Safety Warnings for E-IO Safety System

Blank Page

Disclaimer of Liability
The contents of the publication have been checked for compliance with the hardware and software that are described. Deviations however cannot be entirely excluded, so we undertake no guarantee of complete compliance. The data in this publication are regularly checked and any necessary corrections are incorporated in subsequent issues.

Trademarks
- → Microsoft®, Windows® and the Windows® logo are registered trademarks of Microsoft Corp. in the USA and other countries. in the USA and other countries.
- → EtherCAT® (incl FSoE) is a registered trademark and patented technology
- → PLCopen® is a registered trademark of the PLCopen Association.

Title to all companies and company names mentioned herein as well as to products and product names is held by the respective enterprises.

About this User Manual
This user manual is intended for qualified specialists and contains the information necessary for the correct use of the product.
For proper understanding and error-free application of technical descriptions, instructions for use and particularly of notes of danger and warning, extensive knowledge of automation technology and functional safety is compulsory.

Table of Contents

Document History		
Version	**Date**	**Comments**
1.00	15.03.18	Initial-Version ERRATA Warning #1 added
1.01	24.01.2020	ERRATA Warining#2 and #3 added

FSM - Functional Safety Management

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

Overview

Übersicht							
Warning No.	**Date**	**Comments**	**Affects**	**Ornder number**	**Modul Re-lease**	**CODESYS Safety Reference (if available)**	**fixed?**
#1	22.02.18	Unmapped output bits may be set to 1 on a physical output	SafetyPLC	204909000	1.0x	3S Warning #17 SCDS-4551	No
#2	24.01.20	FSoE watchdog of controller 1 not active	Safety I/O SDI4/SDO2	204809000	1.01	-	Yes
#3	24.01.20	Safety PLC – Wrong Mapping of object 2210	SafetyPLC	204909000	up to 1.04	-	No

Safety Warnings

Safety Warning #1

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

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)
→ that means also Version 1.0x of the E-IO Safety PLC (204908000)

Possible workarounds:

- → 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)

Safety Warning #2, FSOE Watchdog

Title: FSoE Watchdogs can only be detected by Controller 2

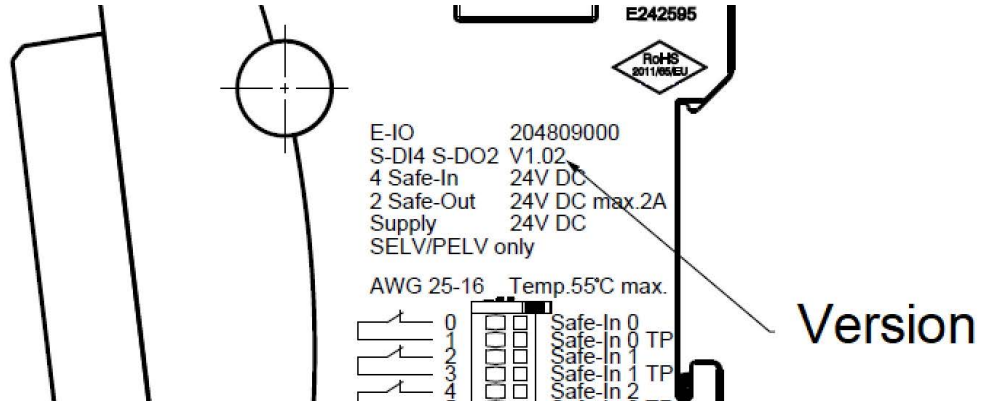
Category: FSOE

Reference:

In May 2017, the software was corrected for the so-called FSoE watchdog, in this change, only an incremen-tal 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 version 1.01, delivered from 15.6.2017.



Action:
All SDI4 SDO2 modules with version 1.01 mustr not be used.

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 spe-cific 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 as-sume the safe state.

Safety Warning #3, Diagnostic Information Object 2210

Title: Safety PLC, Wrong Mapping Description of Object 2210

Category: Diagnistic Information

Reference:

The mapping description of diagnostic object 2210 is worng. This leads to a wrong value in the corresponding data

Details:

a. The wrong old object description of 2210 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 module */
, {DEFTYPE_UNSIGNED16, 0x10, ACCESS_READ} /* SubIdx: 3 - Error line */
};
```

b. 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 al-ways 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 versions of Safety PLC 204909000 up to version 1.04

Action:
The error in the diagnostic information is not safety-relevant and does not affect the safety functions of the module. Therefore, the module can be used without restriction, if necessary after appropriate adaptation of the diagnosis. The error will be fixed with the next release.