SL84 Safety Control Unit

Safety Manual

Version 1.0

DOCUMENT VERSION HISTORY

Version	Date	Notes
0.1	01.09.2020	First version for SL84
1.0	09.11.2020	First released version (rev 5)

TABLE OF CONTENTS

1 GENERAL

1.1 Purpose of This Document

The objective of this manual is to provide all necessary information required to enable safe and reliable implementation of safety related control system using Epec SL84 Safety Control Unit in compliance with IEC 61508, IEC 62061 and ISO 13849.

This document must be used together with the latest revisions of the SL84 Technical Manual including the mechanics and cabling instructions and with *Epec Programming and Libraries Manual*. Documentation is available from Epec's Extranet.

1.2 Scope

This Safety Manual contains requirements for implementation of safety related control system using Epec SL84 Safety Control Unit. This manual shall be carefully read by the system integrator before use of the product.

This Safety Manual overrides other related manuals and documentation. See related documentation in chapter, *Information for Use - Related Documents*.

1.3 Required Skills

This manual is intended to be used by system engineers, application developers, electric engineers and functional safety engineers who have experience in control system design and sufficient knowledge about functional safety.

1.4 Safety Information

The Epec SL84 Safety Control Unit can be used to implement safety-related control systems up to Safety Integrity Level 2 (IEC 61508 and IEC 62061) and Performance level d, Category 2 (EN ISO 13849).

It is highly recommended for the system integrator to contact Epec technical support (techsupport@epec.fi) in case of safety-related issues during the implementation of safety related control system or in operation of the Epec SL84 Safety Control Unit.

1.5 Terms and abbreviations

Abbreviation	Description
Code Template	Application generated by Multitool
ECC	Error Correcting Code.
MCU	Microcontroller
MPU	Memory Protection Unit
NVRAM	Non-Volatile Memory
PRG	CODESYS IEC application program
Reboot	Re-start of SL84 by switching Off and On the power supply
SBC	System Basis Chip. A microchip including intelligent watchdog functionality and power supply/management capabilities when used with a microcontroller.
System integrator	Any user who carry out a design task of the safety-related control system.

1.6 Use of Symbols

This manual uses the following symbol to point out important information or safety instructions:

The functional safety icon indicates important safety related requirements that shall be fulfilled by the end application.

2 SYSTEM INTEGRATOR'S RESPONSIBILITY

FS ID: 1 The system integrator shall determine a safety lifecycle model according to functional safety standards and directives which are relevant to the end application. Safety related control system and application software shall be developed according to this safety lifecycle.

FS ID: 2 The system integrator shall evaluate if the Epec SL84 Safety Control Unit can be used to implement safety functions in accordance to the hazards & risk analysis done by a machine manufacturer.

FS ID: 3 The system integrator shall consider safety functions as a complete system, including input devices (such as sensors), application logic and output devices (such as valves or relays) of the safety function to verify that required risk reduction is achieved. The Epec SL84 Safety Control Unit cannot guarantee safe operation of the system as a whole.

FS ID: 4 The system integrator shall verify and validate that all requirements in this safety manual are fulfilled by the end application.

3 SAFETY CONCEPT

3.1 Overview

The Epec SL84 Safety Control Unit consists of the following hardware and software components:

- Epec SL84 Safety Control Unit / Hardware rev. 9000D05

Figure 1. Hardware revision location on product label (sHW = D05)

The Epec SL84 Safety Control Unit consists of the following hardware and software components:

- Epec SL84 Safety Control Unit / Hardware v. 9000D05
  - The hardware is equipped with a Main CPU and a System Basis Chip acting as an intelligent watchdog.

- Epec SL84 Safety Control Unit / Firmware v. 1.0.0.38307
  - The firmware provides the low-level control for the SL84 hardware and CODESYS Runtime.

- Epec SL84 Safety Control Unit / Device Description v. 3.5.10.6

- Epec Platform Specific Safety Libraries
  - *SafeSL84Int* library v. 1.0.0.0
  - *SafeSSeriesIoDriverExt* library v. 1.0.0.7
  - *SafeSSeriesHardware* library v. 1.3.2.7
- Epec Platform Specific Libraries
  - *SSeriesCanExt* library v. 1.0.0.1
  - *SSeriesHardware* library v. 1.1.3.0
  - *SSeriesNvRamExt* library v. 1.0.0.4
  - *SSeriesSystemExt* library v. 1.0.0.13

- Epec Common Safety Libraries
  - *DiagnosticInterface* library v. 1.0.0.2
  - *SafeCANopenSRDO* library v. 1.1.0.0
  - *SafeConversion* library v. 1.1.0.0
  - *SafeDataValidation* library v. 1.0.0.7
  - *SafeJoystickCalibrationAndDiagnostic* library v. 1.1.0.2
  - *SafeProportionalValvecontrol* library v. 1.1.0.2
  - *SafeSensorCalibration* library v. 1.0.1.2
  - SafeErrorLog v. 1.0.0.0

- Epec Common Libraries
  - *CANopen protocol* library v. 4.0.4.7

It is possible to use also other Epec Common libraries with SL84, e.g. *J1939 library*, but those are not covered by this Safety manual.

3.2 Safety Function

The Epec SL84 Safety Control Unit executes safety related CODESYS application in a fail-safe principle.

Safety function: In case a safety-related internal fault is detected, the product will enter the safe state. In the safe state, all outputs of the SL84 are switched OFF (i.e. de-energized).

The only way to exit the safe state is by switching the power supply OFF and re-starting the system.

FS ID: 5 The system integrator shall ensure that the de-energize of outputs of the SL84's safe state will not cause any new possible hazardous situations of the machine.

FS ID: 6 The system integrator shall ensure that application software provides necessary means to prevent any hazardous movement of the machine when power supply of the SL84 is switched OFF and switched ON again to re-start the SL84.

3.3 Product Architecture

A high-level block diagram of the safety architecture is presented in *Figure 2. The safety architecture of SL84*. The architecture is designed to meet Category 2 (EN ISO 13849-1:2015).

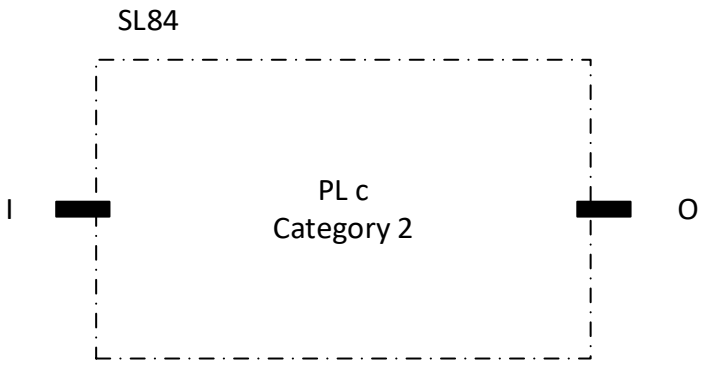

Figure 2. The safety architecture of SL84

3.4 Power supply groups

The Epec SL84 Safety Control Unit has three separate power supply groups.

FS ID: 7 When using mains voltage power supply in safety critical application, it is required to use a power supply which fulfills Hardware Fault Tolerance (HFT) = 1. In case of failure of power supply device supply voltage safety funtion limits output voltage under 30 V after one failure on power supply device.

FS ID: 8 SL84 Safety Control Unit Power supply groups internal circuit can't prevent external voltage flowing from output pins to corresponding Power supply group pins. System integrator must ensure that external voltage in unit output pins does not lead that other devices lose they safety functionality..

The system integrator shall ensure that SL84 is used under operating voltage limits as presented in the Technical Manual. (*Epec SL84 Safety Control Unit Technical Manual).*

Power supply pins are located in the following pins:

Connector / pin number	Pin Type
X3.2 X3.5	Logic/Power Supply 1
X3.3 X3.6	Power Supply 2 for cut-off
X3.1 X3.4	Power Supply 3
X3.7	GND
X3.8	GND
X3.9	GND
X3.10	GND
X3.11	GND
X3.12	GND

For more information how to implement Power supply, refer to *Epec Programming and Libraries Manual and Epec SL84 Safety Control Unit Technical Document.*

The following tables describe Power Supply groups for each output.

3.4.1 Power supply group 1.

Power supply logic operator, CAN buses, memory, inputs pins and some of SL84 output pins. The following table shows the SL84 outputs in power supply group 1.

Pin number	Pin Type	Powered by
X1.39	PWM/DO/CM 3A	Logic/ Power Supply 1
X1.40	PWM/DO/CM 3A	Logic/ Power Supply 1
X1.41	PWM/DO/CM 3A	Logic/ Power Supply 1
X1.42	PWM/DO/CM 3A	Logic/ Power Supply 1
X1.43	PWM/DO/CM 3A	Logic/ Power Supply 1
X1.44	PWM/DO/CM 3A	Logic/ Power Supply 1
X1.45	PWM/DO/CM 3A	Logic/ Power Supply 1
X1.46	PWM/DO/CM 3A	Logic/ Power Supply 1

For more information how to implement Power supply, refer to *Epec Programming and Libraries Manual* and *Epec SL84 Safety Control Unit Technical Manual.*

3.4.2 Power supply group 2.

Power supply SL84 cut-off output pins. The following table shows the SL84 outputs in power supply group 2.

Pin number	Pin Type	Powered by
X2.5	PWM/DO/CM 3A	Cut-off / Power Supply 2
X2.6	PWM/DO/CM 3A	Cut-off / Power Supply 2
X2.7	PWM/DO/CM 3A	Cut-off / Power Supply 2
X2.8	PWM/DO/CM 3A	Cut-off / Power Supply 2
X2.9	PWM/DO/CM 3A	Cut-off / Power Supply 2
X2.10	PWM/DO/CM 3A	Cut-off / Power Supply 2
X2.11	PWM/DO/CM 3A	Cut-off / Power Supply 2
X2.12	PWM/DO/CM 3A	Cut-off / Power Supply 2
X2.13	PWM/DO/CM 3A	Cut-off / Power Supply 2
X2.14	PWM/DO/CM 3A	Cut-off / Power Supply 2

FS ID: 9 Only self-safe units can be be connected to the same power rail. A self-safe unit goes to the safe state by itself. SL84 Cutt off is not a self-safe, therfore, the connection must be made according to Figure 5. Correct connection of cut-off power supply

For more information how to implement Power supply, refer to *Epec Programming and Libraries Manual and Epec SL84 Safety Control Unit Technical Manual.*

3.4.3 Power supply group 3.

Power supply some of SL84 output pins. The following table shows the SL84 outputs in power supply group 3.

Pin number	Pin Type	Powered by
X2.15	PWM/DO/CM 3A	Power Supply 3
X2.31	PWM/DO/CM 3A	Power Supply 3
X1.12	DO 5A	Power Supply 3
X1.13	DO 5A	Power Supply 3
X1.14	DO 5A	Power Supply 3
X1.15	DO 5A	Power Supply 3
X2.45	DO_GND 3 A	Power Supply 3 (only pull up)
X2.46	DO_GND 3 A	Power Supply 3 (only pull up)

For more information how to implement Power supply, refer to *Epec Programming and Libraries Manual and Epec SL84 Safety Control Unit Technical Manual.*

4 SAFETY METRICS

This chapter provides functional safety parameters of Epec SL84 Safety Control Unit. This information is intended to support system integrator's work during design, verification, and validation of a complete safety function.

FS ID: 10 Because Start-up diagnostic functions are carried out during system start-up only, it shall be ensured that the typical continuous working cycle will not exceed 24 hours. This means that SL84 shall be rebooted after each 24 hours to meet given safety values.

4.1 IEC 61508

Parameter	Value	Units
Safety Integrity Level	SIL1	
*PFH	1,8 x 10^{-6}	(1/h)
SFF	> 90	%
HFT	0	
Safety Related Element	Type B	
T1 = Product lifetime	20	years
Manual Proof Tests	not required	

** This value is valid if all I/O pins are used to implement a single safety function. Generally, only a few pins are used to implement a safety function, which leads to a better value.*

For specific application functional safety levels can be up to SIL2.

For more information see chapter *System examples*.

4.2 ISO 13849

Parameter	Value	Units
Performance Level	PL c	
Category	2	
*$MTTF_d$	>22	years
DCavg	>64	%

** This value is valid if all I/O pins are used to implement a single safety function. Generally, only a few pins are used to implement a safety function, which leads to a better value.*

For specific application functional safety levels can be up to PLd Cat. 2.

For more information see chapter *System examples*.

Block	$MTTF_d$ (a)	Max. DCavg (%)
Processing	403	High
AI/DI_Type116_0_0_SL84	2113	Low when using signal range check
PI/DI_Type075_2_0_SL84	2514	Low when using signal range check
PI/DI2_Type039_0_2_SL84	16211	Low when using signal range check
PWM/DO/CM 3 A_Type114_1_4_SL84	1620	Low when using feedback information
PWM/DO/CM 3 A Cut-off_Type114_2_0_SL84	1643	Low when using feedback information
DO/CM 5 A_Type124_1_1_SL84	1145	Low when using feedback information
DO 3 A_Type125_1_0_SL84	959	Low when using feedback information
DO_GND 3 A_Type048_3_1_SL84	3732	Low when using feedback information
CAN 1	1103	Low, with CANopen Safety Medium
CAN 2	2344	Low, with CANopen Safety Medium
Ref +5 V sensor supply	2289	Low when using signal range check

5 SAFETY CONCEPT CUTOFF

5.1 Overview

The product which controls the Epec SL84 Safety Control Unit Cut-off feature must be certified by a notified body, for example, Epec's SC52 Safety Control Unit. The safety level of the product must meet the requirements of the entire control system.

5.2 Safety Function

Safety function: Functional safety is implemented using the Epec SL84 Safety Control Unit, in addition to external components.

External voltage supply shall be cut-off reliably from Power Supply Group 2 (pin X3.3). In order to use SL84 in systems with functional safety level Cat 2 or higher the voltage from Power Supply Group 2 must be verified that there is no remaining voltage by diagnosing pin X3.6 with a safety unit in system level.

The output leakage current is less than 1 mA, when the Power Supply Group 2 is de-energized.

FS ID: 11 The system integrator shall ensure that the de-energizing of the Power Supply Group 2 pins of the SL84 will not cause any new possible hazardous situations of the machine.

FS ID: 12 The system integrator shall ensure that necessary means are implemented to prevent any hazardous movement of the machine when power supply of the SL84 is switched OFF and switched ON again to re-start the control system.

FS ID: 13 Units have to connect so that reverse voltage form SL84 does not compromise functional safety of control system.

5.3 Product Architecture

A high-level block diagram of the safety architecture is presented in *Figure 3. The safety architecture of SL84 cut-off*. The architecture is designed to meet Category 1, 2 or 3 (EN ISO 13849).

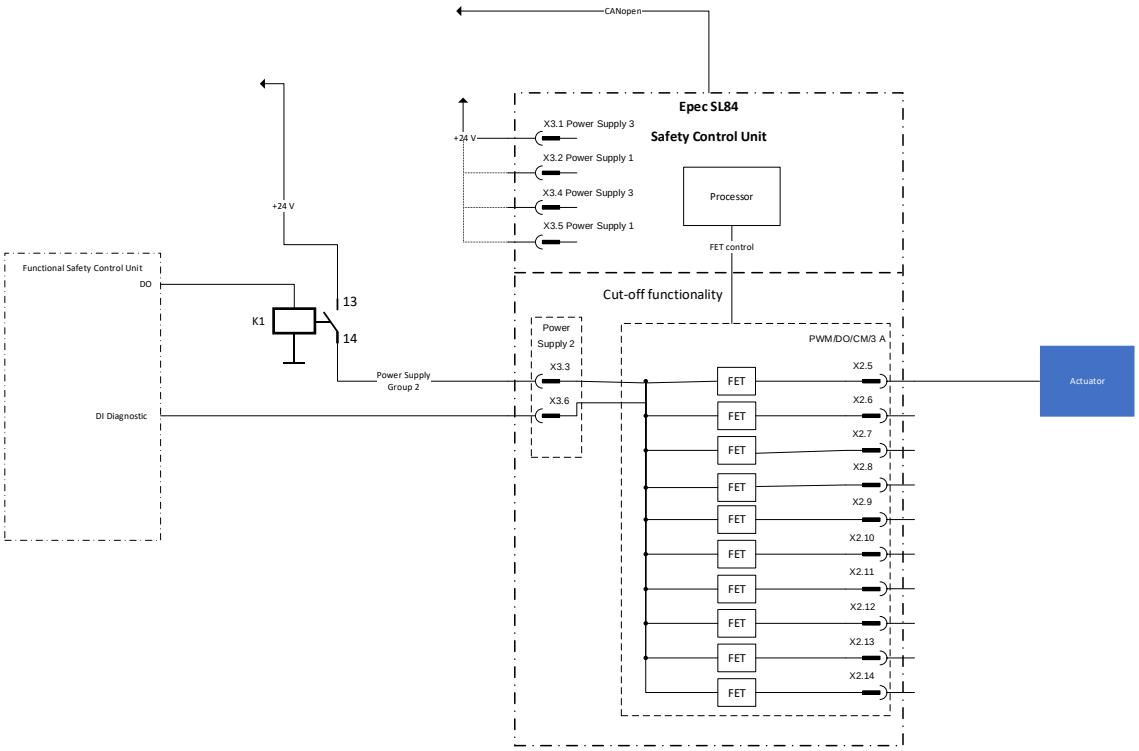

Figure 3. The safety architecture of SL84 cut-off

Power supply pins are located in the following pins:

Connector / pin number	Pin Type
X3.2 X3.5	Logic/Power Supply 1
X3.3 X3.6	Power Supply 2 for cut-off
X3.1 X3.4	Power Supply 3
X3.7	GND
X3.8	GND
X3.9	GND
X3.10	GND
X3.11	GND
X3.12	GND

The following table describes Power Supply 2 cut-off group output pins:

Connector / pin number	Pin Type	Powered by	Current
X2.5	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A
X2.6	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A
X2.7	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A
X2.8	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A
X2.9	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A
X2.10	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A
X2.11	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A
X2.12	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A
X2.13	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A
X2.14	PWM/DO/CM 3A	Power Supply 2 cut-off	3 A

For more information electrical Characteristics, refer to *Epec SL84 Safety Control Unit Technical Manual.*

FS ID: 14 SL84 Safety Control Unit is Category 2 device, system integrator must ensure that external voltage in unit output pins does not lead that other devices lose they safety functionality.

SL84 Cut-off feature power supply 2 connection must be made according to *Figure 5. Correct connection of cut-off power supply*

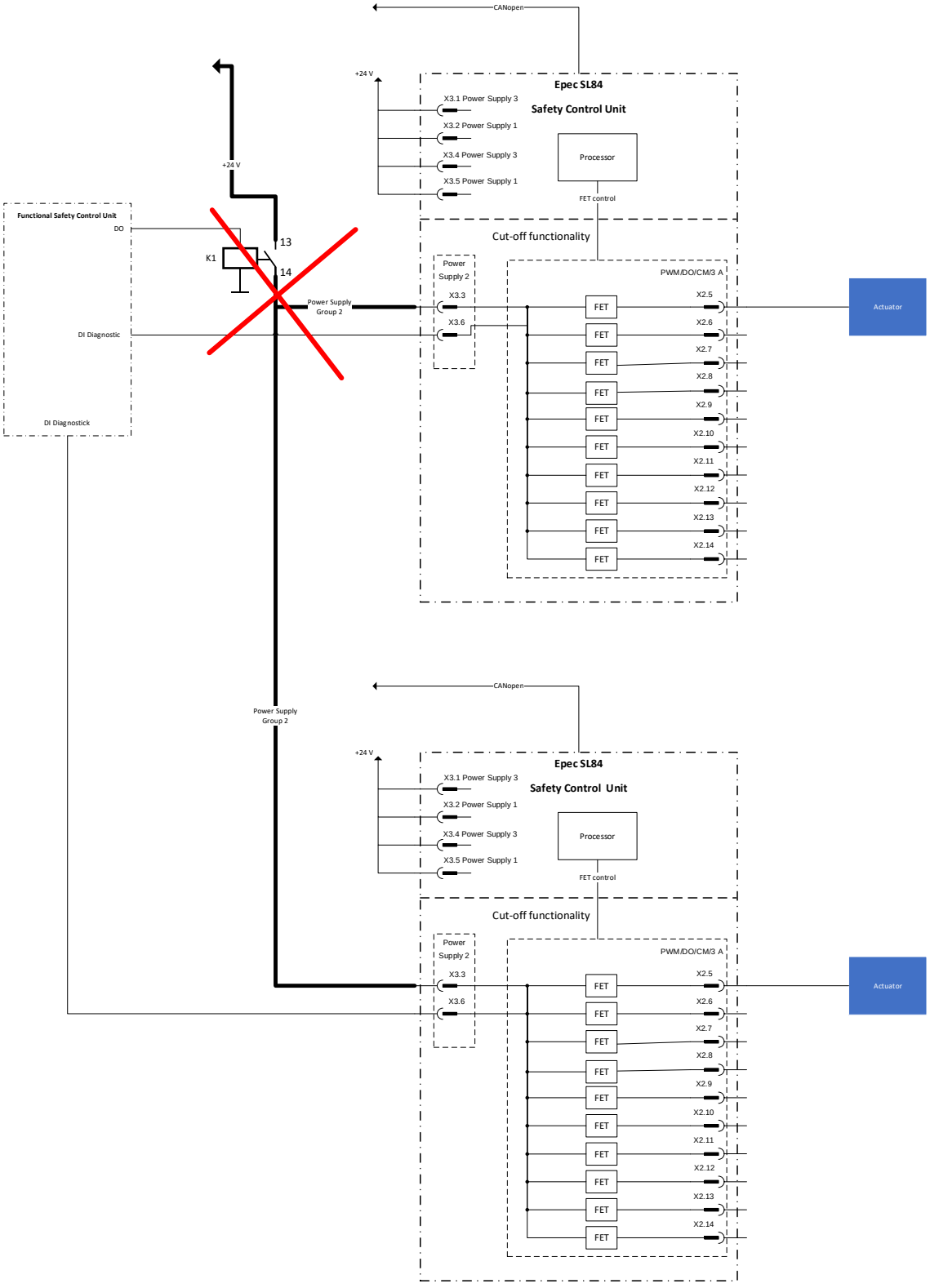

Figure 4. Incorrect connection of cut-off power supply

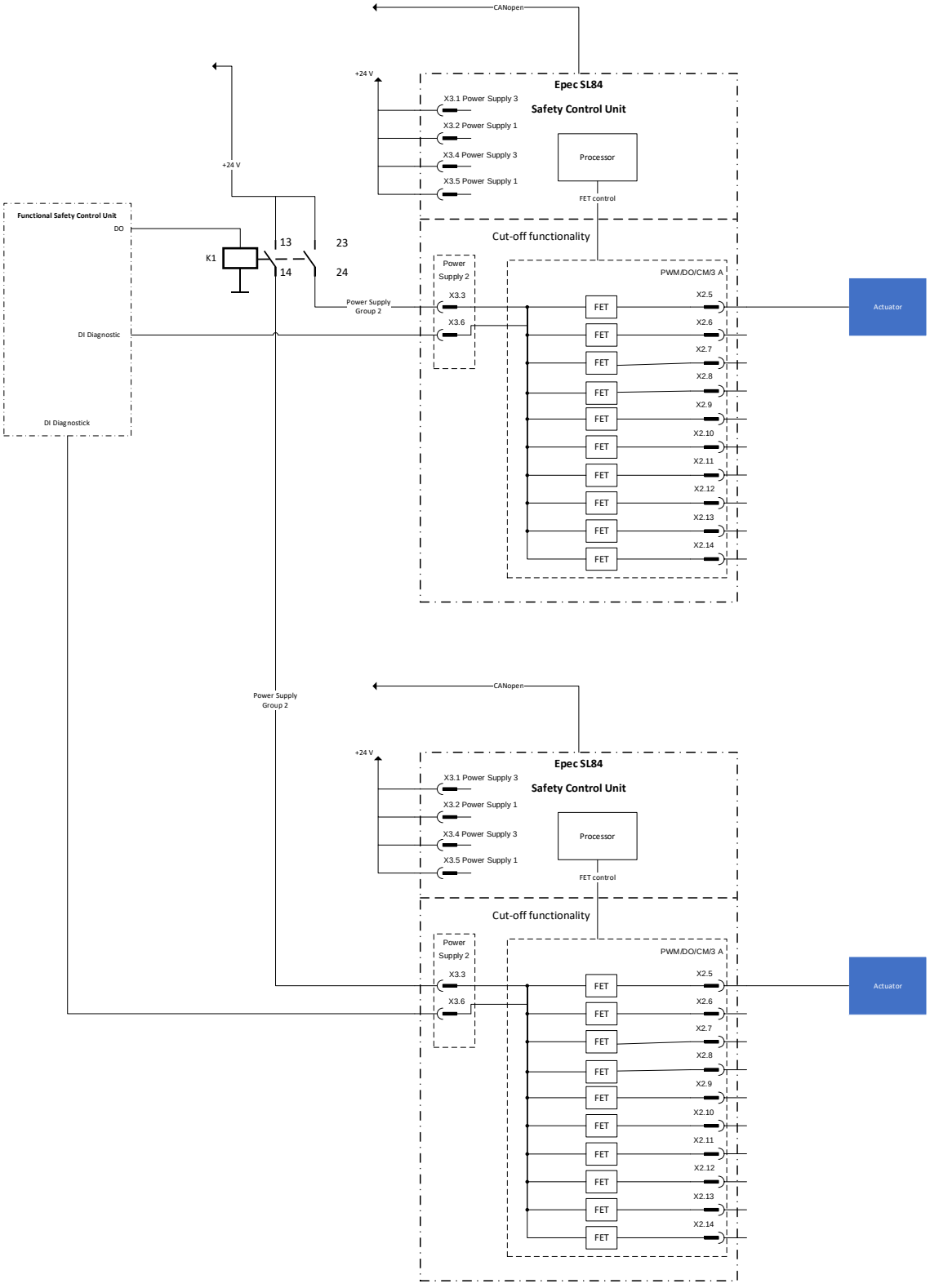

Figure 5. Correct connection of cut-off power supply

6 REQUIREMENTS FOR USING CUTOFF WITH THE EXTERNAL CONTROL SYSTEM

6.1 Overview

This chapter describes how the external control system reliably controls and diagnoses the voltage led to Power Supply Group 2.

If the K1 relay is unable to cut-off voltage to Power Supply Group 2, the functionality of the safety function cannot be guaranteed. Channels in the power group cannot be cut-off safely anymore.

The worst-case time of cutting the voltage from the cut-off group must be taken into account.

6.2 Start-up and online Diagnostics in the control system

Before the K1 relay is connected, ensure that there is no voltage in the DI Diagnostic pin X3.6. After connecting the K1 relay, ensure that there is voltage in the DI Diagnostic pin X3.6 to test measurement correct operation.

Online diagnostics are the diagnostics implemented in the external safety control system.

If the cut-off group's outputs are not controlled by the K1 relay or the SL84 Safety Control Unit, DI diagnostic pins must not have voltage.

6.3 Load dependent cut-off time

The following formula can be used to calculate actual cut-off time:

$$t_{cutoff} = -\frac{C_{SL84} * U_{in}}{I_{load}} * 2 * ln(\frac{U_{off}}{U_{in}})$$

The calculated load-dependent cut-off time must be verified by a test measurement.

Parameter:	Description:
t_{cutoff}	Actual cut-off time
U_{in}	Supply voltage
U_{off}	Voltage, if Output = Off
I_{load}	External load
C_{SL84}	Internal capacitance of SL84 (220 µF)

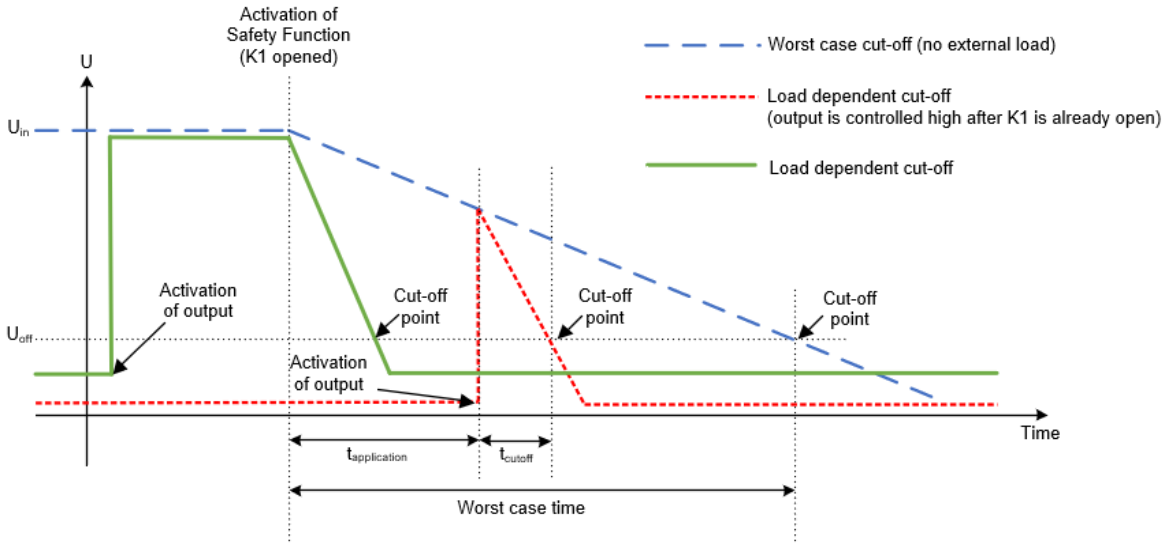

Figure 6. Output behavior following safety request

7 SL84 INTERNAL DIAGNOSTICS

7.1 Overview

This chapter describes internal diagnostics of the SL84. The following subsystems are covered by built-in diagnostic functions of the SL84:

- Safety MCU and SBC
- Flash and RAM memory used by a safety-related software
- Power supply
- Internal temperature

When an internal error is diagnosed, all output pins of the SL84 are de-energized by opening all of the outputs, i.e. the safe state is forced.

Application and code template related diagnostics are described in chapter, *Application Diagnostics*.

7.2 Start-up Diagnostics

To detect possible latent faults, built-in self-tests are executed by the SL84 during start-up. If the start-up diagnostics detects an error, the SL84 will enter the safe state.

The following is covered by Start-up diagnostics:

- Built-in self-tests for the SBC and MCU to detect latent faults
- Integrity check of firmware, application, diagnostic log and parameters before execution
- Test of the execution of the safety function of SL84 (see Chapter, *Safety Function*)

7.3 Online Diagnostics

7.3.1 Description

Online diagnostics are the diagnostics implemented in the firmware. Diagnostics are scheduled independently and automatically until the system is shut down. It is not possible to disable internal diagnostics by the system integrator.

The following are covered by online diagnostics:

- Cross-monitoring of the MCU and SBC
- Monitoring of execution of the application software
- Detection of random hardware faults of the MCU
- Detection of soft errors in safety-related memory and registers
- Detection of random hardware faults of the SBC
- Integrity check of the I/O configuration
- Monitoring operation of A/D conversion
- Internal temperature monitoring
- Operating voltage monitoring of the SL84

7.3.2 Failure Reaction Time

For internal diagnostics, the maximum reaction time is 100 milliseconds.

FS ID: 15 Internal diagnostic reaction time must be taken into account when calculating the whole system failure reaction time.

7.3.3 System Behavior in Voltage Deviation Conditions

Diagnostics monitor undervoltage and overvoltage deviations in 1 millisecond intervals. Voltage fluctuations within the voltage limit values are not monitored by diagnostics.

Undervoltage is detected when supply voltage drops below under 9 V. When voltage drops under 6.1 V unit will shut down.

Overvoltage fault in Power Supply 1 (logic) is detected by Over Voltage Protection (OVP) logic. The limit value is approximately 34 V. When OVP detects overvoltage fault condition, it will go to safe state. To recovery over voltage situation unit need to reboot.

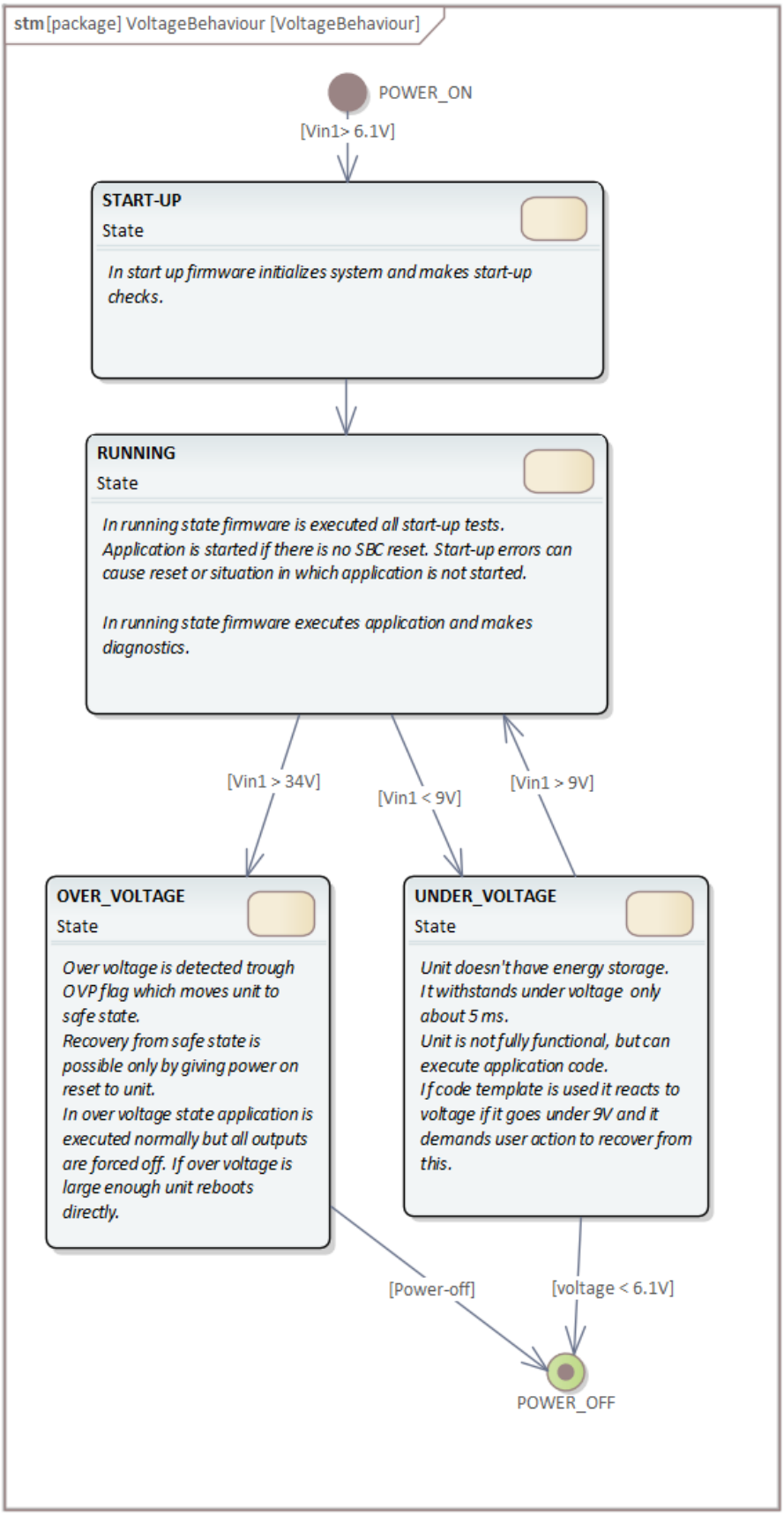

Figure 7. Firmware voltage deviation diagnostic states.

7.4 Sleep mode

Current consumption in sleep mode is low. When the SL84 Safety control unit is in sleep mode, all outputs are in safe state.

- Power supply OVP protects against over voltages
- MCU is unpowered
- SBC is in sleep mode and listens to CAN 2 communication

For more information, refer to *SL84 Technical Manual.*

For more information how to implement sleep mode, refer to *Epec Programming and Libraries Manual.*

7.4.1 Sleep

Sleep mode can be activated from CODESYS application with the *SSeriesSystemExt* library.

- SleepMode (function)

For more information, refer to *SL84 Technical Manual.*

For more information how to implement sleep mode, refer to *Epec Programming and Libraries Manual.*

7.4.2 Wake-up

SL84 can be woken up with any CAN message in can bus 2 or by rebooting power supply 1.
When SL84 wakes up from the sleep mode, it starts up like in a normal power reset. After restarting, the SL84 runs all startup tests.

For more information, refer to *SL84 Technical Manual.*

For more information how to implement sleep mode, refer to *Epec Programming and Libraries Manual.*

7.5 Diagnostic Logs

When a diagnostic error or fault is detected, then the information, i.e. a diagnostic log entry, is saved into diagnostic logs in flash memory. The information is also passed to CODESYS IDE log engine and is visible for developers in every system startup either due to power on reset or system SW reset. System errors can be also read through EPEC *SSeriesSystemExt* library and are also available through the CODESYS IDE's Logs tab of the Device window.

Most of the diagnostic errors in the log are firmware diagnostic specific. However, errors can also be caused due to application exceptions, which lead into a reset cycle.

As an example, in the following picture an application's faulty memory access has generated a Memory Protection Unit (MPU) exception which leads into a reset cycle (*Figure 8. An example of firmware diagnostic errors in the CODESYS IDE Device Log*.) The firmware log contains errors before and after the reset cycle.

- In this specific case *yellow warnings have occurred before the reset cycle and as such indicate what has led into the reset cycle*.

- In this specific case *red errors are new detected errors after the reset and indicate that the SL84 has detected the reset cycle* caused by the MPU exception.
- The highlighted line indicates that MCU has detected an exception in an unsafe application address: 0xc01f3a. The actual error is detected by Memory Protection Unit and indicates invalid write memory access from unsafe PRG to safe memory. Error code 57017 identifies accessed safe memory (dec: 1073808128 / hex: 40010300).

After the reset, SBC detects a sync error with MCU and there are multiple cascading errors leading into the safe state. Safe state is forced until the operator power cycles the device. In the reset cycle, the application is not loaded as it could lead into a reset escalation cycle.

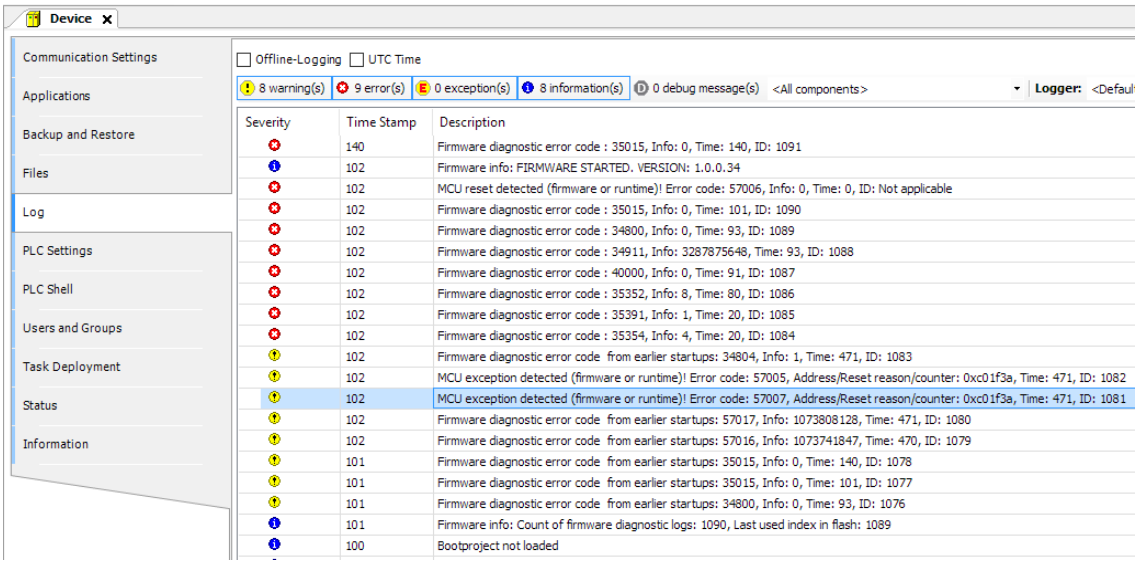

Figure 8. An example of firmware diagnostic errors in the CODESYS IDE Device Log.

Note: Yellow warnings are also always shown after normal power on resets to indicate which errors have occurred in the past. Thus, these do not necessarily mean that the system has started after a system SW reset cycle, only that some errors have been detected in the past.

Red errors always indicate the new errors detected after MCU is started either due to power on reset or system SW reset and always force the safe state.

8 INSTALLATION, CABLING AND CONNECTIONS

8.1 Operating Environment, Installation and Cabling

FS ID: 16 The system integrator shall ensure that SL84 is used under operating conditions which fulfill EMC and environmental specifications as presented in the Technical Manual. (Epec SL84 Safety Control Unit Technical Manual).

FS ID: 17 The system integrator shall notice that if SL84 is operated outside operating temperature range as given in the Technical Manual, SL84 will enter the safe state. (Epec SL84 Safety Control Unit Technical Manual).

FS ID: 18 The system integrator shall ensure that lengths for wires and cables used in connections do not exceed maximum allowed lengths as given in the Technical Manual. (Epec SL84 Safety Control Unit Technical Manual > Input/Output Specifications, for each input type Electrical Characteristics Table)

8.2 I/0 Interface

The Epec SL84 Safety Control Unit includes the following external interfaces.

FS ID: 19 System integrator is responsible to implement required diagnostic functions in application software to achieve sufficient diagnostic coverage for I/O interface of SL84.

8.2.1 AI/DI_Type116_0_0_SL84

This type of input is used to read analog signals from sensors with 0…5 V analog output or 0…22 mA current output and Digital output sensors. This input type has three operating modes: voltage, current and digital input mode. Operating mode selection is possible only in the initialization phase of the application. The default operating mode after power is switched on, is voltage input mode and pin is pull-down to GND true 84,2 kΩ

In Voltage Mode this input type has software selectable 2,2 kΩ to 5 V pull-up resistors.

In Digital input Mode this input type has software selectable 2,2 kΩ to 5 V pull-up resistors.

FS ID: 20 When using this pin type for safety -related application, Ai-BiasVoltage has to be sertain voltage levels, AI-BiasVoltage has to evaluate in every application cycle on application level prior this information is used by safety-related application software.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.1.1 Voltage input mode

The voltage input mode supports 0…5 V voltage range.

Depending on the sensor 82,4 kΩ pull-down to GND and 2,2 kΩ to 5 V pull-up to resistors may be selected.

FS ID: 21 The signal range check shall be used to detect electrical faults, i.e. short-circuits and line breaks.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.1.2 Current input mode

The current measurement mode can be used to read active sensors.

FS ID: 22 When pin is used as Current input mode, programmable pull-up resistors shall not be used for safety related inputs

FS ID: 23 The signal range check shall be used to detect electrical faults, i.e. short-circuits and line breaks.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

When using this pin type in current mode, the input has an overcurrent protection limiting the current to a practical level.

A prolonged time of overcurrent input shall be switched to voltage mode by the application for additional protection.

8.2.1.3 Digital input mode

When using this pin type as a digital input, input threshold voltage levels are selected with a Safe Conversion library.

Depending on the sensor 2,2 kΩ to 5 V pull-up to resistors may be selected.

FS ID: 24 When pin is used as Digital input mode, programmable pull-up resistors shall not be used for safety related inputs.

8.2.2 PI/DI_Type075_2_0_SL84

This type of input is used to read signals from sensors with pulse output and digital output.

This input type has software selectable 12,2 kΩ pull-down and 2,2 kΩ to 5 V pull-up resistors.

This input type has two operating modes: pulse input and digital input mode. The default operating mode is digital input mode and pin is pull-down to GND true 12,2 kΩ.

The operating mode selection is possible only in the initialization phase of the application.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.2.1 Pulse input mode

Depending on the sensor, 12,2 kΩ pull-down and 2,2 kΩ to 5 V pull-up resistors may be selected.

System integrator shall use sensors suitable for the safety feature taking into account process safety time.

8.2.2.2 Digital input mode

When using this pin type as a digital input, voltage levels are fixed. For more information, refer to *SL84 Technical Manual.*

FS ID: 25 When pin is used as PI or DI input mode, programmable pull-up resistors shall not be used and 12,2 kΩ pull-down shall be selected for safety related inputs.

8.2.3 PI/DI_2_type_039_0_2_SL84

This type of input is used to read signals from sensors with pulse output and digital output.

This input type has 10 kΩ pull-down resistor to GND.

This input type has two operating modes: pulse input and digital input mode. The default operating mode is digital input mode.

The operating mode selection is possible only in the initialization phase of the application.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.3.1 Pulse input mode

System integrator shall use sensors suitable for the safety feature taking into account process safety time.

8.2.3.2 Digital input mode

When using this pin type as a digital input, voltage levels are fixed. For more information, refer to *SL84 Technical Manual.*

8.2.4 PWM/DO/CM 3 A_type114_1_4_SL84 (Cat. 2)

This type of output has high-side current measurement.

The output leakage current is less than 5 mA, when the output is de-energized.

This output has three operating modes: disabled, PWM and digital output mode. The default operating mode after the power is switched on, is the disabled output mode.

FS ID: 26 To avoid common-cause failures, the system integrator shall separate EL84 power supply wires and output wires to actuators to claim fault exclusion according to the EN ISO 13849-2.

8.2.4.1 Un-initialized output pins

All un-used pins shall be initialized and add reverse voltage diagnostic to application code. Reverse voltage diagnostic is for diagnose if when application is running and error in wire harness occurs and SL84 output comes voltage.

8.2.4.2 PWM output mode (Cat. 2)

FS ID: 27 The PWM control value shall be monitored by the safety application by using a suitable PWM output diagnostic function.

Possible PWM output diagnostics are status feedback signal (pulse width) and output current measurement. For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.4.3 Digital output mode (Cat. 2)

FS ID: 28 Digital output shall be monitored by the safety application by using the status feedback signal.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.5 PWM/DO/CM 3 A Cut-off_type114_2_0_SL84 (Cat. 2)

This type of output has high-side current measurement. These pins are power true Cut off power supply group 2.

The output leakage current is less than 5 mA, when the output is de-energized

This output has three operating modes: disabled, PWM and digital output mode. The default operating mode after the power is switched on, is the disabled output mode.

FS ID: 29 To avoid common-cause failures, the system integrator shall separate EL84 power supply wires and output wires to actuators to claim fault exclusion according to the EN ISO 13849-2.

8.2.5.1 Un-initialized output pins

All un-used pins shall be initialized and add reverse voltage diagnostic to application code. Reverse voltage diagnostic is for diagnose if when application is running and error in wire harness occurs and SL84 output comes voltage.

8.2.5.2 PWM output mode (Cat. 2)

FS ID: 30 The PWM control value shall be monitored by the safety application by using a suitable PWM output diagnostic function.

Possible PWM output diagnostics are status feedback signal (pulse width) and output current measurement. For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.5.3 Digital output mode (Cat. 2)

FS ID: 31 Digital output shall be monitored by the safety application by using the status feedback signal.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.6 DO/CM 5 A Type_124_1_1_SL84

This type of output has high-side current measurement.

The output leakage current is less than 5 mA, when the output is de-energized.

This output has two operating modes: disabled, digital output mode. The default operating mode after the power is switched on, is the disabled output mode.

FS ID: 32 To avoid common-cause failures, the system integrator shall separate SL84 power supply wires and output wires to actuators to claim fault exclusion according to the EN ISO 13849-2.

8.2.6.1 Digital output mode (Cat. 2)

FS ID: 33 Digital output shall be monitored by the safety application by using by using a suitable DO output diagnostic function.

Possible DO output diagnostics are status feedback signal and output current measurement. For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.6.2 Un-initialized output pins

All un-used pins shall be initialized and add reverse voltage diagnostic to application code. Reverse voltage diagnostic is for diagnose if when application is running and error in wire harness occurs and SL84 output comes voltage.

8.2.7 DO 3 A_type_125_1_0_SL84

This type of output has status information.

The output leakage current is less than 5 mA, when the output is de-energized.

This output has two operating modes: disabled, digital output mode. The default operating mode after the power is switched on, is the disabled output mode.

FS ID: 34 To avoid common-cause failures, the system integrator shall separate SL84 power supply wires and output wires to actuators to claim fault exclusion according to the EN ISO 13849-2.

8.2.7.1 Digital output mode

FS ID: 35 Digital output shall be monitored by the safety application by using the status signal.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.2.7.2 Un-initialized output pins

All un-used pins shall be initialized and add reverse voltage diagnostic to application code. Reverse voltage diagnostic is for diagnose if when application is running and error in wire harness occurs and SL84 output comes voltage.

8.2.8 DO_GND 3 A_Type048_3_1_SL84

This type of output is current sinking output

The output leakage sinking current is less than 5 mA, when the output is de-energized.

This output has two operating modes: disabled and digital output mode. The default operating mode after the power is switched on, is the disabled output mode.

FS ID: 36 The output startup diagnostic needs to be done in user application. Power supply 3 has to be implemented with correct voltage levels before startup diagnostic can be done.

For more information how to implement DO_GND pin startup diagnostic, refer to *Epec Programming and Libraries Manual.*

FS ID: 37 To avoid common-cause failures, the system integrator shall separate SL84 power supply wires and output wires to actuators to claim fault exclusion according to the EN ISO 13849-2.

8.2.8.1 Un-initialized output pins

All un-used pins shall be initialized and add reverse voltage diagnostic to application code. Reverse voltage diagnostic is for diagnose if when application is running and error in wire harness occurs and SL84 output comes voltage.

8.2.8.2 Digital output mode

FS ID: 38 Digital output shall be monitored by the safety application by using the status feedback signal.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

8.3 Sensor Power Supply

SL84 provides a 5 V power supply for external sensors. The sensor power supply is protected against short-circuit to the safety control unit's operating voltage or ground.

The sensor power supply also has overload protection by sensing overtemperature.

This output can be switched on and off by an application. The default setting after power up is OFF.

FS ID: 39 Output voltage of the 5V power supply shall be measured by the application to detect a short-circuit or overload condition. In case of failure, output voltage shall be switched off for additional protection.

FS ID: 40 The system integrator shall analyze effects of Sensor supply voltage fluctuations to safety related sensor signals and possibilities to compensate the effects by measuring Sensor supply voltage.

8.4 AI BIAS voltage

SL84 provides 8 V AI BIAS Voltage for analog inputs current measurement circuits. The voltage has to diagnose in the user application:

- Low voltage (under 7,8 V), analog input signal is not valid
- High voltage (over 8,9 V), analog input signal is not valid

If voltage is not between 7,8 V to 8,9 V then user application has to set safe state.

For more information how to implement diagnostics, refer to *Epec Programming and Libraries Manual.*

9 SYSTEM EXAMPLES

Specific application functional safety levels can be reached up to PLd Cat. 2 and SIL 2.

See the example architecture pictures below.

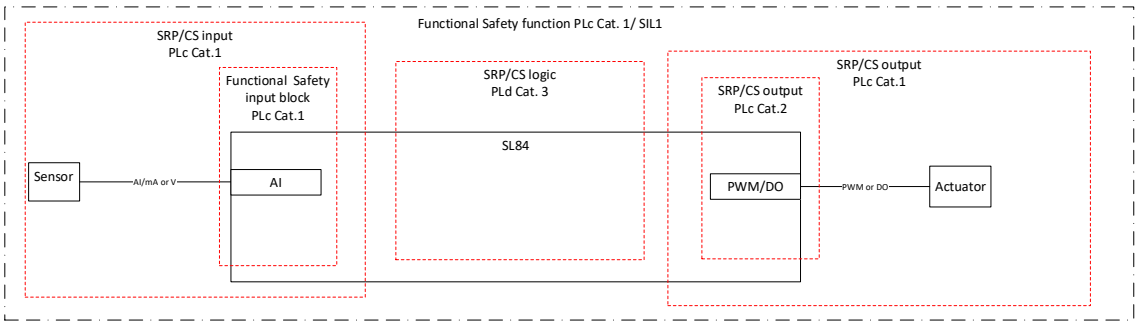

Figure 9 Category 1 architecture.

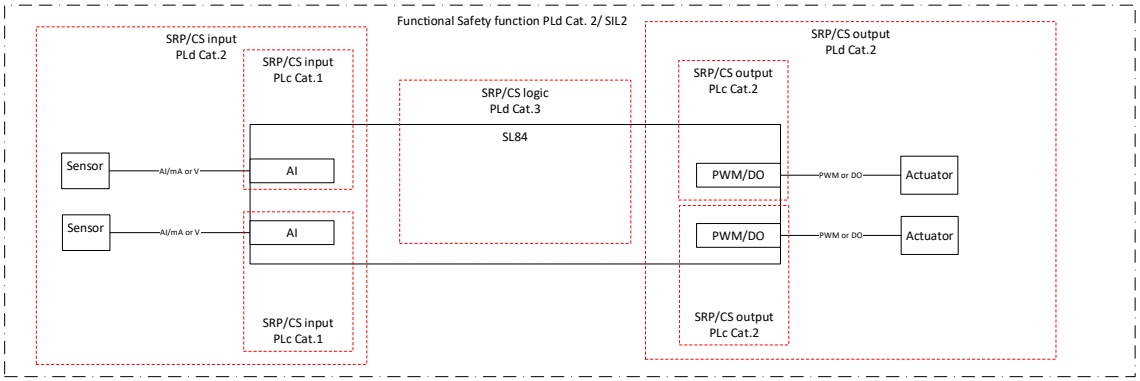

Figure 10 Category 2 architecture (AI+AI and PWM/DO+PWM/DO).

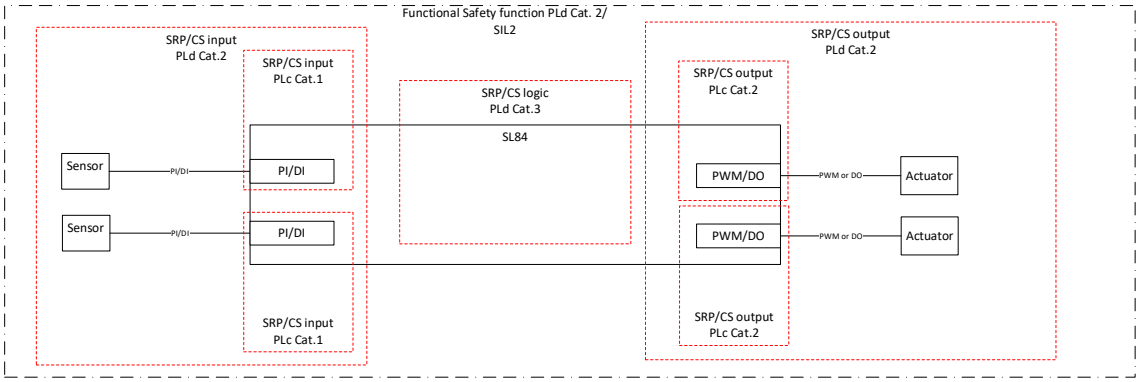

Figure 11 Category 2 architecture (PI/DI+PI/DI and PWM/DO+PWM/DO).

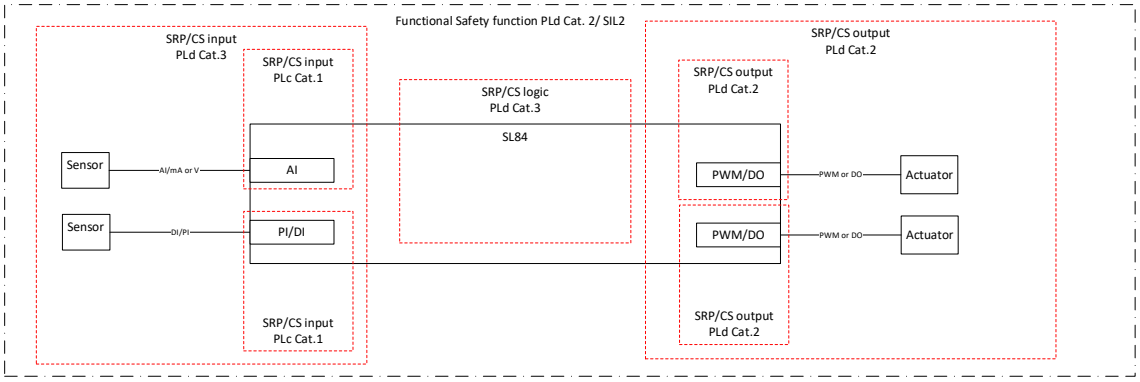

Figure 12 Category 2 architecture (AI+PI/DI and PWM/DO+PWM/DO).

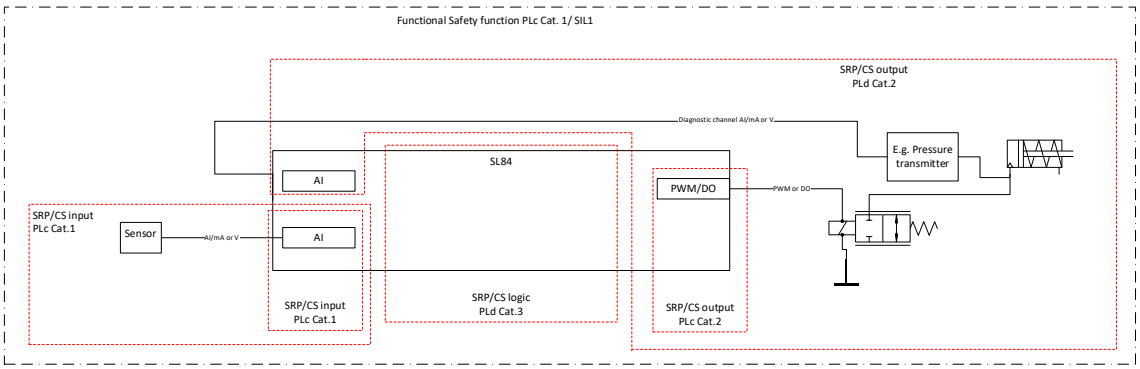

Figure 13 Category 1 architecture (AI and PWM/DO+AI).

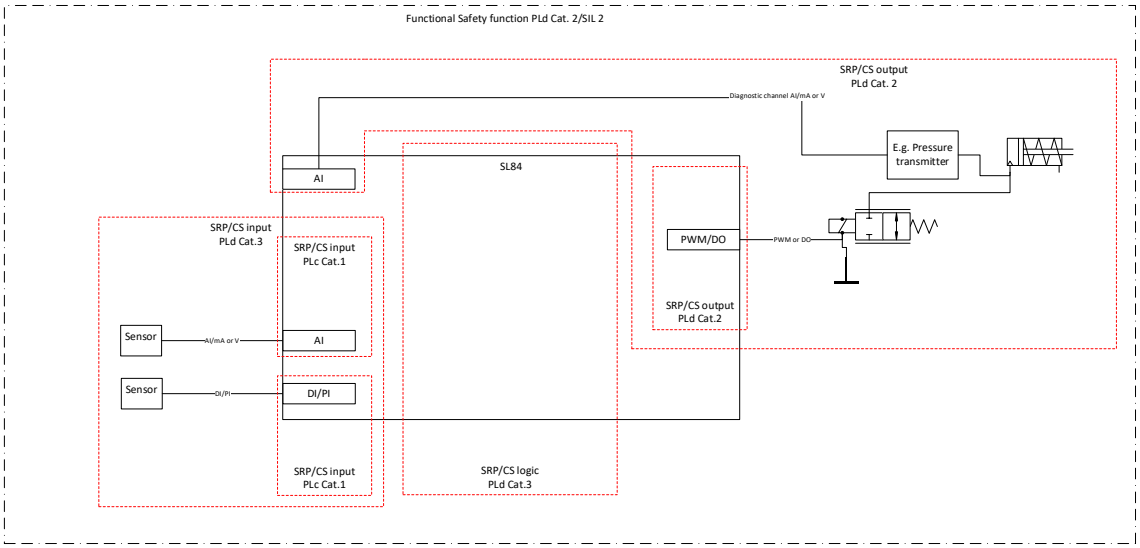

Figure 14 Category 2 architecture (AI and PWM/DO+AI).

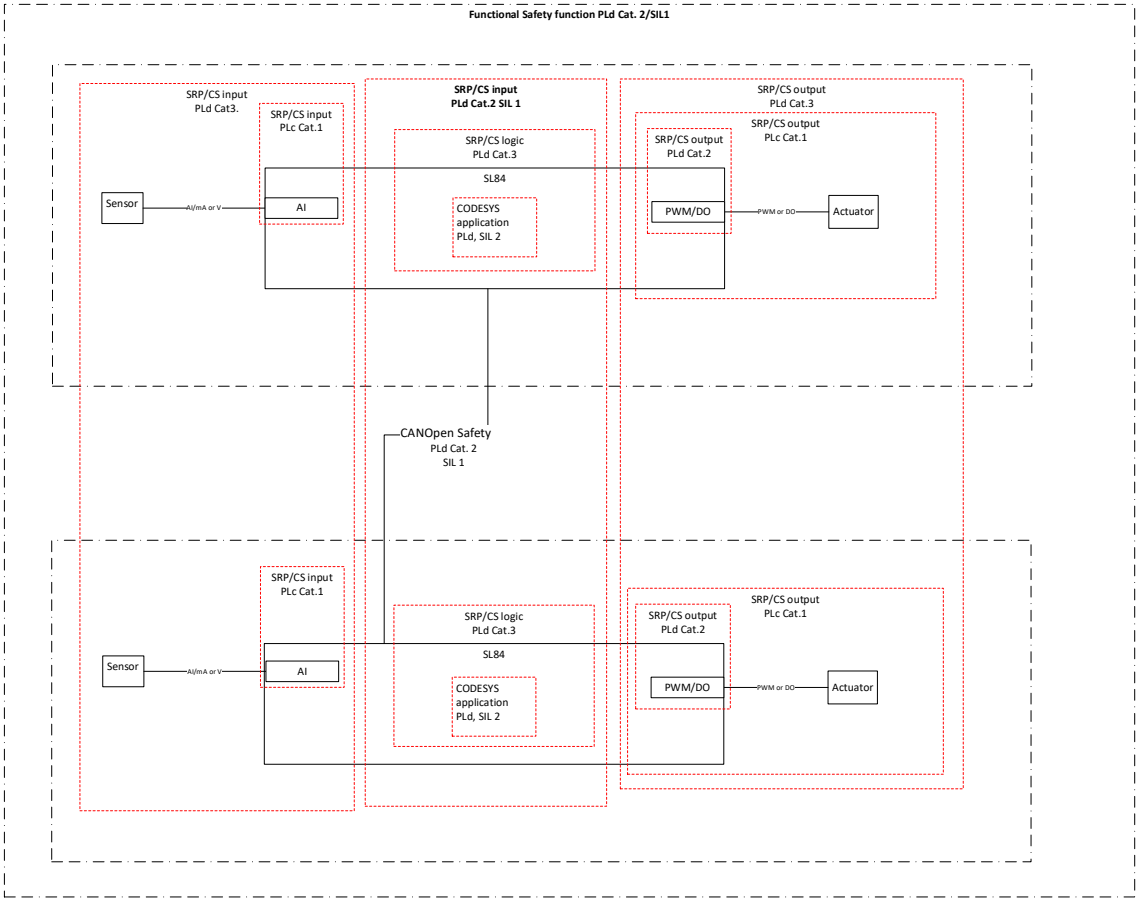

Figure 15 Category 2 architecture (AI+AI and PWM/DO+PWM/DO).

10 SYSTEM EXAMPLES CUTOFF

10.1 In a Cutoff group

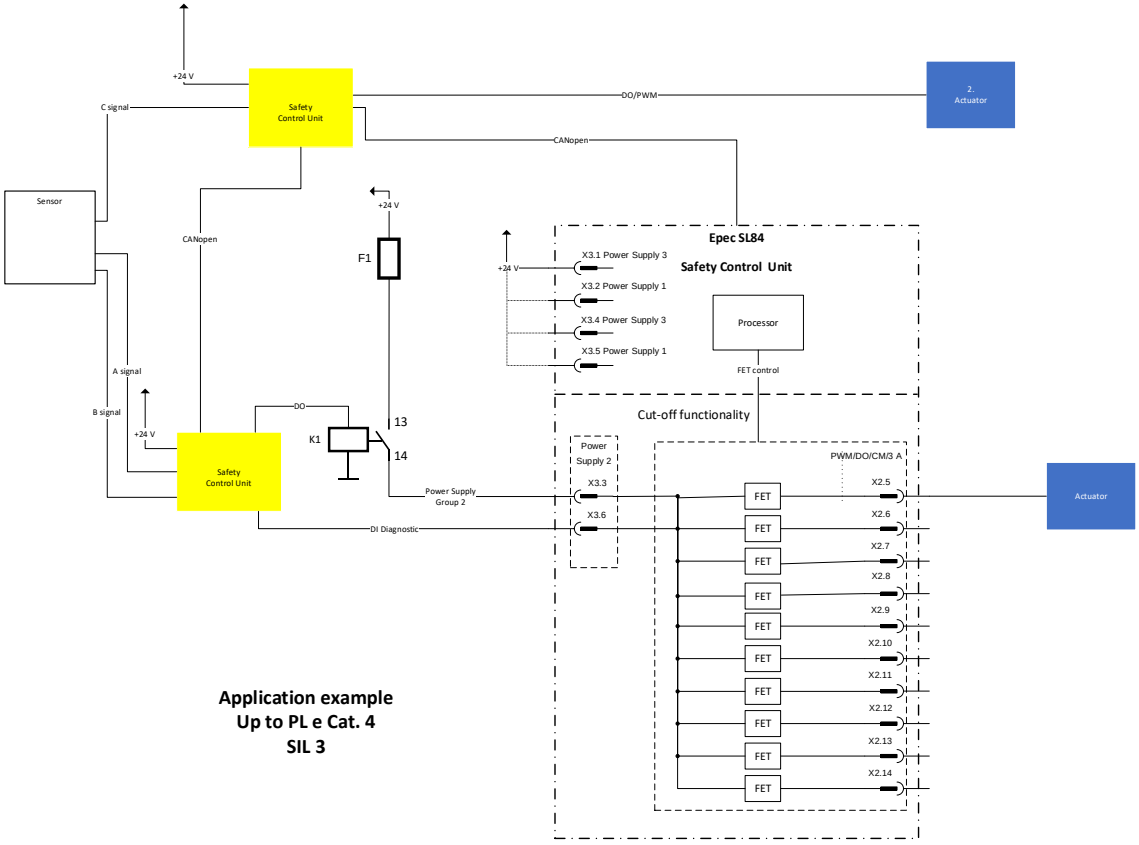

Figure 16 System Example up to PL e Cat. 4, SIL 3, ASIL D

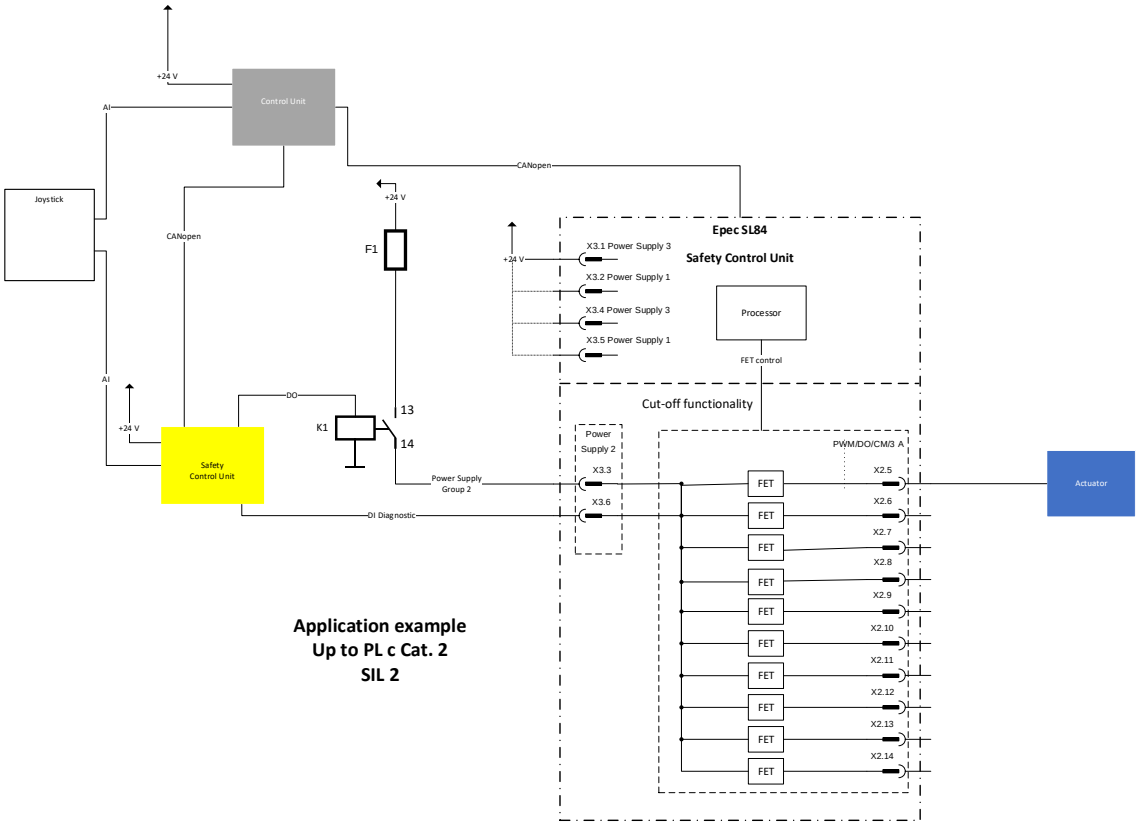

Figure 17 System Example up to PL c Cat. 2, SIL 2, ASIL C

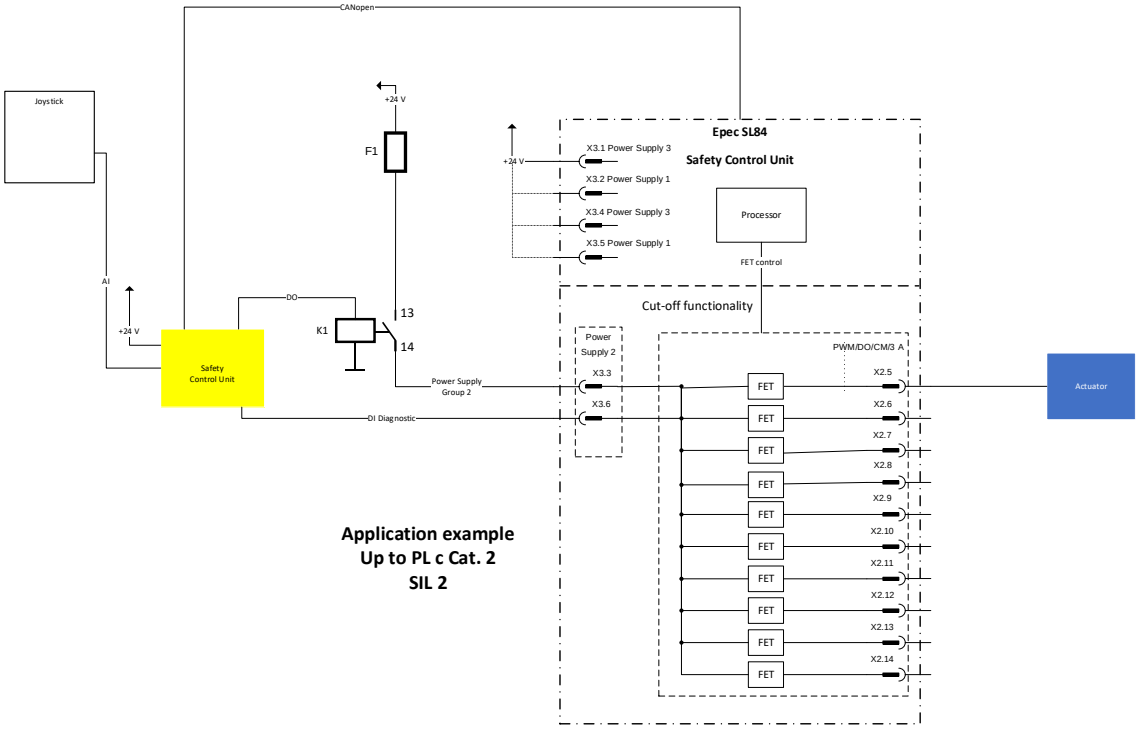

Figure 18 System Example up to PL c Cat. 2, SIL 2, ASIL C

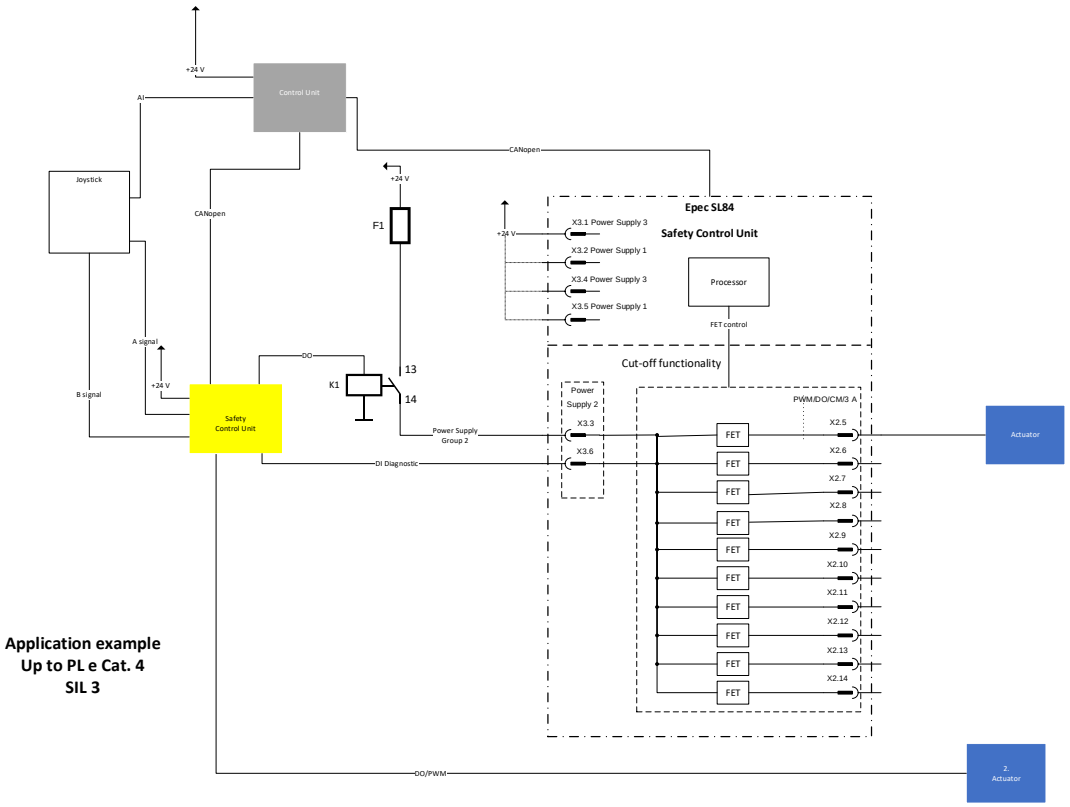

Figure 19 System Example up to PL e Cat. 4, SIL 3, ASIL D

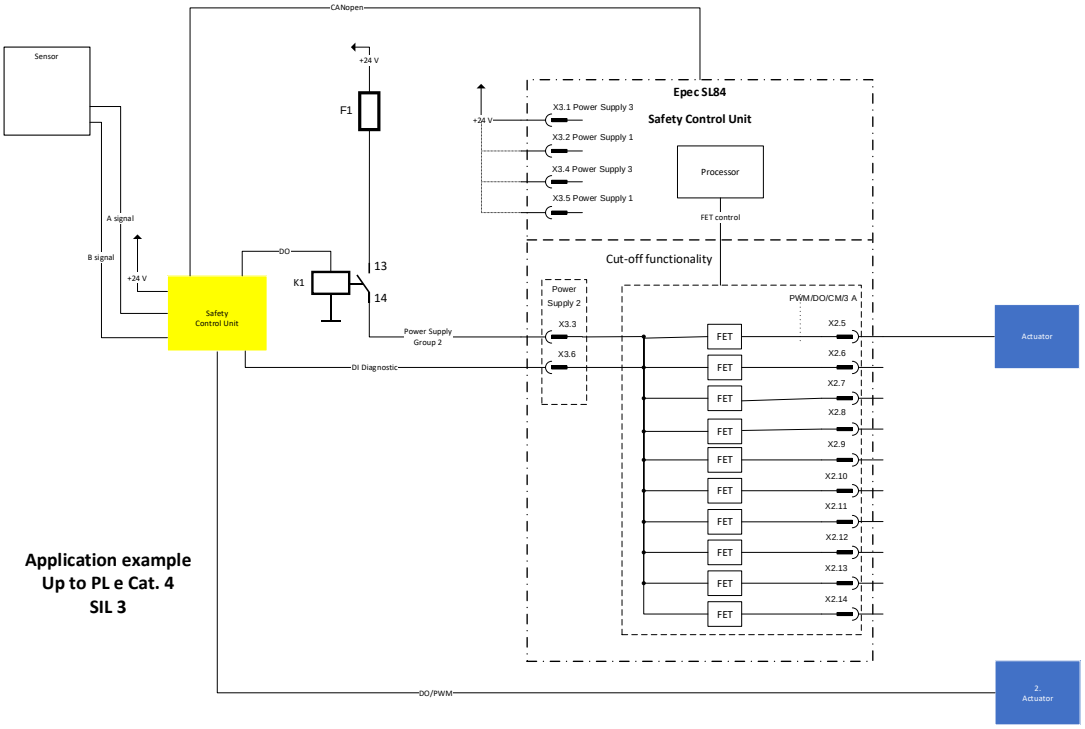

Figure 20 System Example up to PL e Cat. 4, SIL 3, ASIL D

11 SAFETY RELATED APPLICATION DEVELOPMENT

11.1 Development Environment

11.1.1 Application Development

The application development shall be done using the following software versions:

- CODESYS 3.5 SP10 (3.5.10.0)
- SIL2 extension for CODESYS 3.5 SP10
- EPEC SDK 3.9 or later
  - Contains MultiTool 6.7 or later, which supports SL84
  - Available from Epec Extranet

FS ID: 41 The system integrator shall verify that requirement presented in the CODESYS Programming Guidelines (H2) are followed during application development [MAN000613]

Exception: As opposed to presented in the CODESYS Programming Guidelines (H2), MOD, EXPT, COS, ACOS, SIN, ASIN, TAN, ATAN, LOG and SQRT use is permitted in system level when using Structured Text.

11.1.2 Software Download

It is possible to update SL84 firmware and application in the field. This can be done using standard CANopen tool, but it is recommended to use EPEC CANmoon.

FS ID: 42 The machine manufacturer shall ensure that only trained persons are authorized to update software to SL84.

FS ID: 43 Before software download is started, the machine must always be set to a safe position in which deactivation of all outputs does not cause a possible hazardous situation.

For more information, refer to *Epec Programming and Libraries Manual:*

- *Programming> Programming SL84 Safety Control Unit > Updating Firmware*
- *Programming > Downloading PLCopen Application*

11.2 Application download and debugging with CODESYS IDE

11.2.1 Debugging modes

It is possible to debug an application and download the application to SL84 with CODESYS IDE. It must be noticed that there are two different modes in the login state to CODESYS: Debug mode and Safe Run mode.

DEBUG	In the debug mode, it is possible to set break points and force variables. In this mode, there is no memory protection between the safe and non-safe parts of the application. This mode is used only for debugging. It is possible to download an application only in this mode. The safety unit can only be changed to this mode by selection.
SAFE RUN	In the safe run mode, the application runs normally but CODESYS IDE can be used to monitor variables in unit.

CODESYS IDE always demands the password when connected to the SL84. This doesn't depend on the used mode. To change the SL84 to the debug mode, it must be done in CODESYS IDE through the SIL2 menu. If the SL84 is changed to the debug mode, it is possible to change back to the safe run mode, only by giving a power boot up to the SL84.

FS ID: 44 In Debug-mode, the performance and response time characteristics of safety-related application cannot be guaranteed. Therefore, execution of safety-related application shall be considered as non-safe.

FS ID: 45 CODESYS IDE shall not be used to update software in field/production. It shall be only used during the application development phase.

11.3 Application Interface

It is possible to program the SL84 by starting an empty project with CODESYS. However, it is recommended to use MultiTool to make programming easier. MultiTool is used to define, for example, CAN, CANopen, J1939, I/O and parameter configurations.

11.3.1 MultiTool features

The table below lists features that Multitool generates to the code template. The application is developed on top of the code template. The table indicates if the feature is available in non-safety related program or in safety related program. It is important to realize that in this table, safety related does not mean the code is safe as such but refers to in which context the PRG is running. The safety related code has a yellow colored background in CODESYS IDE, to show the difference between safety related and non-safety related code easier.

Feature	Non-safety related	Safety related	Note
I/O	X	X	It is always mandatory to design the machine system to fulfill safety level requirements. I/O initialization is always made in safety related code but it is possible to map I/O variables from the safety and non-safety related code.

I/O Diagnostic		X	I/O diagnostic is always implemented in safety related code.
System Diagnostics		X	System related diagnostics are always executed in safety related code.
CAN	X		It is not possible to use CAN message handling directly from the safety related code.
CANopen	X		It is not possible to use CANopen directly from the safety related code.
J1939	X		It is not possible to use J1939 directly from the safety related code.
SRDO		X	CANopen safety PDOs.
Fast parameters	X		Parameters are used always in the non-safety related code.
Parameters	X		Parameters are used always in the non-safety related code.

11.3.2 Code template

MultiTool generates a code template which contains initialization of the features defined in MultiTool. System integrator shall write code to the following PRGs. The code template should not be modified in CODESYS, because changes are overwritten during next import.

PRG	Non-safety related	Safety related	Note
Main	X		Called cyclically when all initializations are executed.
MainInit	X		Called after code template initializations have been made.
S_Main		X	Called cyclically when all initializations are executed.
S_MainInit		X	Called after code template initializations have been made.

11.3.2.1 Tasks in code template

Code template automatically generates two tasks, each of which is linked to own PRG.

PRG	Task cycle	Context	Watchdog	Priority
S_PLC_PRG	10 ms	Safe	10 ms	0
PLC_PRG	10 ms	Non-safe	No watchdog	1

11.3.2.2 Code Template Validation

A code template generated by MultiTool is divided into safety related and non-safety related parts.

FS ID: 46 System integrator shall verify safety related parts of a code template which is generated by MultiTool.

A review guideline for MultiTool code template is provided in the programming manual. *(Epec Programming & Libraries Manual>Programming>Programming Safety Projects> Code Template Review Instructions)*

11.3.3 SL84 Specific Safety Requirements for Application

FS ID: 47 When using NVRAM to store safety-related data, it shall be protected with a signature using a cyclic redundancy check (CRC-16 or better) algorithm. When the data is read the signature shall be re-calculated and checked. This can be done with SafeDataValidation library's Calculate16bitCRC function.

When MultiTool is used, the code template checks the signature.

11.3.4 Floating point exeptions

FS ID: 48 All functions in the application, which are using the FPU shall be fully tested with all boundary values of all calculations.

For more information, refer to Epec Programming and Libraries Manual > Programming > Programming SL84 Safety Control Unit > Floating point calculations.

SL84 does not fully conform to IEEE 754. Single-precision 32 bit floating point operations can cause exception and the Invalid Operation / Input Error, Divide by Zero, Underflow and Overflow exceptions are enabled. Inexact exception is not enabled, and default floating point rounding mode is to round to nearest. If a floating point operation causes an exception, then the exception information is captured and passed to the application via a diagnostic interface. Floating point calculation results are also passed to the application i.e. the exception does not stop the application execution. All the floating point calculation results are calculated according to the MCU's Embedded Floating-Point Unit.

When a floating point exception occurs, the SL84 does not force safe state and system reset. Instead the application must check the results and diagnostic information before using the values, for example, to control outputs. If the calculations cause exceptions, then the application developer must verify the results and decide when the results can be used, for example, to control outputs. The exceptions are also logged to the CODESYS Device logs and it is possible to double click the exception logs in the CODESYS IDE to find out which line of the application code causes exceptions.

11.4 Application Diagnostics

11.4.1 System Diagnostics in the code template

When Epec Multitool is used to configure the SL84, the Code template uses *S_SL84_Diagnostic* program (from *SafeSSeriesHardware* library), which combines several diagnostic measurements to one global status flag *S_SafeOperationEnable*, which can be used to control the application together with other status flags.

The following diagnostics are implemented to the *S_SL84_Diagnostic* program

- Supply voltages
- 5V REF voltage
- Temperatures (MCU and SBC)
- Firmware errors

FS ID: 49 System integrator shall implement required actions to the application code according to the S_SafeOperationEnable flag. It is recommended to set outputs to safe state by opening the safety switch and setting ouputs controls to safe state. Opening the safety switch from the application adds an error code to the firmware log.

If I/O is configured as an AI, the Code template contains overcurrent protection using *S_AIOverCurrentProtection* function.

11.4.2 Diagnostics in the System integrator specific code

Depending on safety requirements for the system integrator application, some diagnostics shall be implemented to the application. SL84 provides following data to implement diagnostics:

- System information e.g. HW version and FW version
- PCB temperature
- I/O diagnostics (this is described in more details in the following chapter)

11.5 I/O Diagnostics

11.5.1 Description

The internal diagnostic of SL84 and the Code template generated by the Multitool does not cover System integrator specific application I/O diagnostics.

FS ID: 50 System integrator shall implement required I/O diagnostic functions to application software.

Required diagnostics for certain pin types are described in chapter *8.2, I/O Interface*.

Validity checking of the output controls and input signals must always be in the application. Individual output control or input signal is never safe. The required safety level is achieved through system design by using the correct combination of sensors and actuators.

11.6 CAN Interface

11.6.1 Description

Normal data exchange by using standard CAN bus and CANopen protocol shall be considered as unsafe because necessary diagnostic measures are not provided by the communication system.

FS ID: 51 For safety-related communication, CANopen Safety protocol according to EN 50325–5 shall be used. This can be implemented by using Epec CANopen and SafeCANopenSRDO *libraries with SL84.*

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance system
Corruption (see EN 61784–3)							X	
Unintended repetition (see EN 61784–3)							X	
Incorrect sequence (see EN 61784–3)							X	
Loss (see EN 61784–3)							X	
Unacceptable delay (see EN 61784–3)			X					
Insertion (see EN 61784–3)				X			X	
Masquerade (see EN 61784–3)				X				X
Addressing (see EN 61784–3)				X				X

Figure 21. Communication errors and safety measures matrix. (EN 50325-5:2010, Table 1)

11.7 Failure reaction time

Abbreviation	Description
n_{afs}	AI filtering sample count, number of samples used to calculate mean value of analog input.
t_{avd}	AI validation Delay time, fault detection delay parameter for application library.
t_{CPS}	Program cycle time, Safety PRG cycle time
t_{CP}	Program cycle time, Non-safety PRG cycle time
f_{PWM}	PWM frequency
t_{sc}	SRDO message's Refresh time
t_{sct}	EN50325-5 Safety Cycle Time

The worst-case failure reaction time is the sum of subsequent delays:

Without an internal fault of SL84 using local I/O:

Input processing = n_{afs}* 1 ms + t_{avd}
Logic solver = 2 * t_{CPS}
Signal output = 1/ f_{PWM}

Failure reaction time = Input processing + Logic solver + Signal output

Without an internal fault of SL84 using remote I/O:

On transmitting end:

Input processing = n_{afs}* 1 ms + t_{avd}
Safe transmission = x * t_{CP} + 1 * t_{CPS}

Note: x * t_{CP} >= t_{SC}

Note: SRDO message's refresh time t_{sc} shall be greater than 2 * t_{CPS}

On receiving end:

Logic solver = (2 * t_{CP}) + (1 * t_{CPS}) however, at least t_{sct}
Signal output = 1/ f_{PWM}

Failure reaction time = Input processing + Safe transmission + Logic solver + Signal output

Note: EN50325-5 Safety Cycle Time (t_{sct}): 50 milliseconds by default. Application adjustable up to 65535ms.

With an internal fault of SL84:

Maximum 100 ms from the occurrence of an internal fault.

12 SERVICE AND MAINTENANCE

12.1 Service

SL84 is not field-serviceable. If SL84 is disassembled in the field, the system is then considered as unsafe. SL84 repair work is allowed be carried out by Epec After Sales Service only.

FS ID: 52 Machine manufacturer shall inform Epec about any failures of SL84. A faulty SL84 shall be sent to Epec After Sales Service.

12.2 Maintenance

FS ID: 53 Machine manufacturer shall provide Epec a contact information of the person(s) who shall be informed about any potentially safety-related issue related to Epec SL84 Safety Control Unit.

FS ID: 54 Machine manufacturer shall promptly inform Epec about any potentially hazardous event which may be related to SL84. This information shall be delivered to Epec Customer Support.

FS ID: 55 In case of safety related modification of SL84, machine manufacturer shall carry out an impact analysis of the modification and necessary actions resulting from the impact analysis.

13 INFORMATION FOR USE - RELATED DOCUMENTS

13.1 Related standards:

Document name:	Description:
IEC 61508:2010	Functional safety of electric/electronic/programmable electronic safety-related systems.
EN ISO 13849-1:2015	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design.
IEC 62061:2005	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.
EN 50325-5:2010	Industrial communications subsystem based on ISO 11898 (CAN) for controller-device interfaces. Functional safety communication based on EN 50325-4

13.2 Related documentation:

Document name:	ID:
Epec SL84 Safety Unit Technical Manual	MAN000728
Epec Programming and Libraries Manual	MAN000538 v 3.9 or newer
Epec MultiTool User Manual	MAN000316 v 6.7
Epec CANmoon User Manual	MAN000405 v 3.1
CODESYS (Application) Programming Guidelines (-H2)	MAN000613 v6.0 (CODESYS version)

14 LIST OF FIGURES

15 LIST OF FUNCTIONAL SAFETY ID (FS ID)

The following list is compiled of important information or safety instructions, marked by the functional safety icon throughout this manual. These are requirements that shall be fulfilled by the system integrator.