SC52 Safety Control Unit

Safety Manual

Version 3.1

DOCUMENT VERSION HISTORY

Version	Date	Notes
0.1	19.02.2018	First Version
1.0	5.4.2018	Document released (Rev 16)
2.0	25.1.2019	Document released (Rev 17) - Updated new hardware version 8916D01 - Updated Diagnostic Log section - Updated Floating point exception FS ID: 45Updated Floating point exceptions section - Updated chapter 9: Updated headings and added backwards compatibility FS ID: 53 - Document version updated 1.0 -> 2.0 - Chapter 9.2 updated - Page 2, Version 2.0 Date updated - Updated device description and library versions to chapter 3.1
3.0	18.11.2019	Document released (Rev 18) - Updated chapters 6.2.4.2 and 6.2.4.3 title to include Cat. 2 - Updated FS ID 8 - Chapter 6.2.4 updated - Chapter 7.1.1: Added exception to the CODESYS Programming Guidelines
3.1	13.03.2020	Document updated (Rev 19) - Text lost during .pdf conversion; mising text updated to chapter 6.2.3

TABLE OF CONTENTS

Epec Oy reserves all rights for improvements without prior notice

Epec Oy reserves all rights for improvements without prior notice

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 SC52 Safety Control Unit in compliance with IEC 61508 and ISO 13849.

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

Copying of this document without permission is prohibited. All trademarks mentioned in this document are owned by their manufacturers.

1.2 Scope

This Safety Manual contains requirements for implementation of safety related control system using Epec SC52 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 SC52 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 3 (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 SC52 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 SC52 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:

FS

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 SC52 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 SC52 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 SC52 Safety Control Unit consists of the following hardware and software components:

- Epec SC52 Safety Control Unit / Hardware v. 8916D01
  - The hardware is equipped with a Main CPU and a System Basis Chip acting as an intelligent watchdog.

- Epec SC52 Safety Control Unit / Firmware v. 1.2.1.33099
  - The firmware provides the low-level control for the SC52 hardware and CODESYS Runtime.

- Epec SC52 Safety Control Unit / Device Description v. 3.5.10.6

- Epec Platform Specific Safety Libraries
  - *SafeSC52Int* library v. 1.1.0.1
  - *SafeSSeriesIoDriverExt* library v. 1.0.0.6
    SafeSSeriesHardware library v. 1.2.1.1
- Epec Platform Specific Libraries
  - *SSeriesCanExt* library v. 1.0.0.1
  - *SSeriesHardware* library v. 1.0.0.5
  - *SSeriesNvRamExt* library v. 1.0.0.4
  - *SSeriesSystemExt* library v. 1.0.0.12

- Epec Common Safety Libraries
  - *DiagnosticInterface* library v. 1.0.0.1
  - *SafeCANopenSRDO* library v. 1.1.0.0
  - *SafeConversion* library v. 1.0.1.2
  - *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. 4.0.2.4

It is possible to use also other Epec Common libraries with SC52 e.g. J1939 library, but those are not covered by this Safety manual.

3.2 Safety Function

The Epec SC52 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 SC52 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.

Epec Oy reserves all rights for improvements without prior notice

FS *FS ID: 5 The system integrator shall ensure that the de-energize of outputs of the SC52's safe state will not cause any new possible hazardous situations of the machine.*

FS *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 SC52 is switched OFF and switched ON again to re-start the SC52.*

3.3 Product Architecture

A high-level block diagram of the safety architecture is presented in Figure 1. The architecture is designed to meet Category 3 (EN ISO 13849-1:2015) which means that any single fault does not lead to a loss of the safety function.

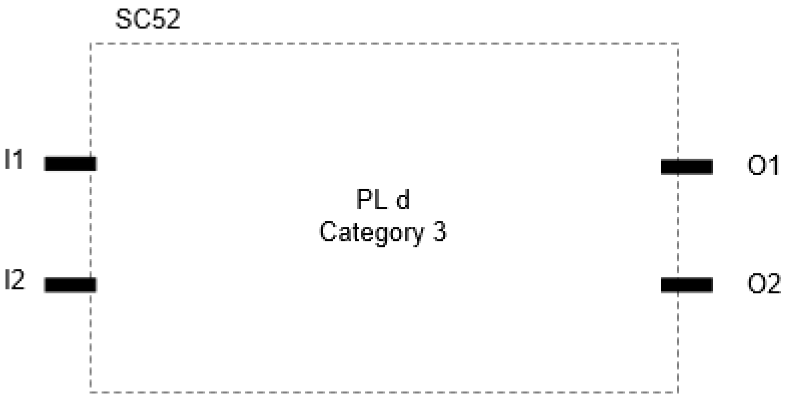


Figure 1. The safety architecture of SC52.

4 SAFETY METRICS

This chapter provides functional safety parameters of Epec SC52 Safety Control Unit. This information is intended to support system integrator's work during design, verification and validation of a complete safety function.

FS

FS ID: 7 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 SC52 shall be rebooted after each 24 hours to meet given safety values.

4.1 IEC 61508

Parameter	Value	Units
Safety Integrity Level	SIL2	
*PFH	8×10^{-8}	(1/h)
SFF	> 90	%
HFT	1	
Safety Related Element	Type B	
T1 (product lifetime)	10	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.*

4.2 ISO 13849

Parameter	Value	Units
Performance Level	PL d	
Category	3	
*MTTF$_d$	30	years
DCavg	>90	%

** 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.*

Block	MTTF$_d$ (a)	Max. DCavg (%)
Processing	159	High
AI/DI	899	Low when using signal range check
AI/DI(CAT2)	561	High
AI/DI/PI	471	Low when using signal range check
CAN1	1063	Low, with CANopen Safety High
CAN2	1676	Low, with CANopen Safety High
+5V sensor supply	680	High
PWM/DO	666	Low when using feedback information

5 SC52 INTERNAL DIAGNOSTICS

5.1 Overview

This chapter describes internal diagnostics of the SC52. The following subsystems are covered by built-in diagnostic functions of the SC52:

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

When an internal error is diagnosed, all output pins of the SC52 are de-energized by opening the safety switch, i.e. the safe state is forced.

Application and code template related diagnostics are described in chapter *7.4 Application Diagnostics*.

5.2 Start-up Diagnostics

To detect possible latent faults, built-in self-tests are executed by the SC52 during start-up. If the start-up diagnostics detects an error, the SC52 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 SC52 (see Chapter *3.2 Safety Function*)
- CAN controller self-test

FS

FS ID: 8 The power supply voltage shall be stable within 100 milliseconds when the power supply of the SC52 is switched ON. Voltage fluctuations after this may be interpreted by a self-test function as a fault condition and the SC52 can enter the safe state or trigger SC52 restart, which can increase system start-up time.

5.3 Online Diagnostics

5.3.1 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
- Voltages over safety switch and expected state of the safety switch
- 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 SC52

5.3.2 Failure Reaction Time

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

FS ID: 9 Internal diagnostic reaction time must be taken into account when calculating the whole system failure reaction time.

5.3.3 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 5 V. SC52 has internal energy storage which can provide backup power for the SC52 MCU while under powered and recovery from undervoltage is possible.

Overvoltage fault is detected by Over Voltage Protection (OVP) logic. The limit value is approximately 36 V. When OVP detects overvoltage fault condition, it will shut down the logic, which will eventually shut down the system. Recovery is only possible through a power OFF/ON cycle by the operator.

Firmware diagnostics has time limit values for voltage deviation:

- When voltage deviation lasts less than 25 milliseconds, operation continues without activating the safe state.

FS ID: 10 If a customer application requires safe state before 25 milliseconds due to voltage deviation, corresponding voltage deviation diagnostics must be implemented in the application.

- When voltage deviation lasts more than 25 milliseconds, the safe state is forced by online diagnostic.
- System shut down is triggered 100 milliseconds after the voltage deviation detection.

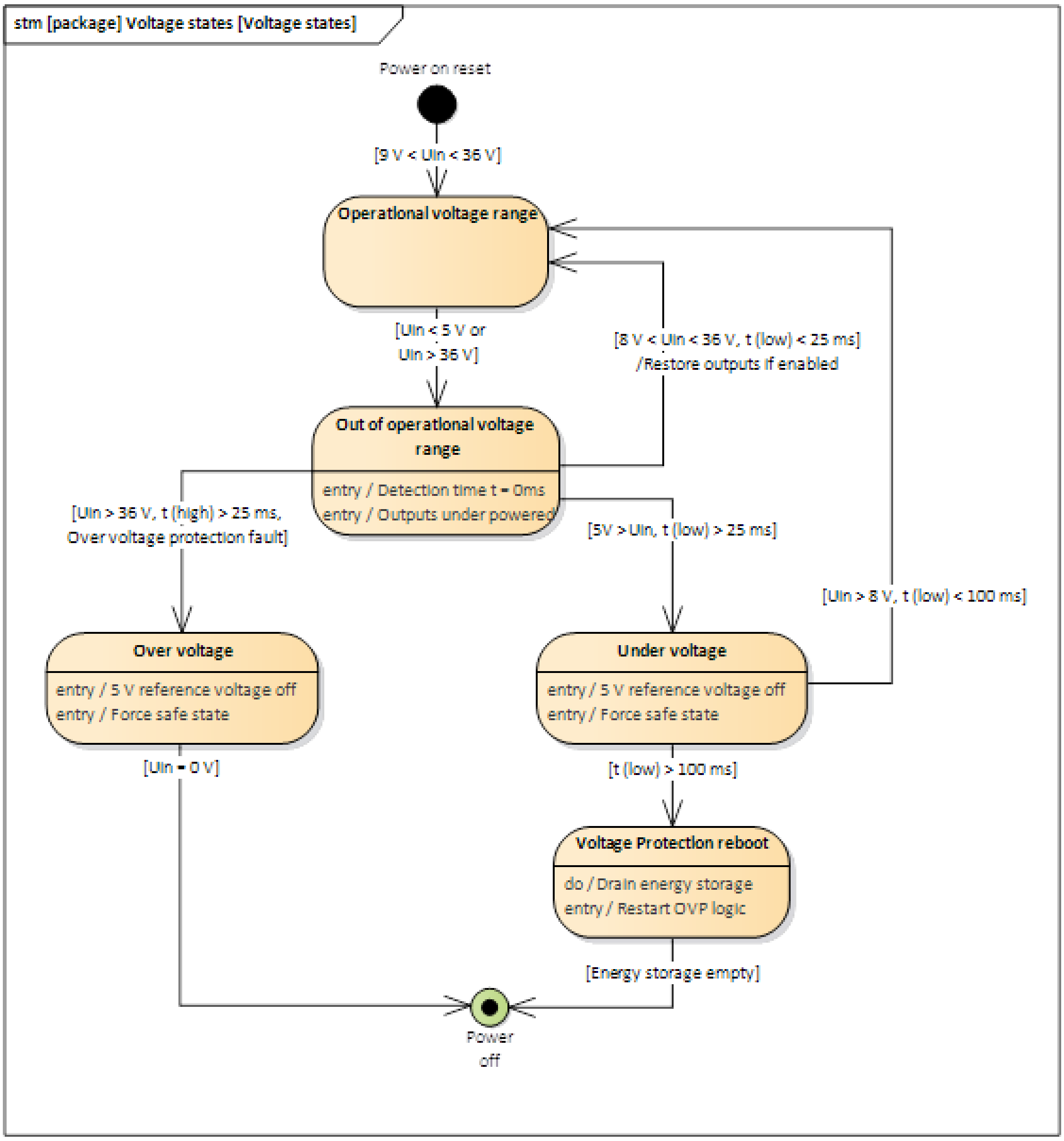

stm [package] Voltage states [Voltage states]
Power on reset
[9 V < Uin < 36 V]
Operational voltage range
[Uin < 5 V or
Uin > 36 V]
[8 V < Uin < 36 V, t (low) < 25 ms]
/Restore outputs if enabled
Out of operational voltage
range
entry / Detection time t = 0ms
entry / Outputs under powered
[Uin > 36 V, t (high) > 25 ms,
Over voltage protection fault]
[5V > Uin, t (low) > 25 ms]
[Uin > 8 V, t (low) < 100 ms]
Over voltage
entry / 5 V reference voltage off
entry / Force safe state
Under voltage
entry / 5 V reference voltage off
entry / Force safe state
[Uin = 0 V]
[t (low) > 100 ms]
Voltage Protection reboot
do / Drain energy storage
entry / Restart OVP logic
[Energy storage empty]
Power
off

Figure 2. Firmware voltage deviation diagnostic states.

The system can withstand under and overvoltage conditions that last for maximum 25 milliseconds.

- Execution of the application guaranteed
- Flash reads guaranteed
- Within 25 milliseconds write access to flash is allowed, if in the safe state
- Within 25 milliseconds access of the full NVRAM area is allowed
- Internal AI-measurements guaranteed

External I/O’s:

- CAN transmission guaranteed
- 5 V reference output not guaranteed as no backup power source
- De-energized safe state always guaranteed
- External AI measurements guaranteed
- External PI measurements guaranteed

DO/PWM outputs:

- Energized state not guaranteed, no backup power source
- De-energized state always guaranteed

In overvoltage conditions, in addition to the above, the following apply:

- 5 V reference output guaranteed
- DO/PWM output pin voltages limited to about 36 V

When an under or overvoltage condition has lasted over 25 milliseconds, the system will continue operation in the safe state until recovered or automatically shut down. Recovery is possible only from an undervoltage condition.

- Safe state is forced and guaranteed
- Writes to NVRAM and flash are prohibited and blocked
- NVRAM and flash reads are allowed
- Internal AI measurements guaranteed

External I/O's:

- CAN transmission guaranteed
- 5 V reference output forced to de-energized state
- External AI measurements guaranteed
- DO/PWM outputs forced to de-energized state

If an undervoltage condition is recovered before 100 milliseconds since detection, then the safe state is maintained, and the system continues operation.

Even if overvoltage condition is recovered, the system will still be shut down due to the OVP logic.

5.4 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.

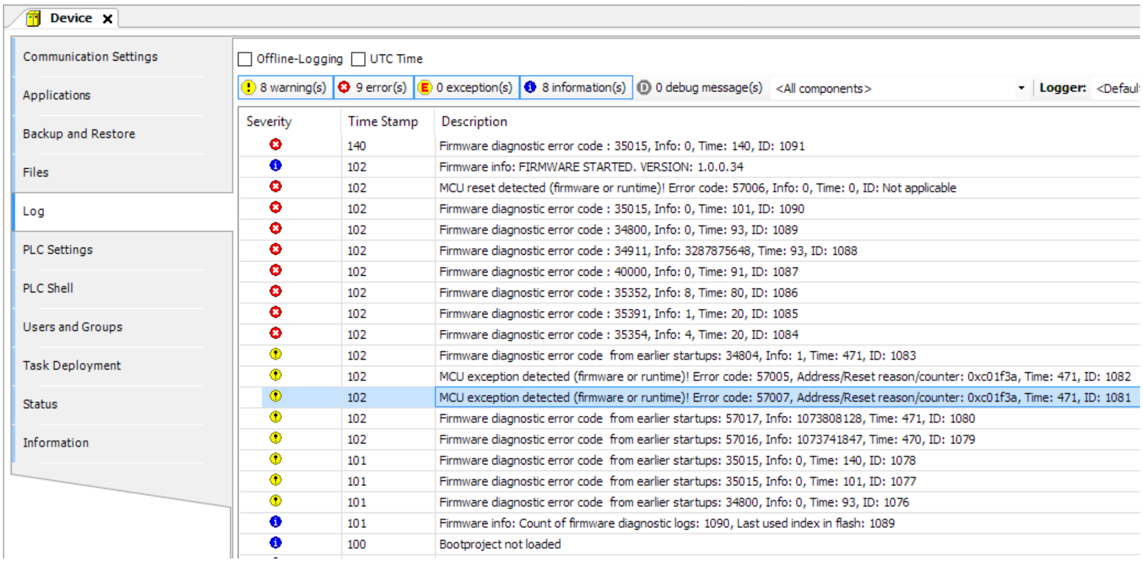
Most of the diagnostic errors in the log are firmware diagnostic specific. However, errors can also be caused due to application exceptions, which lead into a reset cycle.

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 3). 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 SC52 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.

Epec Oy reserves all rights for improvements without prior notice



□ Offline-Logging □ UTC Time

! 8 warning(s) | ⊗ 9 error(s) | E 0 exception(s) | ℹ 8 information(s) | D 0 debug message(s) | <All components> | **Logger:** <Defaul

Severity	Time Stamp	Description
⊗	140	Firmware diagnostic error code : 35015, Info: 0, Time: 140, ID: 1091
ℹ	102	Firmware info: FIRMWARE STARTED. VERSION: 1.0.0.34
⊗	102	MCU reset detected (firmware or runtime)! Error code: 57006, Info: 0, Time: 0, ID: Not applicable
⊗	102	Firmware diagnostic error code : 35015, Info: 0, Time: 101, ID: 1090
⊗	102	Firmware diagnostic error code : 34800, Info: 0, Time: 93, ID: 1089
⊗	102	Firmware diagnostic error code : 34911, Info: 3287875648, Time: 93, ID: 1088
⊗	102	Firmware diagnostic error code : 40000, Info: 0, Time: 91, ID: 1087
⊗	102	Firmware diagnostic error code : 35352, Info: 8, Time: 80, ID: 1086
⊗	102	Firmware diagnostic error code : 35391, Info: 1, Time: 20, ID: 1085
⊗	102	Firmware diagnostic error code : 35354, Info: 4, Time: 20, ID: 1084
!	102	Firmware diagnostic error code from earlier startups: 34804, Info: 1, Time: 471, ID: 1083
!	102	MCU exception detected (firmware or runtime)! Error code: 57005, Address/Reset reason/counter: 0xc01f3a, Time: 471, ID: 1082
!	102	MCU exception detected (firmware or runtime)! Error code: 57007, Address/Reset reason/counter: 0xc01f3a, Time: 471, ID: 1081
!	102	Firmware diagnostic error code from earlier startups: 57017, Info: 1073808128, Time: 471, ID: 1080
!	102	Firmware diagnostic error code from earlier startups: 57016, Info: 1073741847, Time: 470, ID: 1079
!	101	Firmware diagnostic error code from earlier startups: 35015, Info: 0, Time: 140, ID: 1078
!	101	Firmware diagnostic error code from earlier startups: 35015, Info: 0, Time: 101, ID: 1077
!	101	Firmware diagnostic error code from earlier startups: 34800, Info: 0, Time: 93, ID: 1076
ℹ	101	Firmware info: Count of firmware diagnostic logs: 1090, Last used index in flash: 1089
ℹ	100	Bootproject not loaded

Figure 3. 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.

6 INSTALLATION, CABLING AND CONNECTIONS

6.1 Operating Environment, Installation and Cabling

FS ID: 11 The system integrator shall ensure that SC52 is used under operating conditions which fulfill EMC and environmental specifications as presented in the Technical Manual. (Epec SC52 Safety Control Unit Technical Manual).

FS ID: 12 The system integrator shall notice that if SC52 is operated outside operating temperature range as given in the Technical Manual, SC52 will enter the safe state. (Epec SC52 Safety Control Unit Technical Manual).

FS ID: 13 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 SC52 Safety Control Unit Technical Manual > Mechanics and Cabling > Cabling)

6.2 I/0 Interface

The Epec SC52 Safety Control Unit includes the following external interfaces.

FS ID: 14 System integrator is responsible to implement required diagnostic functions in application software to achieve sufficient diagnostic coverage for I/O interface of SC52.

6.2.1 AI/DI_type091

This type of input is used to read analog signals from sensors with 0…10 V analog output or 0…20 mA current output. 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.

FS ID: 15 When using this pin type for safety-related applications, inputs shall be used in pairs. Input values shall be compared on application level prior this information is used by safety-related application software.

FS ID: 16 To avoid possible common-cause failures, input pairs shall be selected according to guidelines provided in the Technical manual (Epec SC52 Safety Control Unit Technical Manual > Input/Output Specifications > I/O List)

6.2.1.1 Voltage input mode

The voltage input mode supports 0…10 V voltage range.

FS ID: 17 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.*

6.2.1.2 Current input mode

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

FS ID: 18 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.

6.2.1.3 Digital input mode

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

6.2.2 AI/DI CAT2 type093

This type of inputs is used to read analog signals from sensors with 0...5 V or 0…10 V analog output or 0…20 mA current output. This input type has tree operating modes: voltage, current and Cat. 2 current mode. The default operating mode after the power is switched on is voltage input mode.

6.2.2.1 Voltage input mode

The voltage input mode supports two voltage ranges 0…5 V or 0…10 V.

FS ID: 19 When using this pin type in voltage mode for safety-related applications, inputs shall be used in pairs. Input values shall be compared on application level prior this information is used by application software.

FS ID: 20 To avoid possible common-cause failures, input pairs shall be selected according to guidelines provided in the Technical manual (Epec SC52 Safety Control Unit Technical Manual > Input/Output Specifications > I/O List).

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.*

6.2.2.2 Current input mode

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

FS ID: 22 When using this pin type in current mode for safety-related applications, inputs shall be used in pairs. Input values shall be compared on application level prior this information is used by application software.

FS ID: 23 To avoid possible common-cause failures, input pairs shall be selected according to guidelines provided in the Technical manual (Epec SC52 Safety Control Unit Technical Manual > Input/Output Specifications > I/O List)

FS ID: 24 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 current to a practical level.

The prolonged time of the overcurrent input is switched to voltage mode for additional protection.

6.2.2.3 Current input mode (Cat. 2)

For Cat. 2 mode of the current measurement input, the internal signal conditioning circuitry of SC52 is redundant. Therefore, two separate analog signals with a known ratio are used to measure one input.

FS ID: 25 When using this pin type in Cat. 2 mode for safety-related applications, the two analog signals shall be compared, and the ratio of the signals shall be within specified limits prior this information is used by application software.

FS ID: 26 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 the Cat. 2 current mode, the input has an overcurrent protection limiting current to a practical level.

The prolonged time of the overcurrent input is switched to voltage mode for additional protection.

6.2.3 DI/PI/AI_type096

This type of input is used to read signals from sensors with pulse output, digital output or 0…5 V analog output.

This input type has software selectable 10 kΩ pull-down and 2,2 kΩ pull-up to 5 V resistors.

This input type has three operating modes: pulse input, digital input and voltage input mode. The default operating mode is digital input mode.

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

FS ID: 27 When using this pin type for safety-related applications, inputs shall be used in pairs. Input values shall be compared on application level prior this information is used by application software.

FS ID: 28 To avoid possible common-cause failures, input pairs shall be selected according to guidelines provided in the Technical manual (Epec SC52 Safety Control Unit Technical Manual > Input/Output Specifications > I/O List)

FS ID: 29 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.*

6.2.3.1 Pulse input mode

Depending on the sensor, 2,2 kΩ pull-up or 10 kΩ pull-down may be selected.

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

6.2.3.2 Digital input mode

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

Epec Oy reserves all rights for improvements without prior notice

FS ID: 30 When pin is used as DI input mode, programmable pull-up resistors shall not be used and 10 kΩ pull-down shall be selected for safety related inputs.

6.2.3.3 Voltage input mode

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

FS ID: 31 In the voltage input mode, neither of the pull-up or pull-down shall not be selected to avoid loading of the measured signal.

6.2.3.4 Measuring Resistive Temperature sensor

When pin is used to measure resistive temperature sensors, the internal 2,2 kΩ pull-up needs to be selected. Resistive temperature sensors are measured with ratiometric measurement. The measured quantity is proportional to a ratio of input voltage and pull-up voltage.

6.2.4 PWM/DO/CM_type086

This type of output has high-side current measurement. A start-up test is executed after the power is switched on.

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: 32 To avoid possible common-cause failures, output pairs shall be selected according to guidelines provided in the Technical manual (Epec SC52 Safety Control Unit Technical Manual > Input/Output Specifications > I/O List)

FS ID: 33 To avoid common-cause failures, the system integrator shall separate SC52 power supply wires and output wires to actuators to claim fault exclusion according to the EN ISO 13849-2.

Do not directly cross connect DI/PI/AI_type096 pins or external voltage to output pins (PWM/DO/CM_type86). Safety unit makes input diagnostic for output pins to check if there is external voltage connected. Threshold level for output pins is quite low (typically 3.5V). Configuration state is set in the start of the IEC application when all IO-pins are initialized. Start-up tests are executed before application is stared, which can lead to a situation where start-up tests diagnose external connected voltage. This leads to safe state.

6.2.4.1 Un-initialized output pins

All un-used pins shall not be initialized. This prevents unintentional use of the pins from the application.

6.2.4.2 PWM output mode (Cat. 2)

FS ID: 34 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.*

6.2.4.3 Digital output mode (Cat. 2)

FS ID: 35 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.*

6.3 Sensor Power Supply

SC52 provides a 5V 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: 36 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: 37 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.

7 SAFETY RELATED APPLICATION DEVELOPMENT

7.1 Development Environment

7.1.1 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 2.9 or later
  - Contains MultiTool 5.7 or later, which supports SC52
  - Available from Epec Extranet

FS ID: 38 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.

7.1.2 Software Download

It is possible to update SC52 firmware and application in the field. This can be done using standard CANopen tool, but it is recommended to use EPEC CANmoon.

FS ID: 39 The machine manufacturer shall ensure that only trained persons are authorized to update software to SC52.

FS ID: 40 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 SC52 Safety Control Unit > Updating Firmware* and *Epec Programming and Libraries Manual> Programming > Downloading PLCopen Application.*

7.2 Application download and debugging with CODESYS IDE

7.2.1 Debugging modes

It is possible to debug an application and download the application to SC52 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 SC52. This doesn’t depend on the used mode. To change the SC52 to the debug mode, it must be done in CODESYS IDE through the SIL2 menu. If the SC52 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 SC52.

FS ID: 41 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: 42 CODESYS IDE shall not be used to update software in field/production. It shall be only used during the application development phase.

7.3 Application Interface

It is possible to program the SC52 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.

7.3.1 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	One I/O channel as such never fulfills SIL2 or PL d requirements (except Cat. 2 input). 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.

7.3.2 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.

7.3.2.1 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	10ms	Safe	10ms	0
PLC_PRG	10ms	Non-safe	No watchdog	1

7.3.2.2 Code Template Validation

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

FS ID: 43 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)*

7.3.3 SC52 Specific Safety Requirements for Application

FS ID: 44 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.

7.3.4 Floating point exeptions

FS ID: 45 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 SC52 Safety Control Unit > Floating point calculations.

SC52 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 SC52 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.

7.3.4.1 Exception handling in the SC52 1.0.0.34 release

SC52 does not fully conform to IEEE 754. 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 floating point operation causes overflow, then positive Infinity (0x7F800000UL) or negative infinity (0xFF800000UL) is generated as the result based upon the sign of the result.

The standard exception handling is used i.e. the application is forced to stop and safe state is forced by resetting the SC52. Exceptions are logged to the firmware log and CODESYS exceptions are logged with the FW_ERR_DIAG_EXCEPTION_CODE error and info field contains the actual exception.

Possible CODESYS IDE exception codes for FPU:

EXCPT_FPU_ERROR	FPU error
EXCPT_FPU_DIVIDEBYZERO	Division by zero

7.4 Application Diagnostics

7.4.1 System Diagnostics in the code template

When Epec Multitool is used to configure the SC52, the Code template uses *S_SC52_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_SC52_Diagnostic* program

- Supply voltage
- Internal reference voltages
- 5V REF voltage
- Safety switch status
- Temperatures (MCU and SBC)
- Firmware errors
- Output group initialization status

FS ID: 46 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.

7.4.2 Diagnostics in the System integrator specific code

Depending on safety requirements for the system integrator application, some diagnostics shall be implemented to the application. SC52 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)
-

7.5 I/O Diagnostics

7.5.1 Description

The internal diagnostic of SC52 and the Code template generated by the Multitool does not cover System integrator specific application I/O diagnostics.

FS ID: 47 System integrator shall implement required I/O diagnostic functions to application software.

Required diagnostics for certain pin types are described in chapter *6.2, 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.

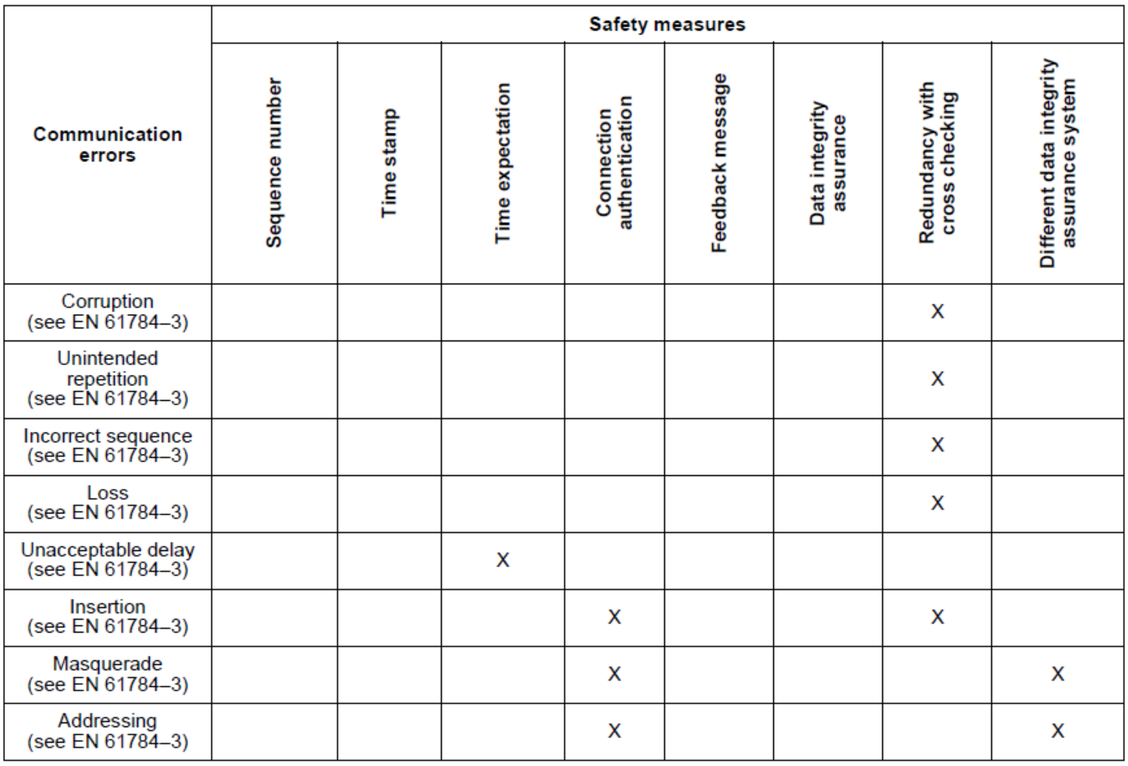
7.6 CAN Interface

7.6.1 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: 48 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 SC52.*

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



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

7.7 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 SC52 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 SC52 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 SC52:

Maximum 100 ms from the occurrence of an internal fault.

Epec Oy reserves all rights for improvements without prior notice

8 SERVICE AND MAINTENANCE

8.1 Service

SC52 is not field-serviceable. If SC52 is disassembled in the field, the system is then considered as unsafe. SC52 repair work is allowed be carried out by Epec After Sales Service only.

FS ID: 49 Machine manufacturer shall inform Epec about any failures of SC52. A faulty SC52 shall be sent to Epec After Sales Service.

8.2 Maintenance

FS ID: 50 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 SC52 Safety Control Unit.

FS ID: 51 Machine manufacturer shall promptly inform Epec about any potentially hazardous event which may be related to SC52. This information shall be delivered to Epec Customer Support.

FS ID: 52 In case of safety related modification of SC52, machine manufacturer shall carry out an impact analysis of the modification and necessary actions resulting from the impact analysis.

9 INFORMATION FOR USE - RELATED DOCUMENTS

9.1 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

9.2 Related documentation:

Document name:	ID:
Epec SC52 Technical Manual	MAN000676 Rev. 1
Epec Programming and Libraries Manual	MAN000538 v3.2 or newer
Epec MultiTool User Manual	MAN000316 v6.0
Epec CANmoon User Manual	MAN000405 v3.1
CODESYS (Application) Programming Guidelines (-H2)	MAN000613 v6.0 (CODESYS version)

9.3 Backward Compatibility

FS ID: 53 Compatibility with previous releases is described in the Epec Programming and Libraries manual. The system integrator shall verify and validate the application against the used hardware, firmware, eTPU and libraries versions.

For more information, refer to Epec Programming and Libraries Manual > Programming > Programming SC52 Safety Control Unit > Backward Compatibility.

Epec Oy reserves all rights for improvements without prior notice

10 LIST OF FIGURES

Epec Oy reserves all rights for improvements without prior notice

11 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.

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............... 7

FS ID: 2 The system integrator shall evaluate if the Epec SC52 Safety Control Unit can be used to implement safety functions in accordance to the hazards & risk analysis done by a machine manufacturer. 7

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 SC52 Safety Control Unit cannot guarantee safe operation of the system as a whole. 7

FS ID: 4 The system integrator shall verify and validate that all requirements in this safety manual are fulfilled by the end application. 7

FS ID: 5 The system integrator shall ensure that the de-energize of outputs of the SC52’s safe state will not cause any new possible hazardous situations of the machine. 9

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 SC52 is switched OFF and switched ON again to re-start the SC52. 9

FS ID: 7 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 SC52 shall be rebooted after each 24 hours to meet given safety values. 10

FS ID: 8 The power supply voltage shall be stable within 100 milliseconds when the power supply of the SC52 is switched ON. Voltage fluctuations after this may be interpreted by a self-test function as a fault condition and the SC52 can enter the safe state or trigger SC52 restart, which can increase system start-up time. 12

FS ID: 9 Internal diagnostic reaction time must be taken into account when calculating the whole system failure reaction time. 13

FS ID: 10 If a customer application requires safe state before 25 milliseconds due to voltage deviation, corresponding voltage deviation diagnostics must be implemented in the application. 13

FS ID: 11 The system integrator shall ensure that SC52 is used under operating conditions which fulfill EMC and environmental specifications as presented in the Technical Manual. (Epec SC52 Safety Control Unit Technical Manual). 17

FS ID: 12 The system integrator shall notice that if SC52 is operated outside operating temperature range as given in the Technical Manual, SC52 will enter the safe state. (Epec SC52 Safety Control Unit Technical Manual). 17