E-IO Safety System - Sicherheitswarnungen

Berghof Automation

BERGHOF

Leerseite

Haftungsausschluss

Der Inhalt dieser Publikation wurde auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Abweichungen können dennoch nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Publikation werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Warenzeichen

- → Microsoft®, Windows® und das Windows® Logo sind eingetragene Warenzeichen der Microsoft Corp. In den USA und anderen Ländern.
- → EtherCAT® (inkl. FSoE) ist ein eingetragenes Warenzeichen und eine patentierte Technologie, lizenziert von der Beckhoff Automation GmbH, Deutschland.
- → PLCopen® ist ein eingetragenes Warenzeichen der PLCopen Association.

Die Rechte aller hier genannten Firmen und Firmennamen sowie Waren und Warennamen liegen bei den jeweiligen Firmen.

Hinweise zu diesem Handbuch

Dieses Handbuch richtet sich an qualifiziertes Fachpersonal und enthält die notwendigen Informationen für den bestimmungsgemäßen Gebrauch des Produkts.
Das richtige Verständnis und die fehlerfreie Umsetzung der technischen Beschreibungen, Bedienin-formationen und insbesondere der Gefahren- und Warnhinweise setzen umfassende Kenntnisse in Automatisierungstechnik und funktionaler Sicherheit voraus.

Inhaltsverzeichnis

Impressum

Kontaktdaten

Berghof Automation GmbH
Harretstr. 1
72800 Eningen
Deutschland
T +49.7121.894-0
F +49.7121.894-100
E-mail: controls@berghof.com
www.berghof-automation.com

Versionsinformation

Handbuchhistorie		
Version	**Datum**	**Beschreibung**
1.00	15.03.18	Erst-Version ERRATA Warnung #1 hinzugefügt
1.01	24.01.2020	ERRATA Warnung #2 und #3 hinzugefügt

FSM - Functional Safety Management

Gemäß unserer FSM Verfahren informieren wir Sie in diesem Dokument über potentielle applikationsab-hängige und sicherheitsrelevante Probleme mit CODESYS Safety bzw. unserem E-IO Safety System.
Bitte informieren Sie ggf. Ihre Kunden über die aufgeführten Punkte (außer Sie können das Auftreten in Ihrem System ausschließen).

Übersicht

Übersicht							
Warnung Nr.	**Datum**	**Kommentare**	**Betrifft**	**Bestell-nummer**	**Modul Release**	**CODESYS Safety Referenz (sofern verfügbar)**	**Gefixed?**
#1	22.02.18	Nicht zugewiesene Ausgangsbits können am physikalischen Ausgang auf den Wert 1 wechseln.	SafetyPLC	204909000	1.0x	3S Warnung #17 SCDS-4551	Nein
#2	24.01.20	FSOE Watchdog des Controllers nicht aktiv	Safety IO SDI4/SDO2	204809000	1.01	-	Ja
#3	24.01.20	Fehlehaftes Mapping für Diagnoseobjekt 2210	Safety PLC	204909000	bis 1.04	-	Nein

Sicherheitswarnungen

Sicherheitswarnung #1

Titel: Nicht zugewiesene (SAFE)BOOL Ausgänge können bei Modulen mit 2-Byte, WORD oder DWORD Ausgangskanälen den Wert 1 (TRUE) annehmen.

Kategorie: Physikalische Ausgänge

Referenz: SCDS-4551

Der folgende Fehler kann auf Ihrer Sicherheitsteuerung im Betrieb mit Sicherheitapplikationen auftreten, die einzelne Bits eines Ausgangsmoduls > 1 Byte direkt ansteuern (alle Feldbusse, alle Safety-Protokolle):
Ein ungemapptes Outputbit, d.h. ein Bit, das nicht mit einer Variable der Applikation belegt ist, kann am physikalischen Ausgang auf den Wert 1 wechseln.
Falls in der Maschine an dieses ungemappte Output-Bit ein sicherheitsrelevanter Aktuator angeschlossen ist, kann dieser Wertewechsel unvermittelt zu einer Gefährdung führen.

Details: Zu dem Fehler kann es nur kommen,

- → wenn die Abbildstruktur des Ausgangsmoduls laut Gerätebeschreibung mehrere Byte-Kanäle, oder mehrere Word- oder mehrere Dword-Kanäle enthält, und
- → wenn von dessen Kanälen nur einzelne Bits auf Variablen der Applikation gemappt sind und andere ungemappt bleiben,
- → und zwar so, dass das gleiche Bit (z.B. Nr. 4) in einem Kanal gemappt ist und im anderen Kanal des gleichen Ausgangsmoduls nicht gemappt ist.

Am physikalischen Ausgang hat dann dieses Bit (z.B. Nr. 4) in beiden Kanälen immer den gleichen Wert. D.h. Wenn die Applikation das gemappte Bit auf 1 setzt, geht gleichzeitig das ungemappte Bit auf 1.

Betroffen: alle Versionen (CODESYS Safety 1.0, 1.1, 1.2, 1.3, 1.4, 1.4.1)
→ Dies betrifft ebenfalls die Version 1.0x der E-IO Safety PLC (204908000)

Mögliche Workarounds:

- → Keine Aktuatoren an ungemappte Outputbits anschließen.
- → Oder keine Ausgangsmodule mit 2 Ausgangskanälen des gleichen binären Typs einsetzen (keine 2 Bytes, keine 2 Words, keine 2 DWords).
- → Oder in den Gerätebeschreibungen für Ausgangsmodule mehrere Byte-Kanäle zu 1 Word oder DWord Kanal zusammenfassen, oder ähnliches.
- → Oder keine ungemappten Outputbits.
- → Oder, wenn ein Bit eines Ausgangskanals ungemappt ist, dann ist es in den anderen Ausgangska-nälen des gleichen Ausgangsmoduls auch ungemappt.

Weitere Schritte: Fehlerbehebung mit CODESYS Safety 1.5 (SCDS-4551) im Runtime. Abhilfe im Feld wird ein Firmware-Update erfordern.

Zusätzliche Informationen

die bislang uns bekannten Fälle, die kritisch von dem Fehler betroffen sind:

→ Sichere Antriebe (zB ETG Safety Drive Profil) mit mehreren Steuerbytes und einer Sicherheitsfunk-tion, die durchgehend aktiv sein soll: Wenn sich der Applikateur entscheidet, diese Sicherheitsfunktion gar nicht über eine Variable der Sicherheitsapplikation anzusteuern,
sondern sich auf Default 0 = aktiv zu verlassen, dann könnte diese Sicherheitsfunktion bei applikativer Deaktivierung einer anderen Sicherheitsfunktion fehlerbedingt gleichzeitig deaktiviert sein.

In folgenden Fällen wirkt sich der Fehler nicht aus:

→ Kanäle, die gar nicht gemappt sind, d.h. kein einziges Bit ist mit einer Variable belegt: Sie bleiben auf 0.

→ Safety NetVars (Der Empfänger hat keinen Zugriff auf im Sender ungemappte Bits; ein 3S spezifischer Laufzeitcheck garantiert, dass Bits in Sender und Empfänger konsistent gemappt sind)

→ Austauschvariablen (Die von Safety-Package definierten logischen Austauschgeräte besitzen nur 1 Kanal)

Sicherheitswarnung #2, FSOE Watchdog

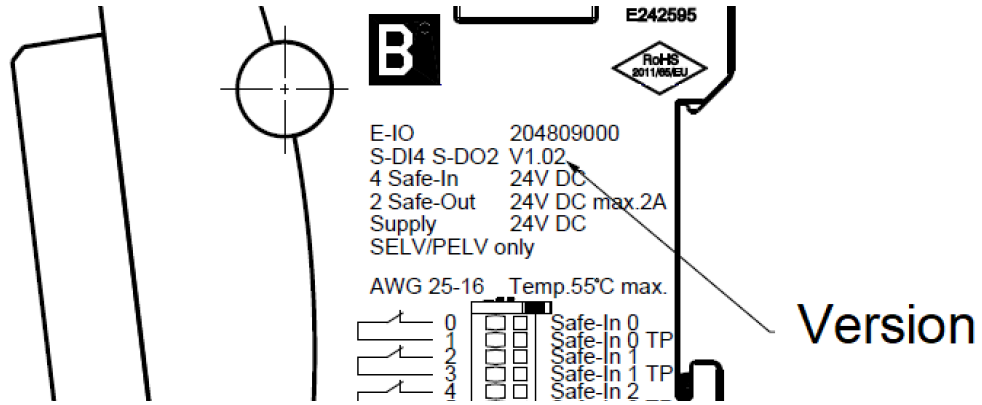
Titel: FSOE Watchdog kann nur bei Controller 2 erkannt werden

Kategorie: FSOE

Im Mai 2017 wurde eine Korrektur der Software bezüglich des sogenannten FSoE-Watchdogs durchgeführt, bei dieser Änderung wurde zur Erstellung der Release-Version lediglich ein inkrementelles Build anstatt eines kompletten Rebuild durchgeführt.

Details:
Es verblieb eine Testroutine im Release, die auf Controller 1 den FSoE-Watchdog-Timer auf den Wert 0 setzt. Dadurch kann nur auf Controller 2 der Watchdog festgestellt werden, was im Folgenden dann zu nicht kongruenten FSoE-Telegrammen von Controller 1 und 2 an den Kommunikationscontroller 3 führt.
Controller 2 meldet FSOE- Watchdog und Controller 1 meldet kein FSOE- Watchdog = inkongruente Telegramme.
Der Kommunikationscontroller 3, setzt einen Fehler, der die Weitergabe von FSoE-Telegrammen vom FSoE-Master verhindert. Dieser Fehler ist nicht rücksetzbar und das Modul bleibt bis zum nächsten Power up im sicheren Zustand.
Zusammenfassend muss festgestellt werden, dass die Einfehlersicherheit des Moduls nicht gewährleistet ist.
Ein Soft-Error in der Timer Komponente oder der Speicherzelle für die Watchdogzeit im Zusammenhang mit dem ausbleiben gültiger FSOE Telegramme führt potenziell zu einem unsicheren Zustand.
Der Status des Moduls ist eingefroren – eingeschaltete Ausgänge bleiben eingeschaltet.
Die spezifizierten Sicherheitskennwerte werden nicht eingehalten!
Dieser Fehler ist daher als sicherheitskritisch anzusehen!

Betroffen:
Es sind alle Module mit dem Versionsstand 1.01, geliefert ab 15.6.2017 betroffen.



Maßnahmen:
Berghof Safety E-I/O SDI4 SDO2 Module mit dem Revisionsstand 1.01 dürfen nicht mehr eingesetzt werden. Sollten Sie noch ein Modul mit der Revision besitzen, setzen Sie sich bitte mit Berghof Automation GmbH in Verbindung

Zusätzliche informationen – Wie kann es zu einem gefährlichen Zustand kommen?
Es muss ein Soft-Error auftreten, der die FSOE Zeitüberwachung des Controller 2 außer Betrieb setzt. Der Soft Error tritt unbemerkt während der Laufzeit auf und kann auch nicht erkannt werden.

Dabei können folgende Zustände auftreten:
- → Timer steht – enable Bit ist umgefallen
- → Timer zu langsam – Taktteiler zu groß
- → Watchdogparameter zu groß – Änderung in der Speicherzelle

Und erst danach müsste die FSOE Kommunikation komplett ausfallen - keine Telegramme mehr.
Dieser Zustand lässt sich nur mit einem Testprogramm, welches den Soft Error durch überschreiben einer bestimmten Speicherzelle simuliert, herstellen.
Wenn dann der Netzwerkstecker abgezogen wird, friert der I/O Zustand auf dem Modul ein und dies könnte potenziell gefährlich sein. Fehlerhafte FSOE Telegramme würde im FSOE Stack aufgedeckt und das Modul würde den sicheren Zustand einnehmen.

Sicherheitswarnung #3, Diagnoseinformation Objekt 2210

Titel: Fehlerhafte Werte bzw fehlerfates Mapping für Objekt 2210
Kategorie: Diagnose Meldung

Die Diagnoseobjekt 2210 enthält falsche Werte bzw fehlerhafte Mappingbeschreibung

Details:

a. Die verwendete Objektbeschreibung hierzu ist wie folgt:

```
OBJCONST TSDOINFOENTRYDESC OBJMEM EntryDesc0x2210 [] =
{
{DEFTYPE_UNSIGNED8, 0x08, ACCESS_READ} /* SubIdx: 0 - Number of entries */
, {DEFTYPE_UNSIGNED16, 0x10, ACCESS_READ} /* SubIdx: 1 - Error number */
, {DEFTYPE_UNSIGNED16, 0x10, ACCESS_READ} /* SubIdx: 2 - Error module */
, {DEFTYPE_UNSIGNED16, 0x10, ACCESS_READ} /* SubIdx: 3 - Error line */
};
```

b. Die korrekte Objektbeschreibung ist aber:

```
OBJCONST TSDOINFOENTRYDESC OBJMEM EntryDesc0x2210 [] =
{
{DEFTYPE_UNSIGNED8, 0x08, ACCESS_READ} /* SubIdx: 0 - Number of entries */
, {DEFTYPE_UNSIGNED16, 0x10, ACCESS_READ} /* SubIdx: 1 - Error number */
, {DEFTYPE_UNSIGNED16, 0x10, ACCESS_READ} /* SubIdx: 2 - Error line */
, {DEFTYPE_UNSIGNED8, 0x08, ACCESS_READ} /* SubIdx: 3 - Error module */
};
```

Dies hat zur Folge, dass beim Auslesen von Subindex 3 als 16 Bit Wert, ein Byte im Speicher gelesen wird, das nicht zu diesem Objekt gehört. Im Speicher liegt dort das niederwertigste Byte der POST-Flags (Objekt 2212), welches nach fehlerfreiem Anlaufen immer auf 0xFF steht.
Zur korrekten Interpretation des ‚Error module' Wertes darf nur dessen low Byte ausgewertet werden.
Für den sicheren Betrieb des Moduls ist das Objekt nicht relevant, da es sich um ein Diagnoseobjekt im unsicheren Teil handelt. Für eine Diagnose ist das Objekt 2210 nur relevant, wenn im Subindex 1 ein Fehler angezeigt wird; andernfalls liegt kein Fehler vor.

Betroffen: Alle Versionen der Safety PLC 204909000 bis Version 1.04

Maßnahmen: Da es sich in diesem Fall um eine nicht sicherheitsrelevante Diagnose handelt, die die Sicher-heitsfunktionen des Moduls nicht beeinträchtigen, kann das Modul, ggf. nach einer entsprechenden Anpassung der Diagnose, uneingeschränkt verwendet werden.
Fehler wird im nächsten Release behoben