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, Bedieninformationen und insbesondere der Gefahren- und Warnhinweise setzen umfassende Kenntnisse in Automatisierungstechnik und funktionaler Sicherheit voraus.

Inhaltsverzeichnis

1. Impressum

1.1. 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

1.2. Versionsinformation

Handbuchhistorie		
Version	**Datum**	**Beschreibung**
1.00	15.03.18	Erst-Version ERRATA Warnung #1 hinzugefügt

1.2.1. FSM - Functional Safety Management

Gemäß unserer FSM Verfahren informieren wir Sie in diesem Dokument über potentielle applikationsabhängige 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).

2. 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

3. Sicherheitswarnungen

3.1. 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)