KENDRION

WE MAGNETISE THE WORLD

INDUSTRIAL CONTROL SYSTEMS

# ERRATA_Sheet_Safety

Safety Warnings V1.03


Safety over EtherCAT®

KUHNKE

# Inhaltsverzeichnis – Table of Contents

# 1 Impressum – Legal Notice

## 1.1 Kontaktdaten – Contact Details

Kendrion Kuhnke Automation GmbH
Industrial Control Systems
Lütjenburger Straße 101
D-23714 Malente, Deutschland

Tel. +49 4523 402-0
Fax +49 4523 402-201

E-Mail sales-ics@kendrion.com
Internet www.kuhnke.kendrion.com

## 1.2 Versionsinformation – Version Details

| Historie - History | | |
|---|---|---|
| Version | Datum - Date | Kommentare / Änderungen – Comments / Modifications |
| 1.00 | 15.03.2018 | Erstversion – First Version<br>ERRATA Warning #17 added |
| 1.01 | 18.12.2018 | ERRATA Warning #18 added<br>Kuhnke FIO SDI4 SDO2 Module mit dem Revisionsstand 1.01 dürfen nicht mehr verwendet werden. - Kuhnke FIO SDI4 SDO2 Modules with revision 1.01 may no longer be used. |
| 1.02 | 26.03.2019 | ERRATA Warning #19 added<br>Fehlermeldungen im Objekt 2210 - Error message in object 2210 |
| 1.03 | 12.02.2020 | ERRATA Warning #17 - ist ab CODESYS Safety Runtime 1.5 gefixed.<br>- is fixed as of CODESYS Safety Runtime 1.5.<br>In the Kuhnke FIO Safety PLC the Runtime version 1.2 is used |

### 1.2.1 FSM - Functional Safety Management

Gemäß unserer FSM Verfahren informierten wir Sie in diesem Dokument über potentielle applikationsabhängige und sicherheitsrelevante Probleme mit CODESYS Safety.
Bitte informieren Sie ggf. Ihre Kunden über das Problem (außer Sie können das Auftreten in Ihrem System ausschließen).

*According to our FSM procedures, we have informed you in this document about potential application-dependent and safety-relevant problems with CODESYS Safety.*
*If necessary, please inform your customers about the problem (unless you can rule out the occurrence in your system).*

# 2 Übersicht - Overview

**Übersicht - Overview**

| ERRATA Nr. | Datum Date | Kommentare Comments | Betrifft Affects | Bestellnummer Order number | Modul Release | CODESYS Safety Version | Gefixed? fixed? |
|---|---|---|---|---|---|---|---|
| #17 | 22.02.2018 | Unmapped output bits may be set to 1 in some cases | SPLC | 694.330.00 | 1.0 | 1.2 | Nein – No |
| #18 | 04.09.2018 | FSoE watchdog of controller 1 not active | SDI4 SDO2 | 694.430.00 | 1.01 | Not relevant | Ja - yes |
| #19 | 19.03.2019 | Safety PLC – Error message in object 2210 | SPLC | 694.330.00 | up to 1.04 | Not relevant | Nein - No |

# 3 Sicherheitswarnungen - Safety Warning

## 3.1 Sicherheitswarnung #17 - Safety Warning #17

**Title:** Unmapped (SAFE)BOOL outputs may go to 1 in output modules with more than 2 BYTE or WORD or DWORD output channels

**Category:** physical output

**Reference:** SCDS-4551

**Deutsch**

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)

**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 Ausgangskanälen 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 Sicherheitsfunktion, 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)

## English

The following error can occur on your safety controller in operation with safety applications which control single bits of an output module > 1 byte (all field busses, all safety protocolls):

An unmapped output bit, i.e. a bit, which is not mapped to a variable of the application, can change to 1 at the physical output.

If, in the machine, a safety relevant actuator is connected to this unmapped output bit, this value change may lead to a sudden hazard.

**Details:**

The error can only occur

- if the image structure of the output module according to the device description contains multiple byte channels, or multiple word or multiple dword channels, and
- if only single bits of these channels are mapped to variables of the application and others remain unmapped,
- namely in such a way, that the same bit (e.g. #4) is mapped in one channel and unmapped in another channel of the same output module.

At the physical output, this bit (e.g. #4) then always has the same value in both channels.
That is, if the application sets the mapped bit to 1, the unmapped bit goes to 1 at the same time.

**Affected:** all versions (CODESYS Safety 1.0, 1.1, 1.2, 1.3, 1.4, 1.4.1)

**Possible work arounds:**

- Don't connect actuators to unmapped output bits.
- Or don't use output modules with 2 output channels of the same binary type (no 2 bytes, no 2 words, no 2 dwords).
- Or change the device descriptions of output modules to merge multiple byte channels to 1 word or dword channel, or similar.
- Or no unmapped output bits.
- Or, if a bit of an output channel is unmapped, then its also unmapped in the other output channels of the same output module.

**Further steps:** Fix with CODESYS Safety 1.5 (SCDS-4551) in the runtime. Remedy in the field will require a firmware update.

**Additional Informations:**

the cases known to us up to now which are critically affected by the bug are:

- safe drives (e.g. ETG safety drive profile) with multiple control bytes and a safety function supposed to be active continuously: If the application engineer decides not to drive this safety function via a variable of the safety application, but to rely on default 0 = active, then, during applicative deactivation of some other safety function, this safety function could be deactivated at the same time because of the bug.

In the following cases, the bug has no effect:

- Channels which are not mapped at all, i.e. no single bit is mapped to a variable: They remain on 0.
- Safety NetVars (The receiver has no access to bits unmapped in the sender; a 3S specific runtime check guarantees that bits are mapped consistently in sender and receiver)
- Exchange variables (The logical exchange devices defined by the Safety Package have only 1 channel)

## 3.2 Sicherheitswarnung #18 - Safety Warning #18

**Title:** FSoE Watchdogs can only be detected by Controller 2

**Category:** FSoE

### Deutsch

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.

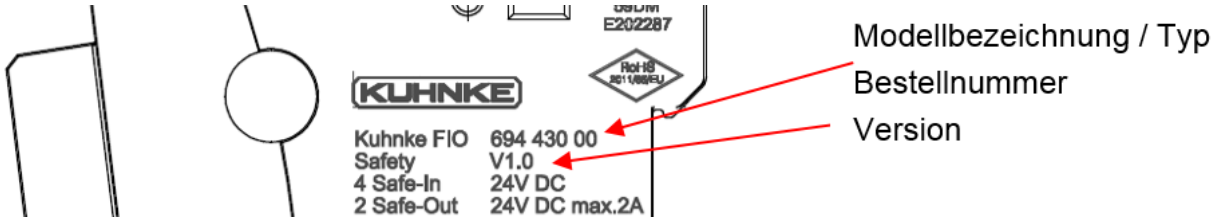
Zusammenfassend muss festgestellt werden, dass die Einfehlersicherheit des Moduls nicht gewährleistet ist.

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!

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




**Maßnahmen:**

Kuhnke FIO Safety 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 dem Hersteller 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.

### English

In May 2017, the software was corrected for the so-called FSoE watchdog, in this change, only an incremental build was performed to create the release version, rather than a complete rebuild.

**Details:**

This left a test routine in the release, which sets the FSoE watchdog timer to 0 on controller 1. As a result, the watchdog can only be detected on controller 2, which then leads to non-congruent FSoE telegrams from controller 1 and 2 to the communication controller 3 in the following.

Controller 2 reports FSOE watchdog and controller 1 reports no FSOE watchdog = incongruent telegrams. The communication controller 3, sets an error that prevents the transfer of FSoE telegrams from the FSoE master. This error can not be reset and the module remains in the safe state until the next power-up.

In summary, it must be stated that the single-fault safety of the module is not guaranteed.

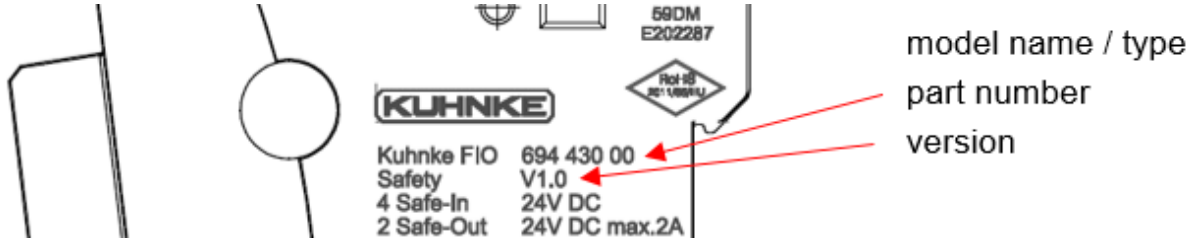
A soft error in the timer component or the memory cell for the watchdog time in connection with the absence of valid FSOE telegrams potentially leads to an unsafe state.

The status of the module is frozen - switched-on outputs remain switched on.

The specified safety characteristics are not adhered to!

It is therefore a security problem!

**Affected:** All modules are affected with the revision level 1.01, delivered from 15.6.2017.




**Activities:**

Kuhnke FIO Safety SDI4 SDO2 modules with revision level 1.01 may no longer be used. If you still have a module with the revision, please contact the manufacturer.

**Additional information - How can a dangerous condition occur?**

There must be a soft error that puts the FSOE timeout of the controller 2 out of service.

The soft error occurs unnoticed during runtime and can not be recognized.

The following states can occur:

- Timer stands - enable bit has fallen over
- Timer too slow - clock divider too big
- Watchdog parameter too large - change in the memory cell

And only then should the FSOE communication fail completely - no more telegrams.

This condition can only be established with a test program that simulates the soft error by overwriting a specific memory cell.

If the network connector is then disconnected, the I / O state on the module freezes and this could potentially be dangerous.

Faulty FSOE telegrams would be revealed in the FSOE stack and the module would assume the safe state.

## 3.3 Sicherheitswarnung #19 - Safety Warning #19

**Title:** Safety PLC – Error message in object 2210

**Category:** diagnostic messages

### Deutsch

In der Objektbeschreibung des Objektes 2210 ist uns ein Fehler unterlaufen.

**Details:** Fehlermeldung der CPU3

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 Kuhnke FIO Safety SPLC bis Version 1.04

**Maßnahmen:** Da es sich in diesem Fall um eine nicht sicherheitsrelevante Diagnose handelt, die die Sicherheitsfunktionen des Moduls nicht beeinträchtigen, kann das Modul, ggf. nach einer entsprechenden Anpassung der Diagnose, uneingeschränkt verwendet werden.

Wir werden dies im nächsten Release entsprechend anpassen.

**English**

We have made an error in the object description of object 2210.

**Details:** Error message of the CPU3

a. The object description used for this is as follows:

```
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. But the correct object description is:

```
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 */
 };
```

As a result, when subindex 3 is read out as a 16-bit value, a byte in the memory is read that does not belong to this object. In the memory there is the least significant byte of the POST flags (object 2212), which is always set to 0xFF after an error-free start.

For correct interpretation of the 'Error module' value, only its low byte may be evaluated.

The object is not relevant for the safe operation of the module, since it is a diagnostic object in the unsafe part. Object 2210 is only relevant for a diagnosis if an error is indicated in subindex 1; otherwise there is no error.

**Affected:** All Kuhnke FIO Safety SPLC up to version 1.04

**Activities:**

Since in this case the diagnosis is not safety-relevant and does not affect the safety functions of the module, the module can be used without restriction, if necessary after appropriate adaptation of the diagnosis.

We will adapt this accordingly in the next release.