(n): • Programmfehler	dient zur Identifizierung der Fehlerursache mögliche Werte: 0 bis 95	dient zur Identifizierung der Fehlerursache	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1069)	Der Platz im SPDO für die zu übertragenden Sicherheitswerte ist zu klein. Mögliche Ursache(n): • Softwarefehler	Index des höchstwertigen Bytes der zu übertragenden Sicherheitswerte.	maximale Größe der zu übertragenden Sicherheitswerte.	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1070)	Kreuzkommunikation funktioniert nicht (Übertragungsfehler). Mögliche Ursache(n): • Hardwarefehler	1 Fehler beim Selbsttest im Post 2 Fehler im UART erkannt	Fehlerflags	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1071)	Nicht verwendet				
ERRVAL(1072)	Es wurde versucht, eine Division durch 0 auszuführen. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1073)	Über die Kreuzkommunikation wurde ein unerwarteter Wert empfangen Mögliche Ursache(n): • Softwarefehler	empfangener Wert	dient zur Identifizierung der Fehlerursache	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1074)	Die logische Programmlaufüberwachung hat festgestellt, dass ein im Op/OpTemp Modus auszuführender Programmteil nicht ausgeführt wurde. Mögliche Ursache(n): • Softwarefehler	ID des Programmteils	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1075)	Die in den beiden Controllern eingelesenen Werte für die lokalen Eingänge weisen für eine unzulässig lange Zeit unterschiedliche Werte auf. Mögliche Ursache(n): • Hardwarefehler • Eingangsschaltung	Bitmaske mit den Eingängen des eigenen Controllers	Bitmaske mit den Eingängen des anderen Controllers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1076)	Kreuzkommunikation funktioniert nicht (Timeout). Mögliche Ursache(n): • Hardwarefehler • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1077)	Der Inhalt einer STDO Antwort ist in beiden Controllern unterschiedlich. Mögliche Ursache(n): • Softwarefehler	0 oder 1, je nach Art des Fehlers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1078)	Die Laufzeitüberwachung wurde unerlaubterweise in einem Operational-Laufzeitzustand deaktiviert. Mögliche Ursache(n): • Softwarefehler	ID des Aufrufers, von dem die Laufzeitüberwachung deaktiviert wurde.	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1079)-ERRVAL(1081)	Kreuzkommunikation funktioniert nicht (unerwarteter Wert empfangen). Mögliche Ursache(n): • Hardwarefehler • Softwarefehler	über die Kreuzkommunikation empfangener Wert	erwarteter Wert (= Soll-Wert)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1082)	Das berechnete Ausgangsabbild ist in den beiden Controllern unterschiedlich. Mögliche Ursache(n): • Softwarefehler • Hardwarefehler	Index der Zelle im Applikationsspeicher, deren Inhalt nicht mit der des anderen Controllers übereinstimmt.	Inhalt der im Reason-Code 0 angeführten Zelle	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1083)	Der andere Controller ist bei der Kreuzkommunikation nicht mehr synchron. Es handelt sich hier noch um keinen Fehler, der den sicheren Zustand herbeiführt. Als Reaktion auf diesen Fehler synchronisieren sich die Controller neu, tauschen Informationen aus und erst dann wird entschieden, ob der sichere Zustand herbeigeführt wird. Mögliche Ursache(n): • ein Controller hat einen Fehler festgestellt, der andere (noch) nicht	immer 0	immer 0	Fehler quittieren, System ev. neu starten Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1084)	Der Inhalt der SD-Karte konnte nicht geladen werden, weil die Konfiguration im Flash nicht vorhanden und auch nicht gelöscht ist. Mögliche Ursache(n): • Anwenderfehler	immer 0	immer 0	Speicher der Safety CPU löschen und nochmals versuchen	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1085)	Die SD-Karte konnte nicht initialisiert werden. Mögliche Ursache(n): • Hardwarefehler	immer 0	immer 0	Andere SD-Karte verwenden Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1086)	Der Inhalt auf der SD-Karte entspricht nicht dem erwarteten Format. Mögliche Ursache(n): • Hardwarefehler • Softwarefehler • Anwenderfehler	immer 0	immer 0	SD-Karte nochmals bespielen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1087)	Die Konfigurationsdaten auf der SD-Karte stimmen nicht mit denen im Flash überein. Mögliche Ursache(n): • Anwenderfehler	CRC der Konfigurationsdaten auf der SD-Karte	CRC der Konfigurationsdaten im Flash	Entweder ist die Konfiguration im Flash zu löschen, falls die Konfiguration der SD-Karte übernommen werden soll. Soll jedoch die Konfiguration von der SD-Karte übernommen werden, so ist die Konfiguration auf dem Flash zu löschen und das System bei eingesteckter SD-Karte neu zu starten.	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1088)	Die SD-Karte wurde eingesteckt, während das Modul eingeschaltet war und sich nicht im Service Mode befand. Beim Start der Applikation ist ein Dongle angesteckt, der Service-Mode kann nicht verlassen werden. Mögliche Ursache(n): • Anwenderfehler • Dongle angesteckt	immer 0	immer 0	SD-Karte wieder entnehmen, Fehler quittieren und in den Service Mode wechseln, dann SD-Karte einstecken. Dongle entfernen, Fehler quittieren und erneut starten.	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1089)	Interner Fehler in einer Ablauftabelle.	dient zur Identifizierung der Fehlerursache Mögliche Werte: 0 bis 1	ungültiger Status bzw. Index	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1090)	Der gemessene Wert des Referenzclocks vom FPGA (REFCLK) ist zu klein. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Hardwarefehler • CPU • FPGA	Anzahl gemessener Flanken	minimale Anzahl der zu messenden Flanken	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1091)	Der gemessene Wert des Referenzclocks vom FPGA (REFCLK) ist zu groß. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Hardwarefehler • CPU • FPGA	Anzahl gemessener Flanken	maximale Anzahl der zu messenden Flanken	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1092)	Beim Warten auf die SSDO Response ist eine Zeitüberschreitung aufgetreten. Mögliche Ursache(n): • Laufzeit über den Bus • Verarbeitungszeit im Zielmodul	immer 0	immer 0	Laufzeiten verringern	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1093)	Der andere Controller hat einen Fehler festgestellt. Mögliche Ursache(n): • Ursache gemäß Fehlercode des anderen Controllers	Fehlercode des anderen Controllers	immer 0	Fehlercode des anderen Controllers prüfen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1094)	Der Konfigurationszustand des anderen Controllers stimmt mit dem eigenen nicht überein. Mögliche Ursache(n): • Modul wurde während des Konfigurierens abgeschaltet	Konfigurationsstatus des eigenen Controllers	Konfigurationsstatus des anderen Controllers	Modul neu konfigurieren	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL1095)	Eine Konstante im Applikationsspeicher wurde verändert und stimmt nicht mehr mit dem im Flash gespeicherten Wert überein. Mögliche Ursache(n): • Hardwarefehler (defektes Flash, defektes RAM) • Softwarefehler	Index der Speicherzelle der fehlerhaften Konstante im Applikationsspeicher	Index der Konstante im Flash	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1096)-ERRVAL(1097)	Nicht verwendet				
ERRVAL(1098)	Die Reaktion auf den internen Test konnte nicht ermittelt werden. Mögliche Ursache(n): • Softwarefehler	Bit-Maske der digitalen Eingänge	0 Fehler bei einem lokalen Eingang 1 Fehler bei einem Safety-Interface-Modul Eingang	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1099)	Beim Eingangstest (interner Test) ist ein Fehler festgestellt worden. Mögliche Ursache(n): • Hardwarefehler	Zustände der digitalen Eingänge	Bit-Maske der digitalen Eingänge	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1100)	Während des externen Tests ist ein interner Test aktiv. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1101)	Die Reaktion auf den externen Test konnte nicht ermittelt werden. Mögliche Ursache(n): • Softwarefehler	Bit-Maske der digitalen Eingänge	0 Fehler bei einem lokalen Eingang 1 Fehler bei einem Safety-Interface-Modul Eingang	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1102)	Externer Test: Bei einem am Takt angeschlossenen Eingang ist der Taktimpuls nicht erkannt worden. Mögliche Ursache(n): • Querschluss	immer 0	immer 0	Verdrahtung des Querschlusses mit der Applikation vergleichen	Error-LED des Sicherheitsmoduls blinkt
ERRVAL(1103)	Externer Test: Bei einem am Takt angeschlossenen Eingang ist der Taktimpuls des anderen Taktausgangs erkannt worden. Mögliche Ursache(n): • Querschluss	immer 0	immer 0	Verdrahtung des Querschlusses mit der Applikation vergleichen	Error-LED des Sicherheitsmoduls blinkt
ERRVAL(1104)	Der Lo-Resolution Timer arbeitet nicht richtig (gemessene Werte sind zu klein). Mögliche Ursache(n): • Hardwarefehler	gemessener Wert des Lo-Resolution Timers	unteres Limit für die Messung	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1105)	Der Lo-Resolution Timer arbeitet nicht richtig (gemessene Werte sind zu groß). Mögliche Ursache(n): • Hardwarefehler	gemessener Wert des Lo-Resolution Timers	oberes Limit für die Messung	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1106)	Der Millisekunden-Timer arbeitet nicht richtig (gemessene Werte sind zu klein). Mögliche Ursache(n): • Hardwarefehler • Softwarefehler	gemessener Wert des Millisekunden-Timers	unteres Limit für die Messung	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1107)	Der Millisekunden-Timer arbeitet nicht richtig (gemessene Werte sind zu groß). Mögliche Ursache(n): • Hardwarefehler • Softwarefehler	gemessener Wert des Millisekunden-Timers	oberes Limit für die Messung	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1108)	Nicht verwendet				
ERRVAL(1109)	Das Format des Info-Sektors im Flash stimmt nicht. Mögliche Ursache(n): • Modul wurde noch nie initialisiert (mit dem Clear-All Befehl) • Hardwarefehler im Flash	immer 0	immer 0	Modul konfigurieren Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERVAL(1110)-ERRVAL(1114)	Das Format der Konfigurationsdaten im Flash stimmt nicht. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	Detailinfo zur Fehlerursache	Detailinfo zur Fehlerursache	Modul konfigurieren Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1115)	Das Format der Konfigurationsdaten im Flash stimmt nicht. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • in den Konfigurationsdaten ist ein nicht unterstütztes Erweiterungsmodul angegeben • Hardwarefehler im Flash	1 nicht unterstütztes Erweiterungsmodul 2-39 Fehlerinformation	bei Reason-Code 0 = 1: Typ des Moduls bei Reason-Code 0 = 2-32: Detailinformation	Modul konfigurieren, prüfen ob ein nicht unterstütztes Erweiterungsmodul angesteckt ist und ggf. eine SCP mit aktueller Firmware verwenden; richtige Parameterversion beim SSI-Modul einstellen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1116)-ERRVAL(1128)	Das Format der Konfigurationsdaten im Flash stimmt nicht. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	Detailinfo zur Fehlerursache	Detailinfo zur Fehlerursache	Modul konfigurieren Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1129)	Bei der Kommunikation mit dem FPGA ist ein Fehler aufgetreten. Mögliche Ursache(n): • Hardwarefehler (FPGA)	Wert, der genauere Informationen über den Fehler liefert 0 SPI Zugriff 0 fehlgeschlagen 1 SPI Zugriff 1 fehlgeschlagen 2 DMA funktioniert nicht mehr 3 ungültige FPGA-Version 4 FPGA nicht bereit	Wert, der genauere Informationen über den Fehler liefert	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1130)	Bei einem Funktionsaufruf wurde ein Buffer als Parameter übergeben. Die Größe des Buffers ist allerdings zu groß. Mögliche Ursache(n): • Programmfehler	tatsächliche Größe des Buffers	maximale Größe des Buffers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1131)	Für den SSDO Befehl wurde ein falscher Frametyp verwendet. Mögliche Ursache(n): • Fehler im Safety-Tool	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1132)	Bei den Modul-Sicherheitsnummern der entfernten Module ist ein Wert doppelt vorhanden. Mögliche Ursache(n): • Beim Ermitteln der Modul-Sicherheitsnummer anhand des Topologiepfads ist ein Fehler aufgetreten	Reason-Code 0: < 1024: Index des Moduls in der Tabelle der entfernten Module Reason-Code 0: = 1024: Eine Sicherheitsnummer eines entfernten Moduls ist gleich wie die eigene Sicherheitsnummer Reason-Code 0: = 1025: Bei Abfrage der eigenen Sicherheitsnummer wurde nicht die eigene Sicherheitsnummer empfangen	doppelt vorhandene Modul-Sicherheitsnummer	- Applikation nochmals starten - Alle Sicherheitsnummern auf Eindeutigkeit prüfen	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1133)	Der Microcontroller befindet sich nicht im korrekten Prozessor-Modus. Entweder sind die Flags für den Prozessor-Modus oder für die Aktivierung der Interrupts im Programm Status-Register nicht korrekt gesetzt, oder es wird der falsche Stack verwendet. Mögliche Ursache(n): • Der Wechsel des Prozessor-Modus funktioniert nicht korrekt (aufgrund Hardware- oder Software-Fehler)	gesetzte Flags im Programm Status-Register oder der Wert des Stack-Pointers	Soll-Wert für die Flags im Programm Status-Register oder untere bzw. obere Grenze des zu verwendenden Stack-Bereichs	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1134)	Das berechnete Ausgangsabbild ist in den beiden Controllern unterschiedlich.	Zustände der lokalen Ausgänge des eigenen Controllers	Zustände der lokalen Ausgänge des anderen Controllers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1135)	Die Versorgungsspannung eines Erweiterungsmoduls ist nicht in Ordnung. Mögliche Ursache(n): • Externe Spannungsversorgung nicht angeschlossen • Hardwarefehler	0 wenn die Versorgungsspannung des CPU Moduls nicht in Ordnung ist 1 wenn bei der Watchdogprüfung ein Fehler festgestellt wurde, welcher wegen einer fehlenden Versorgungsspannung aufgetreten ist	Modulposition (0 = 1. Erweiterungsmodul)	Es ist sicherzustellen, dass die externe Spannungsversorgung der Taktausgänge bei Sicherheitsmodulen mit digitalen Eingängen und die Versorgungsspannung der Ausgänge für Sicherheitsmodule mit digitalen Ausgängen korrekt ist. Nach Anlegen der richtigen Spannung kann der Fehler mit „Quit Error“ beziehungsweise durch einen Wiederanlauf behoben werden.	Error-LED des Sicherheitsmoduls leuchtet rot DCOK-LED leuchtet nicht.
ERRVAL(1136)	Die boolsche Darstellung eines Ausgangs hat einen ungültigen Wert. Mögliche Ursache(n): • Softwarefehler (Speicher wurde an unerlaubter Stelle überschrieben) • Hardwarefehler (RAM defekt)	0x00000000 bedeutet, dass der Fehler beim Dekodieren einer Zelle im Applikationsspeicher entdeckt wurde. 0xFFFFFFFF bedeutet, dass der Fehler beim Kodieren des SAFEBOOL-Wertes für den SPDO-Frame entdeckt wurde.	ungültiger Wert	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1137)	Die Werte der zurückgelesenen Ausgänge stimmen mit den Werten der Sollwerte der Ausgänge nicht überein. Mögliche Ursache(n): • Hardwarefehler (z.B. Ausgangstransistor defekt) • externer Fehler (z.B. Kurzschluss, Versorgungsspannung der Ausgänge fehlt) • Softwarefehler	Sollwerte (Bit 0 = 1. Ausgang)	Istwerte (Bit 0 = 1. Ausgang)	Spannungsversorgung prüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1138)	Beim Watchdog-Test ist ein Fehler aufgetreten. Mögliche Ursache(n): • Hardwarefehler	Bit-Maske zur Identifizierung der Testschritte, bei denen der Fehler entdeckt wurde	aktueller Testschritt	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1139)-ERRVAL(1141)	In der Konfiguration sind beim COPY Befehl ungültige Parameter angegeben. Mögliche Ursache(n): • Es wurde eine fehlerhafte Konfiguration eingespielt • Flash defekt	Index der Quelle bzw. des Ziels	maximale Anzahl vorhandener Zellen bzw. unteres oder oberes Index-Limit	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1142)	Nach dem Einschalten der oberen Ausgangshalbleiter (HSS) ist mind. ein Ausgang auf 1 gegangen, obwohl keiner der unteren Ausgangshalbleiter (FET) eingeschaltet war. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Ausgangshalbleiter (FET) defekt	Sollwert (Bit 0 = 1. Ausgang) immer 0	Istwert, betroffene Ausgänge (Bit 0 = 1. Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1143)	Nach dem Abschalten des HSS Ausgangshalbleiters ist keiner der zuvor gesetzten Ausgänge auf 0 gegangen. Mögliche Ursache(n): • Ausgangshalbleiter (HSS) defekt • unzulässig große kapazitive Last	Werte der Ausgänge nach dem Abschalten des HSS (Bit 0 = 1. Ausgang)	zuvor gesetzte Ausgänge (Bit 0 = 1. Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls blinkt
ERRVAL(1144)	Nach dem Abschalten des FET Ausgangshalbleiters ist der zugehörige Ausgang nicht auf 0 gegangen. Mögliche Ursache(n): • Ausgangshalbleiter (FET) defekt • unzulässig große kapazitive Last	betroffener Ausgang (Bit 0 = 1. Ausgang)	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls blinkt

ERRVAL(1145)	Nach dem Abschalten des FET Ausgangshalbleiters hat ein Ausgang, der nicht über diesen FET angeschlossen ist, seinen Wert geändert. Mögliche Ursache(n): • interner Querschluss im Ausgangskreis	Status der Ausgänge (Bit 0 = 1. Ausgang)	Soll-Status der Ausgänge (Bit 0 = 1. Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls blinkt
ERRVAL(1146)	Die zyklische Verarbeitung ist innerhalb der erlaubten Zeit nicht fertig geworden. Mögliche Ursache(n): • fehlerhafte Applikation	Caller-ID mit der zuletzt die Runtime-Triggerung erfolgte	Code-Adresse, an der nach Beendigung der Interrupt-Funktion fortgesetzt wird	Zykluszeit der SafetyCPU erhöhen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1147)	Die logische Programmlaufüberwachung hat festgestellt, dass ein Programmteil unzulässig lange nicht mehr aufgerufen wurde. Mögliche Ursache(n): • Softwarefehler	SCP010: <100 Index des Programmteils >=100 ID des Programmteils, wo der Fehler festgestellt wurde 100-109 SCP011 & SCP111: <1000 Index des Programmteils >=1000 ID des Programmteils, wo der Fehler festgestellt wurde 1000-1009	SCP010: Reason-Code < 100 einzuhaltende Zeit des Programmteils SCP011 & SCP111: Reason-Code 0: < 1000: einzuhaltende Zeit des Programmteils	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1148)	Die Rücklesung der HS-Transistoren ist nicht in Ordnung. Mögliche Ursache(n): • Hardwarefehler • keine Versorgungsspannung	Position des Erweiterungsmoduls (0 = 1. Modul)	Wert des HS-Signals	Spannungsversorgung prüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1149)	Ein SSI Erweiterungsmodul hat bei einem Eingang einen fehlerhaft kodierten Wert erkannt. Mögliche Ursache(n): • Hardwarefehler	Modulposition und fehlerhaft kodierter Wert	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1150)	Der Eingangswert ist unzulässig lange nicht mehr aktualisiert worden. Mögliche Ursache(n): • Fehler in der Eingangshardware • ständige Änderung des Eingangssignals	betroffener Eingang (Bit 0 = 1. Eingang)	maximales Alter	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1151)	Die reservierten Stackbereiche wurden überschrieben untere Grenze). Mögliche Ursache(n): • Softwarefehler • Stack-Reserve zu klein dimensioniert	ID des betroffenen Stackbereichs	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1152)	Die reservierten Stackbereiche wurden überschrieben (obere Grenze). Mögliche Ursache(n): • Softwarefehler • Stack-Reserve zu klein dimensioniert	ID des betroffenen Stackbereichs	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1153)	Das berechnete Ausgangsabbild ist in den Controllern unterschiedlich. Mögliche Ursache(n): • Softwarefehler	CRC des Sende SPDO Frames und des App-Speichers des eigenen Controllers	CRC des Sende SPDO Frames und des App-Speichers des anderen Controllers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1154)	Die Information über die gespeicherten Sicherheitsnummern der entfernten Module ist inkonsistent. Mögliche Ursache(n): • Programmfehler	Index des gesuchten Moduls	Anzahl der Elemente in der Tabelle der entfernten Module	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1155)	Der CPU-Test hat einen Fehler festgestellt. Mögliche Ursache(n): • CPU-Fehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1156)	Es wurde vom Geber (SSI-Geber, Inkrementalgeber) kein Geberwert eingelesen, da vom CPLD kein Einlesevorgang gestartet wurde. Mögliche Ursache(n): • Standard-Applikation wurde nicht gestartet • Hardwareklasse für das SSI-Modul ist nicht platziert • Hardwareklasse für das SNC-Modul ist nicht platziert	Immer 0	Immer 0	Applikation neu starten Überprüfung, ob der Hardwareaufbau mit der Applikation übereinstimmt; Applikation entsprechend umbauen.	

ERRVAL(1157)	Der maximale Jitter zwischen zwei Einlesevorgängen des Geberwertes wurde nicht eingehalten. Mögliche Ursache(n): • Ungültige Konfiguration durch die Hardwareklassen • Hardwarefehler	immer 0	immer 0	Überprüfung der Versionen von FPGA und Hardwareklasse	
ERRVAL(1158)	Das CPLD für den Geber meldete einen Fehler, wodurch kein Geberwert eingelesen werden konnte. Mögliche Ursache(n): • Einstellungen für den Geber sind nicht korrekt • Geber ist nicht angeschlossen • Geber wird nicht unterstützt • Geber ist defekt	immer 0	immer 0	Überprüfung, ob die Parameter für die Geber aus deren Datenblatt korrekt in der Standard-Applikation, sowie in der sicheren Applikation übernommen wurden. Überprüfung der Kabelverbindung zu den Gebern. Überprüfen, ob der verwendete Geber gemäß Datenblatt des SSI 021 unterstützt wird. Prüfen, ob ein defekter Geber vorliegt.	

ERRVAL(1159)	Die vom CPLD eingelesenen Daten sind ungültig. Mögliche Ursache(n): • Einstellungen für den Geber sind nicht korrekt • Die Einstellungen für den Geber wurden zur Laufzeit geändert. • Geber ist defekt	immer 0	immer 0	Überprüfung, ob die Parameter für die Geber aus deren Datenblatt korrekt in der Standard-Applikation, sowie in der sicheren Applikation übernommen wurden. Überprüfung der Kabelverbindung zu den Gebern. Prüfen, ob ein defekter Geber vorliegt.	
ERRVAL(1160)	Die Versorgungsspannung des Gebers ist nicht in Ordnung. Mögliche Ursache(n): • Versorgungsspannung für die Geber ist nicht vorhanden • Hardwarefehler	immer 0	immer 0	Überprüfung der Verdrahtung der Versorgungsspannung für die Geber	
ERRVAL(1161)	Es liegt ein Fehler in der Konfiguration für das Modul vor. Mögliche Ursache(n): • Geber angeschlossen, obwohl dieser laut Safety-Applikation nicht verwendet wird	immer 0	immer 0	Prüfen, ob für die angeschlossenen Geber in der Safety-Applikation die Parameter korrekt gesetzt wurden	

ERRVAL(1162)	Beim Test der Signale des Inkrementalgebers wurde durch den ersten RS422-Treiber ein Signalfehler detektiert. Mögliche Ursache(n): • Querschluss der Signalleitungen • Kabelbruch • Kurzschluss	immer 0	immer 0	Verdrahtung des Gebers, sowie den Geber überprüfen	Safe DATA OK LED des betreffenden Geber-Kanals leuchtet nicht Geberstatus LED des betreffenden Gebers blinkt
ERRVAL(1163)	Beim Test der Signale des Inkrementalgebers wurde durch den zweiten RS422-Treiber ein Signalfehler detektiert. Mögliche Ursache(n): • Querschluss der Signalleitungen • Kabelbruch • Kurzschluss	immer 0	immer 0	Verdrahtung des Gebers, sowie den Geber überprüfen	Safe DATA OK LED des betreffenden Geber-Kanals leuchtet nicht Geberstatus LED des betreffenden Gebers blinkt
ERRVAL(1164)	Beim Test der Signale der Z-Spur des Inkrementalgebers wurde ein Signalfehler erkannt. Mögliche Ursache(n): • Querschluss der Signalleitungen • Kabelbruch • Kurzschluss	immer 0	immer 0	Verdrahtung des Gebers, sowie den Geber überprüfen	Safe DATA OK LED des betreffenden Geber-Kanals leuchtet nicht Geberstatus LED des betreffenden Gebers blinkt

ERRVAL(1165)	Beim Test der Signale der Z-Spur des Inkrementalgebers wurde erkannt, dass die Signalleitungen Z+ und Z- vertauscht wurden. Mögliche Ursache(n): • Vertausch der Signalleitungen Z+ und Z-	immer 0	immer 0	Verdrahtung des Gebers überprüfen	Safe DATA OK LED des betreffenden Geber-Kanals leuchtet nicht Geberstatus LED des betreffenden Gebers blinkt
ERRVAL(1166)	Es wurde kein Z-Impuls erkannt, obwohl aufgrund der Bewegung ein Z-Impuls aufgetreten sein müsste. Mögliche Ursache(n): • eingestellte Geber-Auflösung stimmt nicht mit tatsächlicher Auflösung des Gebers überein • Geber defekt	immer 0	immer 0		Safe DATA OK LED des betreffenden Geber-Kanals leuchtet nicht
ERRVAL(1167)	Es wurden zwischen zwei Z-Impulsen zu wenig Flanken auf der A- und B-Spur gezählt. Mögliche Ursache(n): • eingestellte Geber-Auflösung stimmt nicht mit tatsächlicher Auflösung des Gebers überein • Geber defekt	immer 0	immer 0		Safe DATA OK LED des betreffenden Geber-Kanals leuchtet nicht

ERRVAL(1168)-ERRVAL(1171)	Ein Eingang oder Ausgang eines Erweiterungsmoduls ist im Fehlerzustand. Mögliche Ursache(n): • Fehler im Erweiterungsmodul	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1172)	Nicht verwendet				
ERRVAL(1173)	Die Werte der zurückgelesenen Ausgänge stimmen nicht mit den Sollwerten überein. Der Sollwert ist 1, der Istwert ist 0. Mögliche Ursache(n): • Hardwarefehler (z.B. Ausgangstransistor defekt) • externer Fehler (z.B. Kurzschluss, Versorgungsspannung der Ausgänge fehlt) • Softwarefehler	immer 0	immer 0	Spannungsversorgung prüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	LED des sicheren Ausgangs blinkt
ERRVAL(1174)	Die Werte der zurückgelesenen Ausgänge stimmen nicht mit den Sollwerten überein. Der Sollwert ist 0, der Istwert ist 1. Mögliche Ursache(n): • Hardwarefehler (z.B. Ausgangstransistor defekt) • externer Fehler (z.B. Kurzschluss, Versorgungsspannung der Ausgänge fehlt) • Softwarefehler	immer 0	immer 0	Spannungsversorgung prüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	LED des sicheren Ausgangs blinkt

ERRVAL(1175)	Die Werte der zurückgelesenen Ausgänge stimmen nicht mit den Sollwerten überein. Mögliche Ursache(n): • Hardwarefehler (z.B. Ausgangstransistor defekt) • externer Fehler (z.B. Kurzschluss, Versorgungsspannung der Ausgänge fehlt) • Softwarefehler	immer 0	immer 0	Spannungsversorgung prüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	LED des sicheren Ausgangs blinkt
ERRVAL(1176)	Das Firmware-Update für ein lokales Erweiterungsmodul ist fehlgeschlagen. Mögliche Ursache(n): • falsches Updatefile • Flashen des Images im Erweiterungsmodul aufgrund eines Hardwaredefekts nicht möglich • Fehler im Erweiterungsmodul • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1177)-ERRVAL(1180)	Nicht verwendet				
ERRVAL(1181)	Der sichere Messbereich des Eingangs wurde unterschritten. Mögliche Ursache(n): • Hardwarefehler • Verdrahtungsfehler	immer 0	immer 0	Verdrahtung überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1182)	Der sichere Messbereich des Eingangs wurde überschritten. Mögliche Ursache(n): • Hardwarefehler • Verdrahtungsfehler	immer 0	immer 0	Verdrahtung überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1183)	Die Toleranz des Endwertes zwischen den Controllern würde überschritten. Mögliche Ursache(n): • Hardwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1184)-ERRVAL(1188)	Nicht verwendet				
ERRVAL(1189)	Der sichere Messbereich des Eingangs wurde unterschritten. Fehler wird automatisch quittiert, wenn der Messwert wieder gültig. Mögliche Ursache(n): • Hardwarefehler • Verdrahtungsfehler	immer 0	immer 0	Verdrahtung überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1190)	Der sichere Messbereich des Eingangs wurde überschritten. Fehler wird automatisch quittiert, wenn der Messwert wieder gültig. Mögliche Ursache(n): • Hardwarefehler • Verdrahtungsfehler	immer 0	immer 0	Verdrahtung überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1191)-ERRVAL(1196)	Nicht verwendet				

ERRVAL(1197)	Es ist eine falsche CRC2 in der Konfiguration. Der Status des Moduls kann nicht auf Konfiguriert geändert werden. Mögliche Ursache(n): • Hardwarefehler • falsche Konfiguration	immer 0	immer 0	Konfiguration auf Gültigkeit prüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1198)	Der interne Zähler für die Zykluszeit arbeitet falsch. Mögliche Ursache(n): • Softwarefehler	letzte Zeitdifferenz	maximale Zeitdifferenz	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1199)	Der entfernte sichere Eingangswert hat das maximale Alter überschritten. Mögliche Ursache(n): • Bus-Übertragungsfehler • Fehler in der Hardware des entfernten Moduls • Softwarefehler im entfernten Modul	immer 0	immer 0	Es ist zu überprüfen, ob die Standardkommunikation zu jedem benötigten Sicherheitsmodul intakt ist. Zudem ist sicherzustellen, dass sich kein benötigtes Sicherheitsmodul im Fehlerzustand befindet. Außerdem kann es sein, dass die maximale Transmission Time zu niedrig konfiguriert wurde. Diese Punkte sind zu überprüfen. Wurde der Fehler behoben, so kann mit einem Quit Error bzw. einem Neustart des Systems der Fehler aufgehoben werden.	Error-LED des Sicherheitsmoduls blinkt
ERRVAL(1200)	Nicht verwendet				

ERRVAL(1201)-ERRVAL(1205)	Es ist eine unerwartete Exception aufgetreten. Mögliche Ursache(n): • Softwarefehler	Adresse des unterbrochenen Codes	bei einer Exception außerhalb des FSB-Aufrufs: - immer 0 bei einer Exception während des FSB-Aufrufs: - FSB-ID in den unteren zwei Bytes - Objekt-Index in den oberen zwei Bytes	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1206)	Die Systemzeiten der Controller haben eine zu große Abweichung. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Hardwarefehler	ermittelte Drift zwischen den beiden Controller-Systemzeiten	maximal zulässiger Drift	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1207)	Die Modul-Art und Modul-Variante in der Firmware stimmt nicht mit den in den unveränderlichen Modulparametern gespeicherten Werten überein. Mögliche Ursache(n): • falsche Firmware	Modul-Art und -Variante des Bootloaders	Modul-Art und -Variante der Firmware	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des entsprechenden Sicherheitsmoduls leuchtet rot
ERRVAL(1208)-ERRVAL(1209)	Die unveränderlichen Modulparameter sind in den Controllern unterschiedlich. Mögliche Ursache(n): • Hardwarefehler • Flash falsch programmiert	Modulparameter des eigenen Controllers	Modulparameter des anderen Controllers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1210)	Die Firmware Versionen sind in den Controllern unterschiedlich. Mögliche Ursache(n): • falsche Firmware	Firmware-Version im eigenen Controller	Firmware-Version im anderen Controller	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1211)-ERRVAL(1212)	Beim ROM-Test in einem unveränderlichen Flash Bereich wurde ein Fehler festgestellt. Hierbei handelt es sich um einen permanenten Fehler, der nicht quittiert werden kann. Mögliche Ursache(n): • Flash defekt	genauere Informationen über die Ursache des Fehlers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1213)-ERRVAL(1217)	Beim ROM-Test in einem änderbaren Flash Bereich wurde ein Fehler festgestellt. Mögliche Ursache(n): • Flash defekt • Modul wurde während des Flash Programmierens ausgeschaltet	genauere Informationen über die Ursache des Fehlers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1218)	Nach dem Einschalten der unteren Ausgangshalbleiter (FET) ist mindestens ein Ausgang auf 1 gegangen, obwohl keiner der oberen Ausgangshalbleiter (HSS) eingeschaltet war. Mögliche Ursache(n): • Ausgangshalbleiter (HSS) defekt	Sollwert (Bit 0 = 1. Ausgang) immer 0	Istwert, betroffene Ausgänge (Bit 0 = 1. Ausgang)	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1219)	Der Inhalt einer SSDO Antwort ist in beiden Controllern unterschiedlich. Mögliche Ursache(n): • Softwarefehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1220)	Es wurde versucht, das Flash mit einer ungültigen Länge zu beschreiben. Mögliche Ursache(n): • Programmfehler	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1221)	Es wurde versucht aus einem Datenbuffer zu lesen, wobei der Buffer weniger als die angeforderte Datenmenge enthält. Mögliche Ursache(n): • Softwarefehler • fehlerhaftes Safety-Tool (SSDO-Befehl)	Anzahl der Bytes, die aus dem Buffer gelesen werden sollten	Größe des Buffers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1222)	Die Zeit für den Testmodus oder die maximale Idle-Zeit ist abgelaufen.	0 Zeit für den Testmodus ist abgelaufen	immer 0	bei abgelaufenem Testmodus die Konfiguration erneut runterspielen und neu starten	Error-LED des Sicherheitsmoduls leuchtet rot
		1 Zeit für die max. Idle-Zeit ist abgelaufen 2 Die Zeit für die max. Check Config Zeit ist abgelaufen	immer 0	bei abgelaufener Idle-Zeit bzw. Check Config Zeit den Fehler quittieren und erneut starten	

ERRVAL(1223)	Der zeitliche Ablauf beim internen Test stimmt nicht. Es wurde versucht einen Test zu starten, während der vorherige Test noch nicht zu Ende ist. Mögliche Ursache(n): • Softwarefehler	Bit-Maske der Eingänge oder Nummer des fehlerhaften Testschrittes	genauere Informationen über die Ursache des Fehlers	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1224)	Der zeitliche Ablauf beim internen Test stimmt nicht. Es wurde versucht einen Test zu starten, während der vorherige Test noch nicht zu Ende ist. Mögliche Ursache(n): • Softwarefehler	Bit-Maske der zu testenden Eingänge	Bit-Maske der zuvor getesteten Eingänge	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1225)	Der Konfigurations-Zustand kann nicht auf 'konfiguriert' gesetzt werden, da die CRCs der zur Konfiguration gehörenden Bereiche ungültig sind. Mögliche Ursache(n): • es wurde ein Firmware-Update durchgeführt • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1226)	Der Konfigurations-Zustand kann nicht auf 'konfiguriert' gesetzt werden, da die vom Aufrufer übergebene CRC nicht mit der tatsächlichen übereinstimmt. Das Modul wechselt nicht in den Fehlerzustand. Es wird der Fehler im SafetyDesigner im Konsolenfenster angezeigt. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	immer 0	immer 0	Das Sicherheitsmodul muss erneut konfiguriert werden Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1227)	Das Format der Konfigurationsdaten im Flash stimmt nicht. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	tatsächlicher Konfigurationszustand	Soll-Konfigurationszustand	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1228)	Der Konfigurations-Zustand kann nicht auf 'konfiguriert' gesetzt werden, da die Konfiguration gelöscht ist. Mögliche Ursache(n): • Modul wurde falsch konfiguriert • Hardwarefehler im Flash	immer 0	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1229)	Die Konfiguration ist nicht in dem Zustand, in dem das Verified-Flag gesetzt werden kann. Mögliche Ursache(n): • die Konfiguration ist noch nie verteilt worden • die Konfiguration ist im Developer-Mode in die Safety-CPU geschrieben worden	immer 0	immer 0	Programm nicht im Developer Mode starten Programm erneut starten und somit Verteilung auslösen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1230)	Der SSDO Befehl kann aufgrund fehlender Berechtigung nicht ausgeführt werden. Mögliche Ursache(n): • Fehler im SafetyDesigner	immer 0	immer 0	Mit dem SafetyDesigner erneut online gehen und Befehle erneut ausführen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1231)	Beim Onlinegehen konnte keine Session geöffnet werden. Mögliche Ursache(n): • ein anderer SafetyDesigner ist bereits online	immer 0	immer 0	Prüfen, ob mehrere SafetyDesigner online sind, es darf nur ein SafetyDesigner zugreifen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1232)	Die max. Anzahl der entfernten Module ist überschritten worden.	Anzahl der entfernten Module	maximale Anzahl möglicher entfernter Module	Anzahl der entfernten Module prüfen und entsprechend ändern	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1233)	Der in den CFG-Pins kodierte Modultyp passt nicht zur Firmware oder es ist eine nicht unterstützte IO-Erweiterungskarte angesteckt. Mögliche Ursache(n): • falsche Firmware	Bit 31 = 0: CFG-Pins laut Hardware Bit 31 = 1: ID der nicht unterstützten Erweiterungskarte Bit 30 = 1: Vendor-ID der nicht unterstützten Erweiterungskarte Bit 29 = 1: ID des nicht unterstützten Safety-Interface Moduls	Wenn Reason Code 0 Bit31 = 0: CFG-Pins laut Firmware Wenn Reason Code 0 Bit31 = 1: immer 0 Wenn Reason Code 0 Bit30 = 1: Device-ID der nicht unterstützten Erweiterungskarte	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1234)	Der SSDO Befehl kann in diesem Laufzeit-Zustand nicht ausgeführt werden. Mögliche Ursache(n): • Fehler im Safety-Tool	immer 0	immer 0	Mit dem SafetyDesigner erneut Online gehen und Befehle erneut ausführen	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1235)	Die Parameter im Firmware-Header der neuen Firmware passen nicht zu diesem Modul. Mögliche Ursache(n): • falsche Firmware	Parameter in der Firmware	Parameter im Bootcode	Es muss ein Modul verwendet werden, dass eine kompatible Firmware besitzt Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1236)	Beim Zugriff auf die SD-Karte ist ein Fehler aufgetreten. Mögliche Ursache(n): • SD-Karte wurde entfernt • defekte oder inkompatible SD-Karte	Identifikation der Fehlerursache	zuletzt aufgetretener Fehler	Es ist zu überprüfen, ob die SD-Karte entfernt wurde. Wurde die SD-Karte nicht entfernt, so ist die SD-Karte auszutauschen. Der Fehler kann mit dem Herausnehmen der SD-Karte und mit einem Quit Error-Befehl zurückgesetzt werden Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1237)	Schreib-/Lesefehler im Interpretercode der Konfiguration. Bei der Prüfung der Konfiguration wurde einer der folgenden Fehler festgestellt: a) Es wurde versucht eine Zelle zu beschreiben, die bereits von einer anderen Quelle beschrieben worden ist (z.B. wenn zwei COPY Befehle mit demselben Ziel existieren, oder wenn ein COPY Befehl eine nicht beschreibbare Zelle als Ziel angibt). b) Es wurde versucht, von einer nicht lesbaren Zelle zu lesen. Eine Zelle ist nicht lesbar, wenn es keine zugehörige Quelle gibt, von der sie beschrieben wurde (nicht initialisiert), oder wenn sie nicht als Quelle eines COPY Befehls verwendet werden darf (z.B. der Header des Objektspeichers). Mögliche Ursache(n): • es wurde eine fehlerhafte Konfiguration eingespielt • Flash defekt	Index der fehlerhaften Zelle	0 Schreibfehler 1 Lesefehler 2 bei FSoE: ein entfernter Eingang wird von mehr als einer Quelle beschrieben	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1238)	Der POST (PowerOn Selbsttest) ist nicht vollständig abgearbeitet worden. Mögliche Ursache(n): • Softwarefehler	Bit-Maske mit den noch ausstehenden POST-Test-Schritten	immer 0	Während des Hochlauftests wurde ein Fehler festgestellt. Über den SafetyDesigner wird angezeigt, um welchen Fehler es sich handelt. Danach kann der Fehler behoben werden Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1239)	Der auf die SD-Karte zu schreibende Sektorpuffer ist in beiden Controllern unterschiedlich. Mögliche Ursache(n): • Softwarefehler	Nummer des zu schreibenden Sektorpuffers	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1240)	Der Force-Modus wurde unzulässig beendet. Mögliche Ursache(n): • Auftreten eines Session-Timeout bzw. Login-Timeout, z.B. aufgrund einer Unterbrechung der Online-Kommunikation mit dem SafetyDesigner • Wechsel des Login-Levels (z.B. Abmelden) • Schließen der Session im SafetyDesigner	immer 0	immer 0	Bei einer Unterbrechung der Kommunikation zwischen SafetyDesigner und Modul, den Fehler quittieren	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1241)	Das Format der Passwörter auf der SD-Karte stimmt nicht. Mögliche Ursache(n): • SD-Karte defekt • Inhalt wurde nachträglich geändert	immer 0	immer 0	Versuche, die SD-Karte neu zu bespielen. Tritt der Fehler immer noch auf, ist die SD-Karte zu tauschen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1242)	Interner Fehler bei der Verarbeitung der STDOs. Mögliche Ursache(n): • Softwarefehler	Länge des zu schreibenden STDOs	maximale Länge eines STDOs	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1243)	Die Information über eine Modul-Sicherheitsnummer eines entfernten Moduls wird benötigt, ist aber nicht vorhanden bzw. ungültig. Mögliche Ursache(n): • Softwarefehler	Wert der ungültigen Modul-Sicherheitsnummer (0 oder 0xFFFFffff)	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot
ERRVAL(1244)	Im Interpretercode der Konfiguration ist eine FSB-ID angegeben, für die kein entsprechender Code existiert. Mögliche Ursache(n): • Fehler im Safety-Tool	FSB-ID	immer 0	Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED des Sicherheitsmoduls leuchtet rot

ERRVAL(1245)	Ein in den Konfigurationsdaten angegebener Wert ist zu groß. Mögliche Ursache(n): • Eingabe eines zu großen Wertes im SafetyDesigner	gibt an, welcher Parameter zu groß ist 0 Testzeit im temporären Operational Zustand 1 Zykluszeit für die Laufzeitüberwachung 2 maximales Alter eines entfernten Eingangs 3 Filterzeit eines lokalen Eingangs 4 Watchdog-Zeit eines Safety-Interface-Eingangs 5 Optional-Flag eines Safety-Interface-Eingangs 6 Cfg-Major Version 7 unbekannte Daten nach dem Container Header 8 am Ende des Funktionsblockbereichs steht kein 0 9 ungültige Länge für die FSoE-Slave-Parameter 10 ungültiger Wert in der FSoE-Konfiguration 11 ungültige FSoE-Connection ID 12 ungültige FSoE-Slave Adresse 13 gespeicherten FSoE-Adressen in den Kontrollern unterschiedlich oder benötigte Anzahl der Adressen stimmt nicht	Limit	Wert in der Konfiguration richtig stellen (kleineren Wert eingeben)	Error-LED des Sicherheitsmoduls leuchtet rot

		14 Slave-Adresse, die zur Beantwortung des C_GET_SLAVEADDR Befehls verwendet wird, konnte nicht eindeutig ermittelt werden			
ERRVAL(1246)	Fehler in den Funktionsblöcken. Mögliche Ursache(n): • Softwarefehler			Wenden Sie sich an SIGMATEK GmbH & Co KG	
ERRVAL(1247)	Fehler in den Funktionsblöcken, Überlauf bei internen Berechnungen. Mögliche Ursache(n): • Softwarefehler • Falsche Parameter • Safedint-Werte außerhalb des zulässigen Bereichs			Überprüfung der Parameter und des eingestellten Wertebereichs, Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	
ERRVAL(1248)	Fehler in den Funktionsblöcken, falsche Safedint-Werte. Mögliche Ursache(n): • Softwarefehler			Wenden Sie sich an SIGMATEK GmbH & Co KG	
ERRVAL(1249)	Fehler in den Funktionsblöcken, falscher interner Status. Mögliche Ursache(n): • Softwarefehler			Wenden Sie sich an SIGMATEK GmbH & Co KG	
ERRVAL(1250)	Fehler in den Funktionsblöcken, falsche Parameter. Mögliche Ursache(n): • Softwarefehler			Wenden Sie sich an SIGMATEK GmbH & Co KG	

ERRVAL(1251)	Fehler in den Funktionsblöcken, falsche Safebool-Werte. Mögliche Ursache(n): • Softwarefehler			Wenden Sie sich an SIGMATEK GmbH & Co KG	
ERRVAL(1252)	Fehler in den Funktionsblöcken, falsche ID des Funktionsblocks. Mögliche Ursache(n): • Softwarefehler			Wenden Sie sich an SIGMATEK GmbH & Co KG	
ERRVAL(1253)	Fehler in den Funktionsblöcken, falsche Ende-Kennung. Mögliche Ursache(n): • Softwarefehler			Wenden Sie sich an SIGMATEK GmbH & Co KG	
ERRVAL(1254)	Fehler in den Funktionsblöcken, falsche Start-Kennung. Mögliche Ursache(n): • Softwarefehler			Wenden Sie sich an SIGMATEK GmbH & Co KG	
ERRVAL(1255)	Nicht verwendet				
ERRVAL(10000)	Die externe Versorgungsspannung der Geber ist nicht in Ordnung. Mögliche Ursache(n): • Externe Versorgungsspannung nicht angeschlossen, • Hardwarefehler	Byte 0 = 0; Beim Hochlauf wurde festgestellt, dass die Versorgungsspannung nicht in Ordnung ist Byte 1: Position des Moduls hinter der Safety CPU	immer 0	Versorgungsspannung prüfen. Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED der Safety-CPU leuchtet rot

ERRVAL(10001)	Der maximal zulässige Strom eines Gebers wurde überschritten (siehe „Technische Daten“ im Produktdatenblatt des SNC 021 Moduls). Mögliche Ursache(n): • Verdrahtungsfehler • Querschluss • Kurzschluss • Verwendung eines falschen Gebers	Byte 0: 0: max. Strom des ersten Gebers überschritten 1: max. Strom des zweiten Gebers überschritten Byte 1: Position des Moduls hinter der Safety CPU	Byte 0 und 1: Max. zulässiger Strom in 10µA Byte 2 und 3: Gemessener Strom des Gebers in 10µA	Strom des Gebers prüfen Verdrahtung des Gebers, sowie den Geber überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED der Safety-CPU leuchtet rot
ERRVAL(10002)	Der für einen Geber gemessene Strom liegt unter dem erlaubten Limit. Mögliche Ursache(n): • Verdrahtungsfehler • Kabelbruch • Geber defekt • Hardwarefehler	Byte 0: 0: das Limit für den Geber 1 ist unterschritten 1: das Limit für den Geber 2 ist unterschritten Byte 1: Position des Moduls hinter der Safety CPU	Byte 0 und 1: Unteres Limit für den erlaubten Strom in 10µA Byte 2 und 3: Gemessener Strom des Gebers in 10µA	Verdrahtung des Gebers, sowie den Geber überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED der Safety-CPU leuchtet rot
ERRVAL(10003)	Der für einen Geber gemessene Strom liegt über dem erlaubten Limit. Mögliche Ursache(n): • Verdrahtungsfehler • Querschluss • Kurzschluss • Geber defekt • Hardwarefehler	Byte 0: 0: das Limit für den Geber 1 ist überschritten 1: das Limit für den Geber 2 ist überschritten Byte 1: Position des Moduls hinter der Safety CPU	Byte 0 und 1: Oberes Limit für den erlaubten Strom in 10µA Byte 2 und 3: Gemessener Strom des Gebers in 10µA	Verdrahtung des Gebers, sowie den Geber überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED der Safety-CPU leuchtet rot

ERRVAL(10004)	Der für einen Geber gemessene Spannungsoffset für die Stromüberwachung liegt bei abgeschaltener Versorgungsspannung unter dem erlaubten Limit Mögliche Ursache(n): • Hardwarefehler	Byte 0: 0: das Limit für den Geber 1 ist unterschritten 1: das Limit für den Geber 2 ist unterschritten Byte 1: Position des Moduls hinter der Safety CPU	Byte 0 und 1: Unteres Limit für den erlaubten Spannungsoffset in mV Byte 2 und 3: Gemessener Spannungsoffset des Gebers in mV	SNC Modul tauschen	Error-LED der Safety-CPU leuchtet rot
ERRVAL(10005)	Der für einen Geber gemessene Spannungsoffset für die Stromüberwachung liegt bei abgeschaltener Versorgungsspannung über dem erlaubten Limit. Mögliche Ursache(n): • Hardwarefehler	Byte 0: 0: das Limit für den Geber 1 ist überschritten 1: das Limit für den Geber 2 ist überschritten Byte 1: Position des Moduls hinter der Safety CPU	Byte 0 und 1: Oberes Limit für den erlaubten Spannungsoffset in mV Byte 2 und 3: Gemessener Spannungsoffset des Gebers in mV	SNC Modul tauschen	Error-LED der Safety-CPU leuchtet rot
ERRVAL(10006)	Die für einen Geber gemessene Versorgungsspannung liegt unter dem erlaubten Limit. Mögliche Ursache(n): • Verdrahtungsfehler • Kabelbruch • Querschluss • Hardwarefehler	Byte 0: 0: das Limit für den Geber 1 ist unterschritten 1: das Limit für den Geber 2 ist unterschritten Byte 1: Position des Moduls hinter der Safety CPU	Byte 0 und 1: Unteres Limit für die erlaubte Spannung in mV Byte 2 und 3: Gemessene Spannung des Gebers in mV	Verdrahtung der externen Spannungsversorgung sowie der Geber überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED der Safety-CPU leuchtet rot

ERRVAL(10007)	Die für einen Geber gemessene Spannung liegt über dem erlaubten Limit. Mögliche Ursache(n): • Verdrahtungsfehler • Hardwarefehler	Byte 0: 0: das Limit für den Geber 1 ist überschritten 1: das Limit für den Geber 2 ist überschritten Byte 1: Position des Moduls hinter der Safety CPU	Byte 0 und 1: Oberes Limit für die erlaubte Spannung in mV Byte 2 und 3: Gemessene Spannung des Gebers in mV	Verdrahtung der externen Spannungsversorgung sowie der Geber überprüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED der Safety-CPU leuchtet rot
ERRVAL(10008)	Die Parameter für die Sollstromvorgabe sind ungültig. Mögliche Ursache(n): • Softwarefehler • Safety CPU nicht kompatibel (siehe Produktdatenblatt des SNC 021 Moduls)	Byte 0: Fehlerinformation Byte 1: Position des Moduls hinter der Safety CPU	immer 0	Safety-CPU prüfen Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED der Safety-CPU leuchtet rot
ERRVAL(10009)	Beim Test der Prüfsumme über die konstanten Elemente für die Stromüberwachung im RAM wurde ein Fehler entdeckt. Mögliche Ursache(n): • Softwarefehler • RAM defekt	Byte 0: Fehlerinformation Byte 1: Position des Moduls hinter der Safety CPU	immer 0	SNC Modul tauschen	Error-LED der Safety-CPU leuchtet rot
ERRVAL(10010)	Die beiden RS422-Treiber liefern für zumindest ein Signal der Geber unterschiedliche Ergebnisse. Mögliche Ursache(n): • Hardwarefehler	Byte 0: Information, welches Signal betroffen ist (Bit 0 = Signal A, Bit 1 = Signal B, Bit 2 = Signal Z) Byte 1: Position des Moduls hinter der Safety CPU	immer 0	SNC Modul tauschen	Error-LED der Safety-CPU leuchtet rot

ERRVAL(10011)	Die max. zulässigen Eingangs- bzw. Zählerfrequenz wurde überschritten (siehe Produktdatenblatt des SNC 021 Moduls). Mögliche Ursache(n): • Geber hat eine zu hohe Auflösung • Geber wird mit einer zu hohen Geschwindigkeit betrieben	Byte 0: 0: die maximale Eingangs- bzw. Zählerfrequenz für den Geber 1 wurde überschritten 1: die maximale Eingangs- bzw. Zählerfrequenz für den Geber 2 wurde überschritten Byte 1: Position des Moduls hinter der Safety CPU	Byte 0 und 1: Maximal zulässige Zählerfrequenz in Inkremente/ms Byte 2 und 3: Gemessene Zählerfrequenz in Inkremente/ms	Überprüfung des Gebers hinsichtlich Geberauflösung und Geschwindigkeit. Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED der Safety-CPU leuchtet rot
ERRVAL(10012)	Die max. zulässige Geberauflösung wurde überschritten (siehe Produktdatenblatt des SNC 021 Moduls). Mögliche Ursache(n): • Geber hat eine zu hohe Auflösung	Byte 0: 0: die maximale Geberauflösung für den Geber 1 wurde überschritten 1: die maximale Geberauflösung für den Geber 2 wurde überschritten Byte 1: Position des Moduls hinter der Safety CPU	Byte 0 und 3: Aktuell konfigurierte Geberauflösung	Überprüfung des Gebers hinsichtlich Geberauflösung. Falls der Fehler weiterhin auftritt: Wenden Sie sich an SIGMATEK GmbH & Co KG	Error-LED der Safety-CPU leuchtet rot

13 Anhang B: Fehlerbehandlung MDD2000

Error Variable	Beschreibung	Reason-Code 0	Reason-Code 1	Reason-Code 2	Maßnahmen
ERRVAL (0)	Kein Fehler				
ERRVAL (256)	Die Synchronisierung zwischen den Sicherheitskernen ist während der Startphase fehlgeschlagen. Mögliche Ursache(n): • Hardware-Fehler • Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (257)	Kommunikationsfehler zwischen Sicherheitskernen auf der UART-Schnittstelle. Mögliche Ursache(n): • Hardware-Fehler • Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (258)	Kommunikationsfehler zwischen Sicherheitskernen auf der SPI-Schnittstelle. Mögliche Ursache(n): • Hardware-Fehler • Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (259)	Die Sicherheitskerne erkennen verschiedene Betriebszustände für den aktuellen Zyklus. Mögliche Ursache(n): • Firmware-Fehler	Laufzeitzustand wird von SC1 nach SC2 übertragen	Laufzeitzustand wird von SC2 nach SC1 übertragen	Aktueller Laufzeitzustand	Wenden Sie sich an SIGMATEK GmbH & Co KG

ERRVAL (260)	Gespeicherte Daten fehlen oder sind ungültig. Mögliche Ursache(n): • Firmware-Fehler				Rücksetzen auf Werkseinstellungen mit Factory Reset im SafetyDesigner
ERRVAL (261)	Das Speichern persistenter Daten ist fehlgeschlagen. Mögliche Ursache(n): • Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (262) - ERRVAL (383)	Nicht verwendet				
ERRVAL (384)	Das Controller- Konfigurationsregister (Peripheriegeräte, MPU, usw.) hat seinen Wert während der Laufzeit geändert, ohne explizit darauf zuzugreifen. Mögliche Ursache(n): • Hardware-Fehler • Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (385)	Die aktive Sicherheitskonfiguration wurde zur Laufzeit geändert (ungültige CRC). Mögliche Ursache(n): Defekte CPU Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG

ERRVAL (386)	Die CPU Board Kalibrierungsdatei ist ungültig (ungültige CRC). Mögliche Ursache(n): • Defekter Flash-Speicher • Defekte CPU • Firmware-Fehler • Fehlende oder ungültige Kalibrierungsdatei				Einspielen einer korrekten Kalibrierungsdatei
ERRVAL (387)	Die CPU Power Kalibrierungsdatei ist ungültig (ungültige CRC). Mögliche Ursache(n): • Defekter Flash-Speicher • Defekte CPU • Firmware-Fehler • Fehlende oder ungültige Kalibrierungsdatei				Einspielen einer korrekten Kalibrierungsdatei
ERRVAL (388)	Die STO PWM Tabelle ist ungültig (ungültige CRC). Mögliche Ursache(n): • Defekter Flash-Speicher • Defekte CPU • Firmware-Fehler • Fehlende oder ungültige Kalibrierungsdatei				Einspielen einer korrekten Tabelle

ERRVAL (389)	Die gespeicherte Sicherheitsnummer bzw. die Modul-ID ist ungültig. Mögliche Ursache(n): • Defekte CPU • Firmware-Fehler • Fehlende oder ungültige Modul-Info				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (390)	Nicht unterstütze Firmware, Versionsnummer für Datentransfer zu niedrig Mögliche Ursach(n): • Veraltete Firmware • Firmware-Fehler	Niedrigste erlaubte Firmware-Nummer für Datentransfer	Firmware-Nummer für Datentransfer auf dem Modul		Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (391) - ERRVAL (415)	Nicht verwendet				
ERRVAL (416)	Die maximal erlaubte Laufzeit für den temporären operational Mode ist abgelaufen. Mögliche Ursache(n): • Maximale Zeit ist abgelaufen	Maximal erlaubte Zeit in [s]			Fehler quittieren und erneut temporären operational Mode starten bzw. Validieren des Drives
ERRVAL (417)	Die maximal erlaubte Geschwindigkeit für den temporären operational Mode wurde überschritten. Mögliche Ursache(n): • Maximale Geschwindigkeit ist überschritten	Index der Achse (Start bei 0)	Geschwindigkeit, die den Fehler verursacht hat (in aktuell eingestellter Einheit)	Maximal erlaubte Geschwindigkeit (in aktuell eingestellter Einheit)	Fehler quittieren und erneut temporären operational Mode starten bzw. Validieren des Drives

ERRVAL (418)	Die maximal erlaubte Positionsfenster für den temporären operational Mode wurde verlassen. Mögliche Ursache(n): • Positionsfenster wurde verlassen				Fehler quittieren und erneut temporären operational Mode starten bzw. Validieren des Drives
ERRVAL (419) - ERRVAL (447)	Nicht verwendet				
ERRVAL (448)	Die maximale Temperatur des Microcontrollers wurde überschritten. Mögliche Ursache(n): • Temperatur zu hoch • Defekt Hardware	Temperatur [°C]	Maximal erlaubte Temperatur [°C]		Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (449)	Es wurde eine Unterspannung an der 24 V-Versorgung erkannt. Mögliche Ursache(n): • Spannung zu gering • Defekt Hardware	Gemessene 24 V-Versorgung in [V]	Minimal benötigte 24 V-Versorgung in [V]		Überprüfen der Versorgungsspannung
ERRVAL (450)	Es wurde eine Unterspannung/Überspannung an der 3V3 Microcontroller Versorgung erkannt. Mögliche Ursache(n): • Defekt Hardware				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (451) - ERRVAL (495)	Nicht verwendet				

ERRVAL (496)	Die FSoE-Verbindung ist abgerissen. Mögliche Ursache(n): • VARAN-Verbindung unterbrochen • LasalClass2 Applikation gestoppt				Überprüfen der VARAN-Verbindungen; Starten der LasalClass2 Applikation
ERRVAL (497)	Es wurden falsche Werte im FSoE- Parameterstatus empfangen. Mögliche Ursache(n): • Routing-Fehler				Überprüfen der LasalClass2 Applikation
ERRVAL (498) - ERRVAL (511)	Nicht verwendet				
ERRVAL (512)	Das Überprüfen der Sicherheitskonfiguration ist fehlgeschlagen. Mögliche Ursache(n): • Falsche Konfiguration				Überprüfen der Sicherheitsapplikation
ERRVAL (513)	Die Default-Sicherheitskonfiguration ist ungültig (ungültige CRC oder falsche Länge). Mögliche Ursache(n): • Defekter Flash-Speicher • Defekte CPU • Firmware-Fehler • Fehlende oder ungültige Default- Sicherheitskonfiguration				Wenden Sie sich an SIGMATEK GmbH & Co KG

ERRVAL (514)	Die aktive Sicherheitskonfiguration ist ungültig (ungültige CRC oder falsche Länge). Mögliche Ursache(n): • Defekter Flash-Speicher • Defekte CPU • Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (515)	Die gespeicherte Sicherheitskonfiguration stimmt nicht mit der CRC überein, welche am Ende der Konfigurationsverteilung gespeichert wurde. Mögliche Ursache(n): • Defekter Flash-Speicher • Defekte CPU • Firmware-Fehler	Gespeicherter CRC der Sicherheitskonfiguration	CRC der gespeicherten Sicherheitskonfiguration		Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (516)	Die eingespielte Sicherheitskonfiguration stimmt nicht mit der Firmwareversion des Moduls überein. Mögliche Ursache(n): • Falscher Konfigurations-Download • Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (517)	Der Zugriff auf die CRC der Sicherheitskonfiguration ist fehlgeschlagen (Lesen oder Schreiben). Mögliche Ursache(n): • FirmwareFehler				Wenden Sie sich an SIGMATEK GmbH & Co KG

ERRVAL (518)	Die Sicherheitskonfiguration enthält ungültige Parameter Mögliche Ursache(n): • Sicherheitskonfiguration und Firmware-Stand passen nicht zusammen	Index des unbekannten Parameters	Subindex des unbekannten Parameters		Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (519)	Die Sicherheitskonfiguration enthält ungültige Parameter für eine Funktion. Mögliche Ursache(n): • Sicherheitskonfiguration und Firmware-Stand passen nicht zusammen	Index der Achse (Start bei 0)	Index und Subindex der betroffenen Funktion	Index und Subindex des betroffenen Parameters	Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (520)	Die Sicherheitskonfiguration enthält ungültige Parameter. Mögliche Ursache(n): • Firmware-Fehler • Ungültige Sicherheitskonfiguration				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (521)	Es gibt unterschiedliche Ergebnisse beim Parsen der Konfiguration in Controller 1 und Controller 2. Mögliche Ursache(n): • Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (522) - ERRVAL (639)	Nicht verwendet				

ERRVAL (640)	Die Plausibiltätsprüfung der Sicherheitsfunktionen während der Initialisierung ist fehlgeschlagen. Mögliche Ursache(n): • Firmware-Fehler • Ungültige Sicherheitskonfiguration				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (641)	Die ausgewählte Sicherheitsfunktion wird von der Firmware nicht unterstützt. Mögliche Ursache(n): • Firmware-Version zu niedrig • Ungültige Sicherheitskonfiguration	Index der Achse (Start bei 0)	Index der unbekannten Sicherheitsfunktion		Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (642)	Die maximale Anzahl der Sicherheitsfunktionen wurde überschritten (max. 48 pro Achse). Mögliche Ursache(n): • Ungültige Sicherheitskonfiguration mit zu vielen Sicherheitsfunktionen				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (643)	Der eingestellte Gebertyp ist mindestens für eine Sicherheitsfunktion nicht zulässig. Mögliche Ursache(n): • Ungültige Gebereinstellung • Falsche Sicherheitsfunktion	Index der Achse (Start bei 0)	Index und Subindex der betroffenen Funktion		Sicherheitsfunktion oder Geber ändern

ERRVAL (644)	Es gibt unterschiedliche Ergebnisse der ausgeführten Sicherheitsfunktion in Controller 1 und Controller 2. Mögliche Ursache(n): • Firmware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (645) - ERRVAL (767)	Nicht verwendet				
ERRVAL (768)	Der Selbsttest des Hardware-Watchdog-Abschaltpfades ist fehlgeschlagen. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (769)	Der Ziel- und Rücklesevergleich des Hardware-Watchdog ist fehlgeschlagen. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (670)	Es gibt unterschiedliche Rücklesevergleiche des Hardware-Watchdog zwischen Controller 1 und Controller 2. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (771) - ERRVAL (783)	Nicht verwendet				

ERRVAL (784)	Der Selbsttest des Eingang- Abschaltpfades ist fehlgeschlagen. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler	Index des Eingangs (Start bei 0)			Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (785)	Es wurde ein Querschluss am Eingang im Pre-Operational Mode erkannt. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler • Falsche Verkabelung	Index des Ausgangs für den Querschluss (Start bei 0)	Eingangsstatus (Bit 0 ist Eingang 1)	Bit-Muster für clock Eingänge, welche 0 sein sollen	Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (786)	Es wurde ein Querschluss am Eingang im Operational Mode erkannt. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler • Falsche Verkabelung	Index des Ausgangs für den Querschluss (Start bei 0)	Eingangsstatus vor dem Clock-Test (Bit 0 ist Eingang 1)	Bit 19-16: Eingangsstatus vor dem Clock-Test, Bit 11-8: Eingangsstatus während des Tests, Bit 3-0 Eingangsstatus nach dem Test (Bit 0 ist Eingang 1)	Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (787)	Es gibt unterschiedliche Eingangswerte zwischen Controller 1 und Controller 2. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler	Index des Eingangs (Start bei 0)	Rücklesewert des Controllers (Bit 0 ist Eingang 1)	Rücklesewert des anderen Controllers (Bit 0 ist Eingang 1)	Wenden Sie sich an SIGMATEK GmbH & Co KG

ERRVAL (788)	Es gibt Unterschiede der Eingangspaare (Zweikanaliges Mapping). Mögliche Ursache(n): • Falsche Konfiguration • Falsche Verkabelung • Firmware-Fehler • Hardware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (789)	Es gibt keine stabile Kombination von Eingängen innerhalb der maximalen erlaubten Zeit. Mögliche Ursache(n): • Falsche Konfiguration • Falsche Verkabelung • Firmware-Fehler • Hardware-Fehler	Index des Eingangspaares (Start bei 0)	Status des Eingangspaares (Bit 0 ist Eingang 1)		Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (790) - ERRVAL (799)	Nicht verwendet				
ERRVAL (800)	Der Selbsttest des Ausgang- Abschaltpfades ist fehlgeschlagen. Mögliche Ursache(n): • Falsche Verkabelung • Firmware-Fehler • Hardware-Fehler	Index des Ausgangs (Start bei 0)	Rücklesewert des Controllers 1 (Bit 0 ist Ausgang 1)	Rücklesewert des Controllers 2 (Bit 0 ist Ausgang 1)	Wenden Sie sich an SIGMATEK GmbH & Co KG

ERRVAL (801)	Der Ziel- und Rücklesevergleich des Ausgangs ist fehlgeschlagen. Mögliche Ursache(n): • Falsche Verkabelung • Firmware-Fehler • Hardware-Fehler	Zielwert des Ausgangsstatus (Bit 0 ist Ausgang 1)	Rücklesewert des Ausgangsstatus		Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (802)	Es gibt unterschiedliche Ausgangswerte zwischen Controller 1 und Controller 2. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler				Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (803) - ERRVAL (815)	Nicht verwendet				
ERRVAL (816)	Der STO-Selbsttest ist fehlgeschlagen (Gate Driver PWM). Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler	Index der Achse (Start bei 0)	Anzahl der ausgelesenen PWM-Zyklen	Ziel-Wert der PWM-Zyklen	Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (817)	Der Ziel- und Rücklesevergleich der Gate Driver PWM ist fehlgeschlagen. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler	Index der Achse (Start bei 0)	Anzahl der Zyklen	Byte 0: Aktueller STO-Status Byte 1: Ziel STO-Status	Wenden Sie sich an SIGMATEK GmbH & Co KG

ERRVAL (818)	Es wurden unterschiedliche Gate Driver PWM Zyklen zwischen Controller 1 und Controller 2 erkannt. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler	Anzahl der Zyklen Controller 1	Anzahl der Zyklen Controller 2		Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (819) - ERRVAL (831)	Nicht verwendet				
ERRVAL (832)	Der Selbsttest des Bremskontroll-Funktions-Abschaltpfades ist fehlgeschlagen. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler	Index der Achse (Start bei 0)			Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (833)	Der Ziel- und Rücklesevergleich der Bremskontroll-Funktion ist fehlgeschlagen. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler	Index der Achse (Start bei 0)	Rücklesewert der SBC	Byte 0: SBC Status im letzten Zyklus Byte 1: Zielwert des SBC Status	Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (834)	Es gibt unterschiedliche SBC-Werte zwischen Controller 1 und Controller 2. Mögliche Ursache(n): • Firmware-Fehler • Hardware-Fehler	Index der Achse (Start bei 0)	Byte 0: SBC Status in Controller 2 Byte 1: SBC Status in Controller 1	Byte 0: SBC Status im letzten Zyklus Byte 1: Zielwert des SBC Status	Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (835) - ERRVAL (1024)	Nicht verwendet				

ERRVAL (1025)	Der eingestellte Geber ist kein SIL Geber. Mögliche Ursache(n): • Falscher Geber • Falsche Konfiguration • Falsches Motor-Kabel	Index der Achse (Start bei 0)			Geber, Konfiguration und Kabel überprüfen
ERRVAL (1026) - ERRVAL (1027)	Nicht verwendet				
ERRVAL (1028)	Der eingestellte Geber wurde nicht gefunden. Mögliche Ursache(n): • Kein Geber angeschlossen • Falscher Geber • Falsche Konfiguration • Falsches Motor-Kabel	Index der Achse (Start bei 0)			Geber, Konfiguration und Kabel überprüfen
ERRVAL (1029)	Nicht verwendet				
ERRVAL (1030)	Es wurden falsche bzw. nicht plausible Daten am Geber erkannt. Mögliche Ursache(n): • Falscher Geber • Defekter Geber • Falsche Konfiguration • Falsches Motor-Kabel	Index der Achse (Start bei 0)			Geber, Konfiguration und Kabel überprüfen
ERRVAL (1031) - ERRVAL (1032)	Nicht verwendet				

ERRVAL (1033)	Die eingestellt Geberauflösung stimmt nicht der Auflösung am Geber überein. Mögliche Ursache(n): • Falscher Geber • Falsche Konfiguration • Falsches Motor-Kabel	Index der Achse (Start bei 0)	Bit 31-16: Eingestellte Auflösung Bit 15-0: Auflösung des Gebers	Bit 31-16: Eingestellte Umdrehungen Bit 15-0: Umdrehungen des Gebers	Geber und Konfiguration überprüfen
ERRVAL (1034) - ERRVAL (1039)	Nicht verwendet				
ERRVAL (1040)	Die gespeichert Seriennummer stimmt nicht mit der Seriennummer des Gebers überein. Mögliche Ursache(n): • Gebertausch	Index der Achse (Start bei 0)	Seriennummer des Gebers (letzte 4 Zeichen)	Gespeichert Seriennummer (letzte 4 Zeichen)	Geber neu validieren
ERRVAL (1040) - ERRVAL (1283)	Nicht verwendet				
ERRVAL (1284)	Kommunikationsfehler bezüglich des Gebers. Mögliche Ursache(n): • Falscher Geber • Defekter Geber • Falsche Konfiguration • Falsches Motor-Kabel	Index der Achse (Start bei 0)			Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (1285) - ERRVAL (1535)	Nicht verwendet				

ERRVAL (1536)	Es wurde eine Unterspannung/Überspannung der Hiperface DSL Versorgung erkannt. Mögliche Ursache(n): • Defekt Hardware • Defekter Geber	Index der Achse (Start bei 0)			Wenden Sie sich an SIGMATEK GmbH & Co KG
ERRVAL (1537)	Die Geber-ID stimmt nicht mit dem erwarteten Wert überein. Mögliche Ursache(n): • Gebertausch	Index der Achse (Start bei 0)	Gespeicherte ID	Erkannte ID	Geber neu validieren

Änderungen der Dokumentation

Änderungsdatum	Betroffene Seite(n)	Kapitel	Vermerk	Version
28.04.2009	Alle		Grundversion der Dokumentation erstellt	0.0
11.05.2010	Alle		Überarbeitete Grundversion	1.0
17.08.2010	63, 64		Zeichnung und Text korrigiert	1.1
23.08.2011	47		Passwortvergabe	1.2
04.10.2011	38		Grafik geändert	1.3
14.03.2012	46 47		Beispiel Kontakterweiterung eingefügt Zweikanaliger Ausgang eingefügt	1.4
23.01.2013	13 14 15 19 21 22 32 37 49-53 56 59 60 62 66 71 72 73		SCP010, SDI100, STO040, SRO020 hinzugefügt SCP 010, SDI 100, STO 040 und SRO 020 hinzugefügt S-DIAS-Safety Systemvoraussetzungen hinzugefügt Kapitel Generelle Topologie: Beschreibung erweitert S-DIAS-Sicherheitsmodule hinzugefügt Kapitel: Kommunikation im Safety-System: Beschreibung erweitert Errorcode 1222 und 28800 Sekunden hinzugefügt Kapitel *Montage eines Sicherheitsmoduls:* Beschreibung erweitert Kapitel *Beispiel 5: Optionale Module (ab CSCP012)* und *Beispiel 6: Interfaces (ab CSCP012)* hinzugefügt Kapitel *Erstellen der Konfiguration*: Beschreibung erweitert Fehlermeldungen 1088 und 1087 hinzugefügt Fehlermeldungen 1086, 1087 und 1009 hinzugefügt Kapitel Maximum Transmission Time: Beschreibung erweitert Fehlercodes 1102 und 1103 hinzugefügt	1.5

	74 75 76 77 78 88 89 91 93 95 96 97 99 103 109		Fehlercode 1009 hinzugefügt Kapitel Berechnung der Monitoring Settings (ab CSCP012): Beschreibung erweitert Reaktionszeitberechnung hinzugefügt (Formel) Reaktionszeitberechnung hinzugefügt (Formel) Reaktionszeitberechnung hinzugefügt (Formel) Reaktionszeitberechnung hinzugefügt (Formel) T_{bus} in der Tabelle hinzugefügt Kapitel *Fixe Zeitparameter, die Einfluss auf die Reaktionszeit haben*: Tabellen erweitert Kapitel *Fehler an sicheren Ausgängen*: Fehler 1137 hinzugefügt Kapitel *Ausgänge lassen sich nicht abschalten*: Fehler 1143 und 1144 hinzugefügt Identifier 5 bis 10 hinzugefügt Fehlercode 1009 hinzugefügt Kapitel *Verwendung optionaler Module (ab CSCP012)* hinzugefügt Kapitel *Verwendung von Interface-Variablen (ab CSCP012)* und *Master- und Slave-Mechanismus beim Modul SCP010* hinzugefügt Kapitel *Verwendung des Moduls SCP010 im Standalone-Betrieb* hinzugefügt Kapitel *Voraussetzungen*: Beschreibung erweitert ERRVAL(9): Beschreibung erweitert ERRVAL(73) hinzugefügt	
22.03.2013	Komplette Dokumentation	1.1.2 Verwendete Symbole 1.1.5. Restrisiken 1.1.6. Besondere Sicherheitshinweise 1.3. Richtlinien und Normen 1.4. Gebrauchsdauer und Verwendungszeit 2.2. Struktur des S-DIAS Safety-Systems	überarbeitet überarbeitet überarbeitet überarbeitet überarbeitet hinzugefügt	1.6

		2.3.4. Handbediengerät	überarbeitet Generelle Überarbeitung – S-DIAS System eingepflegt Alle Kennzeichnungen gelöscht	
24.04.2013		7.1 Verwendung optionaler Module (ab CSCP 012)	"Ab Safety-Firmware V245 ..." Merksatz hinzugefügt	1.7
18.09.2013			Not-Aus überall mit Not-Halt ersetzt	1.8
13.01.2014	11 17 23 25 111		Tabelle mit S-DIAS-Modulen erweitert Dokumentationsliste erweitert SCP011 in der Tabelle hinzugefügt Letzten Absatz mit SCP 011 hinzugefügt Zertifikat S-DIAS I/O System mit internem Bus hinzugefügt	1.9
20.01.2014	Alle 16, 17 18 19 24 26 55 68 97 98 100 103 104 105 149	 1.5 Verwendung von Modulen der Revision 1, Revision 2 und Revision 3 1.7 Systemvoraussetzungen 3.2.1.5 Beispiel 5: Optionale Module (ab Revision 2) 4.4.2.2. Maximum Transmission Time (Output as Input) 6.3.4. Tausch sicherer Eingangs- bzw. Ausgangsmodule bei den Safety-Modulen SCP 010 und SCP 011 7.2 Sicherheitsmaßnahmen und –hinweise	Revisionen 1-3 eingeführt Kapitel hinzugefügt SSI 021 hinzugefügt Kapitel erweitert In Tabelle SDI101, STO081, SRO021 und SSI021 hinzugefügt S-DIAS Sicherheitsmodule hinzugefügt Kapitel hinzugefügt Kapitel hinzugefügt Indentifier 11 bis 13 hinzugefügt Indentifier 14 bis 18 hinzugefügt Kapitel hinzugefügt Letzten Merksatz bezüglich SF_Optional_PwdII hinzugefügt Kapitel hinzugefügt Letzten Merksatz bezüglich Mastersysteme hinzugefügt ERRVAL(1040-1048) hinzugefügt	2.0

	160 161		ERRVAL(1148) geändert und ERRVAL(1149), ERRVAL(1156-1171) und ERRVAL(1172-1196) hinzugefügt ERRVAL(1197) hinzugefügt	
25.04.2014	44		Verdrahtungsbeispiele S-DIAS hinzugefügt	2.1
30.04.2014	18 24 26 28		Ergänzung des Mischmoduls SDM 081 Ergänzung des Mischmoduls SDM 081 Ergänzung des Mischmoduls SDM 081 Ergänzung des Mischmoduls SDM 081	2.2
23.05.2014	109	Kompatibilität der S-DIAS-Sicherheitsbauteile	Kapitel hinzugefügt	2.3
12.01.2015	109		S-DIAS – Safety – IO – Bus Grafik geändert (SSI 021 Kompatibilität)	2.4
25.02.2015	48		Grafik S-DIAS Hardware configuration hinzugefügt	2.4
30.03.2015	74 77	 Überwachung kontaktbehafteter Sensoren am Beispiel Not-Halt	Bild 46 getauscht Kapitel hinzugefügt	2.5
27.05.2015	9 12 18 19 20 22 23 25 27 28 71 83 89, 90 107 112		FSoE in Tabelle und Fußnote hinzugefügt Tabelle mit neuen S-DIAS Modulen erweitert Modul der Revision 4 hinzugefügt und Beschreibung erweitert SCP 111 hinzugefügt Ab Revision 4: hinzufügt Letzten Satz mit SCP 111 FSoE-Sicherheitsprotokoll erweitert Letzten Absatz mit SCP 111 FSoE-Sicherheitsprotokoll erweitert SCP111 in Tabelle hinzugefügt SCP 111 überall im Text hinzugefügt SCP 111 überall im Text hinzugefügt (nicht Revision 4) bei Maximum Transmission hinzugefügt Satz bezüglich Revision 4 im 1. Absatz eingefügt Kapitel Bestimmung der Reaktionszeit mit FSoE-Kommunikation hinzugefügt SCP 111 ergänzt	2.6

	113-116 117 119 171		SCP 111 ergänzt Kapitel Kommunikation über FSoE (Revision 4) hinzugefügt Neue Grafik mit SCP 111 SCP 111 ergänzt Beschreibung von ERRVAL(1148) ergänzt	
23.06.2015	11 21 24 25 26 49 55 61 87 89 112 113 118		2. Aufzählungspunkt in erstem Hinweis geändert (Betriebsanleitung statt Dokumentation) Bild 2 Architektur einer dezentralen Steuerung aktualisiert Bild 5 Architektur einer dezentralen Steuerung aktualisiert Hinweis hinzugefügt, dass die Safety CPU beim Busmaster sitzen muss Bild 6 Beispiel eines Safety-Systems aktualisiert Bild 19 S-DIAS Hardwareaufbau aktualisiert Im Beschreibungstext von Beispiel 3: Zweihandtaster den Text „C-DIAS-Bus“ mit „C-DIAS“ ersetzt, Bild 24 C-DIAS Hardwareaufbau des Beispiels 3 aktualisiert „...sitzen am Bus-Master...“ im Beschreibungstext von Beispiel 6: Interfaces (ab Revision 2) hinzugefügt „C-DIAS-System“ durch „Kommunikationssystem“ ersetzt Zeichnung aktualisiert Hinweis hinzugefügt, dass die Safety-CPUs am Bus-Master sitzen müssen Hinweis hinzugefügt, dass die Safety-CPUs am Bus-Master sitzen müssen Zeichnung aktualisiert	2.7
02.10.2015			Verwendung unsicherer Freigabesignale Grafik geändert	2.8
23.11.2015			Error-Liste komplett überarbeitet	2.8
29.03.2016	105 117-125 172	 7.7 Erstellung einer FSoE Verbindung über eine IP-Adresse	Identifier 19 und 20 hinzugefügt Kapitel hinzugefügt ERRVAL(1004) geändert	2.9

	187 208		ERRVAL(1068) geändert ERRVAL(1233) geändert	
27.06.2016	 102		CAN -> Safety-Interface Fußnote eingefügt	3.0
14.09.2016	114		Kein Standalone mit SSI	3.1
25.10.2016			Fehlerliste erweitert	3.2
22.11.2016			EN 61508 -> EN 62061	3.2
28.03.2017	137		Fehlerliste erweitert (1047-1050, 1156, 1162-1165)	3.3
17.10.2017	Alle		Generelle Überarbeitung	3.4
23.05.2018	81	4.4.3.5 OSSD-Signale an Sigmatek-Safety-SPS Eingängen	Kapitel hinzugefügt	3.5
30.05.2018		11 Anhang A: Fehlerbehandlung	erweitert	3.6
18.06.2018		2.5.1 Konfigurationsmerkmale 4.2.2 Konfiguration des Systems 6.2 Änderung der Konfiguration 6.3 Modultausch 7.1 Verwendung optionaler Module	Hinweis Validierung hinzugefügt	3.7
25.07.2018	34 140	2.3.4 Handbediengerät 7.8 Kompatibilität der S-DIAS-Sicherheitsmodule	Liste der Handbediengeräte erweitert Grafik hinzugefügt Tabelle aktualisiert	3.8
18.09.2018	25	2.2 Struktur des S-DIAS Safety-Systems	Korrektur Text Aufbau Beispiel	3.8
02.04.2019			TÜV-Anpassungen & Aufnahme HGW 1033-32	3.8
18.10.2019	78	4.4.3.1 Einkanaliges Einlesen mit Taktversorgung und Querschlusserkennung	Kapitel hinzugefügt	3.8
23.10.2019	143ff	11 Anhang A: Fehlerbehandlung	Generelle Überarbeitung	3.8
25.05.2020	14 19 21	1.1.3 Allgemeine Sicherheitshinweise 1.5 Gebrauchsdauer, Verwendungszeit und Schaltzykluszeiten 1.7 Dokumentation	Ergänzt um Unterstützung SRO022. Ergänzt um Dokumentation der Nutzung des CAN-Buses.	3.9

	27 29 32ff 36 92 136 185 203	2.3.1 Generelle Topologie 2.3.2 Sicherheitsmodule 2.3.5 CAN-Schnittstelle 2.5.4 Reaktionszeit und Abschaltzeiten 4.8 Reaktionszeit 7.8 Kompatibilität der S-DIAS-Sicherheitsmodule 11 Anhang A: Fehlerbehandlung		
01.07.2020	14, 27		DC 101 und DC 102 hinzugefügt	4.0
01.12.2020	119	7.1 Verwendung optionaler Module (ab Revision 2)	Text vor den Gefahrhinweisen eingefügt	4.0
07.03.2022			Neue Produkte SCP 111-S, SCP 211 und SAI 041 aufgenommen	4.1
18.08.2023	143ff 281ff	8 MDD 2000 (DIAS DRIVE 2000) 12 Anhang B: Fehlerbehandlung MDD2000	Kapitel hinzugefügt	5.0