Application Note

FESTO

Implementing SLS-Safety function based on CMMT-AS X2/X3 encoder evaluation and X10 encoder emulation CMMT-AS-...-S1

CMMT-AS-...-S1

Legal Notice

In the following, the "Festo SE & Co.KG" is designated as "Festo".

This Example circuit is not binding. This example circuit outlines a possible solution for a sample application and makes no claim of completeness, especially with regard to configuration and equipment, as well as any eventualities for your actual application. The Example circuit is not a customised solution, it merely offers assistance with typical task assignments.

The values stated in the Example circuit are partly assumptions and assessments which do not replace a detailed examination based on EN ISO 13849 part 1 and 2.

The actual characteristic values that can be obtained (especially PL, PFH_D, category, DC, $MTTF_D$, CCF) depend on the components used, as well as their conditions of use in the actual application.

The example circuit does not relieve you of the obligation to carry out a risk assessment and a validation of the specific application and to ensure the adherence to all specifications, especially the EC Machinery Directive 2006/42/EG. As the user, you are responsible for your specific application and for the correct operation of the described products.

Festo does not accept any liability for damages arising from the use of any incorrect or incomplete information contained in this documentation or any information missing therefrom. This equally applies to defects resulting from improper handling of devices and modules. In addition, all liability, with the exception of intent or gross negligence on the part of Festo, for damages arising due to non-adherence of the specifications of the EC Machinery Directive 2006/42/EG is also rejected.

The information in this document is in no way intended as a substitute for the operating instructions of the respective manufacturers or the design and testing of the application by the user. The operating instructions for products from Festo can be found at www.festo.com. Users of this document must themselves verify that all the functions described herein also work correctly in the application. Even after examining this document and using the specifications contained herein, users are nevertheless solely responsible for their own application.

Otherwise, all stipulations concerning liability included in the terms and conditions of delivery, payment and use of software from Festo, which can be found at www.festo.com and can be supplied on request, apply.

This document is only suitable for persons with sufficient expertise for machine safety based on EN ISO 12100 and EN ISO 13849. In addition, the following qualifications are required in the project team:

- Specialist in electrical engineering
- Specialist for the programming of control systems and safety switching devices

Copyright Notice

Table of contents

1 Example circuits

- The circuit specified in this document are principle circuits which cannot be complete due to their clarity and scope. Safety commanding device and safety switching device are not part of this document and are given for information only.
- The abbreviations used for the safety sub-functions refer to the definitions in EN 61800-5-2 [1] for electrical power drive systems:
    - o STO: Safe Torque Off
    - o SBC: Safe Brake Control
- Category 3, up to PL e according EN ISO 13849-1 [2].
- To understand this application note, are following documents necessary:
    - o Description "Servo drive CMMT-AS-C2/C4-3A-…". This description is available on the Internet https://www.festo.com/net/en-gb_gb/SupportPortal/Downloads/466851/573769/CMMT-AS-C2_C4-3A_2018-10a_8095049g1.pdf
    - o Description "Safety sub-function STO, SBC, SS1" for servo drive CMMT-AS-…-S1. This description is available on the Internet https://www.festo.com/net/en-gb_gb/SupportPortal/Downloads/466859/573777/CMMT-AS-_-S1_2018-10a_8096257g1.pdf
- The circuits and the procedure described are recommendations which do not exclude other possibilities.

2 Application example

2.1 Application: Safe Limited Speed using CMMT-AS-…-S1 and external Safety PLC

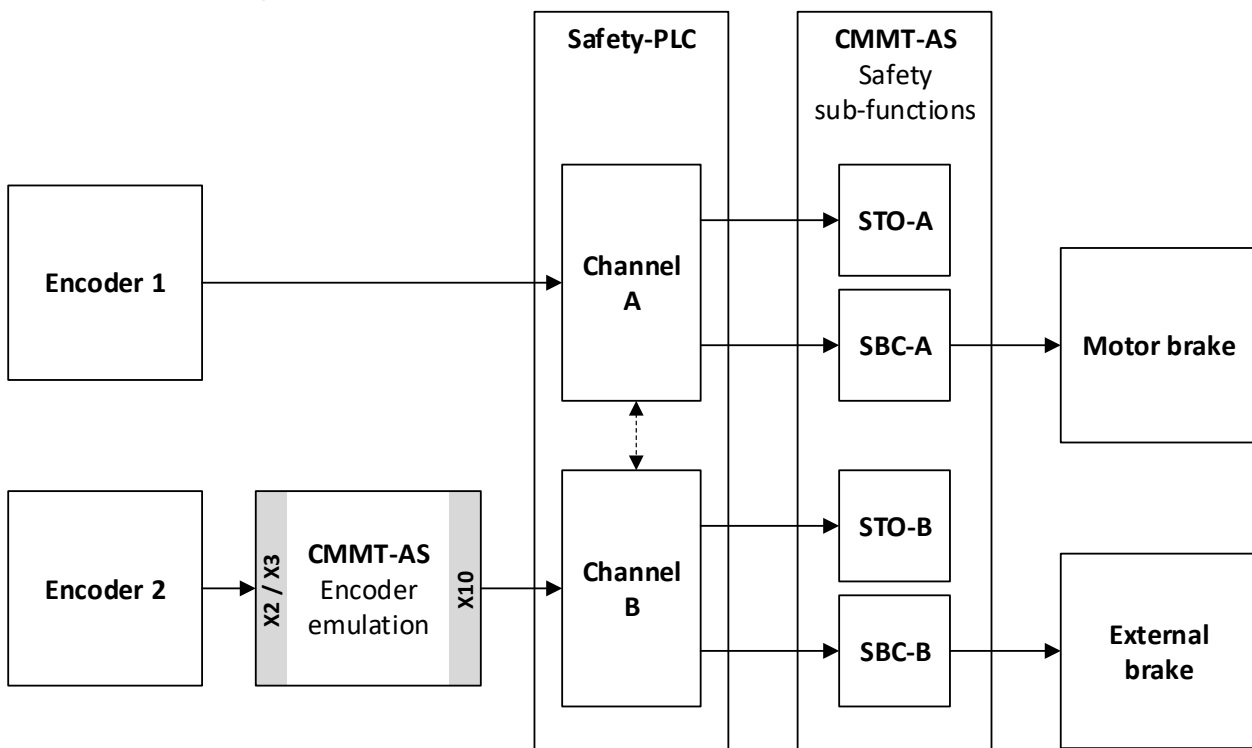The CMMT-AS-…-S1 supports the following safety functions directly:

- Safe Torque Off (STO)
- Safe Brake Control (SBC)

This Application Note describes, how the CMMT-AS-…-S1 could be used in combination with an external Safety PLC in applications requiring a Safe Limited Speed (SLS) function.

- The external Safety PLC performs the Safe Limited Speed monitoring
- To do this, the external Safety PLC requires two independent encoder signal sources
  - One Position encoder connected directly to the safety PLC (e.g. this could be a position encoder assembled to the mechanical axis)
  - One Position encoder connected to the CMMT-AS and via Encoder emulation of the CMMT-AS connected to the safety PLC (e.g. this could be a position encoder inside the servo motor.
- In case of any failure ore violation of the speed limits, the safety PLC uses the STO and SBC-function of the CMMT-AS to bring the system to the safe state.
- Encoder 1 and Encoder 2 must be diverse, e.g. different suppliers, different technology
- To implement this application and to determine the safety classification of the system you will need additional information:
  - the reliability data of the two encoders
  - the reliability data of the CMMT-AS encoder evaluation (see following chapter)
  - the reliability data of the Safety PLC (low / medium / high)

For more details, please refer to 2.3

2.2 Circuit Diagram

2.3   Description

Application	Servo drive with servo motor, axis and two encoders. Speed monitored by Safety-PLC
Triggering event	Request of SLS (Safe Limited Speed) in teach mode
Req. safety level	SIL 2, Cat. 3 / PL d or better
Reaction	• A speed within defined limiting values is commanded to CMMT-AS servo drive, e.g. over the fieldbus interface • The Safety-PLC starts to monitor the speed of the motor/axis
Safe state	The speed of the motor/axis is within safe limits
Function of the circuit	• The above circuit is a 1oo2 safety architecture, compliant to EN ISO 13849-1, Cat. 3 • The safety PLC monitors the signals of Encoder 1 directly • Encoder 2 is connected to CMMT-AS and it is used to control speed and position of the connected motor. • The signals of Encoder 2 are connected to encoder interface X2 (or X3). They are computed inside the CMMT-AS. Position information is then being forwarded to the encoder emulation interface X10. The X10 interface emulates incremental encoders with square wave output signals (A/B/N incremental encoder signals) • The Safety-PLC evaluates the signals of Encoder 1 and the output of CMMT-AS encoder emulation independently. The position values are simultaneously compared in both channels with the safe speed limits
Reaction on limit violations	Failure reaction functions are executed in case of a limit violation: • Safe Toque Off (STO) and • Safe Brake Control (SBC)
Diagnosis	Diagnosis of CMMT-AS encoder emulation by the Safety-PLC (see EN 61800-5-2, chapter D.3.16): • A/B output Signal stops • Only if Zero pulse is used: Zero pulse fails, is too short, too long or repeated Diagnosis of Encoder 1 by the Safety-PLC: • Encoder dependend, e.g. vector length of SIN/COS-encoders Diagnosis by the Safety-PLC: • Cross comparison of encoder position values Diagnosis of STO/SBC by the Safety-PLC: • Monitoring of STA and SBA (depends on required category, performance level and Safety-PLC, see CMMT-AS reliability data)
Fault exclusions	If the two encoders share the same mounting a fault exclusion must be assumed for the movement/encoder coupling for at least one of the two encoders. This has to be proven within a failure mode and effect analysis (FMEA). See EN 61800-5-2, chapter D.3.16.

2.4 Reliability data

⚠️ **Warning**

CMMT-AS encoder evaluation (interface X2/X3) and emulation (interface X10) reliability data

The CMMT-AS encoder evaluation (interface X2/X3) and emulation (interface X10) is **not** a safety sub-function compliant to the requirements of ISO 138149 and/or EN 61800-5-2.
The $MTTF_D$ values within this chapter are based on the assumption that 50 % percent of all failures are dangerous failures (see [2], chapter C.5.1).

To estimate the $MTTF_D$ of the SRP/CS the following values can be used in combination with the parts count method (see [2], annex D):

Environmental temperature [°C]	Load condition (max.)	MTTF CMMT-AS sub-system [years]	$MTTF_D$ CMMT-AS sub-system [years]
› 40 .. ≤ 50	70 %	13,6	27,2
	25 %	24,1	48,2
› 25 .. ≤ 40	100 %	13,6	27,2
	55 %	24,1	48,2
	10 %	42,2	84,4
≤ 25	100 %	24,1	48,2
	55 %	42,2	84,4

Table 2.1: CMMT-AS encoder evaluation (interface X2/X3) and emulation (interface X10) reliability data

2.5 Scope

This reliability data in 0 is only applicable with the following devices:

Device NOC	Device NOC
CMMT-AS-C2-3A-EC-S1	CMMT-AS-C3-11A-EC-S1
CMMT-AS-C2-3A-PN-S1	CMMT-AS-C3-11A-PN-S1
CMMT-AS-C2-3A-EP-S1	CMMT-AS-C3-11A-EP-S1
CMMT-AS-C4-3A-EC-S1	CMMT-AS-C5-11A-EC-S1
CMMT-AS-C4-3A-PN-S1	CMMT-AS-C5-11A-PN-S1
CMMT-AS-C4-3A-EP-S1	CMMT-AS-C5-11A-EP-S1
CMMT-AS-C2-11A-EC-S1	
CMMT-AS-C2-11A-PN-S1	
CMMT-AS-C2-11A-EP-S1	
CMMT-AS-xx-3A-yy-S1-… xx = C2, C4 yy = EC, PN, EP	CMMT-AS-xx-11A-yy-S1-… xx = C2, C3, C5 yy = EC, PN, EP

3 Literature

[1]   DIN EN 61800-5-2:2017-11 - *Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional* (IEC 61800-5-2:2016); German version EN 61800-5-2:2017

[2]   DIN EN ISO 13849-1:2016-06 - *Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design* (ISO 13849-1:2015); German version EN ISO 13849-1:2015

Apfeld, Ralf, *Do safe drive controls also require safe position encoders?,* Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), Sankt Augustin, Division 5: Accident prevention/product safety, December 2013, https://www.dguv.de/medien/ifa/en/pub/rep/pdf/reports2013/ifar0713e/safe_drive_controls.pdf