FORT Safety Manual

Release 1.0.1

Michael Kline <support@fortrobotics.com>

Mar 04, 2026

TABLE OF CONTENTS

FORT SAFETY MANUAL

Table of Contents **i**

1 Safety **2**

1oo2 Safety Architecture with HFT=1 . . . 2
Safety Behavior of an EPC Sender . . . 4
Safety Behavior of an NSC Pro . . . 4
Safety Behavior of an EPC Receiver . . . 4
Safety Behavior of an SRC Pro . . . 4
Safety Behavior of WES Pro . . . 5
Compliance with IEC 61508 requirements as a SIL-3 device . . . 5
Safety Inputs . . . 5
Physical Inputs . . . 5
EPC Physical Inputs . . . 5
SRC Pro Physical Inputs . . . 6
WES Pro Physical Inputs . . . 6
Virtual Inputs . . . 6
Serial Communication with Application Processor (AMCU) . . . 6
Serial Communication between the two Safety Processors (SMCU) . . . 7
Timeout Period for Safety Request Message . . . 7
Safety Processing . . . 7
Safety Outputs . . . 8
EPC Safety Outputs . . . 8
NSC Pro Safety Outputs . . . 8
SRC Pro Safety Outputs . . . 8
WES Pro Safety Outputs . . . 8
Physical Outputs . . . 8
Virtual Outputs . . . 9
User Selectable Safety Configurations (EPC) . . . 9
User Selectable Safety Configurations (NSC Pro) . . . 9
User Selectable Safety Configurations (WES Pro) . . . 10
Transferring Safety Configurations from FORT Manager to the EPC . . . 10
Transferring Safety Configurations from FORT Manager to the WES Pro . . . 10
Mechanical and Electrical Safety (EPC) . . . 10
Humidity and Dust Restrictions (EPC) . . . 10
Vibration Restrictions (EPC) . . . 11
Drop Restrictions (EPC) . . . 11
Water Restrictions (EPC) . . . 11
Proof Test (EPC) . . . 11
Mechanical and Electrical Safety (NSC Pro) . . . 11
Proof Test (NSC Pro) . . . 13

Mechanical and Electrical Safety (SRC Pro) . . . 13
Humidity and Dust Restrictions (SRC Pro) . . . 13
Vibration Restrictions (SRC Pro) . . . 13
Drop Restrictions (SRC Pro) . . . 13
Water Restrictions (SRC Pro) . . . 14
Proof Test (SRC Pro) . . . 14
Mechanical and Electrical Safety (WES Pro) . . . 14
Humidity and Dust Restrictions (WES Pro) . . . 14
Vibration Restrictions (WES Pro) . . . 14
Drop Restrictions (WES Pro) . . . 14
Water Restrictions (WES Pro) . . . 15
Proof Test (WES Pro) . . . 15
FMEDA Summary (EPC) . . . 15
FMEDA Summary (NSC Pro) . . . 16
FMEDA Summary (SRC Pro) . . . 17
FMEDA Summary (WES Pro) . . . 18
Diagnostic Test Intervals . . . 19

This document explains the safety related operations and methods used to achieve functional safety of the Pro Series devices.

Copyright © 2025, 2026 by FORT Robotics, Inc

All rights reserved.

FORT Robotics is a trademark of FORT Robotics.

Proprietary Information Notification:

THE RIGHTS OF FORT ROBOTICS, INC. ARE INCLUDED IN THE INFORMATION DISCLOSED HEREIN. THIS DOCUMENT SHALL NOT BE REPRODUCED OR TRANSFERRED TO OTHER DOCUMENTS OR USED OR DISCLOSED TO OTHERS FOR ANY PURPOSE EXCEPT AS SPECIFICALLY AUTHORIZED IN WRITING BY FORT ROBOTICS, INC.

CHAPTER

ONE

SAFETY

This document explains the safety related operations and methods used to achieve functional safety of the Pro Series devices. This information shall be considered by the designated responsible individuals who would need and use the following information to properly apply to the Pro Series devices.

The only safety relevant function of a Pro Series device (an EPC, NSC Pro,SRC Pro, or WES Pro) is related to handling of the emergency stop (E-Stop) command.

A given EPC, based on how it is configured by the customer (using FORT Manager), can act as a sender that reads the safety input state and transfers each change in state (i.e., emergency stop requests) or it can act as a receiver that receives and acts on emergency stop requests.

An SRC Pro and WES Pro alway act as sender devices. An NSC Pro always acts as a receiver device.

The following sections of this chapter describe the operations inside the EPC, SRC Pro, NSC Pro, and WES Pro, including input, logic, and output, and explain in detail all valid use cases and their functional safety operations.

1oo2 Safety Architecture with HFT=1

The system comprising the hardware and software is designed using the redundant 1oo2 (one out of two) safety architecture approach.

To comply with the 1oo2 safety architecture, the system has two redundant safety hardware components on board the EPC, SRC Pro, NSC Pro, and WES Pro with their own independent input circuitry, processing, output circuitry, and internal monitoring (via a watchdog).

The processors on the two redundant safety subsystems also communicate with each other through a serial link.

The end-to-end redundant architecture used in the EPC, SRC Pro, NSC Pro, and WES Pro achieves a Hardware Fault Tolerance (HFT) of 1, as shown in the following diagram:

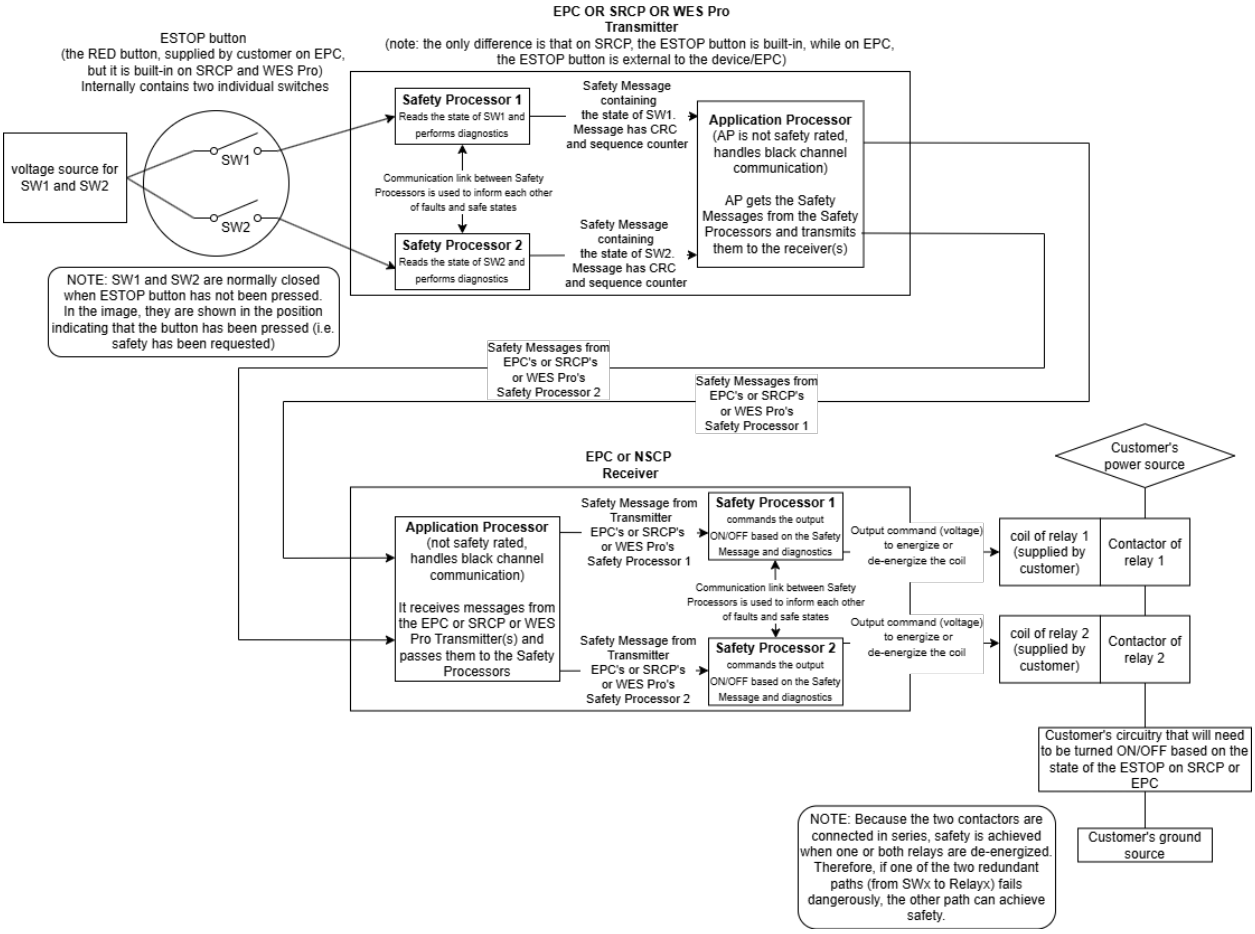


Fig 1.1: 1oo2 Safety Architecture with HFT=1

If one channel stops communicating with the other channel for longer than a specified period of time, then the other channel enters a safe state as follows:

- A sending device (SRC Pro, EPC, or WES Pro) sends a safety message to request safety from the remote device(s).
- A receiving device (EPC or NSC Pro) turns off the relays or actuators that are connected to its outputs.

If either of the two channels encounters a failure, the system is not degraded from 1oo2 to 1oo1; rather, if one of the two channels goes to a safe state the other channel is designed to enter a safe state as well.

The system is designed as a fail-safe system whereby if the system loses power:

- A sending device (SRC Pro EPC, or WES Pro) stops transmitting safety messages which triggers a timeout on receiving EPCs or NSC Pros which then causes the receiving devices to turn off their output relays.
- A receiving device (EPC or NSC Pro) loses power (turns off) which causes all outputs to be open circuit, which in turn causes the connected output relays to turn off.

The two redundant safety subsystems communicate with an onboard non-safety subsystem that sends the safety request messages to and receives them from the safety processors. The non-safety subsystem (called Application Processor or AMCU) functions as part of the black channel communication and transfers the safety messages to and from SMCUs without modifying their content (Redundant with black channel requests).

If the AMCU changes the content of a safety message because of an error, the receiving SMCU will detect the change and will consider the changed message invalid and will not act upon it.

Safety Behavior of an EPC Sender

The external (customer supplied) sensing elements that are connected to the input(s) of the EPC, generate a signal that indicates whether safety has been requested. The EPC (more precisely: the safety processors of the EPC) reads these inputs, interprets them based on the voltage level of the signals, and then generates a safety request message that indicates whether safety is requested. The message is serially passed to the Application Processor (also known as the application microcontroller unit, AMCU) of the EPC.

The Application Processor takes the message and sends it to other receivers (EPCs or NSC Pros) via a communication link.

The AMCU of the receiving devices (EPCs or NSC Pros) receives the safety request messages and sends them serially to the onboard safety processors to be processed and acted upon.

Safety Behavior of an NSC Pro

The NSC Pro receives remote safety request messages from an SRC Pro or an EPC and depending on the request, turns on the relays (customer supplied) that are attached to its output (when the remote device doesn't request safety) or off (when the remote device requests safety). The receiver also checks the output feedback and confirms the output state.

Safety Behavior of an EPC Receiver

The EPC receives remote safety request messages from an SRC Pro, a WES Pro, or another EPC, and depending on the request, turns on the relays (customer supplied) that are attached to its output (when the remote device doesn't request safety) or off (when the remote device requests safety). The receiver also checks the output feedback and confirms the output state.

Safety Behavior of an SRC Pro

The safety behavior of SRC Pro is very similar to that of an EPC Sender.

The emergency stop switch that is built-into an SRC Pro generates a signal that indicates whether safety has been requested. The safety processors of the SRC Pro read this signal, interpret it based on the voltage level of the signal, and then generate a safety request message that indicates whether safety has been requested. The message is serially passed to the Application Processor of the SRC Pro.

The Application Processor receives the message and transmits it to a remote receiver EPC or NSC Pro via a supported communication link.

The AMCU of the receiving device (EPC or NSC Pro) receives the safety request message and sends it serially to the onboard safety processors to be processed and acted upon.

Safety Behavior of WES Pro

The safety behavior of WES Pro is very similar to that of an SRC Pro or EPC Sender.

The emergency stop switch that is built-into a WES Pro generates a signal that indicates whether safety has been requested. The safety processors of the WES Pro read this signal, interpret it based on the voltage level of the signal, and then generate a safety request message that indicates whether safety has been requested. The message is serially passed to the Application Processor of the WES Pro.

The Application Processor receives the message and transmits it to a remote receiver EPC or NSC Pro via a supported communication link.

The AMCU of the receiving device (EPC or NSC Pro) receives the safety request message and sends it serially to the onboard safety processors to be processed and acted upon.

Compliance with IEC 61508 requirements as a SIL-3 device

The emergency stop function is designed in compliance with SIL-3 requirements of IEC 61508.

Compliance with the IEC 61508 requires the system level requirements detailed in the following section.

Note: Although this document fulfills implied functional safety requirements in accordance with IEC 61508 and FORT Robotics engineering development processes, in the event of a conflict between the documents referenced and the contents of this guide, the current document applies.

Safety Inputs

An EPC (more precisely, the safety relevant portion of the EPC) provides support for processing and handling of two types of inputs: physical inputs and virtual inputs.

The SRC Pro and WES Pro support processing and handling of the built-in emergency stop switch.

Physical Inputs

This section describes the physical inputs for the EPC and SRC Pro.

EPC Physical Inputs

Physical input circuitry interfaces with the input devices (mechanical emergency stop switches, and more complex, solid state devices like a light curtain) that the customer connects to the EPC. The input circuitry conditions the input signals and provides them to the safety processors. Safety processors then calculate the magnitude of the signals to determine if safety has been requested or not.

Each EPC provides redundant hardware circuitry and the associated software to support the connection of three external physical input devices that have redundant outputs. The system reads and processes the state of each external physical input as an analog value using ADC (Analog to Digital Conversion) and checks the processed value of analog inputs against specified voltage ranges to determine whether the value of the signal indicates that safety has been requested.

The following external physical input devices are supported:

- E-Stop (Emergency Stop) type switches that are internally redundant (the E-Stop switch has two mechanical switches built inside it).
- Solid state type devices such as a light curtain, proximity sensor, etc., that must have redundant outputs.

If the solid state type device's signal includes a diagnostic off-pulse (known as OSSD), the system does not react to this pulse.

An input of an input-output pair only affects the output that it is paired with; for example, the input of input-output pair 1 can only affect the output of input-output pair 1 and cannot affect the output of input-output pair 2 or 3.

SRC Pro Physical Inputs

Physical input circuitry interfaces with the built-in mechanical emergency stop switch (which internally includes two individual SPST switches). The input circuitry conditions the input signals and provides them to the safety processors. Safety processors then calculate the magnitude of the signals to determine if safety has been requested or not.

The system reads and processes the state of the built-in E-Stop switch as an analog value using ADC (Analog to Digital Conversion) and checks the processed value of analog inputs against specified voltage ranges to determine whether the value of the signal indicates that safety has been requested.

WES Pro Physical Inputs

Physical input circuitry interfaces with the built-in mechanical emergency stop switch (which internally includes two individual SPST switches). The input circuitry conditions the input signals and provides them to the safety processors. Safety processors then calculate the magnitude of the signals to determine if safety has been requested or not.

The system reads and processes the state of the built-in E-Stop switch as an analog value using ADC (Analog to Digital Conversion) and checks the processed value of analog inputs against specified voltage ranges to determine whether the value of the signal indicates that safety has been requested.

Virtual Inputs

Virtual Inputs (applicable only to receiver EPCs or NSC Pros) are safety request messages, generated by the SMCUs of a remote EPC or SRC Pro, that are serially transmitted to the AMCU of the EPC or SRC Pro, which then transmits them using a wired or wireless link to the Application Processor of a remote EPC or NSC Pro.

The Application Processor of the remote EPC or NSC Pro receives the safety request message and then serially transmits the message to the SMCUs.

Serial Communication with Application Processor (AMCU)

On a sender EPC, SRC Pro, or WES Pro, only correct assembly of the safety message is considered safety relevant. Therefore, transmission of the safety request message to the AMCU is not safety relevant; however, if there is a failure in passing the message to AMCU, or if there is a failure on the AMCU side to transmit the message, the remote EPC or NSC Pro will go to safe state if this failure lasts longer than the timeout value.

On a receiving EPC or NSC Pro, if the AMCU doesn't pass the safety message to the SMCU, a timeout occurs that puts the outputs in a safe state. If the AMCU corrupts the safety request message, the CRC (cyclic redundancy check) and other checks by SMCU will detect the error and will not use the content of the message.

In summary: only assembling the safety message and processing the incoming safety request message is safety relevant. The rest of the communication chain is considered a black channel.

Serial Communication between the two Safety Processors (SMCU)

This is applicable to SRC Pro, NSC Pro EPC, and WES Pro. If one of the two channels of the 1oo2 system fails, the system must not degrade to 1oo1 operation. Therefore, when an SMCU detects an error and puts itself in a safe state, it must notify the other SMCU in order for the other SMCU to also go to a safe state. Therefore, the two SMCUs periodically communicate their state to each other by sending a message through a serial link.

Moreover, if an SMCU doesn't receive the periodic message from the other SMCU, after a specified period it goes to a safe state until it receives a valid safety message from the other SMCU.

This message uses the same approach to verify the message (CRC counter, and timeout) as the safety request message (see previous section) and the content of a message that fails the sequence counter check will not be used by the SMCU.

At least one valid message must be received by each SMCU from the other SMCU every timeout period (40ms), otherwise the outputs (both virtual and physical) are put in a safe state. Specifically, the system sends SMCU-to-SMCU messages every 10 ms (within every control loop), and if an SMCU doesn't receive a valid message from the other SMCU for four consecutive loops, it goes to a safe state.

When an SMCU receives a message from the other SMCU that indicates the other SMCU is in a safe state, the first SMCU also transitions to a safe state and puts all of its outputs (physical or virtual) in a safe state.

Timeout Period for Safety Request Message

The Application Processor of an EPC or NSC Pro receives the safety request message from a remote EPC, SRC Pro, or WES Pro, and using a serial link, transmits the message to the safety processors.

Before using any other field of the safety message for any purpose, the safety processors examine the content of the safety request message using the sequence counter and the CRC fields, to determine if the message is valid and has not changed during its transmission from the source to the destination.

At least one valid safety request message must be received by the SMCU within the timeout period since the last valid message, otherwise the outputs will be turned off to put the EUC in a safe state. For example, a safety timeout of 250 ms means that a receiver EPC or NSC Pro must receive at least one valid safety message within 250 ms of receiving the last valid safety message or else it will turn off its outputs.

The allowed timeout periods that can be chosen by the customer (using FORT Manager) are 250 ms, 500 ms, 750 ms and 1 sec, 3 sec, and 5 sec.

Safety Processing

To comply with the 1oo2 safety architecture and SIL requirements, the safety portion of the EPC, SRC Pro, NSC Pro,and WES Pro uses two redundant processing units, referred to as SMCU0 and SMCU1. Each double redundant input is connected to one of the SMCUs. For example, the double redundant E-Stop switch, internally contains two mechanical switches. One switch is connected to SMCU0 and 1 switch is connected to SMCU1.

Each safety processor reads the value of the input signal (virtual or physical) that it receives and based on the magnitude/content of the signal will command the physical outputs to either turn on or off or transmit a message indicating safety being requested or not.

The system complies with highly recommended safety requirements (the micro manufacturer refers to them as CoU, Conditions of Use) that are listed in the manufacturer's safety manual of the specific processor in use.

Important: When any of the safety mechanisms indicates the presence of a failure, the system logs a fault that indicates the reason for the fault, and it places the outputs (both virtual and physical when applicable) in a safe state.

Safety Outputs

This section describes the safety outputs for the EPC, NSC Pro, SRC Pro, and WES Pro.

EPC Safety Outputs

An EPC provides support for processing/handling of two types of outputs: physical outputs and virtual outputs.

An EPC sender provides support for three virtual outputs that indicate the state of the 3 physical inputs of the EPC sender.

An EPC receiver provides support for three redundant and independent physical outputs.

The user must configure the outputs with FORT Manager.

NSC Pro Safety Outputs

An NSC Pro provides support for processing/handling of physical outputs.

Each NSC Pro has two redundant and independent physical outputs.

The outputs must be configured by the user, using FORT Manager.

SRC Pro Safety Outputs

The SRC Pro is a transmitter device and therefore only supports one virtual output that indicates the state of the built-in emergency stop switch.

WES Pro Safety Outputs

The WES Pro is a transmitter device and therefore only supports one virtual output that indicates the state of the built-in emergency stop switch.

Physical Outputs

Physical outputs are only applicable to receiver EPCs and NSC Pros. Physical output circuitry creates a link between the safety processor and the output devices, which are typically relays (or actuators) that a user connects to the outputs of the EPC or NSC Pro. Based on the state of the inputs and the safety system's diagnostics information, the safety processors determine whether the relays need to be turned on or off.

For example, if the state of inputs indicates that safety has been requested, the system turns off the outputs to turn off the external relays, otherwise it keeps the outputs on to keep the external relays on.

Each EPC provides redundant hardware circuitry and the associated software to support the connection of three external and redundant physical output devices. The external physical output devices must be connected in series, such that if one or both of the two devices are turned off, the EUC is turned off.

Each NSC Pro provides redundant hardware circuitry and the associated software to support the connection of two external and redundant physical output devices.

If the state of any virtual input indicates that safety has been requested by a remote device, the output of that device is turned off.

If the system has a fault that could affect all of the outputs, all the outputs will be turned off.

Virtual Outputs

Virtual outputs are applicable to SRC Pros, Sender EPCs, and WES Pros. Virtual outputs are safety request messages generated by the SMCUs of an EPC, SRC Pro, or WES Pro, based on the state of the physical inputs and diagnostics information. Every 40ms these messages are serially transmitted to the AMCU of a transmitting EPC,SRC Pro, or WES Pro, which then transmits them using a wired or wireless link to the Application Processor (AMCU) of a remote EPC or NSC Pro that is connected to a machine. The Application Processor of the remote device receives the safety request message and serially transmits it to its SMCU. See diagram in *1oo2 Safety Architecture with HFT=1*

The AMCU acts as part of a black channel and does not deliberately modify the content of the safety request message. The CRC verification detects accidental corruption of the message at the destination.

The content of the safety request message also includes a sequence counter that is incremented as each new message is transmitted to the AMCU. This enables the remote device to detect out of sequence and old messages that it must not act upon.

The following information is applicable to an EPC and NSC Pro, not to an SRC Pro.

User Selectable Safety Configurations (EPC)

A user must configure an EPC with FORT Manager before the device can be used in a runtime application. See the *Configurations and Use Cases* chapter in the user guide. A subsequent power cycle of the EPC does not erase the configuration stored in the device. Any re-configuration of an EPC must be done by a user with FORT Manager.

Use FORT Manager to configure the EPC, including the inputs and outputs of the safety portion of the EPC:

- Configuration: Identify the sender(s) and receivers for the network.
- Timeout Configuration: Select one of the values 250ms, 500ms, 750ms, 1 second, 3 seconds, or 5 seconds as a timeout.
- Input configuration: Identify the type of device (E-Stop, solid-state, or not used) to attach to each of the three inputs.
- Output configuration: Derived by FORT Manager from the configuration information entered by the user.

User Selectable Safety Configurations (NSC Pro)

The following information is applicable to an NSC Pro only.

A user must configure an NSC Pro with FORT Manager before the device can be used in a runtime application. A subsequent power cycle of the NSC Pro does not erase the configuration stored in the device. Any re-configuration of an NSC Pro must be done by a user with FORT Manager.

Use FORT Manager to build a configuration and to configure the NSC Pro, including the outputs of the safety portion of the NSC Pro:

- Configuration: Identify the sender(s) and receivers for the network.
- Timeout Configuration: Select one of the values 250ms, 500ms, 750ms 1 second, 3 seconds, or 5 seconds as a timeout.
- Input configuration: Identify the type of device (E-Stop, solid-state, or not used) to attach to each of the three inputs.
- Output configuration: Derived by FORT Manager from the configuration information entered by the user.

User Selectable Safety Configurations (WES Pro)

Using FORT Manager, a user must configure which output of the receiver will be controlled by the ESTOP on WES Pro.

Transferring Safety Configurations from FORT Manager to the EPC

When a user configures an EPC with FORT Manager, FORT Manager is not in direct communication with the EPC that is being configured. Therefore, FORT Manager stores the configuration parameters in a file that the user later transfers to the AMCU with the FORT configuration tool or the FORT Manager desktop app.

After each reset or power up, the SMCU of the EPC retrieves the configuration parameters from the AMCU.

To ensure that program file corruption or an accidental change of configurations can be detected, FORT Manager calculates a CRC for SMCU configurations that it transmits to the AMCU and includes as part of the SMCU configuration data. Upon completion of transfer of the configuration to its RAM, the SMCU verifies that the CRC of the configuration matches its content, and if not, logs a fault and resets the SMCU.

After an SMCU receives its configuration, it verifies that the configuration is one of the allowed configurations. If it isn't, the SMCU resets itself and the EPC cannot enter a running state of operation.

Transferring Safety Configurations from FORT Manager to the WES Pro

When a user configures an WES Pro with FORT Manager, FORT Manager is not in direct communication with the WES Pro that is being configured. Therefore, FORT Manager stores the configuration parameters in a file that the user later transfers to the AMCU with the FORT configuration tool or the FORT Manager desktop app.

After each reset or power up, the SMCU of the WES Pro retrieves the configuration parameters from the AMCU.

To ensure that program file corruption or an accidental change of configurations can be detected, FORT Manager calculates a CRC for SMCU configurations that it transmits to the AMCU and includes as part of the SMCU configuration data. Upon completion of transfer of the configuration to its RAM, the SMCU verifies that the CRC of the configuration matches its content, and if not, logs a fault and resets the SMCU.

After an SMCU receives its configuration, it verifies that the configuration is one of the allowed configurations. If it isn't, the SMCU resets itself and the WES Pro cannot enter a running state of operation.

Mechanical and Electrical Safety (EPC)

The EPC is designed and built to operate in extreme environmental conditions. As such, we've subjected it to rigorous mechanical and electrical tests.

Humidity and Dust Restrictions (EPC)

The EPC has no humidity restrictions (tested to MIL-STD-810H) or dust restrictions (IP65 verified).

Vibration Restrictions (EPC)

The EPC meets vibration standards per SAE (Society of Automotive Engineers) J1455. It was subjected to 8.00 G-rms of random (Gaussian) vibration for six hours each in three separate planes with results as shown in the following table:

Table 1.1: Vibration Power Spectral Density (PSD) Results (EPC)

Frequency (Hz)	PSD (G^2/Hz)
24	0.040
60	0.500
102	0.500
300	0.010
2000	0.010

Drop Restrictions (EPC)

The EPC has been tested by dropping from a height of one meter. It should continue to function after occasional drops but avoid dropping it repeatedly to prevent damage and malfunctioning.

Water Restrictions (EPC)

The EPC enclosure is IP65 rated (protected against exposure to water including low pressure sprays). Do not subject it to high pressure nor immersion in water. Note that if the EPC is operating in an environment in which it is exposed to water you must mount it vertically. Mounting it horizontally allows water to pool and block a breathable membrane causing the device to malfunction.

Proof Test (EPC)

A proof test is a periodic test that is performed to detect dangerous hidden failures in a safety-related system. If the proof test detects any failures, then a repair must be performed as soon as possible to restore the system to its "as new" condition or as close as practical to this condition.

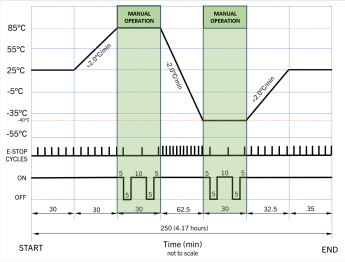
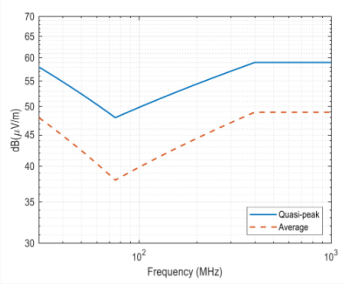
Based on your application, you should determine how frequently you must perform a proof test on the system.

See User Guide Proof Testing for a number of suggested proof tests.

Mechanical and Electrical Safety (NSC Pro)

The NSC Pro is an embedded board that is designed and built to operate in extreme temperature ranges (-40 °C -85 °C). We've subjected it to the following tests:

Table 1.2: NSC Pro Environmental Tests

Test Type	Standard	Parameters	Image[Page 12, 1]
Humidity	IEC 60068-2-78:2012	30±2°C 0 – 93 ±3% relative humidity range non-condensing 24 hour duration	
Thermal Cycling	IEC 60654-1	-40°C to +85°C (±3°C) 4.16Hr test time	
Swept Sinusoidal Vibration Test	IEC 60068-2-6	Frequency range: 55–500 Hz Acceleration amplitude: 6g 10 sweep cycles per plane Sweep rate: 1 octave/minute Resulting test duration: 1 hour per plane	
Shock	IEC 60068-2-27	25g acceleration 6ms pulse duration Half-sine pulse shape 1000 ±10 shocks in each direction per plane Performed on 3 planes	
Ingress Protection	IEC 60529	IP00	
Radiated Emissions, Near Field	EC-42 Test 4.1 / ISO 13766		
High Frequency Immunity	EC-42 Test 3.1	30V/m, ISO 11452-2	
Medium Frequency Immunity	EC-42 Test 3.2	30V/m, ISO 11452-2, ISO 11452-4 or ISO 11452-5	
Low Frequency Immunity	EC-42 Test 3.3	30V/m, ISO 11452-4 or ISO 11452-5	
Functional Safety	IEC 61508	Up to SIL 3	

[1] Click on a figure to see an enlarged image or right-click to view it in a separate browser tab.

Proof Test (NSC Pro)

A proof test is a periodic test that is performed to detect dangerous hidden failures in a safety-related system. If the proof test detects any failures, then a repair must be performed as soon as possible to restore the system to its "as new" condition or as close as practical to this condition.

Based on your application, you should determine how frequently you must perform a proof test on the system.

See User Guide Proof Testing for a number of suggested proof tests.

Mechanical and Electrical Safety (SRC Pro)

The Safe Remote Controller Pro is designed and built to operate in extreme environmental conditions. As such, we've subjected it to rigorous mechanical and electrical tests.

Humidity and Dust Restrictions (SRC Pro)

The SRC Pro has no humidity restrictions (tested to MIL-STD-810H) or dust restrictions (IP65 verified).

Vibration Restrictions (SRC Pro)

The SRC Pro meets vibration standards per SAE J1455. It was subjected to 8.00 G-rms of random (Gaussian) vibration for two hours each in three separate planes with results as shown in the following table:

Table 1.3: Vibration Power Spectral Density (PSD) Results (SRC Pro)

Frequency (Hz)	PSD (G^2/Hz)
20	0.010
80	0.040
350	0.040
2000	0.007

Drop Restrictions (SRC Pro)

The SRC Pro has been tested by dropping from a height of one meter once on each side of the device. It should continue to function after occasional drops but avoid dropping it repeatedly to prevent damage and malfunctioning.

Water Restrictions (SRC Pro)

The SRC Pro enclosure is IPx5 rated (protected against exposure to water including low pressure sprays). Do not subject it to high pressure nor immersion in water.

Proof Test (SRC Pro)

A proof test is a periodic test that is performed to detect dangerous hidden failures in a safety-related system. If the proof test detects any failures, then a repair must be performed as soon as possible to restore the system to its "as new" condition or as close as practical to this condition. Based on your application, you should determine how frequently you must perform a proof test on the system.

See User Guide Proof Testing for a number of suggested proof tests.

Mechanical and Electrical Safety (WES Pro)

The WES Pro is designed and built to operate in extreme environmental conditions. As such, we've subjected it to rigorous mechanical and electrical tests.

Humidity and Dust Restrictions (WES Pro)

The WES Pro has no humidity restrictions (tested to MIL-STD-810H) or dust restrictions (IP65 verified).

Vibration Restrictions (WES Pro)

The WES Pro meets vibration standards per SAE J1455. It was subjected to 8.00 G-rms of random (Gaussian) vibration for two hours each in three separate planes with results as shown in the following table:

Table 1.4: Vibration Power Spectral Density (PSD) Results (WES Pro)

Frequency (Hz)	PSD (G^2/Hz)
20	0.010
80	0.040
350	0.040
2000	0.007

Drop Restrictions (WES Pro)

The WES Pro has been tested by dropping from a height of one meter once on each side of the device. It should continue to function after occasional drops but avoid dropping it repeatedly to prevent damage and malfunctioning.

Water Restrictions (WES Pro)

The WES Pro enclosure is IPx5 rated (protected against exposure to water including low pressure sprays). Do not subject it to high pressure nor immersion in water.

Proof Test (WES Pro)

A proof test is a periodic test that is performed to detect dangerous hidden failures in a safety-related system. If the proof test detects any failures, then a repair must be performed as soon as possible to restore the system to its "as new" condition or as close as practical to this condition. Based on your application, you should determine how frequently you must perform a proof test on the system.

See User Guide Proof Testing for a number of suggested proof tests.

FMEDA Summary (EPC)

This section summarizes the expected failure rates for the EPC obtained from the failure modes, effects, and diagnostic analysis (FMEDA) tests performed by Exida corporation.

The following two tables list the failure rates for the EPC using a site safety index (SSI) of 2 (good site maintenance practices).

Table 1.5: EPC Failure Rates (Sender) Good Maintenance Assumptions in FIT @SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	9,034
Fail Safe Undetected	120
Fail Dangerous Detected	9,558
Fail Dangerous Undetected	92
No Effect	499
Annunciation Detected	34
Annunciation Undetected	23

Table 1.6: EPC Failure Rates (Receiver) Good Maintenance Assumptions FIT @SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	9,030
Fail Safe Undetected	178
Fail Dangerous Detected	9,534
Fail Dangerous Undetected	92
No Effect	544
Annunciation Detected	50
Annunciation Undetected	23

The following table lists the failure rates for the EPC according to IEC 61508.

Table 1.7: EPC Failure Rates Good Maintenance Assumptions in FIT @SSI=2 EEC 61508

Application/Device Configuration	λSD	λSU	λDD	λDU	#	SFF
Sender	9,067	120	9,558	92	522	99.5%
Receiver	9.080	178	9,534	92	567	99.5%

Where:

λSD = Fail Safe Detected **λSU** = Fail Safe Undetected **λDD** = Fail Dangerous Detected **λDU** = Fail Dangerous Undetected **#** = No Effect Failures

Note that *No Effect Failures* are no longer included in the *Safe Undetected* category according to IEC 61508, ed2, 2010.

The analysis shows that the EPC has a safe failure fraction (SFF) greater than 99% indicating that it meets hardware architectural constraints for up to SIL 3 as a single device.

FMEDA Summary (NSC Pro)

This section summarizes the expected failure rates for the NSC Pro obtained from the failure modes, effects, and diagnostic analysis (FMEDA) tests performed by Exida corporation.

Note: **Note:** The failure rate tables make the assumptions that the altitude/SER is 200 m, failure rates apply to the NSC Pro only, and external components (E-Stop switch and safety relays) are not covered.

The following table lists the failure rates for the NSC Pro using a site safety index (SSI) of 2 (good site maintenance practices).

Table 1.8: NSC Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	588
Fail Safe Undetected	76
Fail Dangerous Detected	547
Fail Dangerous Undetected	9
No Effect	266
Annunciation Detected	39
Annunciation Undetected	7

The following table lists the failure rates for the NSC Pro according to IEC 61508.

Table 1.9: NSC Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2 EEC 61508

Application/Device Configuration	λSD	λSU	λDD	λDU	#	SFF
NSC Pro	627	76	547	9	273	99.3%

Where:

- **λSD** = Fail Safe Detected
- **λSU** = Fail Safe Undetected
- **λDD** = Fail Dangerous Detected
- **λDU** = Fail Dangerous Undetected
- **#** = No Effect Failures

Note that *No Effect Failures* are no longer included in the *Safe Undetected* category according to IEC 61508, ed2, 2010.

The analysis shows that the NSC Pro has a safe failure fraction (SFF) greater than 99% indicating that it meets hardware architectural constraints for up to SIL 3 as a single device.

FMEDA Summary (SRC Pro)

This section summarizes the expected failure rates for the Safety Remote Control Pro obtained from the failure modes, effects, and diagnostic analysis (FMEDA) tests performed by Exida corporation.

The following table lists the failure rates for the SRC Pro using a site safety index (SSI) of 2 (good site maintenance practices).

Table 1.10: SRC Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	4779
Fail Safe Undetected	64
Fail Dangerous Detected	5021
Fail Dangerous Undetected	52
No Effect	649
Annunciation Detected	33
Annunciation Undetected	13

The following table lists the failure rates for the SRC Pro according to IEC 61508.

Table 1.11: SRC Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2 EEC 61508

Application/Device Configuration	λSD	λSU	λDD	λDU	#	SFF
SRC Pro	4811	64	5021	52	662	99.5%

Where:

λSD = Fail Safe Detected
λ**SU** = Fail Safe Undetected λ**DD** = Fail Dangerous Detected λ**DU** = Fail Dangerous Undetected **#** = No Effect Failures

Note that *No Effect Failures* are no longer included in the *Safe Undetected* category according to IEC 61508, ed2, 2010

The analysis shows that the SRC Pro has a safe failure fraction (SFF) greater than 99% indicating that it meets hardware architectural constraints for up to SIL 3 as a single device.

FMEDA Summary (WES Pro)

This section summarizes the expected failure rates for the Wireless E-Stop (WES) Pro obtained from the failure modes, effects, and diagnostic analysis (FMEDA) tests performed by Exida corporation.

The *useful life* of the safety circuitry of the device predicted by component failure data is 50 years.

The following table lists the failure rates for the WES Pro using a site safety index (SSI) of 2 (good site maintenance practices).

Table 1.12: WES Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2

Failure Category	Failure Rate (FIT)
Fail Safe Detected	4792
Fail Safe Undetected	72
Fail Dangerous Detected	5016
Fail Dangerous Undetected	54
No Effect	3518
Annunciation Detected	72
Annunciation Undetected	31

The following table lists the failure rates for the WES Pro according to IEC 61508.

Table 1.13: WES Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2 EEC 61508

Application/Device Configuration	λSD	λSU	λDD	λDU	#	SFF
WES Pro	4864	72	50215016	54	3549	99.5%

Where:

λSD = Fail Safe Detected
λ**SU** = Fail Safe Undetected λ**DD** = Fail Dangerous Detected λ**DU** = Fail Dangerous Undetected **#** = No Effect Failures

Note that *No Effect Failures* are no longer included in the *Safe Undetected* category according to IEC 61508, ed2, 2010

The analysis shows that the WES Pro has a safe failure fraction (SFF) greater than 99% indicating that it meets hardware architectural constraints for up to SIL 3 as a single device.

Diagnostic Test Intervals

The diagnostic test interval (DTI) is the interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage. The DTI for EPC, NSC Pro, SRC Pro, and WES Pro is 50 milliseconds.

All the EPC, NSC Pro, SRC Pro, and WES Pro safety software (including diagnostic checks) run within a 10 ms control loop (except the Short-to-Battery test, which runs every 200 ms). However, not all online tests run every 10 ms and for those that do run every 10 ms, the software does some filtering on the faults to avoid the system entering a safe state unnecessarily. Because of filtering some tests may take up to 50 ms to determine that a fault exists. In addition, some tests, such as the flash test, comprise five parts such that a complete flash test takes five control loops (50 ms) to complete.

For example, the two safety processors (SMCU0 and SMCU1) exchange information about their state every 10 ms via serial messages. However, they enter a safe state whenever either of the following occurs:

- They haven't received a valid status message for four consecutive control loops (i.e., 40 ms) from the other SMCU.
- They receive a valid safety message from the other SMCU indicating that it has entered a safe state.

The following table provides a summary of the diagnostic tests that are performed on the inputs, outputs, and internal parts of the system, how frequently they are performed, whether there is filtering, and the criteria for declaring a fault (i.e., entering a safe state).

Table 1.14: Diagnostic Tests

Test name / Description	Applicability	What it does	How often it runs
State of Inputs Checks the state of the E-Stop switch(es) or the solid state input device(s) for faults.	Sender EPC, SRC Pro, and WES Pro	Checks whether the state of the switch/input indicates a fault. If the test fails, the output is turned off until the fault goes away.	Every 10 ms to sample the state of the input
Output Command to State Comparison Compares the output command(s) to the state of the output pin(s).	Receiver EPC or NSC Pro	Checks whether the voltage level at the output pin corresponds to the output command. If the test fails, the corresponding output is turned off until the system is reset.	Every 10 ms to make the comparison.
Short to Battery Checks whether a short to battery exists at the output pin(s) while the output(s) is commanded on (i.e., safety is not being requested). This test prevents a scenario in which, over a long period of time (potentially many months), and while safety is not being requested, both outputs are shorted to battery without the system being aware of the failure. If this scenario were to occur, and safety is requested at some point, a safe state cannot be achieved since both outputs have been shorted to battery.	Receiver EPC or NSC Pro	While safety is not being requested, the test momentarily (for less than 0.5 ms) turns off the output to check if the output indeed turned off (i.e., there is no failure) or if the output remains on (a short to battery is present). If the test fails, the corresponding output is turned off until the system performs a reset.	The test runs every 200 ms. This value is not used for DTI since it is a special test to prevent *double-point failures*, and the *Output Command to State Comparison* test performs a similar check every 10 milliseconds. There is no filtering of the test result.

continues on next page

Table 1.14 – continued from previous page

Test name / Description	Applicability	What it does	How often it runs
Communication Timeout Checks whether a communication timeout exists between the sender and receivers. The scope of this test is limited to the safety request message.	Receiver EPC or NSC Pro	Checks whether a new and valid safety message has been received from each expected sender (could be an EPC or SRC Pro or both in the case of a hybrid configuration) since the last timeout period (as set by the user in FORT Manager). If a timeout is detected, the outputs are turned off until a valid safety message is received.	Checks the timeout counter(s) every 10 ms for a timeout.
Safety Processors Communication Timeout Checks for communication timeout between the two redundant safety processors	Sender EPC, SRC Pro, WES Pro, and Receiver EPC, NSC Pro	Run by each safety processor to check if it is receiving safety data from the other safety processor. Each safety processor must receive a safety message from the other processor at least every 40ms. If a timeout is detected, the outputs are turned off until a valid safety message is received.	Every 10ms each safety processor checks timeout counter for communication between safety processors.
Other internal diagnostics Each safety processor runs a series of checks on the health of the system such as ADC, RAM, FLASH, CPU, etc.	Sender EPC, Receiver EPC, NSC Pro, WES Pro	Each safety processor runs a series of tests to ensure that the subsystems of each processor are working correctly. The tests are based on the requirements of the safety manual of the safety processors. If a test fails, the system resets. During the reset, the outputs are forced OFF by the hardware.	Every 10ms.