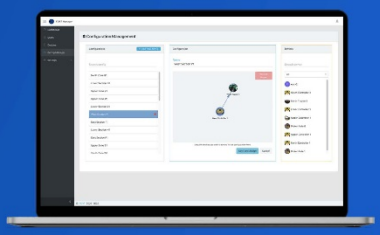
Pro Series User Guide

FORT

FORT PRO SERIES

User Manual
Safe Remote Control Pro (SRC Pro) Release Candidate
Endpoint Controller (EPC)
FORT Manager



FORT Robotics, 2023, fortrobotics.com

Document part number: 400-0044

Version *1.6.0 v1*

FORT Robotics
1608 Walnut St floor 12
Philadelphia, PA 19103

PREFACE

About this Guide

This document shows how to integrate the FORT Pro Series devices with your smart machines to enable secure transmission of wireless safety and control commands. It is intended for OEM developers who want to build safety solutions into their machines as well as integrators and end users of those machines.

Warnings Notes and Cautions

The guide provides safety warnings and cautions, as well as notes where appropriate to alert you to potential hazards when using, wiring, configuring, and mounting a device. These alerts are formatted as follows:

INJURY OR LOSS OF LIFE

⚠ **WARNING:** Could cause injury or loss of life.

EQUIPMENT DAMAGE

⚠ **CAUTION:** Could cause equipment damage.

IMPORTANT TO KNOW

⚠ **NOTE:** Could lead to loss of data or time, or is easy to overlook.

Standards

This document uses the international standard (ISO 8601) for dates (*YYYY-MM-DD*). For example, the 31st of October, 2023 is shown as 2023-10-31.

Note that the version of this guide corresponds to the date on which it is published and uses the same format.

Table of Contents

List of Tables

List of Figures

CHAPTER 1 *Introduction*

This document shows how to integrate the FORT Pro Series devices with your smart machines to enable secure transmission of wireless safety and control commands. FORT helps protect people and organizations from injury, damage, and downtime with trusted control & communication for any machine. With built in functional safety and security, FORT's Pro Series delivers machine control and communication you can trust.

The Pro Series includes:

- **Endpoint Controller (EPC)** — A mountable sender and receiver that can execute trusted commands over Bluetooth low energy, Wi-Fi, Ethernet, and ISM Radio. It can be used as a sender, to send safety signals to other Endpoint Controllers, or as a receiver, wired into a machine for control and safety functions sent by another Endpoint Controller or by a Safe Remote Control Pro with which it is paired.
- **Safe Remote Control Pro (SRC Pro)** — Used as a sender to wirelessly connect to an Endpoint Controller, it provides both wireless E-Stop and remote operator control of a machine at a safe distance.
- **FORT Manager** — Provides device registration, configuration, management and updates, and management of users through a web-based application and APIs. You can access the FORT Manager Web App at: https://app.fortrobotics.com, and the FORT Developer Portal at: https://www.fortrobotics.com/dev-portal).

This guide is intended for OEM developers who want to build safety solutions into their machines as well as integrators and end users of those machines.

⚠ NOTE: Unless otherwise noted, the features described in this document are available as of the date of the latest revision.[1]

1. See the "Revision History" appendix for a list of updates in the current version of the manual as well as for details about the product versions to which it applies.

Key Features

The **Safe Remote Control Pro** is an easy-to-use controller designed to wirelessly operate machines. It allows a user to take temporary manual control of equipment or activate an E-Stop from a remote location. Some key features of the Safe Remote Control Pro are:

- Wireless interface that supports Bluetooth low energy (BLE), ISM 902-928 MHz (NA), and ISM 868 MHz (EU).Two 2-axis joysticks, two 1-axis finger sticks, eight programmable buttons, and a red E-Stop button.
- Safety features that meet IEC 61508 standards, including dual safety processors, dual channel E-Stop, drop and idle detection, and vibration feedback.
- Enclosure is IP65 rated in accordance wit*1.6.0 v1* IC-60529, has ruggedized rubber grips, a sunlight-readable LCD for device information, and measures 181 mm x 155 mm x 83 mm.
- Security is built in through tamper proofing device, secure boot, secure configuration, secure updates, and trusted communications.
- Operates in temperatures from -20 °C - +60 °C with a battery life of 18 hours (chargeable through USB).

See “SRC Pro Technical Specifications” on page B-1 for detailed technical specifications for the Safe Remote Control Pro.

The **Endpoint Controller** makes it possible to send and receive trusted safety commands over a variety of networks. You can mount it on a machine, or machine attachment, for remote control. You can also use it to send safety commands to up to 30 Endpoint Controller-equipped machines simultaneously. Some key features of the Endpoint Controller are:

- Designed for 12V DC or 24V DC systems with 8V DC to 32V DC operating voltage.
- Wireless interface that supports Bluetooth low energy (BLE), ISM 902-928 MHz (NA), ISM 868 MHz (EU), and Wi-Fi.
- Electrical safeguards, including transient protection per ISO 16750 and ISO 7637-2, reverse battery, load dump, and jump-start protection, as well as electrostatic discharge protection.
- IP65 rated aluminum enclosure in accordance with IEC-60529.
- Comes with one or two RP-TNC antenna connectors and two M12 Ethernet connectors; 23 pin main integration connector for TE connectivity; CAN (controller area network) bus.
- Measures 228 mm x 176 mm x 70 mm.
- Provides three dual-channel safety inputs and three dual channel safety outputs; dual safety processors are the core of a redundant, one out of two (1oo2) safety architecture.
- Security is built in through tamper proofing device, secure boot, secure configuration, secure updates, and trusted communications.
- Operates in temperatures from -40 °C to +85 °C.

See “EPC Technical Specifications” on page A-1 for detailed technical specifications for the Endpoint Controller.

Overview

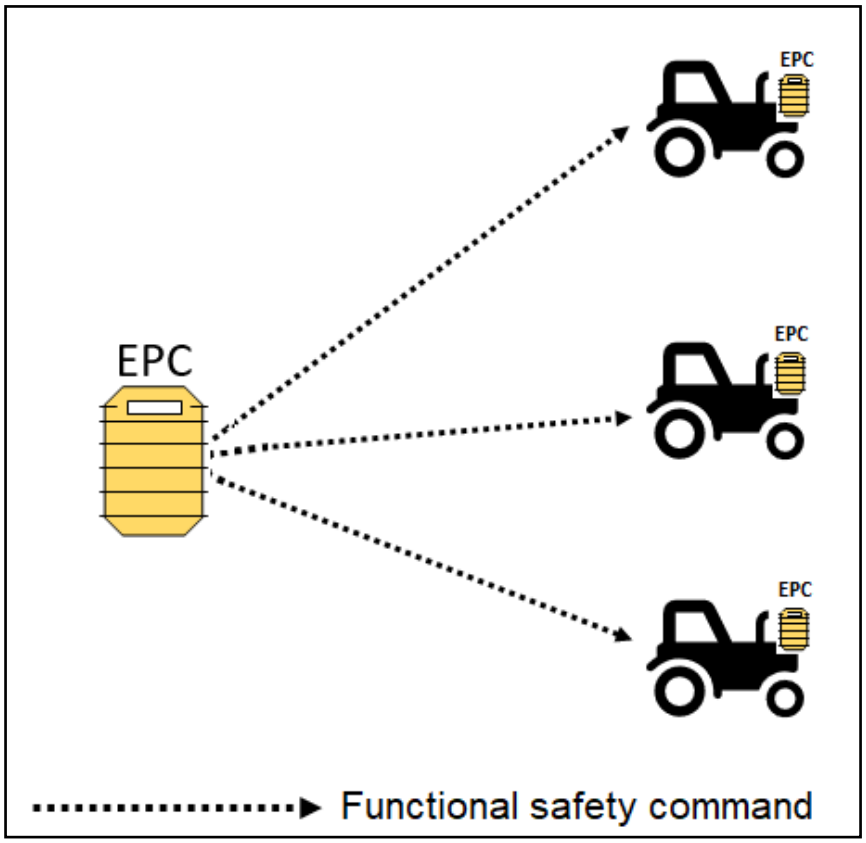
The primary function of the system is the ability to wirelessly send a safety signal from a remote device sender to one or more receivers that are wired to pieces of equipment (henceforth known as the EUC, or equipment under control). Additionally, a Safe Remote Control Pro provides the ability to remotely control and maneuver the EUC.

There are various ways to configure the system, using FORT Manager, depending on your specific situation, but at a basic level, every configuration has:

- A network that allows devices to communicate.
- An Endpoint Controller wired to each EUC.
- A remote controller (an Endpoint Controller, Safe Remote Control Pro, or both) that communicates wirelessly with the EPCs attached to the EUCs to send safety signals, and in the case of the SRC Pro, safety and control signals.[2]

The following figure illustrates a basic configuration:

FIGURE 1-1. *Basic Configuration*



2. How you wire the EPC to an EUC determines the effect of the safety signal. For example, you could wire the EPC to the engine (to shut off the EUC), to the braking system (to slow it down), to a particular part of the equipment (to stop a robotic arm), etc.

The basic operational philosophy of the Endpoint Controller is that it allows the EUC to move between the safe state and the normal state.

The safe state causes the equipment under control (EUC) to cease whatever dangerous function it is performing. Depending on the equipment and how you wired and configured it, this could mean shutting down the machine entirely, slowing it down, turning off a specific function such as a robotic arm, or something else entirely. Depending on the configuration, any of the following situations trigger the safe state:

- An equipment operator perceives that the EUC has encountered a major problem that requires it to be stopped immediately and presses the E-Stop button to do so.
- A solid state safety device (such as a programmable logic controller (PLC), or light curtain) that is wired to an EPC is monitoring an area and a worker opens a guard or reaches into a hazardous area, which causes the EPC to initiate the safe state.
- The system detects an automatic diagnostic fault and initiates the safe state.

The normal state means that an E-Stop command has not been requested, no diagnostic faults are detected, and the EUC is powered.

Getting Started

The following bullets outline the process for getting your Pro Series devices up and running. Although we show Plan as the first step, this manual assumes that you have already determined how many devices you need and have purchased them.

- **Plan —** Determine the type of configuration to build. "Configurations and Use Cases" on page 2-1 provides an overview to the types of configurations that we support and the use case for each one.

  In addition, be certain to involve a safety expert in the planning process to develop a safety plan for integrating the FORT Pro Series devices with your equipment.
- **Configure —** Use FORT Manager to build a logical configuration ("Configurations and Use Cases" on page 2-1):
  - Log in to FORT Manager and register your devices.
  - Add them to a configuration.
  - Set device and network parameters, including communication channels, timeout value, and types of inputs.
- **Load —** Load the configuration onto each device ("Loading a Configuration onto Your Devices" on page 2-15).
- **Wire —** Wire the inputs and outputs ("Installation — Wire and Mount Endpoint Controller" on page 3-1).
  - On the input device (sender), wire the inputs to an E-Stop type device or to a Solid State Safety Device (SSD).
  - Wire the output devices (receiver) to the EUC.
- **Test —** Verify that the system performs as expected before deploying it. For example, pressing an E-Stop button stops the EUC, walking in front of a light curtain slows or stops the EUC, and so on. Be certain that a safety expert verifies that the system is operating in accordance with your safety plan.

⚠ **WARNING:** Safe operation of the system requires that you thoroughly test the system before putting it into a production environment. Testing includes training your personnel on both the manual functions (pressing an E-Stop button, using an SRC Pro to maneuver an EUC, etc.) and automatic functions

of the system (solid state devices triggering safety, exceeding the timeout value, loss of radio signal, etc.).

Registering Devices

Before you can use your FORT Pro series devices, you must register them in FORT Manager, which is available as a web-based application or APIs. If you've already registered your devices, skip this procedure and go to the next chapter to add the devices to a configuration.

BEFORE YOU BEGIN:

This section assumes that:

- You have set up a FORT Manager account, which requires an invitation email from FORT Manager, and a device serial number (see the Getting Started Guide for more information).
- You, or someone in your company has set up your organization, added user accounts, and assigned roles in FORT Manager.
- You have the serial number for each device that you purchased (either from the plate on the device or emailed to you by FORT).
- You have mapped out your configuration in terms of protocols, naming conventions, connections, etc.

⚠ **NOTE:** If you are having any problems with the FORT Manager Web App, such as launching or logging in, or you don't have the serial number for your devices, submit a request on the Support Portal to get help. Click **Sign up** to create a Zendesk account if you don't already have one.

TO ADD DEVICES TO FORT MANAGER:

(Requires DeviceManager or Admin role.)

1. Navigate to the FORT Manager Web App (https://app.fortrobotics.com) and enter your username and password when prompted.

   FORT Manager is invite-only. If you don't have an account, ask the person at your company who initially set up the FORT Manager account (your FORT Manager Admin) to create one for you. If you don't know your company's FORT Manager Admin, reach out to us at support@fortrobotics.com.
2. Click the **Devices** tile at the top of the dashboard (or **Devices** in the left navigation pane).
3. Click the **Add device** button on the upper right.
4. Type the serial number for the device (on a plate on each device you received — or emailed by FORT) and click **Next**.
5. Type a name for the device, optionally click the picture icon to add a picture (EPC only, SRC Pro has a fixed image), and click **Register**.

   We recommend assigning names that describe the function or location of the device or the EUC, for example, *South Tractor Remote Control*, or *Observation Deck Controller* for sending devices, and *South Tractor*, *Thresher*, *AMR-1*, etc. for EPCs attached to EUCs.

   You can rename a device at any time (select it in the Device Registration page and click the **Edit** icon); FORT Manager updates the name wherever else it appears, such as in Config Manager.
6. Add all the devices that you have purchased.

   Devices appear in the Device Registration page after you add them. Click **Devices** to see a list and click any device to see details about it.

CHAPTER 2

Configurations and Use Cases

After you register your FORT Pro Series devices, you can add them to a configuration in FORT Manager, which is available as a web-based application.

A configuration allows you to:

- Add devices to a network enabling them to communicate with each other.
- Configure device settings (including CAN settings, timeout period and voltage).
- Select communication method (Ethernet, Wi-Fi, BLE (Bluetooth low energy), ISM).
- Designate the type of sender for the configuration.
- Configure the inputs on the sender.The Pro series supports the following configurations:
- "EPC to EPC Configuration" on page 1 — A single Endpoint Controller connects to one or more Endpoint Controllers (up to 30) with the ability to send safety signals simultaneously to all of the equipment in the configuration.
- "SRC Pro to EPC Configuration" on page 5 — A Safe Remote Control Pro can connect to one Endpoint Controller at a time out of multiple Endpoint Controllers in the configuration (up to 30) to send safety and control signals.
- "Hybrid Configuration (SRC Pro and EPC to EPC)" on page 12 — An Endpoint Controller and Safe Remote Control Pro are both able to communicate with multiple Endpoint Controllers (up to 30). The Endpoint Controller can send a safety signal to all the Endpoint Controllers at once. The Safe Remote Control Pro can connect to one of multiple Endpoint Controllers (up to 30) at a time to send safety and control signals.

You use FORT Manager to build these configurations and your laptop to tether to powered devices and apply the configurations. You can find specific instructions at the end of each of the following sections.

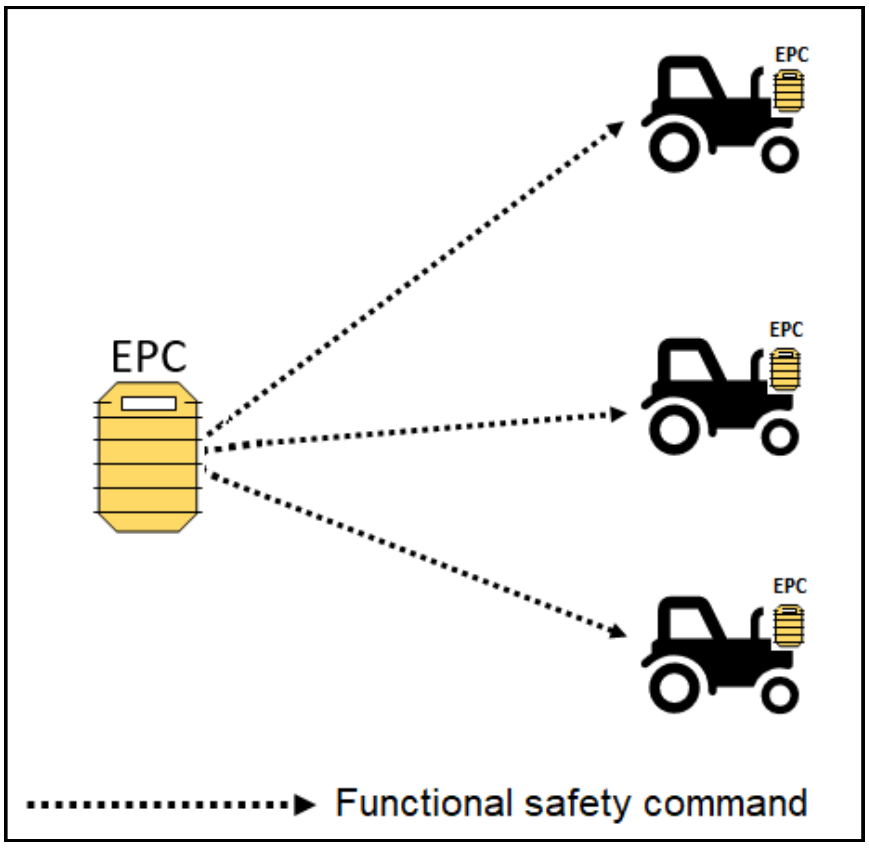
EPC to EPC Configuration

In an EPC to EPC configuration, you configure a single Endpoint Controller as the sender for up to 30 receiver Endpoint Controllers. The sender Endpoint Controller is able to send up to two safety signals to every Endpoint Controller in the configuration at once.

For example, if a number of machines are operating in a warehouse area, you can wire a light curtain to the Endpoint Controller sender that shuts down all the machines if someone walks into the area. Likewise, you can wire an E-Stop switch to the Endpoint Controller sender and place it at the entrance to the area, allowing an operator to temporarily shut down the machines if anything looks dangerous, or for another reason, such as pulling out a particular machine for inspection or maintenance.

The following diagram shows a configuration with an Endpoint Controller sender and three Endpoint Controller (EPC) receivers:

FIGURE 2-1. *EPC to EPC Configuration*



The following table shows details about an EPC-to-EPC configuration:

TABLE 2-1. *EPC-EPC Configuration*

Sender	Inputs	Receivers	Communication
EPC	One or two independent safety rated inputs	Up to 30 EPCs	Ethernet or Wi-Fi

Building an EPC to EPC Configuration

This procedure shows how to build a configuration that consists of one Endpoint Controller sender and up to 30 Endpoint Controller receivers.

TO BUILD A CONFIGURATION WITH AN EPC SENDER:

(Requires ConfigManager or Admin role.)

1. Navigate to the FORT Manager Web App (https://app.fortrobotics.com) and enter your credentials when prompted.
2. Click the **Config Management** tile at the top of the dashboard or **Config Manager** in the left navigation pane.
3. Click **Add new config**.
4. In the **Configuration** pane, in the **Name** field, type a meaningful name for the configuration.

5. In the **Devices** pane, select an EPC from the list and drag it to the **Configuration** pane.
   The device you bring in first becomes the sender and those you drag in later become receivers.
6. In the **Devices** pane, select an EPC to use as a receiver and drag it to the **Configuration** pane.
   Continue to add EPC devices (up to 30) or stop at one if you only have one EUC to control.
7. From the drop-down underneath the configuration, select the communication protocol for the network.
   The default is Ethernet.
8. Click **Settings** to set configuration wide settings:
   - For **Ethernet**, set:
     - **Netmask** Defaults to 255.255.255.0.
     - **Gateway** The gateway IP address, such as 192.168.1.1.
     - **Name Server** A name server IP address, such as 192.168.1.2

       You can identify multiple name servers. Click **Add** after specifying each one. The order in which you add name servers is the order in which the EPC looks for them. If it can't reach the first server it goes to the second server in the list, and so on until it reaches one.
   - For Wi-Fi, set:
     - **SSID** The network ID.
     - **Password** The network password.
     - **Netmask** Defaults to 255.255.255.0.
     - Gateway The gateway IP address, such as 192.168.1.1.

       Be certain to set this parameter to the router address to avoid slow connections and possible timeouts during operation.
     - **Name Server** A name server IP address, such as 192.168.1.2.

       You can identify multiple name servers. Click **Add** after specifying each one. The order in which you add name servers is the order in which the EPC looks for them. If it can't reach the first server it goes to the second server in the list, and so on until it reaches one.

Other settings:

- **Safety Timeout:** Select a value for the safety communication timeout (default is 250 msec for Ethernet or. 500 msec for Wi-Fi).

⚠ WARNING: To optimize safety, we strongly recommend that you keep the default value (Ethernet: 250 msec; Wi-Fi 500 msec). If you consider changing the value, do so only after first consulting with your system safety manager.

A receiver EPC expects to receive at least one valid safety message from the sender EPC within the timeout period or else it enters the safe state (turns off its outputs). For example, a safety timeout of 500 msec means that a receiver EPC must receive at least one valid safety message within 500 ms of receiving the last valid safety message or it turns off its outputs.

A higher value, which makes the EPC less sensitive to communication loss, means that if an EPC loses communication with its sender, the EUC will run for a longer period before stopping automatically. On the other hand, a lower timeout value, which reduces the risk of the EUC running without connection to the safety controller, increases the sensitivity to communication loss.

⚠ IMPORTANT: Wi-Fi networks vary in signal reliability. While testing your system, if you experience signal drops with the default timeout setting, test with a higher value to see if that fixes the problem.

- **Voltage Level** Select the voltage from the dropdown, either 12 Volts (default) or 24 Volts.

- **CAN Mode** The Controller Area Network (CAN) is disabled by default. You can enable it by selecting either of these protocols from the drop down:
  - CANOpen
  - *J1939*
- **CAN Bitrate** (250 kbit default): If you selected a CAN mode, accept the default bitrate, or use the drop down menu to select a value that is more optimal for your application.

  You cannot adjust the bitrate through the CANopen NMT protocol but must do so here or with the CLI tool.

9. Click **OK** to save the configuration settings.

   If you enable a CAN mode, each EPC receiver requires a Node ID or address; FORT Manager provides a default value, but in Step 12you have the option to change the CAN ID.

10. Select the sender EPC (the red dot indicates that it requires one or more configuration parameters) and click **Settings** in the upper right corner to set its IP address and configure its inputs:
    - **IP Address** Enter a unique IP address for the device, for example: 192.168.1.2.

      You are configuring the J3 port's IP address for use on your safety network. To avoid conflicts with the J2 management port, which is configured by default to 192.168.3.10, don't specify an address in the subnet: 192.168.3.0/24.
    - **Input 1**, **Input 2** Select a value from the drop-down menus for **Input** 1 and **Input 2** to identify the type of device that you intend to wire to the EPC inputs. The inputs are independent of each other such that you can wire one type of device to Input 1 and a different type to Input 2 (or wire the same type to each one). You must specify a device for at least one input and specify Not Used for an input that you are not going to use:
      - *Not Used* The default value; leave an input as *Not used* if you are not going to wire a device to it.
      - *E-Stop Type Device* An E-Stop type switch.
      - *Solid State Safety Device* A device such as a light curtain, PLC, etc.
    - **Input 3** Reserved for use with an SRC Pro and not settable in the current configuration.
11. Click **OK** to save the settings for the sender; the green dot indicates that you have set required parameters.
12. Select an EPC receiver in the configuration (the red dot indicates one or more configuration parameters are required) and click **Settings** in the upper right corner:
    a. In **IP Address**, type a unique IP address for the device, for example: 192.168.1.2.

       You are configuring the J3 port's IP address for use on your safety network. To avoid conflicts with the J2 management port, which is configured by default to 192.168.3.10, don't specify an address in the subnet: 192.168.3.0/24.

    b. Optionally, if you enabled a CAN mode, you can change the node ID or address for each EPC receiver — however, FORT Manager applies a default value of 3 to each EPC.

       You cannot change the Node ID through the CANopen NMT protocol but must do so here.

       The node ID or address uniquely identifies the EPC on the CAN system. Potentially, each piece of your equipment could have multiple CAN elements, each of which requires a unique ID. Therefore, you must be certain that whatever value you set in FORT Manager doesn't conflict with a different CAN element on any of your equipment. Setting a single value for all EPCs means that you must only check one value against any CAN components on the equipment.

       If, on the other hand, to avoid conflicts you must change the CAN mode for one or more EPCs, enter a value in CANOpen Node ID (between 1-127) or J1939 Address (1-255) depending on which CAN protocol you previously selected.

    c. Click **OK** to save the settings for the selected receiver.

13. Repeat the previous step to assign an IP address to every EPC receiver in the configuration (and optionally change the Node ID or address.
14. Click **Save and Assign** to save the new configuration.

    FORT Manager displays a message after it successfully saves the configuration. You can view and make changes to this configuration at any time by selecting it in the Configuration Management tab.

NEXT STEPS

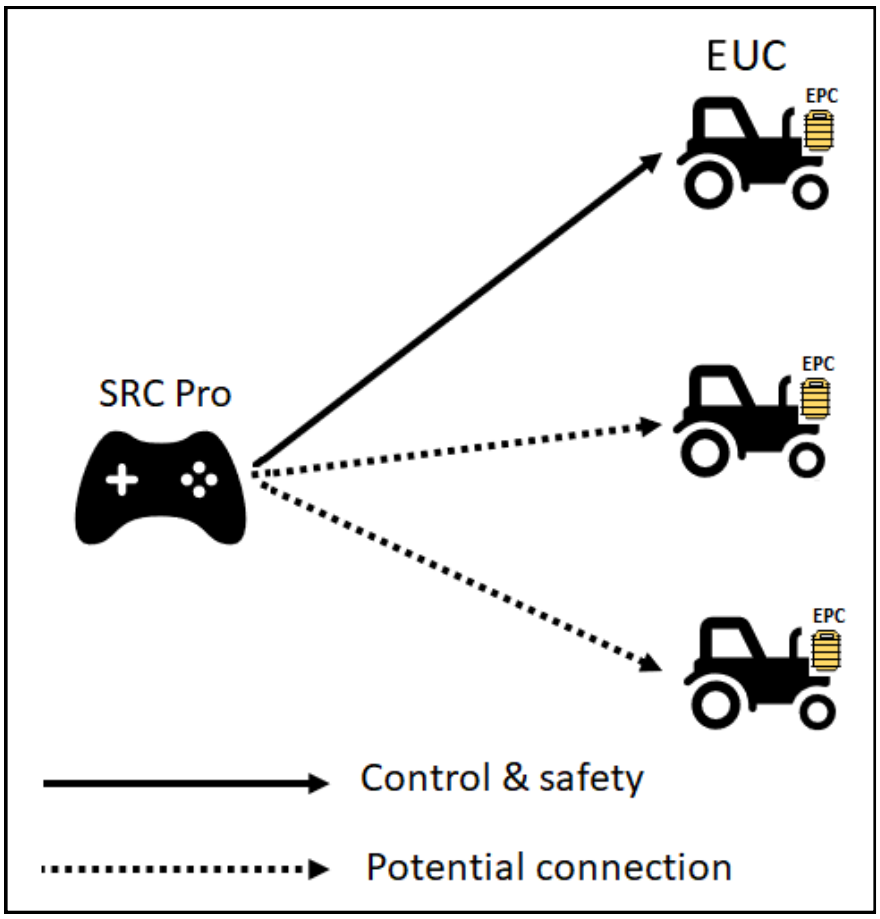
Go to "Loading a Configuration onto Your Devices" on page 15 for instructions on how to load the configuration you just created onto your devices.

SRC Pro to EPC Configuration

In this configuration, you configure a single Safe Remote Control Pro as the controller for one or more Endpoint Controllers (up to 30). The Safe Remote Control Pro can only connect to one Endpoint Controller at a time to send safety and control signals.

For example, you might store multiple machines in a yard overnight. In the morning, an operator can connect the Safe Remote Control Pro to the Endpoint Controller on one of the machines and use the Safe Remote Control Pro to drive the machine to a work area. At the work area the operator can disconnect the Safe Remote Control Pro from the machine and return to the yard to connect to another Endpoint Controller and drive out a different machine. Meanwhile, the first machine can work autonomously in autonomous (unsupervised) mode (see "Machine Select" on page 6).

FIGURE 2-2. *SRC Pro to EPC Configuration*



The following table shows details about a Safe Remote Control Pro to EPC configuration:

TABLE 2-2. *SRC Pro to EPC configuration*

Sender	Inputs	Receivers	Communication
SRC Pro	Integrated E-Stop switch	Up to 30 devices in a configuration, but only one connection at a time	Bluetooth or ISM

Machine Select

The machine select function allows a user of a Safe Remote Control Pro to select and connect to one Endpoint Controller at a time (by picking from a list of available devices that is displayed on the LCD screen).

When the user selects a machine and successfully connects to the Endpoint Controller on that machine, the Endpoint Controller is always put in supervised mode. The user later can change the mode to autonomous mode (if applicable and needed).

Supervised mode means that the Safe Remote Control Pro is connected to the Endpoint Controller and is sending input data such as joystick movements, safety messages, etc. to the selected machine. If an operator pushes the E-Stop button, the Endpoint Controller enters the safe state. If the Safe Remote Control Pro stops communicating with the Endpoint Controller, resulting in a timeout, the Endpoint Controller enters the safe state.

Autonomous (unsupervised) mode is meant to be used with machines that have autonomous capability. In autonomous mode, the SRC Pro and the EPC are not communicating with each other, so the SRC Pro is not sending safety or control information to the EPC. Rather, the EPC attached to the equipment monitors the customer supplied "Connecting the SRC Pro to an EPC" on page 4-3safety signal, and if that signal changes out of the normal state, the EPC enters the safe state and breaks the circuit to the equipment under control.

"Connecting the SRC Pro to an EPC" on page 4-3 explains how to connect an SRC Pro to an EPC and sub sections explain how to change the mode as well as implications of operating in each mode.

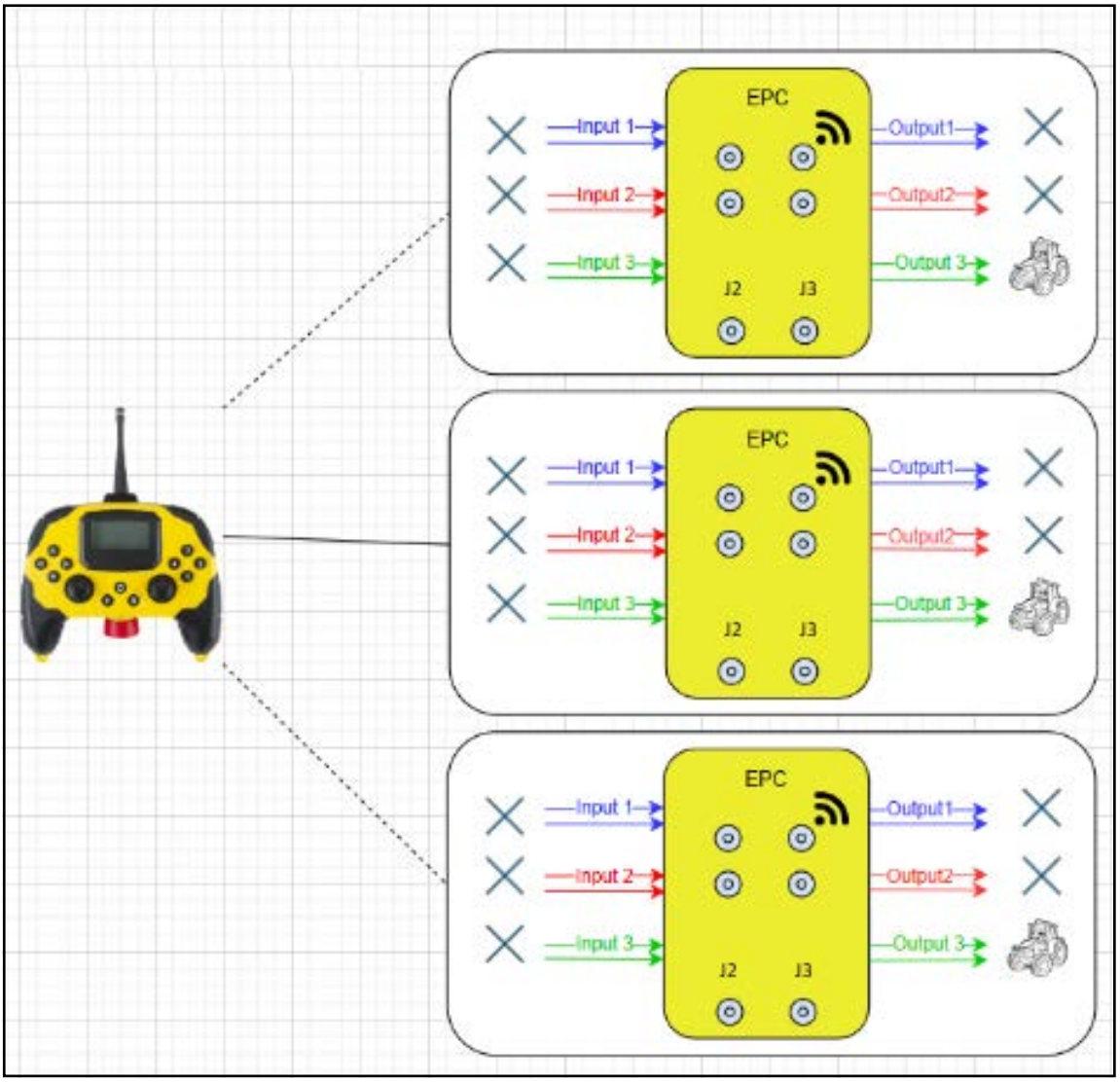
Wiring an EPC for use with Machines Without Autonomous Capability

This section shows how to wire an EPC to a machine that does not have autonomous capability. Machine such as this, can operate in supervised mode only.

As shown in the following figure, you must connect Output 3 on each of the Endpoint Controllers (EPC) to the equipment under control (EUC). "Wiring Outputs on EPC Receivers" on page 3-8 provides details about the wiring, but essentially, both channels of Output 3 are connected to two relays in series. The circuit that is defined by these relays controls connection of a solenoid to the equipment under control. If safety is not requested, the Endpoint Controller keeps the output on to keep the relays' contactors closed. On the other hand, if safety is requested, the Endpoint Controller turns off the outputs, which opens the relays and breaks connection of the circuit to the EUC. In this case, if the EUC is using the circuit for power, when the contactors open, the machine shuts off.

The following figure illustrates the wiring for machines that don't require autonomous (unsupervised) mode. See "Input 3 Asserted on EPC Receiver" on page 2-9 for the wiring for machines that do require autonomous.

FIGURE 2-3. *Machine Select Supervised Mode*



Initially, when a user selects a machine and connects to it, the Endpoint Controller is put in supervised mode. Using the LCD display and Safe Remote Control Pro controls, the user can change the mode of the Endpoint Controller to autonomous.

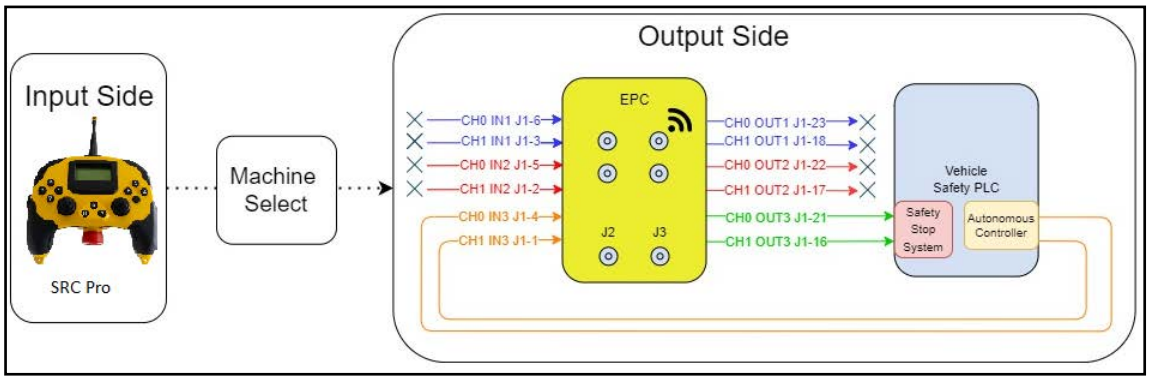
Input 3 is the way that you (the customer) control the safety system when an SRC Pro is not connected. (Note that you could also build a hybrid configuration and use Global E-Stop with an EPC sender to control the safety system when the SRC Pro is not connected to the EPC).

In autonomous mode, and as long as Input 3 of the Endpoint Controller is high, the Endpoint Controller keeps the two relays connected to Output 3 powered while ignoring an E-Stop press on the Safe Remote Control Pro as well as not responding to joystick movements and button presses on the SRC Pro.

Wiring an EPC for use with Machines With Autonomous Capability

The following figure illustrates the wiring for machines with autonomous capability that require operation in autonomous mode.

FIGURE 2-4. *Input 3 Asserted on EPC Receiver*



As long as the customer safety signal to Input 3 on the Endpoint Controller remains in the normal state (high), the machine remains powered up and running. If the customer safety signal to the Endpoint Controller changes out of the normal state, the Endpoint Controller automatically switches to safe mode, turning off Output 3, and breaking the power connection to the EUC.

Machines such as this can operate in supervised or autonomous mode. In fact, when first connected to an SRC Pro, they are always in supervised mode.

Building an SRC Pro to EPC Configuration

This procedure shows how to build a configuration that uses a Safe Remote Control Pro as the sender and up to 30 Endpoint Controller receivers.

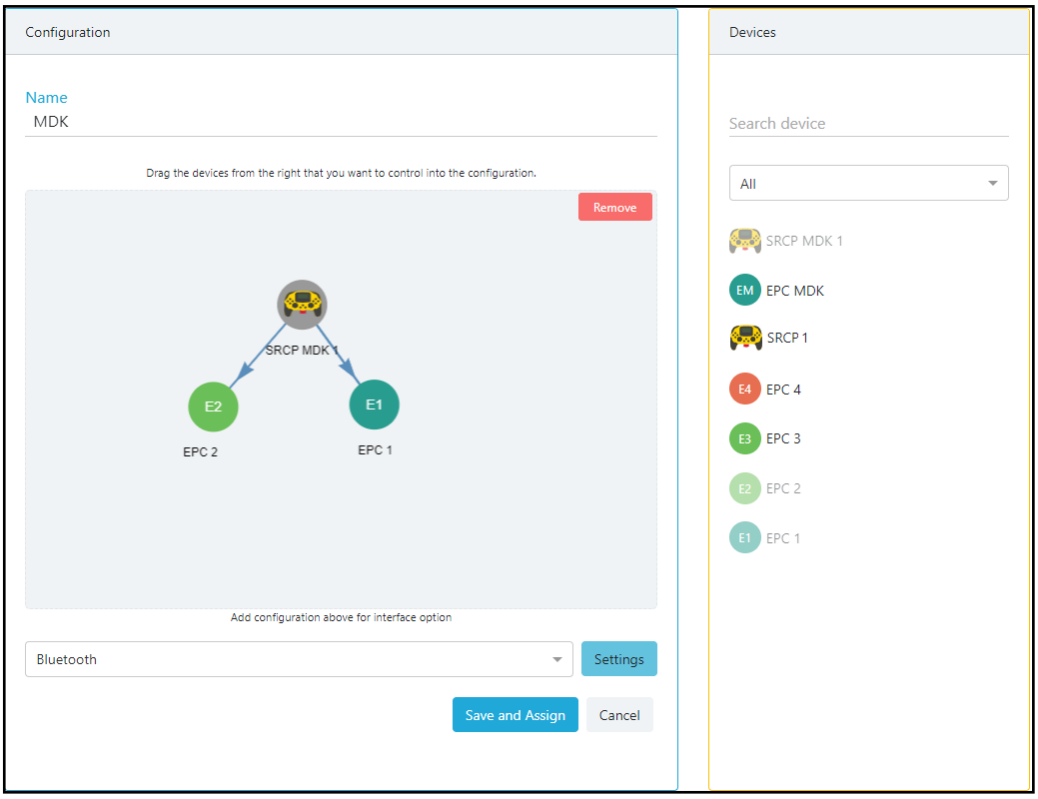
⚠ **NOTE:** If you are planning to build a hybrid configuration, you first use the current procedure to create a base configuration, then modify the configuration with the steps in "Building a Hybrid Configuration" on page 2-13.

TO BUILD A CONFIGURATION WITH AN SRC PRO REMOTE:

(Requires ConfigManager or Admin role.)

1. Navigate to the FORT Manager Web App (https://app.fortrobotics.com and enter your credentials when prompted.
2. Click the Config Management tile at the top of the dashboard or Config Manager in the left navigation pane.
3. Click Add new config.

4. In the Configuration pane, in the **Name** field, type a meaningful name for the configuration.
5. In the Devices pane, select an SRC Pro from the list and drag it to the Configuration pane.
   The device you bring in first becomes the sender and those you drag in later become receivers.
6. In the Devices pane, select an EPC to use as a receiver and drag it into the Configuration pane.
   Continue to add EPC devices (up to 30) or stop at one if you only have one EUC to control.



7. From the drop-down underneath the configuration, select the communication protocol for the network. The default is Bluetooth. If you change it to ISM, use Settings as described in the next step to set ISM parameters.
8. Click **Settings** to set configuration-wide settings:
   - **ISM Transmission Power:** (if you selected ISM) Select a value from the drop down list:
     - *Low* Use for indoor or close range use.
     - *Medium* (default) Use for outdoor and mid-range distance.
     - *High* Use for outdoor and maximum range.

     Although higher settings allow for greater range, they reduce battery life.
   - **ISM Transmission Channel:** Enter a value for the transmission channel (default is 1).

     European radios (EPC-SRC Pro 1002) support one channel only so the field is read-only, and you can't change the default value (1).

     North American radios (EPC-SRC Pro 1001) support channels from 1 - 21. Your system may suffer from interference if other ISM networks are operating in the same location. Be certain that each network has a unique transmission channel and experiment with changing the ISM Transmission Channel to find the clearest signal.
   - **Safety Timeout:** Select a value for the safety communication timeout (250 msec default).

⚠ WARNING: To optimize safety, we strongly recommend that you keep the default value (250 msec). If you consider changing the value, do so only after first consulting with your system safety manager.

A receiver EPC expects to receive at least one valid safety message from the sender within the timeout period or else it enters the safe state (turns off its outputs). For example, a safety timeout of 250 msec means that a receiver EPC 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.

A higher value, which makes the EPC less sensitive to communication loss, means that if an EPC loses communication with its sender, the EUC will run for a longer period before stopping automatically. On the

other hand, a lower timeout value, which reduces the risk of the EUC running without connection to the safety controller, increases the sensitivity to communication loss.

⚠ NOTE: Although signal drops should be rare with Bluetooth or ISM, if you experience them while testing your system with the default timeout setting, test with a higher value to see if that fixes the problem.

Voltage Level: Select the voltage from the dropdown, either 12 Volts (default) or 24 Volts.

CAN Mode: The Controller Area Network (CAN) is disabled by default. You can enable it by selecting either of these protocols from the drop down:

- CANOpen
- *J1939*

- **CAN Bitrate (250 kbit default)**: If you selected a CAN mode, accept the default bitrate, or use the drop down menu to select a value that is more optimal for your application.

  You cannot adjust the bitrate through the CANopen NMT protocol but must do so here or with the CLI tool.

If you enable a CAN mode, each EPC receiver requires a Node ID or address; FORT Manager provides a default value, but in Step 11 you have the option to change the CAN ID.

9. Click **OK** to save the configuration settings.
10. Optionally, if you selected ISM, you can set a unique radio ID for each device (a green dot appears on each device icon indicating configuration options are available)— however, FORT Manager applies default IDs for each device (in a range, starting with 1) when you save the configuration.
    a. Select a device and click Settings in the upper right corner of the Configuration pane.
    b. Type a number between 1 and 128 to ID the device (FORT Manager verifies that the number isn't already taken for a different device) and click **OK**.
11. Optionally, if you enabled a CAN mode, you can change the node ID or address for each EPC receiver (a green dot appears on each device icon indicating that configuration options are available) — however, FORT Manager applies a default value of 3 to each EPC.

    You cannot change the Node ID through the CANopen NMT protocol but must do so here.

    The node ID or address uniquely identifies the EPC on the CAN system. Potentially, each piece of your equipment could have multiple CAN elements, each of which requires a unique ID. Therefore, you must be certain that whatever value you set in FORT Manager doesn't conflict with a different CAN element on any of your equipment. Setting a single value for all EPCs means that you must only check one value against any CAN components on the equipment.

    If, on the other hand, to avoid conflicts you must change the CAN mode for one or more EPCs, do the following:

    a. Select a device, click Settings in the upper right corner, and enter a value in CANOpen Node ID (between 1-127) or J1939 Address (1-255) depending on which CAN protocol you previously selected.
    b. Click OK to save the value.
    c. Repeat for other EPCs.
12. Click **Save and Assign** to save the new configuration

    FORT Manager displays a message after it successfully saves the configuration. You can view and make changes to this configuration at any time by selecting it in the Configuration Management tab.

NEXT STEPS

Go to "Loading a Configuration onto Your Devices" on page 2-15 for instructions on how to load the configuration you just created onto your devices.

Hybrid Configuration (SRC Pro and EPC to EPC)

An SRC Pro and EPC Hybrid Configuration (also known as a Global E-Stop configuration) combines the SRC Pro to EPC and the EPC to EPC configurations, allowing one Safe Remote Control Pro and one Endpoint Controller to control multiple (up to 30 Endpoint Controllers attached to EUCs.

The Safe Remote Control Pro can control and send safety signals to any one Endpoint Controller at a time and the Endpoint Controller sender can send safety signals to all the Endpoint Controllers in the configuration at once.

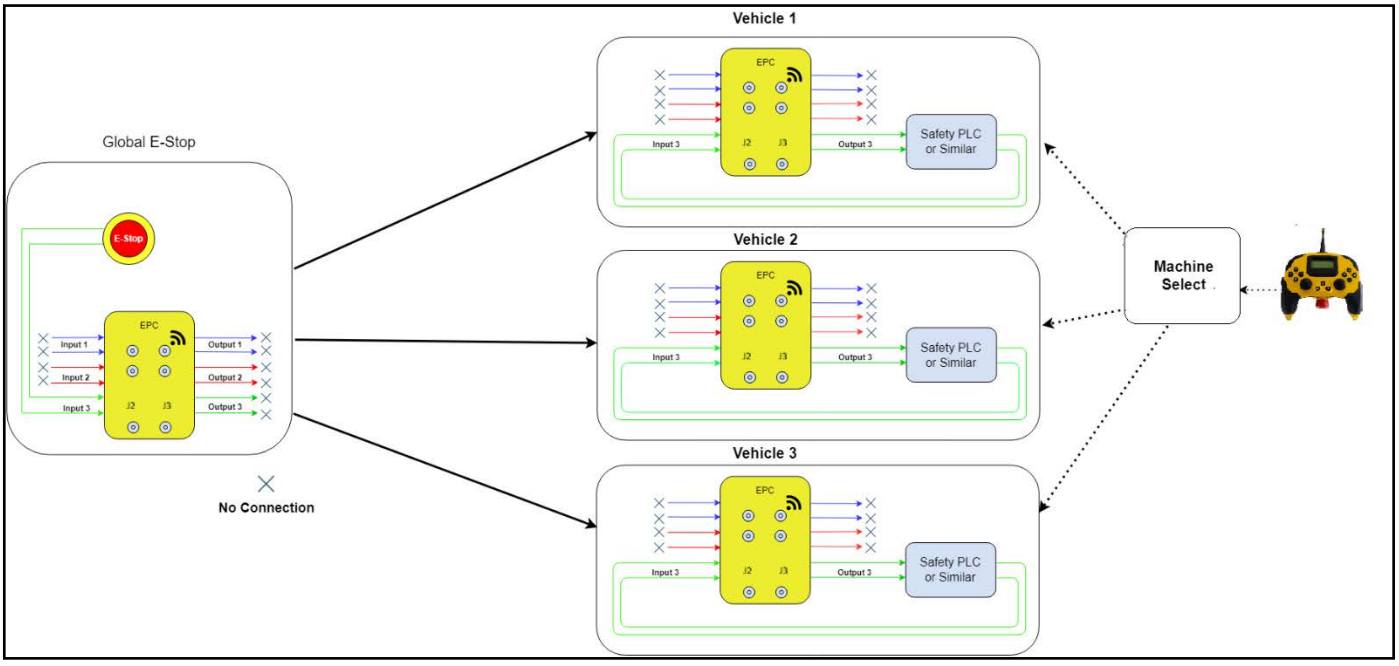
For example, imagine a situation in which you have a number of autonomous machines that are parked in a yard for the night. At the beginning of the workday, you use a Safe Remote Control Pro to connect to one of the machines and drive it to the work area. Once the machine is at the work site, you put the Endpoint Controller in autonomous (unsupervised) mode so the machine can work autonomously. You now walk back to the yard and use the Safe Remote Control Pro to connect to and pull out another machine.

At this point, the first machine that you moved is operating without the Safe Remote Control Pro in control. However, with this configuration, an Endpoint Controller is still connected to the machine that is operating autonomously, allowing a supervisor to press the E-Stop button on the sender Endpoint Controller and stop the machine if necessary.

In practice you could place an Endpoint Controller sender in a location, such as a balcony, that overlooks the entire work area. After an operator releases one or more machines to work autonomously and walks out of the work area, a supervisor could still monitor the autonomous machines and issue an E-Stop command at any time.

The following figure illustrates this configuration. The Endpoint Controller sender can send an E-Stop to every Endpoint Controller that is connected to a vehicle and the Safe Remote Control Pro (using machine select) can connect to any one Endpoint Controller at a time for safety and control functions.

FIGURE 2-5. *SRC Pro and EPC Hybrid Configuration*



Note these points about this configuration:

- Inputs 1 and 2 are unused on the sender Endpoint Controller (single EPC on the left of the figure).
- Outputs 1 and 2 are unused on the receiver Endpoint Controllers (three EPCs on the right of the figure).
- When a Safe Remote Control Pro is connected to a receiver Endpoint Controller in supervised mode, pressing either the global E-Stop[1] on the Endpoint Controller or the E-Stop button on the Safe Remote Control Pro turns off Output 3 on the receiver Endpoint Controller (also note that the Safe Remote Control Pro affects the connected machine only, whereas the global E-Stop shuts off Output 3 on all devices).
- When a Safe Remote Control Pro is connected to a receiver Endpoint Controller in autonomous (unsupervised) mode, only pressing the global E-Stop[1] on the Endpoint Controller will turn off Output 3 on the receiver Endpoint Controllers. The Safe Remote Control Pro E-Stop is ignored and will not turn off Output 3.

The following table shows details about an SRC Pro and EPC Hybrid configuration:

TABLE 2-3. *SRC Pro and EPC Hybrid configuration*

Sender	Inputs	Receivers	Communication
One SRC Pro and one EPC	Two safety rated inputs: one on the SRC Pro and one on the EPC	Up to 30 devices in a configuration; all 30 in communication with the controlling EPC, but only one connection at a time to the SRC Pro	SRC Pro: Bluetooth or ISM EPC: Ethernet or Wi-Fi

Building a Hybrid Configuration

An SRC Pro and EPC Hybrid configuration has two senders, a Safe Remote Control Pro and an Endpoint Controller, and up to 30 Endpoint Controller receivers. To build this configuration, you first build an SRC Pro to EPC configuration (which we call the base configuration) and then add an Endpoint Controller sender to it to create a Hybrid configuration.

BEFORE YOU BEGIN

This section assumes that you have already built and identified a configuration to use as the base for the hybrid configuration. If not, follow the steps in "Building an SRC Pro to EPC Configuration" on page 2-9 to build a configuration with a Safe Remote Control Pro and up to 30 Endpoint Controller receivers to use as the base, then complete the following procedure.

TO BUILD A HYBRID CONFIGURATION:

(Requires ConfigManager or Admin role.)

1. Navigate to the FORT Manager Web App (https://app.fortrobotics.com) and enter your credentials when prompted.
2. Click the Config Management tile at the top of the dashboard or Config Manager in the left navigation pane.
3. Click the Global E-Stop [2]tab and click Add new.
   FORT Manager opens a wizard to step you through the process of adding an E-Stop device to this configuration.

1. Although we refer to this as a global E-Stop on the EPC, you could use a solid state device instead of an E-Stop switch. The effect is the same: triggering the solid state device turns off Output 3 on the connected device.

4. (Step 1/5) Select the basic configuration to use from the list and click Continue.
   If you haven't built a base configuration, follow the steps in "Building an SRC Pro to EPC Configuration" on page 2-9 to do so.

> ⚠ **IMPORTANT:** Be certain that everything is correct with the basic configuration that you selected. Once you complete this wizard, you can't make any changes to the new Global E-Stop configuration, nor to the basic configuration without deleting the Global E-Stop configuration.
> At any point in the wizard, you can click **Go Back** to change a selection that you made.

5. (Step 2/5) Select an EPC from the list to use as the sender and click Continue.
6. (Step 3/5) Select the type of device to attach to Input 3:

   Note that Input 1 and Input 2 are not available in this configuration. Both the EPC sender and the SRC Pro use Input 3.

   - Input3 Select a value from the drop-down menu for Input 3 to identify the type of device that you intend to wire to the EPC inputs:
     - **E-Stop Type Device** An E-Stop type switch.
     - **Solid State Safety Device** A device such as a light curtain, PLC, etc.
7. Click **Continue**.
8. (Step 4/5) Adjust the configuration wide settings.
   a. From the drop-down underneath the configuration, select the communication protocol for the network: Ethernet (default) or WiFi.
   - For **Ethernet**, set:
     - **Netmask** Defaults to 255.255.255.0.
     - **Gateway** The gateway IP address, such as 192.168.1.1.
     - **Name Server** A name server IP address, such as 192.168.1.2.

       You can identify multiple name servers. Click **Add** after specifying each one. The order in which you add name servers is the order in which the EPC looks for them. If it can't reach the first server it goes to the second server in the list, and so on until it reaches one.
   - For **Wi-Fi,** set:
     - **SSID** The network ID.
     - **Password** The network password.
     - **Netmask** Defaults to 255.255.255.0.
     - **Gateway** The gateway IP address, such as 192.168.1.1.

       Be certain to set this parameter to the router address to avoid slow connections and possible timeouts during operation.
     - **Name Server** A name server IP address, such as 192.168.1.2.
       You can identify multiple name servers. Click **Add** after specifying each one. The order in which you add name servers is the order in which the EPC looks for them. If it can't reach the first server it goes to the second server in the list, and so on until it reaches one.

   b. Click **Continue**.

2. A hybrid configuration was previously called a Global E-Stop configuration and the FORT Manager interface reflects this name. Subsequent versions of FORT Manager will not use this terminology and in this guide, we refer to a hybrid configuration or a configuration with both SRC Pro and EPC senders.

9. (Step 5/5) Enter a unique IP address for each EPC in the configuration, including the sender.

⚠ **NOTE:** Be certain that everything is correct with the configuration before completing the wizard. At this time, it is not possible to make any changes once you click **Finish Configuration** other than delete the Global E-Stop configuration and redo it.
However, you can click **Go Back** to return to a previous page and adjust settings or make different selections.

10. Click **Finish Configuration**.

The new configuration appears under the Global E-Stop tab with Global E-Stop appended to the basic configuration name. In the Configuration Management tab, the basic configuration appears with Estop Added after the name.

NEXT STEPS

Go to the next section, "Loading a Configuration onto Your Devices", for instructions on how to load the configuration you just created onto your devices.

Loading a Configuration onto Your Devices

After you build a configuration, you need to load it onto your devices by using the FORT CLI (Command Line Interface) Tool in a Linux environment. We provide separate instructions for:

- Loading a configuration onto an EPC (next section).
- Loading a configuration onto an SRC Pro (section after next).

You configure Endpoint Controllers via Ethernet and a Safe Remote Control Pro via a USB connector.

Loading a Configuration onto an EPC

This section shows how to load a configuration onto an Endpoint Controller. You configure Endpoint Controllers via Ethernet.

REQUIRED ITEMS:

- A configuration that you built in FORT Manager.
- Linux computer running Ubuntu 20.04 with Ethernet networking capability
  Use M12-RJ45 cable for connecting directly to an EPC (e.g., ASI-M12-RJ45-11101).
- Latest FORT CLI Configuration Tool (`fort_cli_cfg-<version>.tar.gz`).
  If you don't already have it, you can download it from FORT Manager. See "FORT CLI Configuration Tool" on page D-1 for more information, including installation instructions for the tool.
- The EPC and any connected machines are in a safe state to be configured.

TO LOAD A CONFIGURATION TO AN EPC:

1. Boot up your EPC by applying power to `PVin_IN` (pins 14 & 15).

2. Allow up to a minute for the EPC to boot up. You can continuously ping the J2 port to see when the device has booted up.

   Connect your computer over Ethernet to port J2 on the EPC. Using the M12-RJ45 cable.
3. In a Linux environment, open a Terminal window and navigate to the folder containing the FORT CLI configuration tool.
4. Run the following command to load the configuration for the EPC:

   ```
   $ fort_cli_cfg -w -e 192.168.3.10
   ```

   Where:

   `-w (--web)`
   Specifies to upload a single configuration from FORT Manager.

   `-e (--epc) 192.168.3.10`
   Specifies an EPC device and the (default) IP address for the J2 connector. Your address could be different.

   The CLI tool returns a code. The browser opens a window that asks you to confirm that the displayed code matches that in the CLI tool.
5. Press Enter to confirm that the codes match.
6. If you aren't already authenticated, enter your FORT Manager username and password to authenticate to FORT Manager.
7. Return to the CLI tool where you are prompted to enter the device serial number:
8. Type the serial number (found on the EPC device name place and also in FORT Manager on the Devices page) and press **Enter**.
9. Press **Enter** to load the configuration to the device.
   The tool finishes with the EPC by writing all the relevant configuration parameters.
10. Reboot the EPC.

Repeat this procedure for each Endpoint Controller in your configuration.

NEXT STEPS

If your configuration has a Safe Remote Control Pro as the sender, complete the steps in the following procedure ("Loading a Configuration onto an SRC Pro") to load the configuration onto it.

If your configuration has an Endpoint Controller as the sender:

- For a Wi-Fi network, as soon as the EPCs are turned on and are in range, they automatically connect to the assigned network and the receivers all pair with the sender. The system is ready to use.
- For an Ethernet network, use an Ethernet cable to connect the J3 port on each Endpoint Controller to the network. When all the EPCs are connected and turned on, the receivers pair with the sender and the system is ready to use.

Loading a Configuration onto an SRC Pro

REQUIRED ITEMS:

- A configuration that you built in FORT Manager.
- Linux computer running Ubuntu 20.04
- Latest FORT CLI Configuration Tool (`fort_cli_cfg-<version>.tar.gz`).

If you don't already have it, you can download it from FORT Manager. See "FORT CLI Configuration Tool" on page D-1 for more information, including installation instructions for the tool).

- The SRC Pro is in a safe state to be configured.

TO LOAD A CONFIGURATION TO AN SRC PRO:

1. Boot up your SRC Pro.
2. Connect the computer through USB to the SRC Pro.
3. In a Linux environment, open a Terminal window and navigate to the folder containing the FORT CLI configuration tool.
4. Run a command similar to the following to launch the configuration tool for the SRC Pro (your /dev/tty port could be different):

   ```
   $ fort_cli_cfg -w -n /dev/ttyACM0
   ```

   Note that you need execute permission to /dev/ttyACM0, or whichever virtual port you are using for the SRC Pro. If you receive a permission error, run the following command to add yourself to the dialout group:

   ```
   sudo -a -G dialout $USER
   ```

5. After running the command, log out of the Linux section, then log back in and rerun the configuration tool.

   The parameters you specify for the CLI tool are as follows:

   `-w` (`--web`)
   : Specifies to upload a single configuration from FORT Manager.

   `-n` (`--nxp`) `/dev/ttyACM0`
   : Specifies an SRC Pro device and identifies the USB port in use; your port could be different.

   The CLI tool returns a code. The browser opens a window that asks you to confirm that the displayed code matches that in the CLI tool.
6. Press **Enter** to confirm that the codes match.
7. If you aren't already authenticated, enter your FORT Manager username and password to authenticate to FORT Manager.
8. Return to the CLI tool where you are prompted to enter the device serial number:

   ```
   Enter device serial number:
   ```

9. Type the serial number (found on the SRC Pro device and also in FORT Manager on the Devices page) and press **Enter**.
10. Press **Enter** to load the configuration to the device.

    The tool finishes with the SRC Pro by writing all the relevant configuration parameters.
11. Reboot the SRC Pro.

Once you complete the steps in "Loading a Configuration onto an EPC" on page 2-15 to load the configuration onto the Endpoint Controllers, you can connect the Safe Remote Control Pro to one of the Endpoint Controllers in the configuration ("Connecting the SRC Pro to an EPC" on page 4-3).

Connecting EPCs to a network

In a configuration with an Endpoint Controller as the sender, the devices communicate over an Ethernet or Wi-Fi network. In FORT Manager, you specify which one to use and identify the network attributes (gateway, netmask, name server, etc.) as well as the IP address for each device.

When you load a configuration onto devices, as described in the previous section, each EPC receives the IP address you assigned to it in FORT Manager.

For a Wi-Fi network, as soon as the EPCs are turned on and are in range, they automatically connect to the assigned network and the receivers all pair with the sender. The system is ready to use.

For an Ethernet network, use an Ethernet cable to connect the J3 port on each Endpoint Controller to the network. When all the EPCs are connected and turned on, the receivers all pair with the sender and the system is ready to use.

CHAPTER 3

Installation — Wire and Mount Endpoint Controller

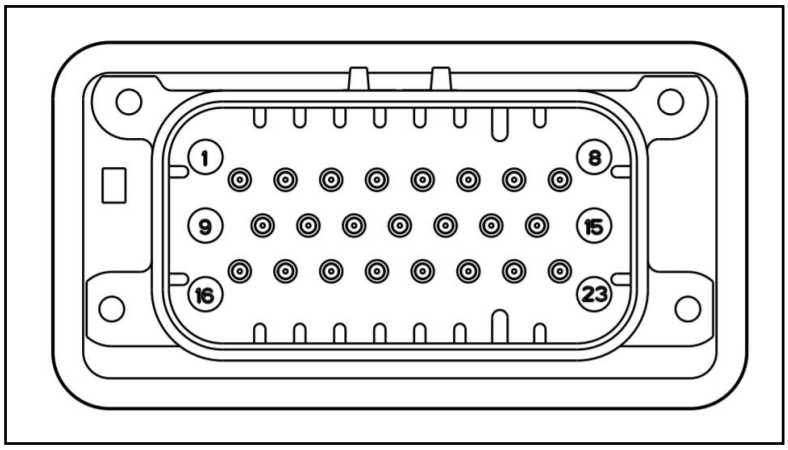
This chapter explains how to wire and mount an Endpoint Controller device to your equipment.

I/O Connector Pinout and Cable

The following figure shows a diagram of the EPC's 23 pin I/O connector (the J1 connector on the Endpoint Controller — See "EPC Mechanical Drawing" on page A-2).

The table after the figure describes each of the connector signals. Refer to the diagram and table when wiring devices to an Endpoint Controller sender ("Wiring Inputs on EPC Sender" on page 3-5) or receiver ("Wiring Outputs on EPC Receivers" on page 3-8).

FIGURE 3-1. *EPC I/O Connector Pinout (TE 1-776228-1*



⚠ **NOTE:** The suggested mating connector to this port is a TE 770680-1 and the cable is the FORT #100-0256 Integration Cable.

TABLE 3-1. *Connector pinout and signal descriptions*

Pin #[a]	Name	Description	Wire Color FORT integration[b]
1	IN5_CONN	Channel 1, Input 3	White
2	IN4_CONN	Channel 1, Input 2	White
3	IN3_CONN	Channel 1, Input 1	White
4	IN2_CONN	Channel 0, Input 3	White
5	IN1_CONN	Channel 0, Input 2	White
6	IN0_CONN	Channel 0, Input 1	White
7[c]	PVin_RTN	Voltage Negative Polarity	White
8[c]	PVin_RTN	Voltage Negative Polarity	White
9	CH_GND	Chassis to Ground Connection; Connect to power supply common if an earth ground is not available (such as in a moving vehicle). See "Grounding" after table for details.	White
10	Reserved	Do not connect	
11	CAN1_L	CAN Low, Twisted with 12	Green
12	CAN1_H	CAN Hi, Twisted with 11	Yellow
13	CAN1_SHIELD	CAN Bus Shielding; See "Shielding" after the table for wiring details.	
14[d]	PVin_IN	Voltage Positive Polarity	White
15	PVin_IN	Voltage Positive Polarity	White
16	OUT5_CONN	Channel 1, Output 3	White
17	OUT4_CONN	Channel 1, Output 2	White
18	OUT3_CONN	Channel 1, Output 1	White
19	Reserved	Do not connect	
20	Reserved	Do not connect	
21	OUT2_CONN	Channel 0, Output 3	White
22	OUT1_CONN	Channel 0, Output 2	White
23	OUT0_CONN	Channel 0, Output 1	White

a. Connector pinouts and signal descriptions are subject to change before release.
b. Wire colors apply to the FORT Part #100-0256 integration cable.
c. Connect Pins 7 & 8 together at the same place.
d. Connect Pins 14 & 15 together at the same power source.

⚠ **IMPORTANT:** We highly recommend ordering and using the FORT supplied integration cable (#100-0256). Consult with customer support before using a custom cable.

Connecting Pins Together

Pins 7 and 8 (PVin_RTN) are both required, and you should connect them together at the same place.

Pins 14 & 15 (PVin_IN) are both required, and you should connect them together at the same power source.

Shielding

If you are using a shield, we recommend crimping a short pigtail to the shield end at each connector and then bringing it through a separate connector pin to a ground pin located as close to the connector as possible. You should ground the network to a single point at the source location. This prevents parasitic currents from flowing in the shield between ground connections. If you shield individual signal pairs, use the same terminating technique as for the overall shield.

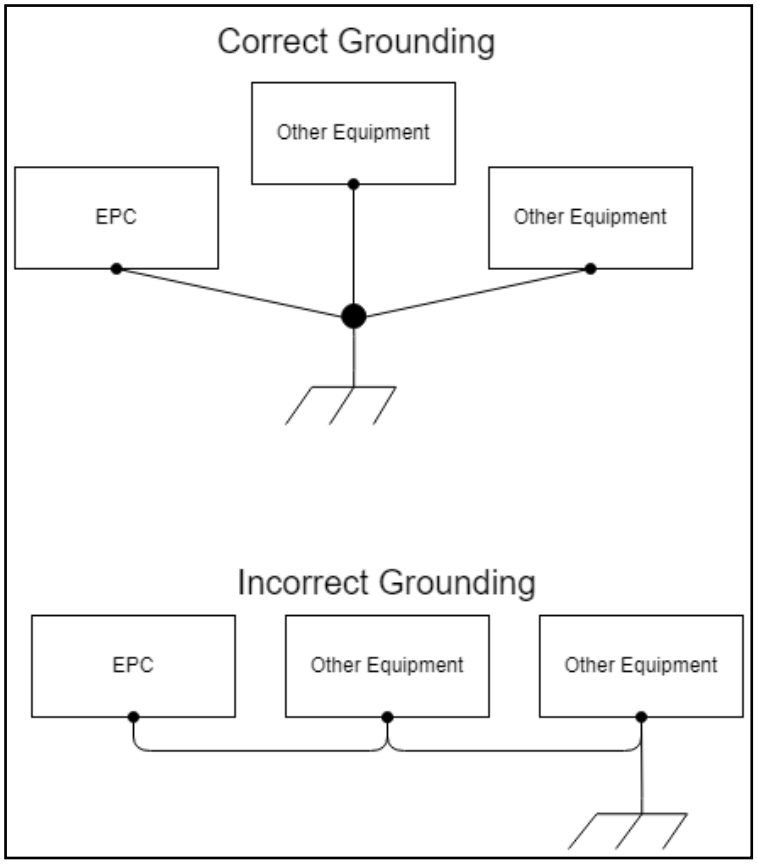
Grounding

⚠ **NOTE:** Connect Pin 9 CH_GND to power supply common if an earth ground is not available (such as in a moving vehicle).

Be certain that there is only one path for return current between the host and receiving nodes (as discussed in the previous section, Shielding). Otherwise, if a network is grounded in more than one location, parasitic current will flow. By grounding a network only at the source, you avoid potentially hazardous ground loops. We recommend using digital isolators such as the ISO721 (SLLS629) if you must connect the grounds of different sources. Be certain that unused pins in connectors as well as unused wires in cables are single point grounded at the connector. Ground unused wires at alternate ends to nearby ground pins.

The following diagram shows examples of both correct and incorrect grounding:

FIGURE 3-2. *Examples of Correct and Incorrect Grounding*



Engine Cranking

If you attach the EPC to an ignition circuit, be aware that engine cranking can drop the voltage below 8 V (on a 12 V system) causing the EPC to turn off the outputs and triggering a safe state. In addition, cranking may drop the voltage low enough that the EPC temporarily stops functioning and resets.

You should assess whether this behavior is a safety issue for your application. It may not be. For example, if the EPC doesn't power up until after the equipment is running, cranking the engine shouldn't affect the EPC.

On the other hand, you can avoid this problem altogether by making certain that the EPC is not part of an ignition circuit.

Relationship of Inputs and Outputs

In an EPC to EPC Configuration there is a one-to-one correspondence between each input of a sender Endpoint Controller and each output of all receiver Endpoint Controllers in the configuration. That is, Input 1 of the sender corresponds to Output 1 of a receiver, and the same for Output 2. For example, if you connect Input 1 of a sender Endpoint Controller to an E-Stop switch, you must connect Output 1 of a receiver Endpoint Controller to two relays in series that connect to the EUC. When the E-Stop button attached to Input 1 on the sender Endpoint Controller is pushed, the relays attached to Output 1 on the receiver Endpoint Controller open, breaking the connection to the EUC (for example, stopping it if the circuit is connected to the power supply).

Conversely, when Input 1 on the sender Endpoint Controller is asserted (ON state), the relays on Output 1 on the receiver Endpoint Controller should energize, enabling the EUC.

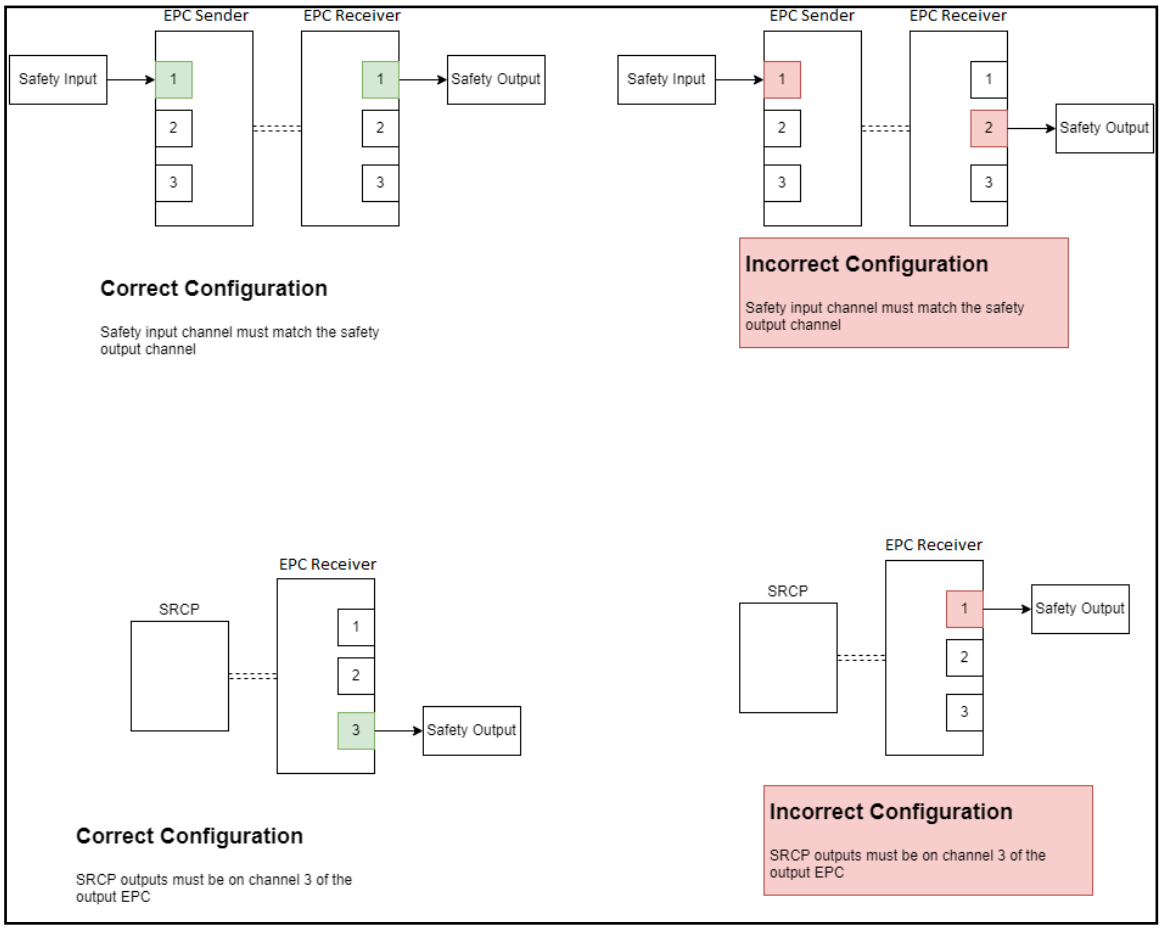
⚠ **IMPORTANT:** It is up to you (the user) to properly design your application to accommodate the behavior of the EPC's inputs and outputs from changes in state.

Note that Output 3 is not used in an EPC to EPC configuration (it is reserved for a configuration with an SRCP) and therefore in this configuration you should not connect safety input devices to Input 3 of the sender Endpoint Controller nor relays to Output 3 of the receiver Endpoint Controller(s).

In an SRC Pro to EPC configuration the built-in E-Stop button is pre-defined to control Output 3 so you must connect safety relays on the receiver Endpoint Controller(s) to Output 3.

The following diagram illustrates these relationships.

FIGURE 3-3. *Examples of Correct and Incorrect Wiring Diagrams*



Wiring Inputs on EPC Sender

You can connect either one of two types of devices to any input channel on an Endpoint Controller:

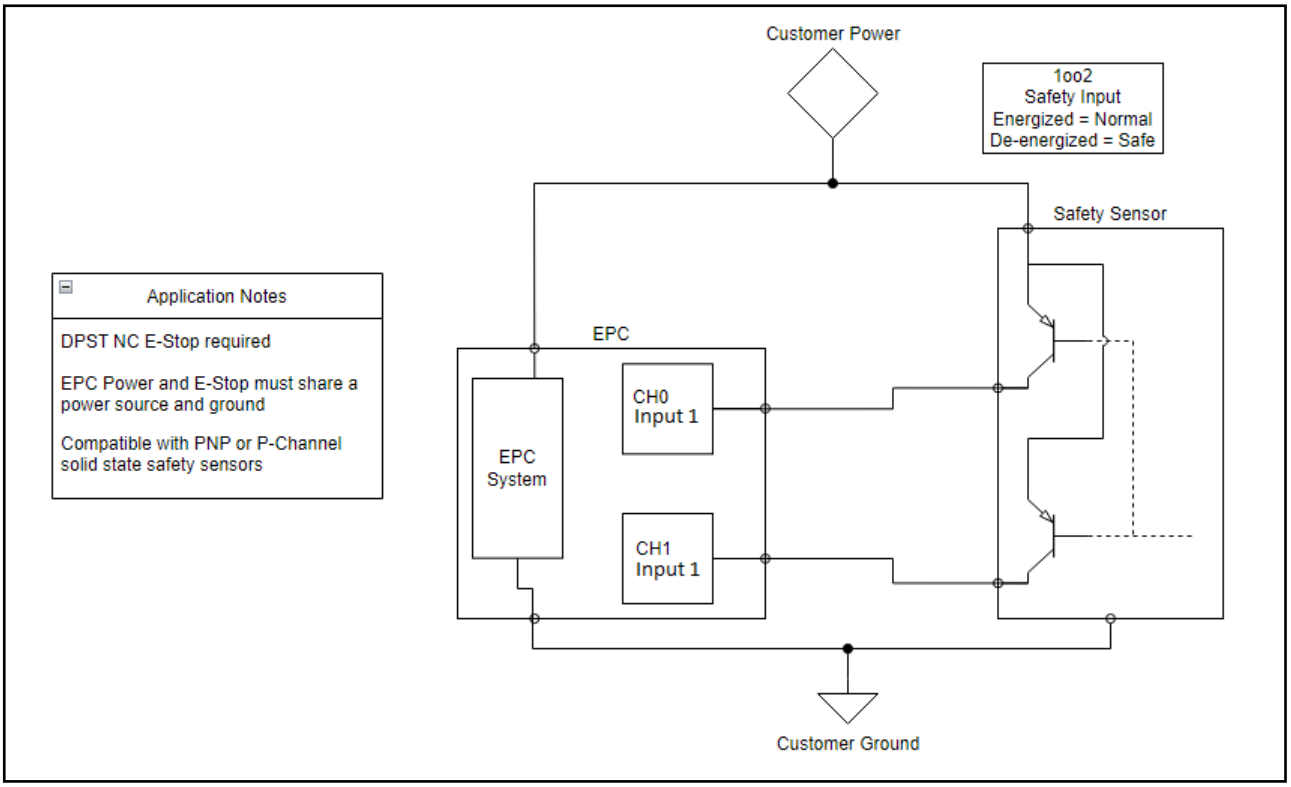
- An E-Stop type switch, which is a mechanical switch (internally contains two redundant switches). Switches are closed unless someone pushes the E-Stop button which opens the internal switches.
- A solid state safety device.[1]

See “I/O Connector Pinout and Cable” on page 3-1 for details of the EPC I/O connector and cable to use for connecting input devices to an Endpoint Controller sender.

The following figure shows a diagram of a solid state device, such as a light curtain, wired to one of the dual channel inputs on an Endpoint Controller sender.

1. You can use a PLC with no pulse testing on the PLC outputs, which provides a category 3 circuit (meeting SIL 2 and PLd standards). Getting a SIL 3 rating ideally requires a SIL 3 or PLe rated input device. Note that you can configure the safety PLC with pulse testing enabled on the outputs tied to the EPC, which is essentially the same as using an OSSD device.

FIGURE 3-4. *Solid State Device Wired to EPC*

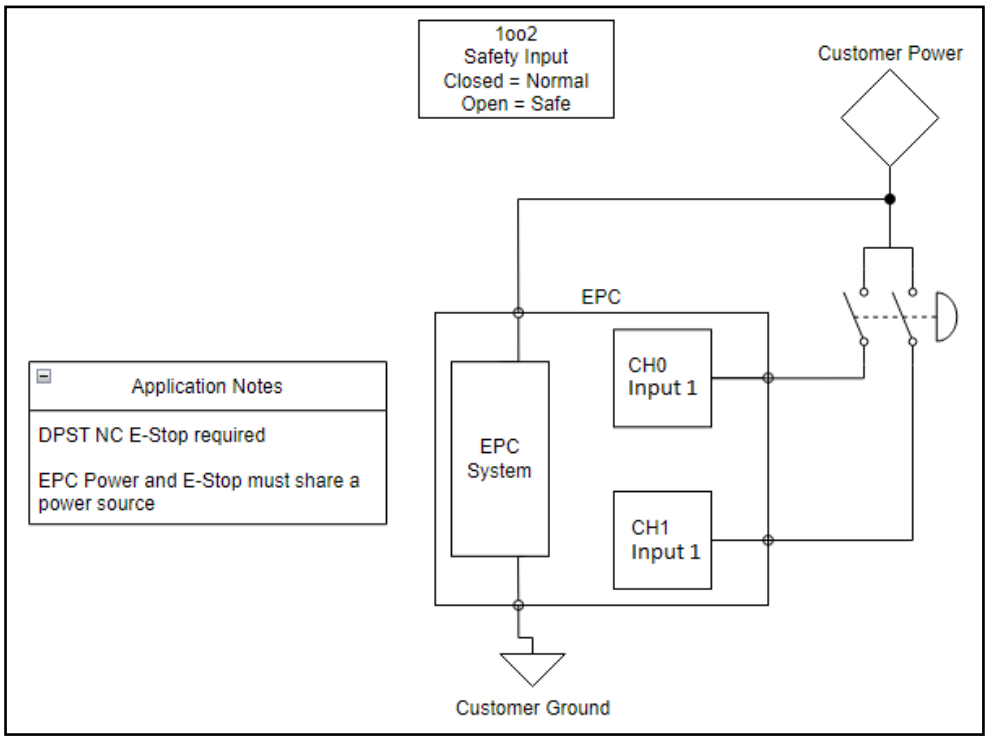


Note the following about this setup:

- A DPST NC (double-pole single-throw, normally closed) safety sensor is required so that both switches activate at the same time.
- The Endpoint Controller power and the safety sensor must share a power source and ground.
- You can use a PNP or P-Channel solid state safety sensor.

The following figure shows a diagram of an E-Stop switch wired to one of the dual channel inputs on an Endpoint Controller sender.

FIGURE 3-5. *E-Stop Switch Wired to EPC*



⚠ **NOTE:** Input 3 is reserved for use in a configuration with an SRC Pro as the sender.

Note the following about this setup:

- A DPST NC (double-pole single-throw, normally closed) E-Stop is required so that both switches activate at the same time.
- The Endpoint Controller power and E-Stop must share a power source.

The following table provides guidelines for the types of devices that you can use.

TABLE 3-2. *Requirements for Devices Connected to EPC Inputs*

Device	Requirement
Emergency stop switches	Use approved devices with direct opening mechanisms that comply with IEC/EN 60947-5-1.
Door interlocking switches, limit switches	Use approved devices with direct opening mechanisms that comply with IEC/EN 60947-5-1 and capable of switching micro loads of 24V DC, 3 mA.
Safety sensors	Use approved devices that comply with the relevant product standards, regulations, and rules in the country in which they are used.
Relays with forcibly- guided contacts, contactors	Use approved devices with forcibly guided contacts that comply with EN 50205. For feedback purposes, use devices with contacts capable of switching micro loads of 24V DC, 3 mA.
Other devices	Evaluate whether devices to use are appropriate to satisfy the requirements of safety category levels.

Keep the following points in mind when wiring inputs on an Endpoint Controller:

- You must use redundant connections. Each input has two channels, and you must wire the device to both channels.
- Input 1 and Input 2 are independent of each other. Although you don't have to use both inputs, you can do so. For example, you can wire an E-Stop to one input and a light curtain or some other SSD to the other.
- You configure the inputs in FORT Manager when you build a configuration. Be certain that the actual wiring you do matches the values you specify in FORT Manager (*E-Stop Type Device*, *Solid State Device*, *Not Used*), otherwise the system will not perform properly.

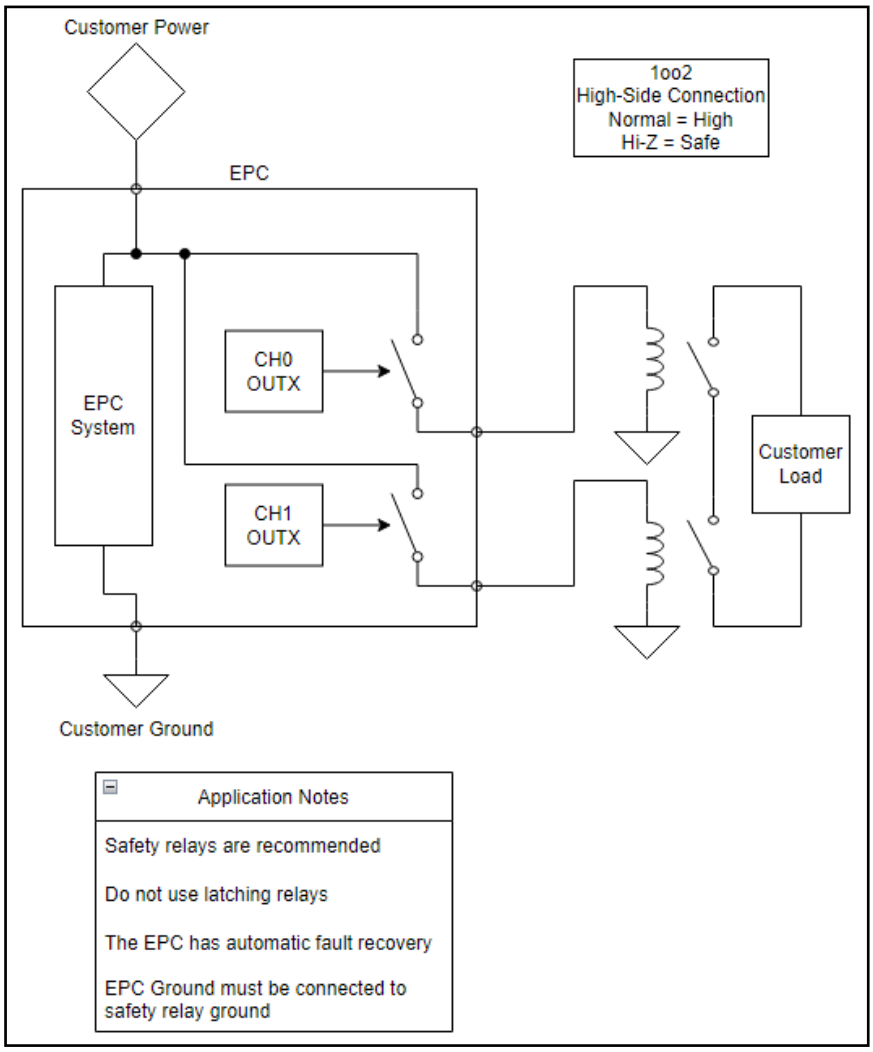
Wiring Outputs on EPC Receivers

For each Endpoint Controller output that you want to use, you must connect both channels to two relays that are connected in series, or to a dual channel safety relay. The circuit that is defined by these relays controls connection of a solenoid to the equipment under control. If safety is not requested, the Endpoint Controller keeps the output on to keep the relays closed. On the other hand, if safety is requested, the Endpoint Controller turns off the outputs, which opens the relays and breaks connection of the circuit to the EUC. In this case, if the EUC is using the circuit for power, when the contactors open, the machine shuts off.

⚠ CAUTION:	Each output on the EPC is designed with short circuit protection circuitry inside the EPC device. However, drawing more than 750 mA must be avoided since it won't activate short circuit protection and could potentially damage the device. To satisfy applicable wiring codes and conditions, you are responsible for protection of field devices and wiring through appropriate fusing of the circuitry.

The following figure shows an example of the two channels (Ch0 and Ch1) of one Endpoint Controller (EPC) output connected to two relays in series to control the power supply of the EUC:

FIGURE 3-6. *Output Diagram*



Note the following about this setup:

- You must connect the EPC ground to the safety relay ground.
- The Endpoint Controller has automatic fault recovery.
- We recommend using one of the relays that we have tested (from the following table) but if you don't use one of these, be certain to use a safety relay.
- Do not use latching relays.

> ⚠ **WARNING:** Do not connect latching relays to the EPC outputs because they prevent the emergency stop from working.

See "I/O Connector Pinout and Cable" on page 3-1 for details of the EPC I/O connector and cable to use for connecting an Endpoint Controller receiver to the EUC.

TABLE 3-3. *Recommended and Tested Relays*

Manufacturer	Model	Supply Voltage
Allen-Bradley	MSR127TP	24V
EATON	ESR5-NV3-30	24V
PILZ	751104	24V
IDEM	SCR-3-1P-i	24V
OMRON	G7SA-3A1B	24V
PANASONIC	SFS3-L-DC12V-D	12V

See “Recommended Relays” on page E-1 for wiring diagrams for each of these relays.

Selecting Automatic or Manual Reset for Relays

A crucial point to consider when attaching relays to the Endpoint Controller outputs is how you want the equipment under control (EUC) to behave after a fault or safety demand is cleared. Do you want it to restart automatically, or do you require manual intervention?

The Endpoint Controller behavior is as follows: Immediately after a power up or a reset (for example, to clear an internal fault), the Endpoint Controller enters start-up mode in which all outputs are disabled (not sourcing or sinking) until the system successfully completes its startup tests, at which point the system enters run mode. If a startup test fails, the Endpoint Controller will reset itself and try again to see if the fault has cleared.

While in run mode, the Endpoint Controller output(s) are turned on if there is no request for safety (e.g., E-Stop button has not been pressed) and there are no internal faults or a timeout. On the other hand, while in run mode, the Endpoint Controller output(s) are turned off if there is a request for safety (e.g., E-Stop switch on the Sender device is pressed), because of internal faults, or if the Endpoint Controller encounters a timeout due to not receiving safety messages from the sender.

In terms of your EUC, if you use a relay configured for automatic reset, then the EUC resumes automatically after a fault is cleared or the E-Stop button is released. On the other hand, if you configure the relays for manual reset, the EUC won’t resume operation until someone manually resets the relays.

⚠ WARNING: If your machinery is connected to relays that reset automatically, be certain that your operators are aware that the machinery can restart suddenly without warning once a fault or E-Stop is cleared on the EPC.

Consult the documentation that comes with your relay devices for information about how to wire relays and configure them for manual or automatic reset.

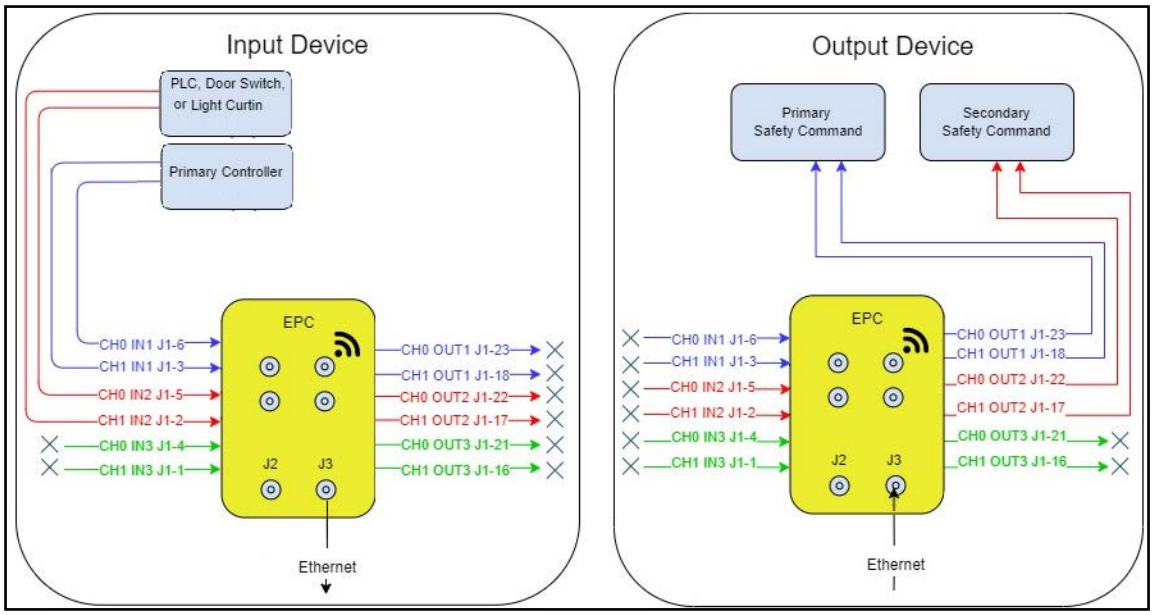
In addition, be aware of the following warning regarding relays:

⚠ WARNING: Do not connect latching relays to the EPC outputs because they prevent the emergency stop from working.

Sample EPC-EPC Paired Configuration

The following figure demonstrates the wiring and communication between two Endpoint Controller devices, one configured as a sender and the other as a receiver. See "Building an EPC to EPC Configuration" on page 2-2 for information on setting up a configuration with an Endpoint Controller as the sender (input controller).

FIGURE 3-7. *Sample EPC Paired Configuration with two Inputs*



Mounting an EPC

An Endpoint Controller has four mounting holes to attach it to the equipment under control (EUC) as shown in Figure A-1, "EPC-1001 Mechanical Drawing," on page 2. We recommend using ¼-20 or M6 machine screws for mounting.

⚠ CAUTION: If you are locating the EPC outside or attaching it to equipment that is operating outside or can be exposed to any amount of water, you must mount the EPC vertically. Mounting the EPC horizontally allows water to pool and block airflow through a membrane, potentially causing the EPC to malfunction.

In addition, avoid placing the EPC in an area or on a machine with extended exposure to direct sunlight.

Selecting and Placing an Antenna

FORT offers a variety of antenna options for our senders and receivers. The antennas for the Safe Remote Control Pro are built into the device so you must select one prior to purchase. The antennas for senders and receivers are accessories and you can purchase them at any time.

⚠ **IMPORTANT:** You cannot use your own antenna; you must use one of the antennas available from FORT.

Choose an antenna based on the wireless communication type you plan to use as shown in the following table (Usage row):

TABLE 3-4. *Antennas*

	275-0002	275-0080	275-0096
			
FORT Device	EPC 1002, SRC Pro 1002	EPC 1001, SRC Pro 1001	EPC
Antenna Type	Whip, Straight	Whip, Straight	Dome
Usage	ISM EU Bands	ISM NA Bands	Wi-Fi, BLE
Frequency Range	750–950MHz	865-965MHz	2.4 - 2.5GHz (5.1 to 5.9GHz pending tests)
Peak Gain	1.1 dBi	1.8 dBi	4.5dBi @ 5.1-5.9Ghz band and 7.2dBi in the 2.4 to 2.5Ghz band
Ideal Placement	Elevated, pointed straight up, clear LOS	Elevated, pointed straight up, clear LOS	Elevated, pointed straight up, clear LOS
Termination	RP-SMA Male	RP-SMA Male	N Type Female

Use grommets when routing the antenna cable through enclosures.

⚠ **CAUTION:** If your device has an ISM radio, you must attach an antenna. Operating an ISM radio without an antenna installed could damage the unit.

Ideally, you should place the antenna such that is has a clear line of sight (LOS), it's not too high or too low, no metal is between it and the sender, and it's pointed straight up (whip antenna), or pointed towards other devices (puck antenna)

The following table shows rules for using approved antennas in the USA, Canada, and Europe:

TABLE 3-5. *Rules for using Approved Antennas*

Device	FCC ID (US)	IC (Canada)	CE (Europe)
EPC	CFR title 47, part 15, subpart C, section 15.247	RSS-247, Issue 2 RSS-Gen Issue 5	EN 301 489-1 & -3 EN 300 220 RED 2014/53/EU
SRC Pro	CFR title 47, part 15, subpart C, section 15.247	RSS-247, Issue 2 RSS-Gen Issue 5	EN 301 489-1 & -3 EN 300 220 RED 2014/53/EU

CHAPTER 4 *Understanding and Using an SRC Pro*

This chapter describes the features of the Safe Remote Control Pro in more detail, explains how to connect a Safe Remote Control Pro to an Endpoint Controller, and explains the modes in which it connects to an Endpoint Controller.

SRC Pro Features

The following figure highlights the Safe Remote Control Pro Features:

FIGURE 4-1. *SRC Pro Features*

JOYSTICKS

The Safe Remote Control Pro is a 6-axis controller with three on each hand. The X axis and Y axis are mapped to the thumb stick on top of the Safe Remote Control Pro, while the Z axis is mapped to the finger stick underneath.

BUTTONS

The buttons on the Safe Remote Control Pro are configured in a diamond; those on the left hand side are: Up, Down, Left, and Right. Those on the right are numbered 1 through 4.

POWER BUTTON

When the Safe Remote Control Pro is off, push the power button to turn it on. The LCD screen lights up and the device vibrates when it is ready to use.

When you push the power button to turn it off, the Safe Remote Control Pro stops sending valid safety messages to the connected Endpoint Controller, which causes it to go to safe state after the timeout period is exceeded.

PAUSE BUTTON

Press the Pause button to enter Pause Mode. See "Pause Mode" on page 4-2 for details.

Modes

This section explains the different modes for the Safe Remote Control Pro.

Pause Mode

In Pause Mode, the Safe Remote Control Pro continues to send valid safety messages to the connected Endpoint Controller (if any) keeping the relays closed and the Endpoint Controller operating normally (not requesting safety). The Safe Remote Control Pro also continues to output the joystick message but with all values set to 0 to guarantee that no motion will occur.

The Safe Remote Control Pro enters pause node for any of the following reasons:

- The Safe Remote Control Pro user presses the pause button.
- The remote detects that it has been dropped (is free falling).
- The remote detects an orientation fault (such as the remote has moved to the user's side or has been turned on its face).
- The remote detects lack of motion for the timeout period (user configurable in one minute increments from 2 - 10).

Menu Mode

Menu Mode allows you to change system settings on the Safe Remote Control Pro.

In Menu Mode, the Safe Remote Control Pro continues to send valid safety messages to any connected Endpoint Controller keeping the relays closed and the EPC operating normally (not requesting safety). The Safe Remote Control Pro also continues to output the joystick message but with all values set to 0 to guarantee that no motion will occur.

Connecting the SRC Pro to an EPC

Once you have loaded the configuration onto the Safe Remote Control Pro and Endpoint Controllers, you can connect the SRC Pro to any EPC in the configuration — this feature is called: machine select.

BEFORE YOU BEGIN

Make certain that

- Both devices are powered up and in range of each other.
- You understand how machine-select works and the difference between supervised and autonomous modes ("Machine Select" on page 2-6). Briefly, supervised means that the SRC Pro is sending joystick movements and safety data to the machine, while autonomous means that the machine is operating independently, with its own safety mechanism, and with no communication with the SRC Pro. When you first connect to an EPC, the mode is always supervised. You can change the mode at any time after connecting ("Changing the Mode" on page 4-4).

TO CONNECT AN SRC PRO TO AN EPC:

1. Power up both devices and keep them within range of each other.
2. As a safety precaution, press the E-Stop button.

   (When you finish connecting to the new device, the E-Stop signal guarantees that the equipment won't start operating unexpectedly.)

   The SRC Pro displays a warning screen indicating that the E-Stop button has been pressed.
3. Press the Menu button to exit the E-Stop activated screen.
4. On the SRC Pro LCD screen, use the arrow keys to navigate to the Machine tab.

   The screen shows a list of devices that you added to the configuration in FORT Manager.

5. Use the arrow keys to highlight a machine and press 1 to select it.

The screen displays a confirmation code.

6. Press the number buttons to enter the code to confirm the selection.

   If you change your mind, you can press the menu button to quit and return to the selection menu. Note that pressing an incorrect number sequence also returns you to the selection menu.

7. Wait for the connection to be established and when confirmed, press **1** to close the window.

   At this point, the SRC Pro has transitioned to supervised mode.

   If the connection attempt fails, you can repeat the connection process.

8. When it is safe to do so, release the E-Stop button.

At this point, you can use the Safe Remote Control Pro to control the movements of the EUC and if necessary, press the E-Stop button to send a safety signal to it.

Connecting an SRC Pro to a different EPC

You can change the device that a Safe Remote Control Pro is connected to at any time. To do so, make sure both devices are powered up and in range of each other, then follow the connection procedure in the previous section. Note the following about the previously connected device:

- If the previous machine was in autonomous mode, the equipment under control will remain powered up and running.
- If the previous machine was in supervised mode, it no longer receives a safety message from the SRC Pro and will go to safe state once the timeout value is reached.

Changing the Mode

Whenever you connect a Safe Remote Control Pro to an Endpoint Controller, the SRC Pro sets the mode of the EPC to supervised. At any time after connecting to an EPC in supervised mode you can change its mode to autonomous if the machine has autonomous capability and has been wired appropriately as described in Figure 2-4, “Input 3 Asserted on EPC Receiver,” on page 9.

TO CHANGE THE MODE:

Make certain that:

- Both devices are powered up and in range of each other.
- The SRC Pro is connected to the EPC.

> ⚠ **CAUTION:** If you are changing the mode from supervised to autonomous, be certain that the EPC is connected to a machine with autonomous capability and that it has been wired appropriately for autonomous mode as shown in Figure 2-4, "Input 3 Asserted on EPC Receiver," on page 9. Otherwise, if the machine does not have autonomous capability, and has not been wired appropriately, the EPC will transition to safe state when you change the mode to autonomous.

1. On the SRC Pro LCD screen, navigate to the Machine tab.
2. Use the arrow keys to highlight the machine to which the SRC Pro is currently connected and press **1** to select it.

   The screen displays a confirmation code and a prompt for the mode to change to (`Autonomous` on the sample display).

3. Press the number buttons to enter the code to confirm the selection.

   If you change your mind, you can press the menu button to quit and return to the selection menu. Note that pressing an incorrect number sequence also returns you to the selection menu.
4. Wait for the connection to be established and when confirmed, press **1** to close the window.
5. After the mode change is successful, press the **Menu** button to close the prompt.

The screen displays the new mode. For example, if you began in supervised mode, the screen should show: AUTO.

Viewing the Connection Status

At any given time, an SRC Pro can only be connected to one machine in supervised mode (indicated by SUPR after the machine name on the LCD display) The SRC Pro can also set the mode of multiple machines to autonomous (indicated by AUTO after the machine name on the LCD display)

To see the mode of all machines in the configuration, press the Menu button, then navigate to the Machine tab of the SRC Pro LCD screen:

- AUTO autonomous mode
- SUPR supervised mode
- <*blank*> unknown (or no mode)

Turning the SRC Pro Off and Back On

When you turn an SRC Pro off, machines that were in autonomous mode will continue to operate in autonomous mode. If the SRC Pro was connected to a machine in supervised mode, that machine will experience a timeout and transition to safe state.

After you turn the SRC Pro back on, machines that were in autonomous mode will continue to operate in autonomous mode, but the display will show these machines as blank.

If the SRC Pro was connected to a machine in supervised mode, it will no longer have a connection unless you reestablish one. The display mode for that machine will be blank until you reconnect.

⚠ **NOTE:** An SRC Pro does not remember the displayed mode after it is turned off and then turned back on. Therefore, the displayed modes for all machines is blank after power cycling the SRC Pro.

Turning the EPC Off and Back On

When the EPC installed on a machine is turned off, the relays will open and put the machine in a safe state, but the displayed mode associated with the machine will remain as before.

When the EPC is turned back on, the relays will remain open and keep the machine in a safe state until you use the SRC Pro to connect to the EPC and change its mode to supervised or autonomous. The displayed mode on the SRC Pro for the machine will continue to be the same as it was before the EPC was power cycled.

⚠ NOTE: The displayed mode on the SRC Pro only indicates the mode that the user set the EPC to. It does not reflect the actual state of the EPC. For example: you set the mode of the EPC on Machine-1 to autonomous and then use the SRC Pro to connect to Machine-2. Later, Machine-1 moves out of range of the SRC Pro, or it is turned off, but since the SRC Pro doesn't have communication with that EPC, it continues to show the mode as AUTO.

CHAPTER 5 CAN Application Support

The EPC's CAN application supports sending and receiving message using the CANopen or the J1939 protocol.

This chapter provides the following information:

- "CANopen Implementation" describes transmitting joystick data using the CANopen protocol.
- "J1939 Implementation" describes transmitting joystick data using the J1939 protocol.
- "SRC Pro Control Messages" describes control messages for both protocols.
- "Status Messages" describes status messages for both protocols.
- "EPC Heartbeat Message" describes a message that has been deprecated in favor of the "EPC Output Status 1 Message". This section is included for anyone using a previous firmware version.

CANopen Implementation

This section shows how to send joystick using CANopen.

The SRC Pro-via-EPC CANopen integration provides a CiA 301 (CAN in Automation), 401 Part 1, and 401 Part 2 interoperable network slave.

⚠ WARNING: The SRC Pro commands made available on CAN network are not safety certified, therefore you must assess the suitability of using this data in safety relevant applications.

At present, while the integration is intended to be compatible with a CANopen compliant network, the full capability set described in the standards is not yet implemented.

You can find a sample EDS (Electronic Data Sheet) file to download from the Customer Support Portal in the Endpoint Controller article.

The following table provides an overview of the different types of CANopen joystick data.

TABLE 5-1. *CANopen*

Description	Direction	Frequency
Joystick Data – Buttons (See Table 5-2, “TPDO1 Buttons,” on page 3).	Transmit	~20 Hz (buttons actively pressed.) ~4 Hz (inactive & buttons not pressed)
Joystick Data - Thumbstick Axes (See Table 5-3, “TPDO2 Thumbstick Axes,” on page 3).	Transmit	~20 Hz
Joystick Data - Trigger Axes (See Table 5-4, “TPDO3 Trigger Axes,” on page 4).	Transmit	~20 Hz

Joystick and Button Data Representation

The device implements a CiA 401 Part 2 compatible representation of a multi-axis joystick. It presents as a Device Type (OD Entry 0x1000) as 0x01 (i.e., “Joystick with digital inputs without digital outputs”). See CiA 401 Part 2 Section 10.2 “Device type”. As per the standard’s representation, the device uses:

- TPDO1 (Transmit Process Data Object) protocol to convey the Boolean values of the Safe Remote Control Pro’s buttons.
- TPDO2 to convey the analog values of the four axes on the face of the Safe Remote Control Pro.
- TPDO3 to convey the analog values of the two triggers at the rear of the Safe Remote Control Pro.

The following table lists the TPDO1 (0x180 + Node ID — default Node ID is 3) buttons. TPDO1 conveys the Boolean values of the Safe Remote Control Pro’s buttons.

Each sub index is an 8-bit unsigned integer (UINT8)

The following table shows the TPDO1 buttons.

TABLE 5-2. *TPDO1 Buttons*

Object Dictionary Index (hex)	Sub-Index	Bit	Name	Usage
60.00	01	00, 01, 02	memory x-axis, memory y-axis, memory z-axis	Unused - Fixed 0
60.00	01	03, 04, 05, 06, 07	ms	Unused
60.00	02	00	b1	Down
60.00	02	01	b2	Right
60.00	02	02	b3	Up
60.00	02	03	b4	Left
60.00	02	04	b5	Pause
60.00	02	05, 06, 07	b6, b7, b8	Unused
60.00	03	00	b9	1 Key
60.00	03	01	b10	2 Key
60.00	03	02	b11	3 Key
60.00	03	03	b12	4 Key
60.00	03	04	b13	Menu
60.00	03	05, 06, 07	b14, b15, b16	Unused

The following table lists the TPDO2 (0x280 + Node ID — default Node ID is 3) thumbstick axes. TPDO2 conveys the analog values of the four axes on the face of the Safe Remote Control Pro.

Each value is a full range 16-bit signed integer (int16) that produces a zero-value when the stick is at rest/centered. The axis shows a positive value when pushed up (Y) or right (X) and a negative value when pushed down (Y) or left (X).

TABLE 5-3. *TPDO2 Thumbstick Axes*

Object Dictionary Index (hex)	Sub-Index	Type	Usage
64.01	01	INT16	Left Stick X
64.01	02	INT16	Left Stick Y
64.01	03	INT16	Right Stick X
64.01	04	INT16	Right Stick Y

The following table lists the TPDO3 (0x380 + Node ID — default Node ID is 3) trigger axes. TPDO3 conveys the analog values of the two triggers at the rear of the Safe Remote Control Pro.

Each value is a full range 16-bit signed integer (int16) that produces a zero-value when the trigger is at rest/centered. The axis shows a positive value when pulled up and a negative value when pushed down.

TABLE 5-4. *TPDO3 Trigger Axes*

Object Dictionary Index (hex)	Sub-Index	Type	Usage
64.01	05	INT16	Left Trigger
64.01	06	INT16	Right Trigger

CANopen Limitations

The device implementation currently lacks some CANopen standard functionality that you should be aware of:

⚠ **WARNING:** The data available on CANopen is not safety rated, therefore you should not use this data to perform safety functions.

- The default bitrate of the CAN interface is 250000. You *cannot* adjust the bitrate through the CANopen NMT protocol but must do so by using FORT Manager or the FORT CLI Config Tool.
- The default device Node ID is 3. You cannot change the device address through the CANopen NMT functionality but must do so by using FORT Manager. Contact FORT support if you require a value other than the default and need more information.

J1939 Implementation

The Endpoint Controller's CAN application supports sending and receiving message using the J1939 protocol. The Endpoint Controller uses the Emota J1939 stack to provide the full functionality of the J1939 protocol. The following table provides an overview of the J1939 messages.

⚠ **WARNING:** The data available on CAN J1939 is not safety rated, therefore you should not use this data to perform safety functions.

At present, while the integration is intended to be compatible with a J1939 compliant network, the full capability set described in the standards is not yet implemented.

You can find a sample DBC (Database Container) file to download on the Customer Support Portal in the Endpoint Controller article.

The following table provides an overview of the different types of J1939 messages.

TABLE 5-5. *CAN J1939*

PGN	PGN (Hex)	Description	Direction	Freq
	0xEE00	Address Claiming	Transmit	
64982	0xFDD6	Left Joystick - J1939 Basic Joystick Message 1	Transmit	~16 Hz
64983	0xFDD7	Left Joystick - J1939 Extended Joystick Message 1	Transmit	~16 Hz
64984	0xFDD8	Right Joystick - J1939 Basic Joystick Message 2	Transmit	~16 Hz
64985	0xFDD9	Right Joystick - J1939 Extended Joystick Message 2	Transmit	~16 Hz

Address Claiming

The EPC CAN supports the standard J1939 Address Claim functionality. The Endpoint Controller's Manufacturer Code is 1262 (decimal).

Left Joystick - J1939 Basic Joystick Message

The following table shows the basic message fields for the left joystick.

TABLE 5-6. *J1939 Left Joystick Basic Messages*

Bytes	Bits	J1939 PGN 64982 Data field	Description
1	2 bits	00b: not in neutral position 01b: in neutral position 10b: error indicator 11b: NA	X-Axis neutral position status
	2 bits	00b: Not on negative side of Neutral 01b: On negative side of Neutral 10b: error indicator 11b: NA	X-Axis Lever Left Negative Position Status
	2 bits	00b: Not on Positive side of Neutral 01b: On Positive side of Neutral 10b: error indicator 11b: NA	X-Axis Lever Right Positive Position Status
1/2	10 bits	The position of the joystick in the relative motion of travel from the neutral position. Position value of 0 is Neutral and position value 1000 (100%) is the end of linear zone. Value of 1022 indicates an error has occurred.	X-Axis Position
3	2 bits	00b: not in neutral position 01b: in neutral position 10b: error indicator 11b: NA	Y-Axis neutral position status
	2 bits	00b: Not on negative side of Neutral 01b: On negative side of Neutral 10b: error indicator 11b: NA	Y-Axis Lever Left Negative Position Status
	2 bits	00b: Not on Positive side of Neutral 01b: On Positive side of Neutral 10b: error indicator 11b: NA	Y-Axis Lever Right Positive Position Status
3/4	10 bits	The position of the joystick in the relative motion of travel from the neutral position. Position value of 0 is Neutral and position value 1000 (100%) is the end of linear zone. Value of 1022 indicates an error has occurred.	Y-Axis Position
5	2 bits		Y-Axis Detent Position Status
5	2 bits		X-Axis Detent Position Status
6	2 bits	00b: Button not pressed 01b: Button pressed 10b: Error Indicator 11b: NA	Keypad button Left second has been pressed. As per j1939 DA it is Joystick button 4 (up arrow)
6	2 bits		**Keypad** button **Left third** has been pressed. As per j1939 DA it is Joystick button 3 (left arrow)
6	2 bits		**Keypad** button **Pause** has been pressed. As per j1939 DA it is Joystick button 2

Bytes	Bits	J1939 PGN 64982 Data field	Description
6	2 bits		Joystick button **Power** has been pressed. As per j1939 DA it is Joystick button 1
7	2 bits	00b: Button not pressed 01b: Button pressed 10b: Error Indicator 11b: Not Available	**Keypad** button **Right Third** has been pressed. As per j1939 DA it is Joystick button 8 (button 4 on device)
7	2 bits		**Keypad** button **Menu** has been pressed As per j1939 DA it is Joystick button 7
7	2 bits		**Keypad** button **Left Home** has been pressed As per j1939 DA it is Joystick button 6 (down arrow)
7	2 bits		**Keypad** button **Left First** has been pressed. As per j1939 DA it is Joystick button 5 (right arrow)
8	2 bits	00b: Button not pressed 01b: Button pressed 10b: Error Indicator 11b: Not Available	EPC Reserved As per j1939 DA it is Joystick button 12
8	2 bits		**Keypad** button **Right Home** has been pressed As per j1939 DA it is Joystick button 11 (button 1 on device)
8	2 bits		**Keypad** button **Right First** has been pressed As per j1939 DA it is Joystick button 10 (button 2 on device)
8	2 bits		**Keypad** button **Right Second** has been pressed As per j1939 DA it is Joystick button 9 (button 3 on device)

Left Joystick - J1939 Extended Joystick Message 1

The following table shows the J1939 extended message 1 for the left joystick.

TABLE 5-7. *J1939 Left Joystick Extended Message*

Bytes	Bits	J1939 PGN 64983 Data field	Description
1	2 bits	00b: not in neutral position 01b: in neutral position 10b: error indicator 11b: NA	Z-axis neutral position status
	2 bits	00b: Not on negative side of Neutral 01b: On negative side of Neutral 10b: error indicator 11b: NA	Z-Axis Lever Left Negative Position Status
	2 bits	00b: Not on Positive side of Neutral 01b: On Positive side of Neutral 10b: error indicator 11b: NA	Z-Axis Lever Right Positive Position Status
1/2	10 bits	The position of the joystick in the relative motion of travel from the neutral position. Position value of 0 is Neutral and position value 1000 (100%) is the end of linear zone. Value of 1022 indicates an error has occurred.	Z-Axis Position

Right Joystick - J1939 Basic Joystick Message 2

Same as Left Joystick - J1939 Basic Joystick Message 1

Right Joystick - J1939 Extended Joystick Message 2

Same as Left Joystick - J1939 Extended Joystick Message 1

SRC Pro Control Messages

The EPC supports receiving messages that can change settings on a connected SRCP. If an SRCP is not connected, though, any received commands are ignored.

SRCP control messages are received on CANopen via RPDO1 and RPDO2 as shown in the following tables:

TABLE 5-8. *RPDO1 (0x200 + Node ID) - SRC Pro Settings Message*

Object Dictionary Index (hex)	Sub-Index	Type	Usage
20.00	01	Octet String (0x0000a) size - 8 bytes or 64 bits 0x40 bits	SRC Pro Setting Message

TABLE 5-9. *RPDO2 (0x300 + Node ID) - User Display Text String*

Object Dictionary Index (hex)	Sub-Index	Type	Usage
20.01	01	Octet String (0x0000a) size - 8 bytes or 64 bits 0x40 bits	Display Text Data

SRC Pro control messages are received on J1939 via proprietary message PGNs.

TABLE 5-10. *CAN J1939 SRC Pro Settings Message*

PGN	PGN (Hex)	Description	Direction	Freq
65281	0xFF01	SRC Pro Settings Command - J1939 Proprietary Message	Receive	N/A
65282	0xFF02	User Display Text String - J1939 Proprietary Message	Receive	N/A

SRC Pro Settings Message

The Endpoint Controller supports receiving an SRC Pro Settings message to change settings on a connected Safe Remote Control Pro. This message is only supported for an Endpoint Controller that is connected to a Safe Remote Control Pro.

⚠ **CAUTION:** Vibration messages are rate limited to 1 message per 100 ms. Additional vibration messages received beyond the limit will be ignored.

The following table shows the SRC Pro Settings message format:

TABLE 5-11. *SRC Pro Settings Message Format*

Byte Offset	Size	Description	Value
0	1	Setting Key	SRC Pro Setting to Change
1	4	Setting Value	Value of the setting (little endian)
5	3	Reserved for Future Use	

The following table shows the Safe Remote Control Pro setting keys.

TABLE 5-12. *SRC Pro Setting Keys*

Key	Name	Description	Minimum SRC Pro Version
1-9	Reserved		
10	Left Motor Vibrate	1 = Vibrates the left motor for 100 ms	3.2.2
11	Right Motor Vibrate	1 = Vibrates the right motor for 100 ms	3.2.2
12	Both Motor Vibrate	1 = Vibrates both motors for 100 ms	3.2.2
99	Display Mode	0 = Default Display Mode 1 = User Text Display Mode (4 Lines)	3.2.2

SRC Pro User Display Text String Message

The Endpoint Controller supports receiving an SRC Pro user display text message to set the display text on the connected Safe Remote Control Pro when the Safe Remote Control Pro is in user-text mode. You can use the SRC Pro Settings message to change the display mode of the Safe Remote Control Pro.

This message is only supported when an Endpoint Controller is connected to a Safe Remote Control Pro.

The User Display Text String message to the Endpoint Controller allows updating the displayed text on the connected Safe Remote Control Pro when the Safe Remote Control Pro is in user text mode. The user string is built using three segments of six characters each to build an 18-character string.

⚠ CAUTION: This message is rate limited and only 1 message can be received per 100 ms. Additional messages received beyond the limit will be ignored.

TABLE 5-13. *User Display Text Message Format*

Byte Offset	Size	Description	Value
0	1	User Text Key	0-3
1	1	Segment	0-2
2	6	User Text String	6 ASCII Characters

The following keys are currently defined by the system for user strings:

TABLE 5-14. *User String Keys*

Key	Name	Description
0	Custom Display Text Line 1	In display mode 1, this is the first line of custom text that is displayed.
1	Custom Display Text Line 2	In display mode 1, this is the second line of custom text that is displayed.
2	Custom Display Text Line 3	In display mode 1, this is the third line of custom text that is displayed.
3	Custom Display Text Line 4	In display mode 1, this is the fourth line of custom text that is displayed.

Status Messages

⚠ **CAUTION:** This section describes functionality that is available in EPC 1.6.0 or later. If you are using a previous firmware version, and want to use one of these messages, update your firmware to the latest version (see "Updating EPC Firmware").

Status messages use custom formats that remain the same between CANopen and J1939.

The following table shows the Object Dictionary definition of all CANopen EPC Status messages:

TABLE 5-15. *TPDO4: (0x480 + Node ID) - EPC Status Messages*

Object Dictionary Index (hex)	Sub-Index	Data Type	Name
30.00	01	Octet String (0x0000a) size - 8 bytes or 64 bits 0x40 bits	EPC status messages

The following table shows the PGN for J1939 status messages.

TABLE 5-16. *J1939 EPC Status Messages*

PGN	Description	Direction
65280 (0xFF00)	EPC status messages - J1939 Proprietary Message	Transmit

All EPC status messages use the same CANopen TPDO or J1939 PGN format and are differentiated by an ID field within the message data itself, as shown in the following table:

TABLE 5-17. *Message Identifiers and Frequencies*

Name	Identifier	Frequency	Notes
EPC Output Status 1	0	200 ms and on change	
EPC Connected Device Latency	1	1 sec	
SRC Pro System Status	2	1s normally; 10s if no data received from SRCP for >= 5 seconds	
ISM Connection Status	3	1 sec	Enabled only if ISM is configured

EPC Output Status 1 Message

The Endpoint Controller transmits an output message to provide status for various Endpoint Controller functionality. It uses the TPD04 protocol to transmit the message at a rate (trigger) of every 200 ms and upon status changes. The following table shows the status message format.

⚠ **NOTE:** This message requires EPC firmware 1.6.0 or later.

TABLE 5-18. *EPC Output Status 1 (formerly EPC Heartbeat Message)*

Byte Offset	Size	Description	Value
0	1	Message ID	Identifier for “EPC Output Status 1” message - 0x00
1	1	Status Sequence ID	8-bit Unsigned Integer that increments a sequence number to associate messages related to the EPC status to a single time
2	1	Output 1 State	Bits 3:0 - SMCU0 State Bits 7:4 - SMCU1 State 0000 - SAFETY_REQUESTED; cause is unspecified 0001 - SAFETY_NOT_REQUESTED 0010 - SAFETY_FAULT 0100 - Safety from input timeout 1000 - Safety from input request
3	1	Output 2 State	Same as Output 1 State
4	1	Output 3 State	Same as Output 1 State
5	1	Mode	Bits 3:0 - SMCU0 State Bits 7:4 - SMCU1 State 0000 - No Mode (Error State) 0001 - Supervised 0010 - Autonomous (Unsupervised) 0011 - Not Applicable (EPC to EPC Pairing)
6	1	Reserved	Reserved for future use
7	1	Reserved	Reserved for future use

EPC Connected Device Latency Message

The rate (trigger) for this message is 1 second.

⚠ **NOTE:** This message requires EPC firmware 1.6.0 or later.

TABLE 5-19. *EPC Connected Device Latency*

Byte Offset	Size	Description	Value
0	1		Identifier for “EPC Connected Device Latency” message - 0x01
1	1	Status Sequence ID	Integer Incrementing sequence number to associate messages related to the EPC status to a single time
2	1	Care List Index	Index of the remote device (a separate value from the Device ID)
3	2	SMCU0 Measurement	16-bit latency measurement for this remote device, from Safety MCU 0
5	2	SMCU1 Measurement	16-bit latency measurement for this remote device, from Safety MCU 1
7	1	Reserved	0xFF

SRC Pro System Status Message

The rate (trigger) for this message is normally 1 second unless no data is received from the SRC Pro for 5 seconds or more, in which case it is 10 seconds.

⚠ **NOTE:** This message requires EPC firmware 1.6.0 or later.

TABLE 5-20. *SRC Pro System Status*

Byte Offset	Size	Description	Value
0	1	Message ID	Identifier for 'SRCP System Status' message - 0x02
1	1	Status Sequence ID	Integer Incrementing sequence number to associate messages related to the SRCP System Status to a single time
2	1	USB Connected	Bit Meanings • Bit 7: 1 = USB connected, 0 = USB disconnected • Bit 6: 1 = USB charging, 0 = USB not charging • Bits 5:0: Reserved
3	1	Battery Percentage	Battery Percentage from 0 (Decimal)% to 100 (Decimal)%
4	1	Mode	Mode Values: • 0x04: Local Mode - Device is not yet paired. • 0x06: Remote Mode - Device is paired, but not yet sending button/joystick state. • 0x09: Operational Mode - Device is paired, and is sending button/joystick state. • 0x0A: Menu mode - Device is in its menu. If connected, it will not send button/joystick state. • 0x0B: Pause mode - Device is paused. If connected, it will not send button/joystick state.
5	1	Cause of Pause	Value to indicate the reason that the SRC Pro is in Pause mode Pause Cause Values: - 0: None - 1: Manual pause - 2: Free fall - 3: Orientation - 4: Inactivity
6	1	Reserved	0xFF
7	1	No message	Bit Encoding • Bit 7: 1 = No status messages received for >= 5 seconds, information may be out of date. • Bits 6:0: Reserved

ISM Connection Status Message

The message rate (trigger) is 1 second but is enabled only when ISM is configured.

⚠ **NOTE:** This message requires EPC firmware 1.6.0 or later.

TABLE 5-21. *ISM Connection Status*

Byte Offset	Size	Description	Value
0	1	Message ID	Identifier for 'ISM Connection Status' message - 0x03
1	1	Status Sequence ID	Integer Incrementing sequence number to associate messages related to the ISM Connection Status to a single time
2	1	RSSI Value	8-bit Signed Integer indicates the RSSI (Received Signal Strength Indicator) value which ranges between -120 (0x88) to +20 (0x14). The value is -128 (0x80) when ISM is configured but not in “connected” state.
3	1	Reserved	
4	1	Reserved	
5	1	Reserved	
6	1	Reserved	
7	1	Reserved	

EPC Heartbeat Message

⚠ **NOTE:** This message has been deprecated in favor of the “EPC Output Status 1 Message” for EPC 1.6.0 and later. This section is included in case you are using a previous EPC firmware version and want to implement an EPC status message. If you are running EPC 1.6.0 or later firmware, use the EPC Output Status 1 message.

The Endpoint Controller transmits a heartbeat message to provide status for various Endpoint Controller functionality. It uses the TPDO4 protocol to transmit the heartbeat message at a rate of every 5 Hz.

The following table shows the Object Dictionary definition of the heartbeat message.

TABLE 5-22. *TPDO4: (0x480 + Node ID) - EPC Heartbeat Message*

Object Dictionary Index (hex)	Sub-Index	Type	Usage
30.00	01	Octet String (0x0000a) size - 8 bytes or 64 bits 0x40 bits	EPC Heartbeat Message

The following table shows the J1939 PGN for the EPC Heartbeat Message.

TABLE 5-23. *J1939*

PGN	PGN (Hex)	Description	Direction	Freq
65280	0xFF00	EPC Heartbeat - J1939 Proprietary Message	Transmit	5 Hz

The following table shows the EPC heartbeat message format.

TABLE 5-24. *EPC Heartbeat Message Format*[1]

Byte Offset	Size	Description	Value
0	2	Message ID	16-bit Unsigned Integer (little-endian)
1	1	Status Sequence ID	Incrementing sequence number to associate messages related to the EPC status to a single time
2	1	Output 1 State	A value of 0x11 indicates SAFETY_NOT_REQUESTED, 0x00 indicates SAFETY_REQUESTED for Output 1. Any other value is partial or faulty/unknown. Bits 3:0 - SMCU0 State 0000 - SAFETY_REQUESTED 0001 - SAFETY_NOT_REQUESTED 0010 - SAFETY_FAULT Bits 7:4 - SMCU1 State 0000 - SAFETY_REQUESTED 0001 - SAFETY_NOT_REQUESTED 0010 - SAFETY_FAULT
3	1	Output 2 State	Same as Output 1 State
4	1	Output 3 State	Same as Output 1 State
5	1	Output 1 Mode	Modes for Output 1 0x00 - No Mode (Error State) 0x11 - Supervised 0x22 – Autonomous (Unsupervised) 0x33 - Not Applicable (EPC to EPC Pairing) Bits 3:0 - SMCU0 Mode 0000 - No Mode (Error State) 0001 - Supervised 0010 – Autonomous (Unsupervised) 0011 - Not Applicable (EPC to EPC Pairing) Bits 7:4 - SMCU1 Mode 0000 - No Mode (Error State) 0001 - Supervised 0010 – Autonomous (Unsupervised) 0011 - Not Applicable (EPC to EPC Pairing)
6	1	Output 2 Mode	Reserved for future use
7	1	Output 3 Mode	Reserved for future use

1. This message format has been replaced by "EPC Output Status 1 Message" for EPC 1.6.0 and later.

CHAPTER 6 Security

The FORT Robotics security approach for Pro Series devices aligns with the National Institute of Standards and Technology (NIST) guidance for device security best practices.

With security defined as the state of being free from danger or threat, FORT's security mission is to ensure that every capability we deliver in any form — hardware, software, cloud, mobile, any data, or something else — works correctly and completely throughout its life cycle, without inspection or influence from malicious actors.

Toward that goal, we've built foundational cybersecurity capability into the full Pro Series hardware, software, and cloud-connected stack, protecting those devices from the moment they start through their complete life cycle.

The Endpoint Controller and Safe Remote Control Pro provide the security features described in the following sections:

Tamper-proofing devices

To prevent hackers from altering the hardware of the device or circumventing the startup process, each device is hardened as its final production step, prior to delivery to customers. Hardening includes One-Time Programming (OTP), a physical process of blowing transistors to ensure that no software attack can re-enable any interfaces used by development and test, as well as a secure hardware linkage to prevent removal and replacement of critical hardware elements.

The hardening process includes:

- Disabling "debug" interfaces.
- Disabling unused and unneeded ports.
- Disabling all forms of boot except FORT's secure boot.
- Protecting against removal of Processor or Secure Element.

Secure boot on devices

To prevent hackers from inserting security threats during startup, each device starts securely with a chain of trust that ensures the device boots with signed firmware only.

The device startup process securely starts the device using three steps to ensure that only FORT-signed firmware is running. The operating system is cryptographically validated each time the device starts up to ensure trusted machine control.

Secure boot process:

- **Step 1 -** A hardware cryptographic check ensures the boot loader has not been tampered with in any way.

- **Step 2 -** The now-trusted boot loader checks and loads the libraries that are essential for starting the rest of the operating system.
- **Step 3 -** After software checks on the libraries pass, the boot process loads and checks the rest of the operating system.

Secure device configuration

Configurations created in FORT Manager define the pairing between FORT devices, and are critically important for device-to-device communication. Configurations (including any changes) are authenticated cryptographically to prevent forgery or corruption by a malicious actor. As such, the device configuration digital signature is cryptographically authenticated by each device using certificates stored on the Secure Element before every use.

Steps for creation and review of configuration files:

- **Step 1 -** A user creates or updates a configuration in FORT Manager.
- **Step 2 -** FORT Manager uses FORT's digital signing service to apply a digital signature to the configuration.
- **Step 3 -** A user loads the configuration file to their FORT devices.
- **Step 4 -** The FORT device checks the digital signature against certificates in the Secure Element.
- **Step 5 -** If the signature passes inspection, the configuration is loaded and applied.

Trusted communication

To prevent FORT devices from communicating with unknown entities FORT constructs a whitelist of trusted devices. The whitelist forms a "care list" for each device from a communication and safety perspective, helping it communicate with only trusted devices using functional safety (FuSa) communication channels to protect the exchange:

- Each configuration contains a trusted device list that describes the only other entities with which the device is able to communicate.
- Altering the configuration file in any way destroys its digital signature, preventing hackers from inserting their own details.

Secure device update

To prevent hackers from inserting security threats during firmware updates, we ensure that firmware updates are digitally signed, and that the device authenticates an update before installing it.

This builds on the secure boot capability, as after a new update is applied, the device will reboot and leverage that second series of three-step checks to ensure that the entire process executed successfully:

- The device validates the digital signature of the firmware update before installing the update.
- Images that pass validation are applied to the device.

- Devices also have update rollback capabilities — in case of failure, the device rolls back to the last known good firmware.

CHAPTER 7

FORT Manager

Our cloud-hosted FORT Manager solution gives you the ability to securely manage and configure your Pro Series devices, as well as the ability to manage the personnel in charge of their deployment, configuration, and upkeep.

To use FORT Manager, open a browser and navigate to the FORT Manager URL: https://app.fortrobotics.com and log in with your email address and password.

FORT Manager is invite-only. If you don't have an account, ask the person at your company who initially set up the FORT Manager account (your FORT Manager Admin) to create one for you. If you don't know your company's FORT Manager Admin, reach out to us at support@fortrobotics.com.

For more information about how to get started with FORT Manager, see our getting started guide.

Logging in for the First Time

FORT Manager is by invite only, so look for an invitation email from FORT Robotics.

TO SET UP YOUR ACCOUNT

1. Open the email from FORT Robotics and click **Accept Invitation**.
2. Type a password and re-enter it in the confirmation field, then click **Reset password**.
3. In the confirmation dialog, click **Back to FORT Manager**.
4. Type your email address and password and click **Continue** to launch FORT Manager.
5. Enter your first and last names.
6. Optionally upload an image to display when you log in.

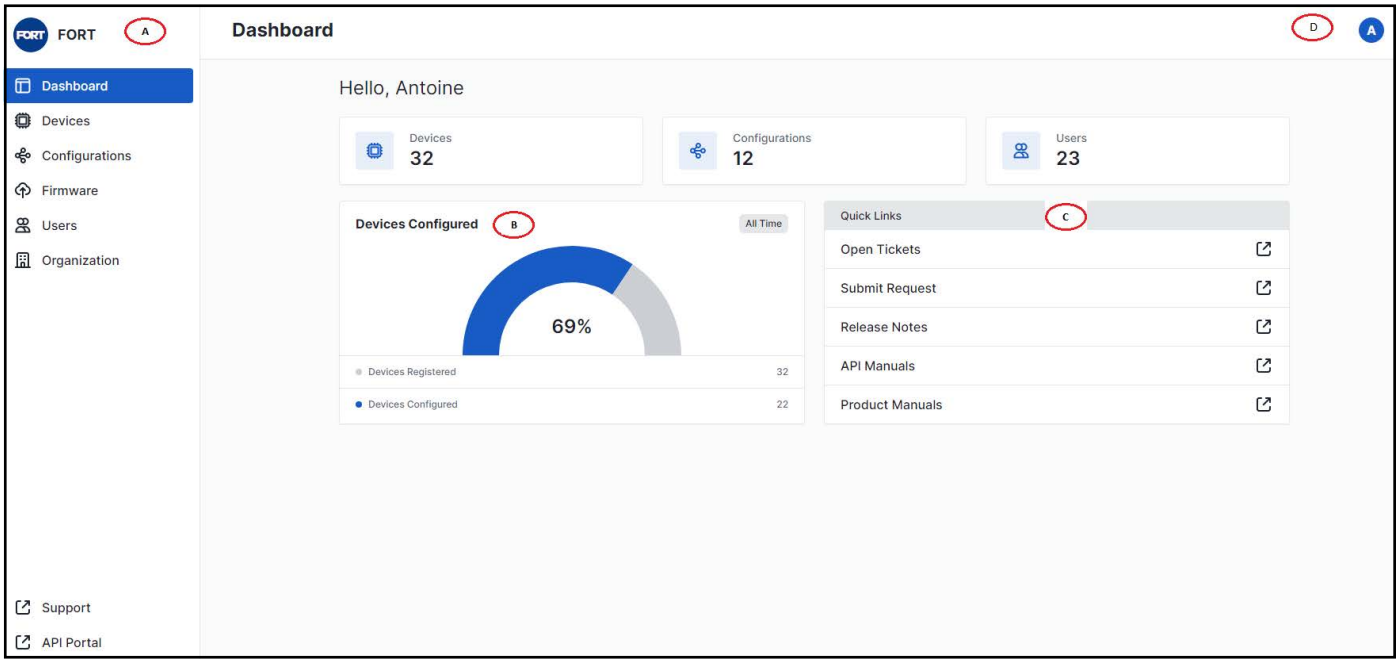
   If you don't upload an image, FORT Manager automatically creates an icon to display based on your name. You can change the icon, as well as your personal information and password at any time by editing your "Personal Settings".
7. Click **Finish**.

Launch FORT Manager and enter your email address and password. If multi-factor authentication is enabled for your account, follow the instructions to set it up.

Dashboard

When you first log into FORT Manager, you are in the dashboard view. If you navigate away from the dashboard, you can return at any time by clicking **Dashboard** in the left navigation pane.

FIGURE 7-1. *Dashboard*



- [A] Items in the left pane enable you to navigate to different pages in FORT Manager, as well as to open a new browser window to go directly to the FORT Robotics support website or to the API Portal.

  This pane remains constant no matter which page you are on in the app.

> ⚠ **NOTE:** The items that are visible in the left pane (and hence the pages that you can navigate to) depend on your assigned role. For example, if your role doesn't have permission for user management, Users is not visible in the navigation pane. In addition, some roles provide view-only access to certain pages; for example, if your role provides view-only access to devices, Devices is available in the navigation pane and you can view the devices page to see a list of devices, but you can't add, delete, or modify a device.
> "Users" on page 7-5 explains roles and permissions in more detail.

- [B] The middle pane displays information about your configuration, for example the number of devices your organization has registered and the number and percentage that have been added to a configuration.[1]
- [C] The **Quick Links** section allows you to do any of the following in a new browser window:
  - See any of your open tickets.
  - Submit a new request for technical support, to repair or RMA a device, or to provide feedback.
  - View release notes and manuals.

    You can also click the Support item in the left pane to go to the FORT help center and browse or search our knowledge base for specific information.
- [D] The icon in the upper right corner allows you to view and edit your profile or to sign out.

  To edit your profile, click the icon and click **Settings**. Click **Edit** next to any item to make changes (see the next section for more details).

1. Future versions of FORT Manager will enable the display of additional information about your organization in addition to percentage of devices that are configured. Please use the **Submit Request** Quick Link to ask for enhancements that you would like to see.

⚠ **NOTE:** Your role is set by your admin and you cannot change it. Also, although you can independently set up multi-factor authentication for your account, if your admin has required it for your role, you won't be able to disable it.

Personal Settings

All users can view or change their personal settings from any page in FORT Manager, including name, icon to display, email address, and password. You can see your role (but only an admin can change it) and you can turn on multi-factor authentication for yourself, but if an admin has enabled it for your role, you cannot disable it.

TO CHANGE YOUR PERSONAL SETTINGS

1. Click the icon in the upper right corner.
2. Click **Settings**.
3. Click **Edit** next to any item to make changes and click **Save** when done.

⚠ **NOTE:** Your role is set by an administrator and you cannot change it.

4. To enable multi-factor authentication for yourself, move the slider next to **MFA** and follow the instructions to set it up (log out and scan the QR code).

   Each subsequent time that you log into FORT Manager you must provide the code from the authenticator app in addition to your password.

⚠ **NOTE:** Although you may set an MFA requirement for yourself even if an admin hasn't required it for your role, you cannot disable an MFA requirement that an administrator has enabled.

Devices

Devices that have already been activated are visible in the center pane, along with clickable details for every device.

Additionally, if you have Admin or Device Manager permissions, you have the ability to:

- Add a new FORT device.
- Edit the custom details for a device.

TO ADD A DEVICE

(Requires Device Manager or Admin role)

1. Click **Devices** and click **Add device** in the upper right corner.
2. Type the serial number for the device (found on the back plate of the device or emailed to you by FORT) and click **Continue**.
3. Type a name for the device, optionally click the picture icon to add a picture, and click **Register**.

We recommend assigning names that describe the function or location of the device or the equipment under control (EUC), for example, South Tractor Remote Control, or Observation Deck Controller for sending devices, and South Tractor, Thresher, AMR-1, etc. for receiver devices attached to EUCs.

TO EDIT A DEVICE

(Requires DeviceManager or Admin role)

1. Click **Devices** and click the edit icon in the **Action** column for the device.
2. Type a new name for the device or select the picture for the device and navigate to and select a new picture.
3. Click **Save** to save the new details or **Cancel** to discard the changes.

FORT Manager updates the name for the device and picture on the Devices page as well as anywhere else they appear, such as on the Configurations page.

Configurations

(Requires Config Manager or Admin role to build a configuration)

The Configurations page enables you to see, as well as build or manage (with appropriate permissions), configurations for your organization. With a configuration you build out all of the wired or wireless pairings between your Pro Series devices.

All users can view the Configurations page but only Admins and users with Config Manager permission are able to make updates, including building a new configuration.

The following sections explain in detail the characteristics of particular configurations and how to use Config Management in FORT Manager to build them:

- "Building an EPC to EPC Configuration" on page 2-2
- "Building an SRC Pro to EPC Configuration" on page 2-9
- "Building a Hybrid Configuration" on page 2-13

Firmware

(Requires Device Manager or Admin role)

The Firmware page enables you to download firmware files to update the firmware on your devices. You can also download the latest version of the CLI Tool that you can use to install the firmware files.

TO DOWNLOAD FIRMWARE UPDATES OR THE CLI TOOL

(Requires Device Manager or Admin role)

1. To download firmware, click the **Download** link to the right of the file to download.
2. To download the CLI Tool, click **Download CLI Tool**.

FORT Manager copies the file to the Download folder on your computer. Follow the appropriate instructions for the type of file that you downloaded:

- "Loading a Configuration onto an EPC" on page 2-15
- "Loading a Configuration onto an SRC Pro" on page 2-16
- "Updating EPC Firmware" on page G-4
- "Updating SRC Pro Firmware" on page G-5

Users

(Requires Admin role)

The Users page allows you to add or delete members from your organization, as well as assign roles (permissions) to users. The available roles are:

- **Admin** — Has all the permissions listed for the other roles as well as all user and organizational management capabilities.
- **Config Manager** —Create, edit, and delete configurations.
  - Has has read-only view of the Devices page.
- **Device Manager** —Create, edit, and delete devices
  - Has read-only view of the Configurations page.
  - Has full access to the Firmware tab to download firmware files and the CLI tool.
- **Operator** — Read-only permissions across FORT Manager but can't make changes.
  - Is not able to see the Users, Organization, or Firmware pages.
  - (Outside of FORT Manager) Is able to execute the CLI tool to load configurations to devices or to update the firmware on a device.

All users are able to turn on multi-factor authentication (MFA) for their own account.

When you add a user to FORT Manager, you specify their email address and assign one or more roles. FORT Manager sends an email invite to the user and guides them through the registration process.

To Add a User

(Requires Admin role)

1. Click **Users** to go to the Users page (make sure the Active tab is selected) and click **Add User** in the upper right of the screen.
2. Type the email address for the user and click **Continue**.
3. Select one or more roles from the drop-down box and click **Send**.

You should see a message that the invitation was sent successfully and see details about it in the Pending tab. The invitation expires after two days.

The selected user receives an email from you (the FORT Manager Admin) with a link to create an account in FORT Manager. After the user logs in and creates an account, you can see their details on the Active tab on the Users page.

To Edit or Delete Roles for an Existing User

(Requires Admin role)

1. Click **Users** and double click the user's name or click the edit icon in the **Actions** column for the user.
2. Do either of the following:
   a. To add roles, select the box for one or more roles and click **Save**.
   b. To remove roles, click the box for a role with a check mark to deselect it and click **Save**.
   You cannot remove all roles for a user; you must assign at least one role.

To Delete an Existing User

(Requires Admin role)

1. Click **Users** and click the delete icon in the **Actions** column for the user.
   FORT Manager displays a warning message.
2. Click **Delete** to delete the user or **Cancel** to keep them.

⚠ **Caution:** To prevent your organization from ending up without an admin account, admin users are not able to delete themselves. If you want to delete a specific admin account, you must have at least one other admin account that you can use for that purpose.

Organization

(Requires the Admin role)

The Organization page enables an admin to view or edit basic information for the organization, and to view and manage multi-factor authentication (MFA) settings for users.

Click the **Basic Info** tab to view or update information such as your organization name, logo, location, and so on. The organization name and logo appear in the upper left corner of the page for all users.

Click the **Settings** tab to view or update MFA requirements. You can require MFA for your entire organization or apply it selectively based on *role*.

⚠ **Note:** Individual users may set an MFA requirement for themselves even if an admin hasn't required it for their role, however, they cannot disable an MFA requirement that an administrator has enabled.

The first time a user logs into their account after an admin requires MFA, FORT Manager guides them through the process of setting up an authenticator app by scanning a QR code. Subsequently, users must provide the code from the authenticator app in addition to their password each time that they log in.

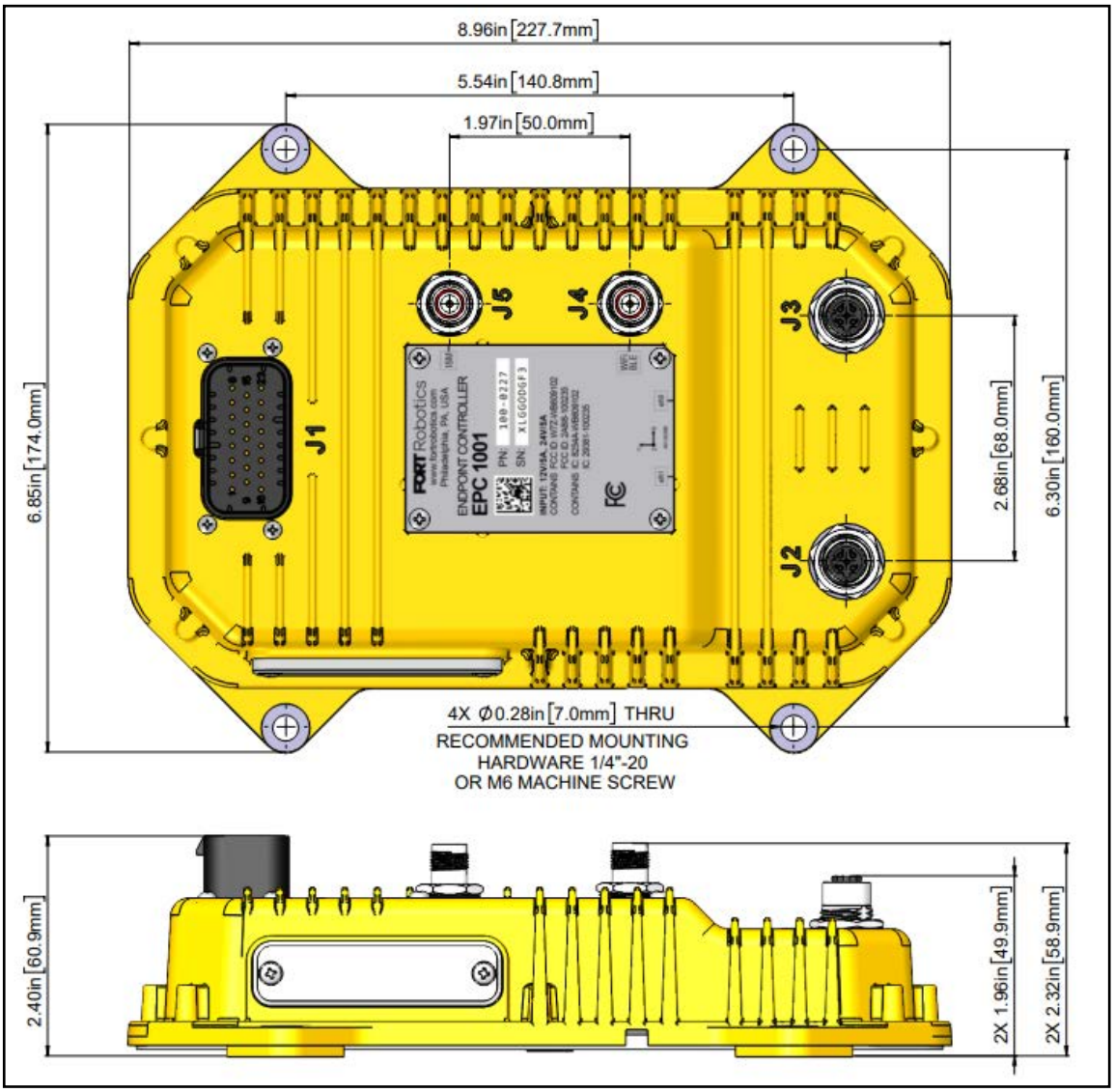
APPENDIX A *EPC Technical Specifications*

This appendix provides details of the Endpoint Controller hardware.

EPC Mechanical Drawing

The following figure shows a mechanical drawing of the EPC 1001. Note that all models have the same dimensions.

FIGURE A-1. *EPC-1001 Mechanical Drawing*



The following table shows the recommended connectors for an Endpoint Controller device.

TABLE A-1. *Suggested EPC Connector Types*

Connector Number	Suggested Mating Connector Type for EPC
J1	TE 770680-1.
J2	Ethernet M12 – D Type for management port connection. Connect the J2 connector on an EPC to a port on a Linux machine to update firmware or load a configuration to the EPC.
J3	Ethernet M12 – D Type for connection to safety network.
J4	RP-TNC Plug (male) with center socket (female) quick disconnect antenna port for 2.4 GHz BLE & Wi-Fi antenna.
J5	RP-TNC Plug (male) with center socket (female) quick disconnect antenna port for 8xx and 9xx ISM antenna.
Side Door	MICRO SD
Side Door	RECPT, MINI USB B
Side Door	MICRO-SIM CARD, 6 CONTACTS

⚠ **CAUTION:** Connectors are designed to be hand tightened only. Use of a wrench or other tool will cause damage to the connector or cabling.

Recommended and Absolute Maximum Ratings (EPC)

The following table shows the recommended and absolute maximum ratings for the Endpoint Controller.

TABLE A-2. *EPC Recommended- and Absolute-Maximum*

Specification	Minimum	Typical	Maximum
PVin (12V operation)	9.6	12	14.4
PVin (24V operation)	19.2	24	28.8
PVin (V)	8	-	32
Input Voltage	0 V		Vin+0.7 V
Current (not including output loads)	87 mA @32V		273 mA @8 V
Weight		878 g | 1.9lb	
Ingress Protection		IP65	
Dimensions		228 mm x 176 mm x 70 mm 6.85" x 8.99" x 2.40"	
Operating and Storage Temperature	-40 °C		85 °C

Safety Input Specifications

The following table provides specifications for the safety inputs:

TABLE A-3. *Safety Input Specifications*

Specification	Minimum	Typical	Maximum
Safety Inputs		Three dual channel inputs	
Input Voltage	0 V		Vin+0.7 V
Input Current	5.75 mA @8 V		51.35 mA @32 V
Normal State Input	8		32
Safe State Input		Open Circuit/Hi-Z	
Input state for logic ON/HIGH[a]	8VDC	12VDC (or 24VDC)	32VDC
Input state for logic OFF/LOW	0VDC	0 ~ 1VDC	Less Than 8VDC
Input Impedance		TBD	

a. This applies to 12 VDC and 24 VDC supplied EPC Equipment.

Safety Output Specifications

The following table provides specifications for the safety outputs:

TABLE A-4. *Safety Output Specifications*

Specification	Minimum	Typical	Maximum
PVin (12V operation)	9.6	12	14.4
Output ON State	9.6V	12	14.4
On-state Voltage Drop			1.057 V
PVin (24V operation)	19.2	24	28.8
Output ON State	9.6V	24V	28.8
Safety Outputs		Three dual channel outputs	
Output safe state (logic OFF/ LOW)	0 V	0V	0V
Output Type		Current Sourcing	
Current (per output channel)			750 mA
Current (off)	0.714 uA @8 V		0.892 uA @32 V
Leakage Current (OFF state)	0.714 uA @8 V		0.892 uA @32 V
OSSD Pulse Width		300 µS	
OSSD Pulse Period		200 mS	

Wireless Radio Specifications (EPC)

You can configure the Endpoint Controller with several different radios based on frequency requirements and local regulations. Prior to ordering and deployment, consult local regulations to ensure that you are installing the proper radio.

North America ISM Radio (EPC)

The following table provides the specifications for North America ISM radio 902-928 MHz:

TABLE A-5. *(EPC) North America ISM Radio Specifications*

Specification	Minimum	Typical	Maximum
Frequency	902 MHz		928 MHz
Bandwidth		600 kHz	
Channels		21	
Receive Sensitivity		-100 dBm	
Modulation		2-GFSK	

European ISM Radio (EPC)

The following table provides specifications for the European ISM radio:

TABLE A-6. *European ISM Radio Specifications*

Specification	Minimum	Typical	Maximum
Frequency	869.4 MHz		869.653 MHz
Bandwidth		250 kHz	
Channels		1	
Receive Sensitivity		-100 dBm	
Modulation		2-GFSK	
Baud Rate		200 kbps	
Power (conducted RF output)	-10 dBm		27 dBm
EPC Part number	EU ISM radio is available in EPC model 1002		

Bluetooth Low Energy (BLE) Radio (EPC)

The following table provides specifications for the BLE radio:

TABLE A-7. *BLE Radio Specifications*

Specification	Minimum	Typical	Maximum
BLE Version		5.1	
Baud Rate		1 Mbps	
Power (conducted RF output)			4 dBm
Receive Sensitivity	-99 dBm		

Ethernet Specifications

The following table provides Ethernet specifications:

TABLE A-8. *Ethernet Specifications*

Specifications	Minimum	Typical	Maximum
Speed		10/100 Mbps	

Data Interfaces

The Endpoint Controller's integration interface is USB or CAN (Controller Area Network). "CANopen Implementation" on page 5-1 describes CAN communication specifications (data rates and protocol). Use the Endpoint Controller's dual safety outputs to prevent any motion of the equipment under control (EUC) when the Endpoint Controller receives an emergency stop from either the connected remote device or its wired emergency stop

input. The emergency stop inputs are relative to PVin. Maintain a single ground reference for all power and reverence voltages.

The following table provides specifications for the CAN interface.

TABLE A-9. *CAN Bus Specifications*

Specification	Minimum	Typical	Maximum
Common Mode Voltage	-30V		30 V
Positive Going Input	900 mV		
Negative Going Input			500 mV
Diff Input Resistance	30 k		80 k
Single Input Resistance	15 k		40k
Driver output current	-100 mA during short-circuit conditions		100 mA during short-circuit conditions
Driver input current	-4 mA		4 mA

APPENDIX B

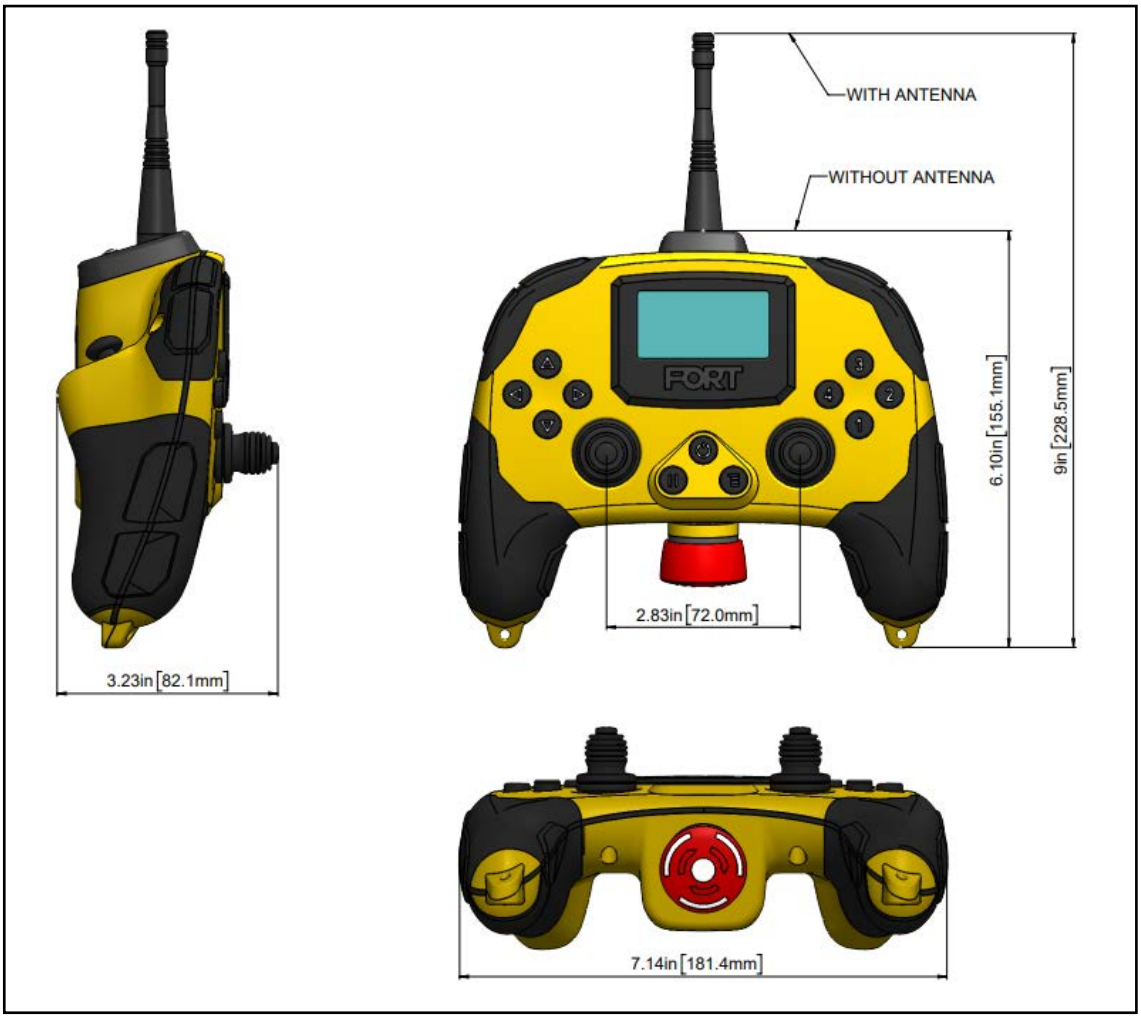
SRC Pro Technical Specifications

This appendix provides details of the Safe Remote Control Pro hardware.

SRC Pro Mechanical drawing

The following drawing shows the dimensions of the Safe Remote Control Pro 1000. Models SRC Pro 1001 and 1002 have larger antennas coming out the top.

FIGURE B-1. *SRC Pro Mechanical Drawing*



Recommended and Absolute Maximum Ratings (SRC Pro)

The following table lists the technical specifications for the Safe Remote Control Pro:

TABLE B-1. *(SRC Pro) Absolute and Recommended Specifications*

Specification	Min	Typical	Max
Vin (V)		5 VDC (USB)	
Current		1.6 A	
Weight		726 g | 1.6 lb	
Dimensions		181 mm x 155 mm x 83 mm 7.14" x 6.10" x 3.23"	
Ingress Protection		IP65	
Operating Temperature (internally limited)	-20 °C		60 °C
Charging Temperature (internally limited)	0 °C		45 °C
Battery Type		Lithium Polymer	
Battery Size		4000 mAh	
Charge Time		4.5 hours	
Run Time (Bluetooth)	19 hours		22 hours
Run Time (ISM)	18 hours		21 hours

Wireless Radio Specifications (SRC Pro)

You can configure the Safe Remote Control Pro with several different radios based on frequency requirements and local regulations. Prior to ordering and deployment, consult local regulations to ensure that you are installing the proper radio.

North America ISM Radio (SRC Pro)

The following table provides the specifications for North America ISM radio 902-928 MHz:

TABLE B-2. *(SRC Pro) North America ISM Radio Specifications*

Specification	Minimum	Typical	Maximum
Frequency	902 MHz		928 MHz
Bandwidth		600 kHz	
Channels		26	
Receive Sensitivity		-100 dBm	
Modulation		2-GFSK	
Baud Rate		500 kbps	
Power (conducted RF output)	-10 dBm		27 dBm
SRC Pro Part number	North America ISM radio is available in SRC Pro model 1001		

European ISM Radio (SRC Pro)

The following table provides specifications for the European ISM radio:

TABLE B-3. *European ISM Radio Specifications*

Specification	Minimum	Typical	Maximum
Frequency	869.4 MHz		869.653 MHz
Bandwidth		250 kHz	
Channels		1	
Receive Sensitivity		-100 dBm	
Modulation		2-GFSK	
Baud Rate		200 kbps	
Power (conducted RF output)	-10 dBm		27 dBm
SRC Pro Part number	EU ISM radio is available in SRC Pro model 1002		

Bluetooth Low Energy (BLE) Radio (SRC Pro)

The following table provides specifications for the BLE radio:

TABLE B-4. *BLE Radio Specifications*

Specification	Minimum	Typical	Maximum
BLE Version		5.1	
Baud Rate		1 Mbps	
Power (conducted RF output)			4 dBm
Receive Sensitivity	-99d dBm		

APPENDIX C *Safety*

This Appendix 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 an EPC or SRC pro is related to handling of the emergency stop (E-Stop) command.

A given Endpoint Controller, 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.

SRC Pro always acts as a sender device.

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

Safety Behavior of an EPC Sender

The external (customer supplied) sensing elements that are connected to the input(s) of the Endpoint Controller, generate a signal that indicates whether safety has been requested. The Endpoint Controller (more precisely: the safety processors of the Endpoint Controller) 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 Endpoint Controller.

The Application Processor takes the message and sends it to other receiver Endpoint Controller(s) via a communication link.

The AMCU of the receiving Endpoint Controllers receives the safety request messages and sends them serially to the onboard safety processors to be processed and acted upon.

Safety Behavior of an EPC Receiver

The Endpoint Controller receives remote safety request messages from an SRC Pro or another Endpoint Controller, 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 Endpoint Controller via a supported communication link.

The AMCU of the receiving Endpoint Controller 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-2 device

The emergency stop function is designed in compliance with SIL-2 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.

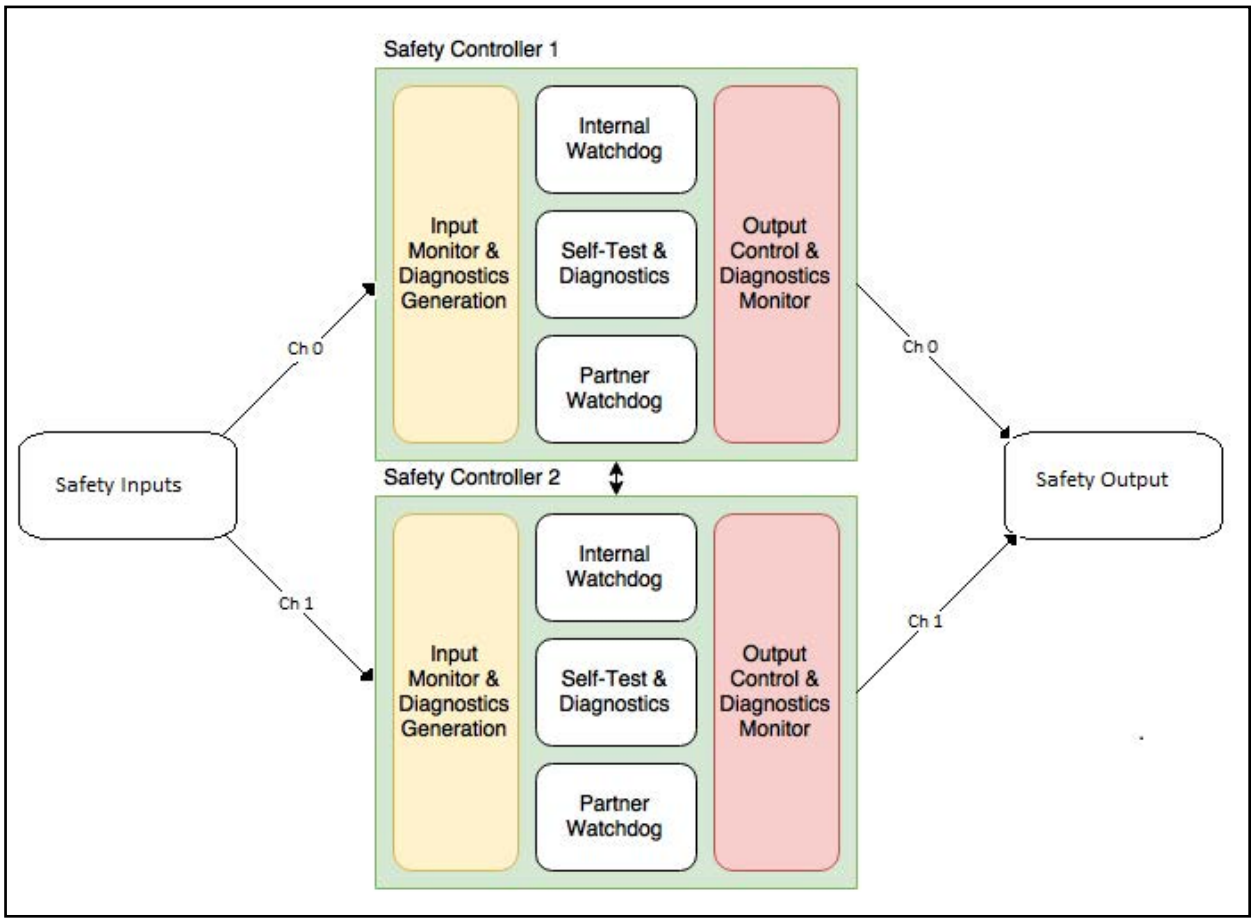
1oo2 Safety Architecture

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 Endpoint Controller and SRC pro with their own independent input circuitry, processing, output circuitry, and external monitoring (via a watchdog). The external watchdog is only required for EPCs and not SRC Pros.

The processors on the two redundant safety subsystems also communicate with each other through a serial link. The following diagram shows the 1oo2 architecture used in the Endpoint Controller and SRC pro:

FIGURE C-1. *1oo2 Safety Architecture*



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 (SRCP or EPC)** sends a safety message to request safety from the remote device(s).
- A **receiving device (EPC)** 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 (SRCP or EPC)** stops transmitting safety messages which triggers a timeout on receiving EPCs which then causes the receiving devices to turn off their output relays.
- A **receiving device (EPC)** 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). The following diagrams show the flow of safety data and commands, from one Endpoint Controller (EPC) to another Endpoint Controller, and from an SRC Pro to an EPC.

FIGURE C-2. *Command Flow from EPC to EPC*

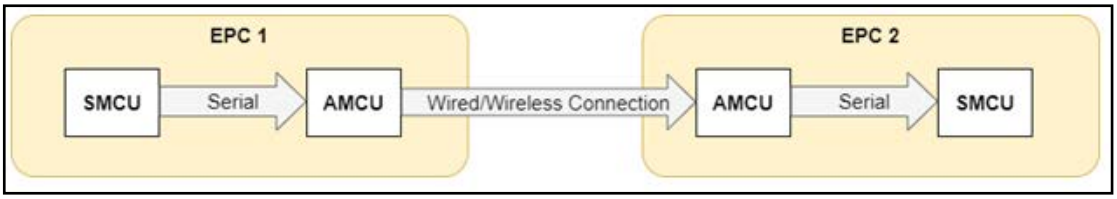


FIGURE C-3. *Command Flow from SRC Pro to EPC*

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 Inputs

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

The SRC Pro supports 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 Endpoint Controller. 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 Endpoint Controller 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.

Virtual Inputs

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

The Application Processor of the remote Endpoint Controller (EPC) receives the safety request message and then serially transmits the message to the SMCUs. The following diagram shows this message transmission:

FIGURE C-4. *Serial Communication*

Serial Communication with Application Processor (AMCU)

On a sender Endpoint Controller or SRC 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 Endpoint Controller **will** go to safe state if this failure lasts longer than the timeout value.

On a receiving Endpoint Controller, 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 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 both SRC Pro and EPC. 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 Endpoint Controller receives the safety request message from a remote Endpoint Controller or an SRC 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 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 1000 ms (1 sec).

Safety Processing

To comply with the 1oo2 safety architecture and SIL requirements, the safety portion of the Endpoint Controller and SRC 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 and SRC Pro.

EPC Safety Outputs

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

Each Endpoint Controller has 3 independent input-output pairs (input-output pair 1, input-output pair 2, input-output pair 3). An input of an input-output pair can only affect the output that it is paired with; so, for example, input of input-output pair 1 cannot affect the output of input-output pair 2 and the user will not be allowed to create such a configuration.

The output of each input-output pair 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.

Physical Outputs

Physical outputs are only applicable to receiver EPCs. 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 Endpoint Controller. 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 Endpoint Controller 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.

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 and Sender EPCs. Virtual outputs are safety request messages generated by the SMCUs of an Endpoint Controller or SRC 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 Endpoint Controller (EPC 1 in the diagram) or SRCP, which then transmits them using a wired or wireless link to the Application Processor (AMCU) of a remote Endpoint Controller that is connected to a machine. The Application Processor of the remote Endpoint Controller (EPC 2 or EPC in the diagram) receives the safety request message and serially transmits it to its SMCU as shown in the following diagram:

FIGURE C-5. *Serial Communication EPC - EPC*

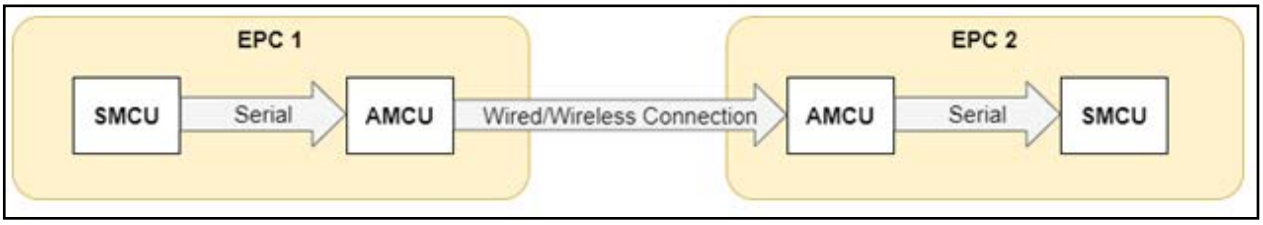
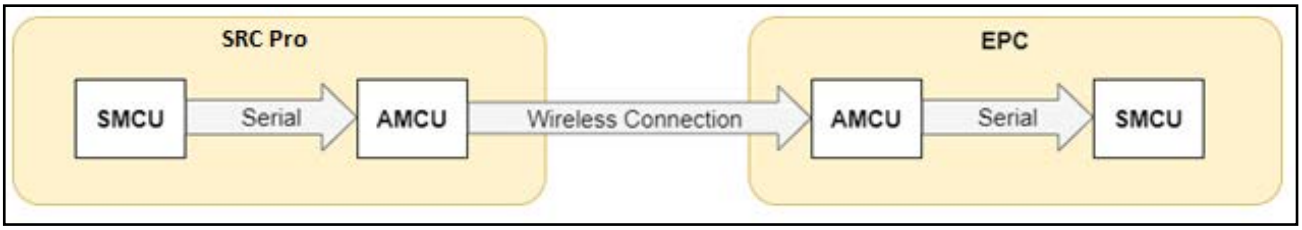


FIGURE C-6. *Serial Communication SRC Pro - EPC*



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.

User Selectable Safety Configurations

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

A user must configure an Endpoint Controller with FORT Manager before the device can be used in a runtime application. See "Configurations and Use Cases" on page 2-1. A subsequent power cycle of the Endpoint Controller does not erase the configuration stored in the device. Any re-configuration of an Endpoint Controller must be done by a user with FORT Manager.

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

- **Configuration:** Identify the sender(s) and receivers for the network.

- **Timeout Configuration:** Select one of the values 250ms, 500ms, 750ms or 1 second as a timeout.
- **Supply voltage configuration:** For each EPC device, select the supply voltage to the EPC, which can be either 12 or 24 Volts.
- **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.

Transferring Safety Configurations from Fort Manager to the EPC

When a user configures an Endpoint Controller with FORT Manager, FORT Manager is not in direct communication with the Endpoint Controller 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. See "Loading a Configuration onto Your Devices" on page 2-15. 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.

Mechanical and Electrical Safety (EPC)

The Endpoint Controller 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 (IP6*x* 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 C-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 IP*x*5 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 “Proof Testing” on page G-2 for a couple 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 (IP6*x* 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 C-2. *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 IP*x*5 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 “Proof Testing” on page G-2 for some suggested proof tests.

FMEDA Summary (EPC)

This section summarizes the expected failure rates for the Endpoint Controller 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 C-3. *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 C-4. *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 C-5. *EPC Failure Rates Good Maintenance Assumptions in FIT @SSI=2 EEC 61508*

Application/Device Configuration	λ_{SD}	λ_{SU}[a]	λ_{DD}	λ_{DU}	#	SFF
Sender	9,067	120	9,558	92	522	99.5%
Receiver	9.080	178	9,534	92	567	99.5%

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

Where:

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

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 (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 EPC using a site safety index (SSI) of 2 (good site maintenance practices).

TABLE C-6. *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 C-7. *SRC Pro Failure Rates Good Maintenance Assumptions in FIT @SSI=2 EEC 61508*

Application/Device Configuration	λ_{SD}	λ_{SU}[a]	λ_{DD}	λ_{DU}	#	SFF
SRC Pro	4811	64	5021	52	662	99.5%

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

Where:

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

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.

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 both EPC and SRC Pro is 50 milliseconds**.

All the EPC and SRC 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 C-8. *Table 50 Diagnostic Tests*

Test name / Description	Applicability	What does the test do	How often it runs
State of Inputs Checks the state of the E-Stop switch(es) or the solid state input device(s).	Sender EPC and SRC 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 Due to filtering, it may take up to 50ms to detect and declare a fault.
Output Command to State Comparison Compares the output command(s) vs the state of the output pin(s).	Receiver EPC	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 makes the comparison. There is no filtering of the comparison result.
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) The purpose of this test is to prevent 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	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. Note 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.
Communication Timeout Checks whether a communication timeout exists between the EPCs or between the SRC Pro and EPC. Note that the scope of this test/check is limited to the safety request message	Receiver EPC	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 (i.e., 250 ms, 500 ms, 750 ms, or 1 sec 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.

Test name / Description	Applicability	What does the test do	How often it runs
Checks for communication timeout between the two redundant safety processors	Sender EPC, receiver EPC, and SRC Pro	Each safety processor checks 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 the timeout counter for communication between the two safety processors. If a valid safety message is not received for 40ms, the fault is considered detected.
Other internal diagnostics that each safety processor runs to check the health of the system such as ADC, RAM, FLASH, CPU, etc.	Sender EPC, receiver EPC, and SRC 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. As soon as a fault is detected it takes effect (causes a reset of the safety processor).

APPENDIX D FORT CLI Configuration Tool

You use the FORT CLI Configuration tool on a Linux computer to load a configuration onto an Endpoint Controller or a Safe Remote Control Pro, and to update the Endpoint Controller firmware (you use the FORT Configuration Tool utility to update Safe Remote Control Pro firmware).

This chapter explains how to download and install the CLI Configuration tool and provides an overview of its functions.

Downloading the Tool

If you don't have CLI tool or want to be certain you have the most current version, you can download it from FORT Manager by using the following procedure.

TO DOWNLOAD THE CLI CONFIGURATION TOOL

(Requires DeviceManager or Admin role.)

1. Launch FORT Manager and enter your username and password when prompted.
2. Click **Firmware** in the left navigation pane.
3. Click **Download CLI Tool**.

FORT Manager downloads the file: `fort_cli_cfg-<version>.tar.gz` to the Downloads folder on your computer.

Installing the CLI Configuration Tool

To install and use the CLI Configuration tool you need the following items:

- Linux computer running Ubuntu 20.04 with Ethernet networking capability.
- Latest FORT CLI Configuration Tool (`fort_cli_cfg-<version>.tar.gz`).
  See previous section.
- You must install `pip` using the steps here: https://linuxize.com/post/how-to-install-pip-on-ubuntu-18.04/.

TO INSTALL THE CLI CONFIGURATION TOOL

1. Copy the tar archive file (`fort_cli_cfg-<version>.tar.gz`) from a directory on your Windows machine to the home directory on your Linux computer by using the secure copy command (`scp`)
   a. Open a terminal on a Windows machine.
   b. Type the following (replace the values in brackets with your values):
      `scp C:\<myDir>\fort_cli_cfg-<version>.tar.gz muser1@<ipaddress>:/home/<username>`

2. Open a terminal on your Linux machine.
3. Install the tool by using `pip` and the `.tar` file; navigate to the appropriate directory and use the following command:

   `pip install ./fort_cli_cfg-<version>.tar.gz`
4. Add yourself to the `dialout` user group so you won't need `sudo` permission when using the `fort_cli_cfg` tool to access the serial device:

   `sudo usermod -a -G dialout $USER`
5. Reboot your Linux machine.
6. Verify that the tool has been successfully installed and that you can run it by typing the following command in a terminal window:

   `fort_cli_cfg --version`

   If you see the version displayed, the tool is ready to use.
7. If you get a `command not found` error, verify that your `$PATH` variable contains `.local/bin`, which is where `pip` installs applications. For example, in a terminal, type:

   `echo $PATH (Enter)`

   `-bash: /home/user/.local/bin:/home/<username>/.local/bin:/usr/local/sbin: …`
8. If `.local/bin` is not in your `$PATH`, add the following line to your `.bashrc` file:

   `export PATH="$HOME/.local/bin:$PATH"`
9. Restart the terminal.

To get help with the options for this tool, open a terminal and type:

`fort_cli_cfg --help`

For step-by-step instructions on using this tool, see:

- "Loading a Configuration onto an EPC" on page 2-15.
- "Loading a Configuration onto an SRC Pro" on page 2-16.
- "Updating EPC Firmware" on page G-4.
- "Updating SRC Pro Firmware" on page G-5.

APPENDIX E Recommended Relays

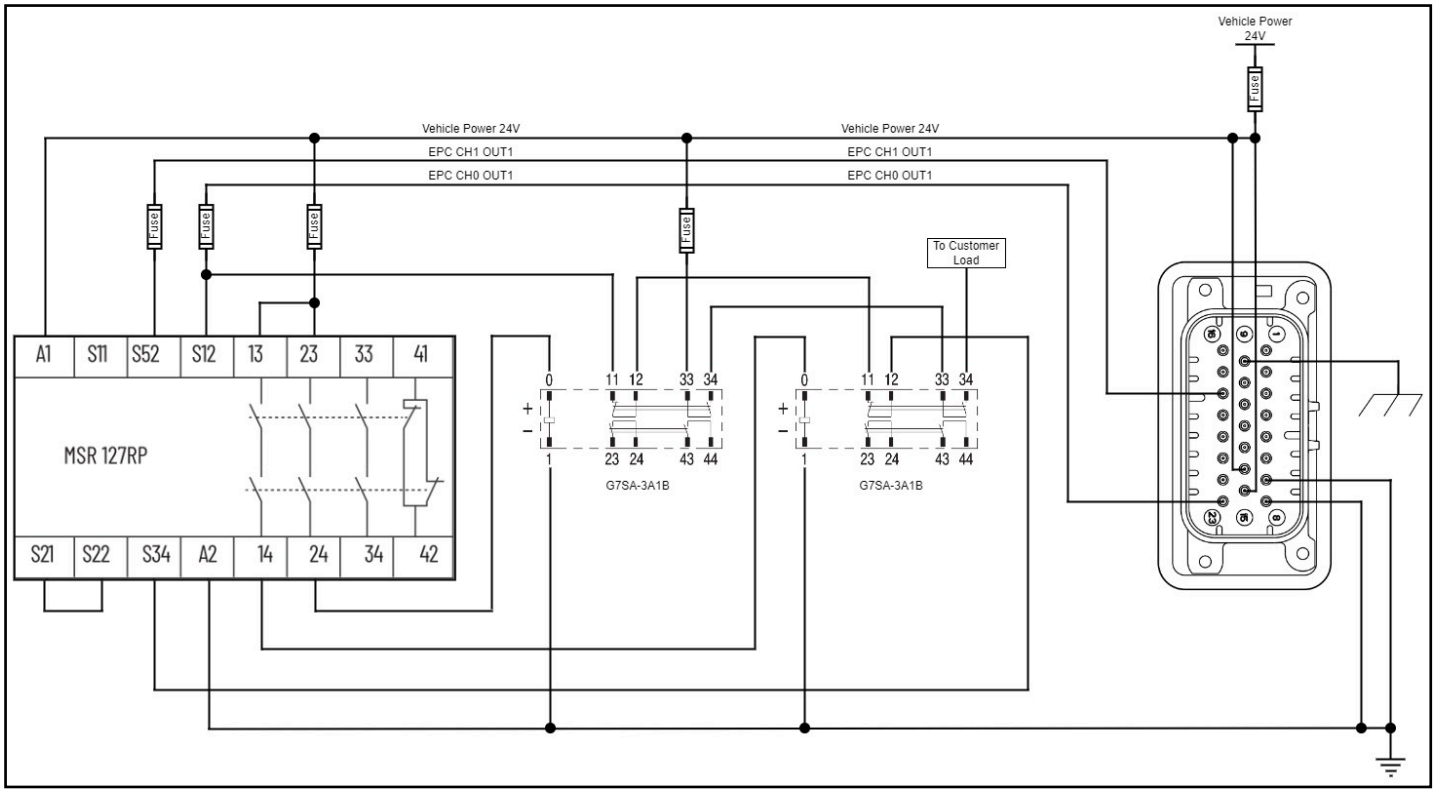
This appendix describes the relays that we have tested for use with an Endpoint Controller (listed in the table). The sections that follow provide a wiring diagram for each relay.

TABLE E-1. *Table 51 Recommended and Tested Relays*

Manufacturer	Model	Supply Voltage
Allen-Bradley	MSR127TP	24V
EATON	ESR5-NV3-30	24V
PILZ	751104	24V
IDEM	SCR-3-1P-i	24V
OMRON	G7SA-3A1B	24V
PANASONIC	SFS3-L-DC12V-D	12V

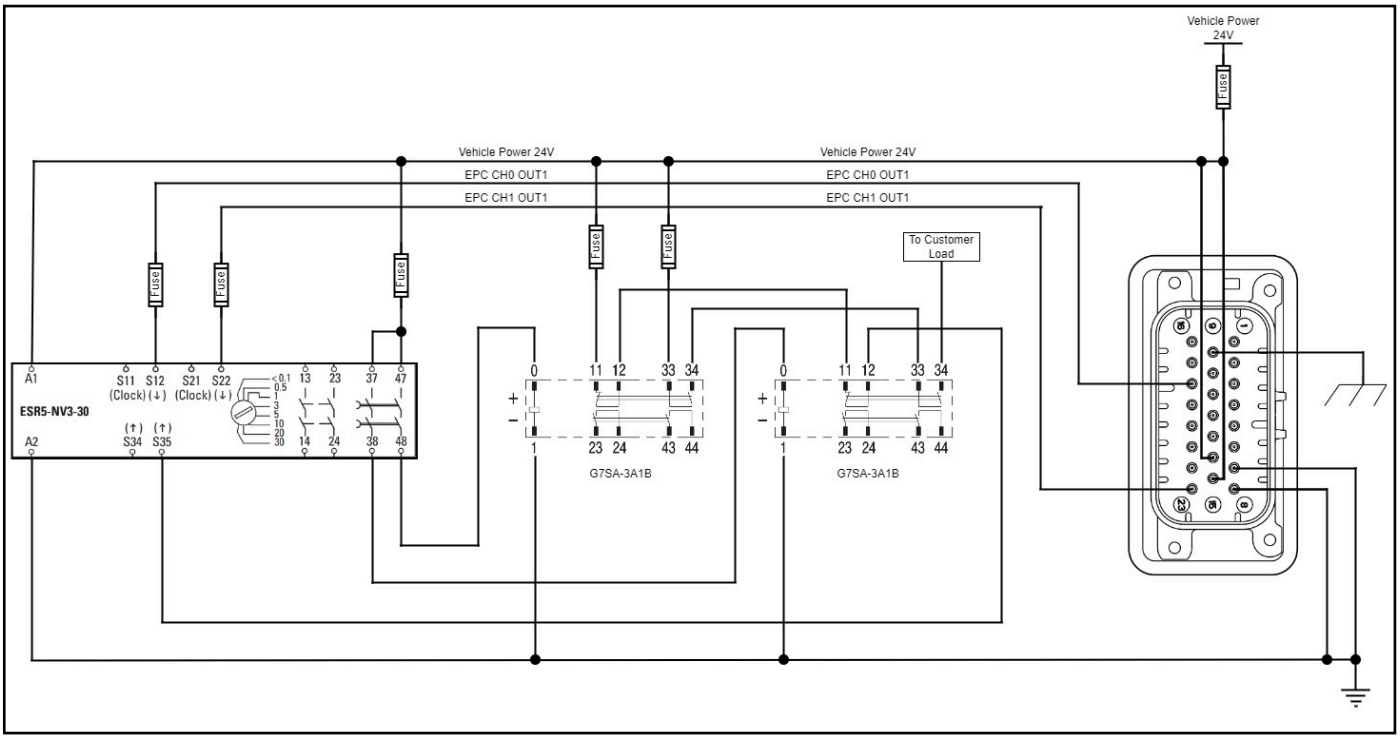
ALLEN-BRADLEY, MSR127TP

FIGURE E-1. *Allen-Bradley MSR127TP Relay Wiring Diagram*



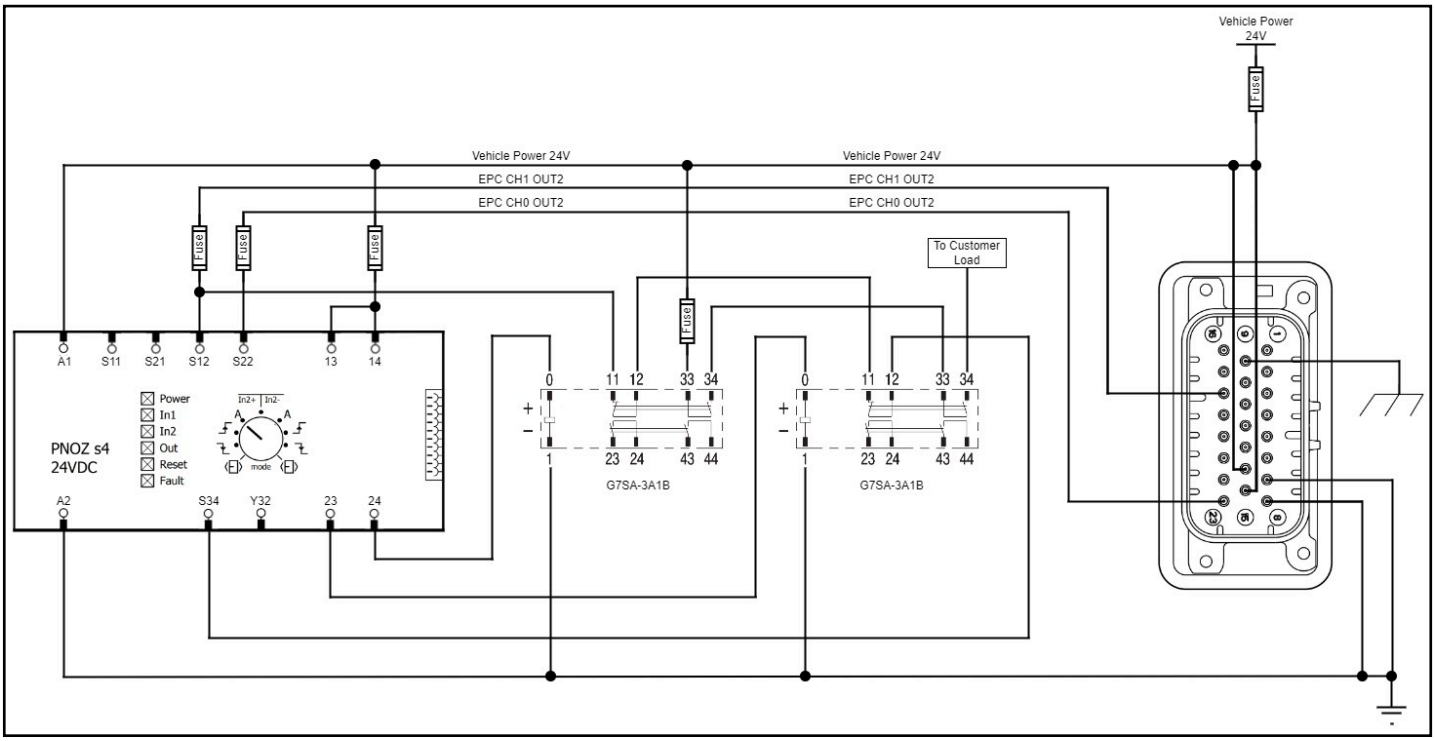
EATON ESR5-NV3-30

FIGURE E-2. *Eaton ESR5-NV3-30 Relay Wiring Diagram*



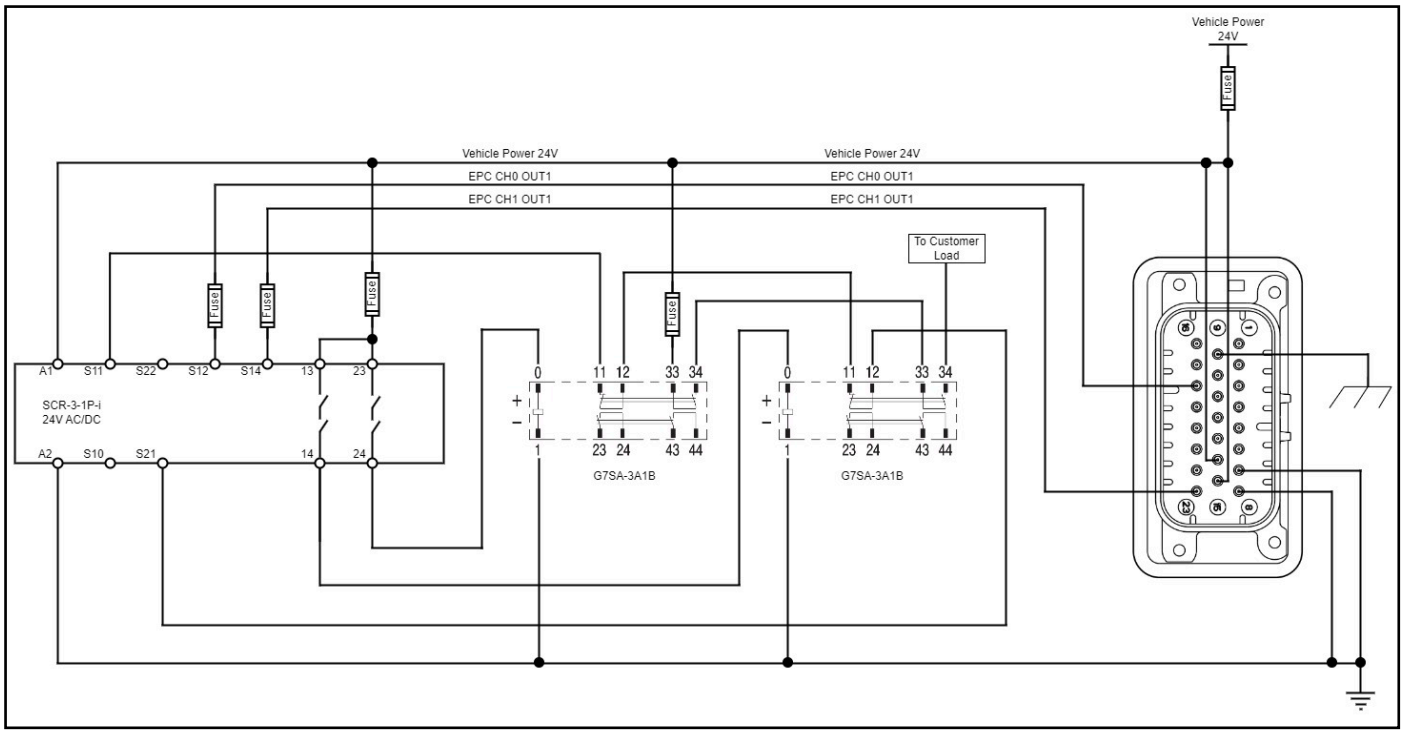
PILZ 751104

FIGURE E-3. *PILZ 7751104 Relay Wiring Diagram*



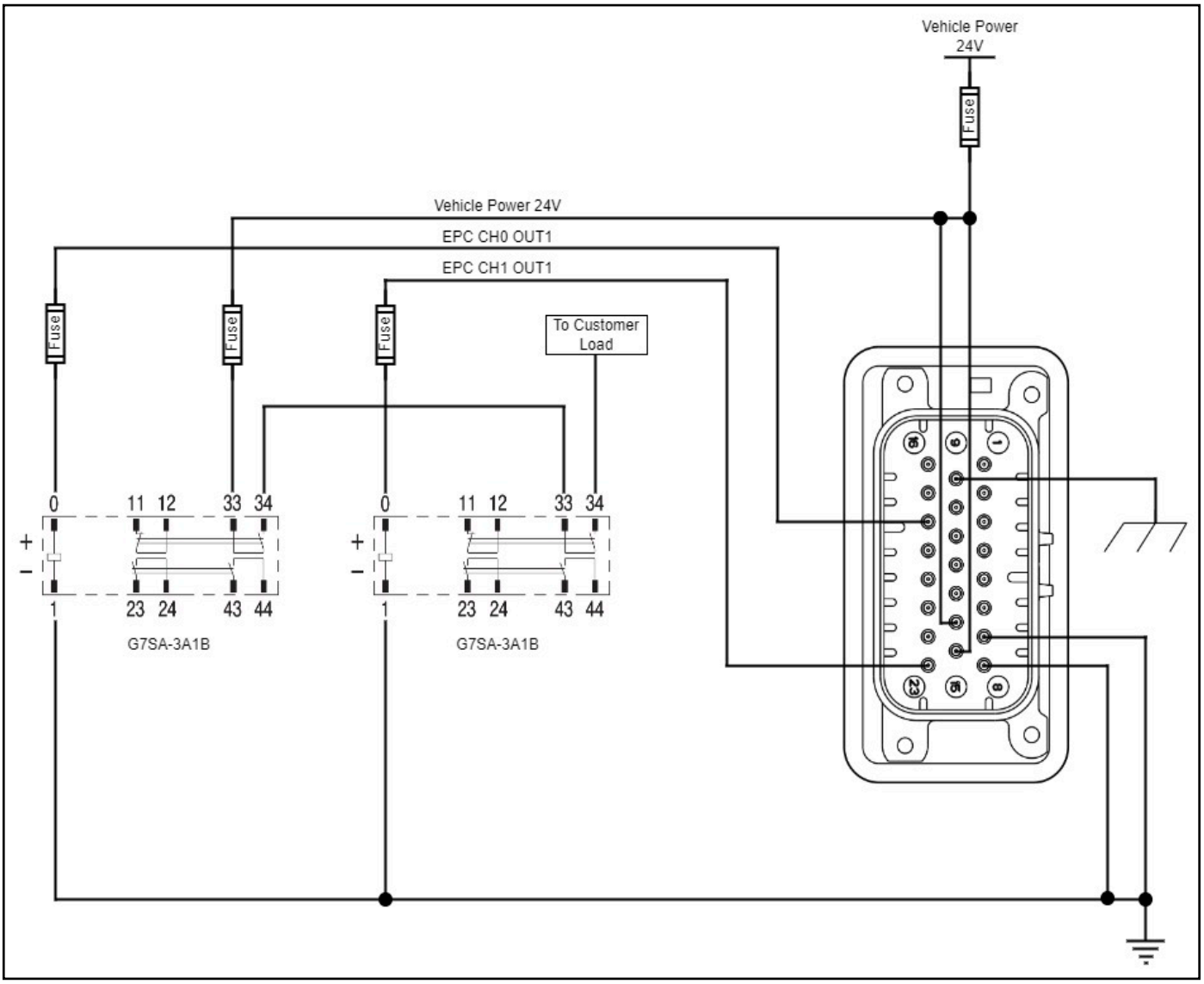
IDEM SCR-3-1P-I

FIGURE E-4. *IDEM SCR-3-1P-I Relay Wiring Diagram*



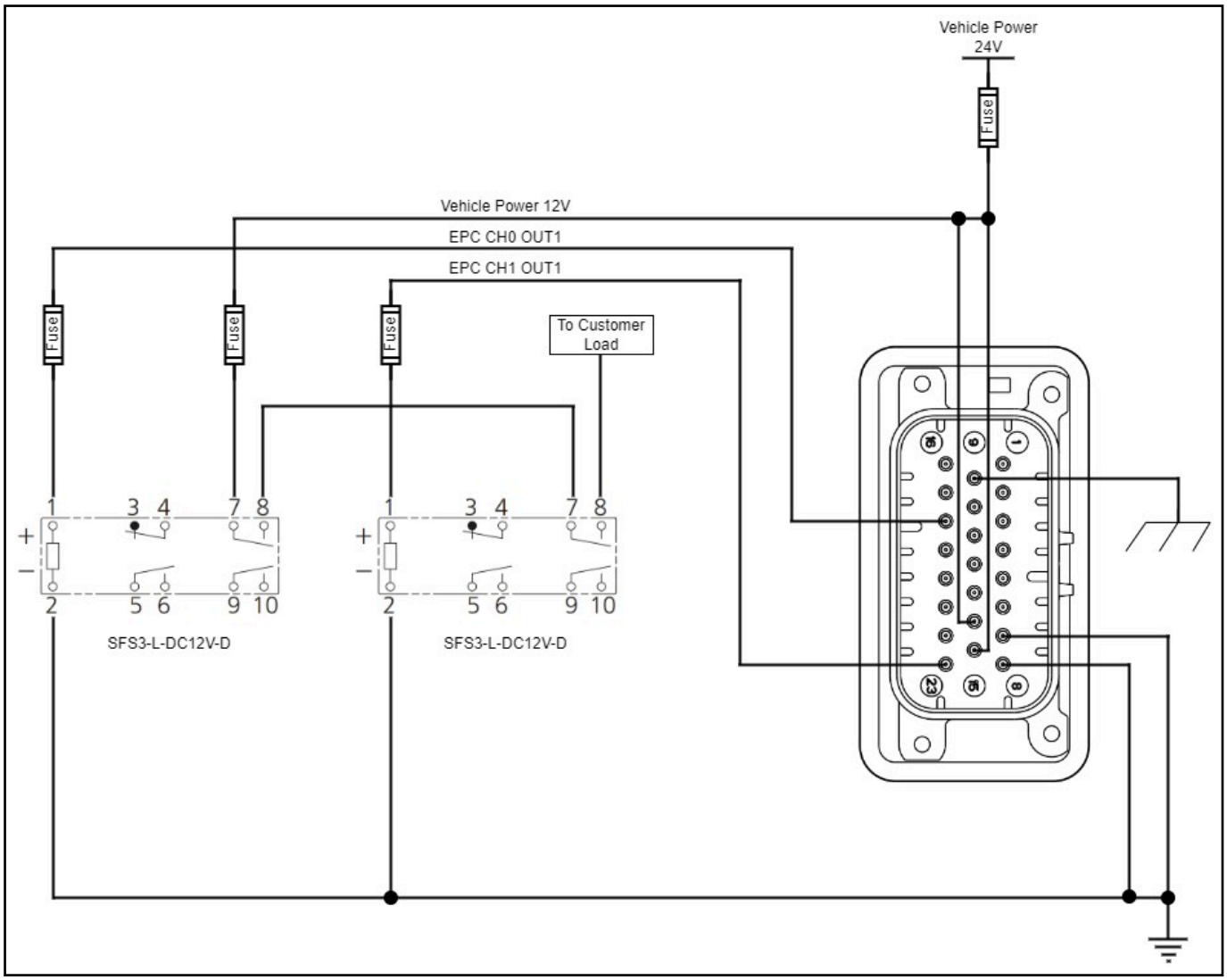
OMRON G7SA-3A1B

FIGURE E-5. *OMRON G7SA-3A1B Relay Wiring Diagram*



PANASONIC SFS3-L-DC12V-D

FIGURE E-6. *PANASONIC SFS3-L-DC12V-D Relay Wiring Diagram*



APPENDIX F *Notifications and Certifications*

This appendix provides notifications and certifications regarding the product described in the guide.

FCC Notifications

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: 1) This device may not cause harmful interference and 2) this device must accept any interference received, including interference that may cause undesired operation.

IC Notifications

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device must not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Ce dispositif est conforme aux norms permis-exemptes du Canada RSS d'industrie. L'opération est sujette aux deux conditions suivates: (1) ce dispositive peut ne pas l'interférence, et (2) ce dispositif doit accepter n'importe quelle interference, y compris l'interférence qui peut causer le fonctionnement peu desire du dispositif

The declaration of conformity is available upon request.

Certifications

The Endpoint Controller is in the process of certification for functional safety by Exida corporation.

APPENDIX G

Product Maintenance

This section explains how to care for your devices, how to handle a device that is damaged or fails for any reason, and how to update the firmware as necessary.

Care and Handling

The Endpoint Controller and Safe Remote Controller Pro are designed and built to operate in extreme environmental conditions and as such, have been subjected to rigorous mechanical and electrical tests. Keep the following points in mind when handling your devices:

- You can safely operate the EPC and SRC Pro in a humid or dusty environment without fear of damaging the device.
- You can operate both devices in the rain. However, when you are locating the EPC outside or attaching it to equipment that is operating outside or can be exposed to any amount of water, you must **mount the EPC vertically**. Mounting the EPC horizontally allows water to pool and block airflow through a membrane, potentially causing the EPC to malfunction.
- Avoid placing the EPC in an area or on a machine with extended exposure to direct sunlight.
- The SRC Pro and EPC are able to withstand an occasional drop from a height of one meter or less onto a hard surface, however, be careful not to repeatedly them. Although they are durable, they are not unbreakable, so (especially with the SRC Pro) **be careful not to set them down and run over them with heavy equipment.**
- You can clean them with a mild detergent and cloth.

⚠ CAUTION: Do not apply harsh chemicals to clean the SRC Pro and EPC. Do not immerse them in water, avoid spilling liquids on it (wipe them off immediately if this happens), and do not subject them to intense water jets.

Device Failure

⚠ CAUTION: The EPC and SRC Pro have no user-serviceable parts. Do not attempt to make any changes or repairs to these devices. If you have maintenance or repair questions fill out a request on the customer support portal: https://support.fortrobotics.com/.

If a device fails for any reason, do the following:

- Discontinue use.
- Reboot the device.

If rebooting does not resolve your issue, fill out a request on the customer support portal: https://support.fortrobotics.com/ to address the issue.

In the meantime, to keep your system functioning, you can use FORT Manager to replace the damaged device in your network if you have another device available. See "Configurations and Use Cases" on page 2-1.

Proof Testing

Before integrating an Endpoint Controller with your work environment — and at periodic intervals — you must perform some basic safety (proof) tests to detect dangerous hidden failures in the EPC's safety system. If the proof test detects any failures, you must perform immediate repairs to restore the system to its *as new* condition or as close to as new as possible.

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

⚠ WARNING: Safe operation of the system requires that you thoroughly test the system before putting it into a production environment. Testing includes training your personnel on both the manual functions (pressing an E-Stop button, using an SRC Pro to maneuver an EUC, etc.) and automatic functions of the system (solid state devices triggering safety, exceeding the timeout value, loss of radio signal, etc.).

We recommend the tests for an EPC to EPC configuration and one for an SRC Pro to EPC configuration, but you need to develop specific tests for each of your configurations as well.

TO PROOF TEST AN EPC TO EPC CONFIGURATION

⚠ WARNING: Before performing the following steps, ensure that you can perform all of these activities safely.

To verify that inputs connected to a sender EPC and outputs connected to a receiver EPC are working correctly and can cause an emergency stop on demand, perform the following procedure:

1. Make sure that the sender and receiver are up and running and communicating with each other.
2. While safety is *not* being requested by the *sender* EPC, measure the voltages at the input pins of the sending EPC.
   The voltages should be high and close to the supply voltage of the EPC.
   a. If any of the measured voltages is low, or much lower than the supply voltage, then a failure is present and you must inspect the wiring and the connected components to identify the source of failure.
   b. If no error is present, verify that the contactors of the relays attached to the *receiver* EPC(s) are all *closed*. If any of the contactors is open, investigate the source of the failure.
3. Request safety (by activating the safety sensor/element attached to the input(s) of the sending EPC); the contactors of the relays attached to the receiver EPC should all be *open*.
   a. Verify that both of the voltages at the input pins of the sending EPC indicate a low voltage. If one or both voltages are high, it indicates that a failure is present at the external input wiring (this includes switches or solid state devices that are connected to the inputs of the EPC). Inspect the wiring and connected input devices to find the source of failure.
   b. Verify that both contactors on the relays connected to the receiver EPC(s) are open. If one or both contactors are *not* open it indicates a failure is present. Inspect the wiring and the relays to find the source of failure.
4. Remove the request for safety and verify that the devices are up and running.

TO PROOF TEST AN SRC PRO TO EPC CONFIGURATION

⚠ WARNING: Before performing the following steps, ensure that you can perform all of these activities safely.

To verify that outputs connected to a receiver EPC are working correctly and can cause an emergency stop on demand, perform the following procedure:

1. While the SRC Pro is up and running, use machine select and mode select to connect it to a running EPC in the configuration.
2. While safety is *not* being requested, verify that the contactors on the receiver EPC are all closed.
   If any of the contactors is open, investigate and identify the source of the failure.
3. Request safety by pressing the E-Stop button on the SRC Pro and verify that both contactors on the relay connected to the receiver EPC are open.

   If one or both contactors are *not* open, which indicates a failure, inspect the wiring and the relays to find the source of the failure.
4. Remove the request for safety on the SRC Pro and verify that the devices are up and running.

Repeat this procedure for each EPC in the configuration.

Wireless Communication Loss

A wide range of events can cause loss of signal events; for example, moving the SRC Pro out of range of the Endpoint Controller, introducing enough interference or obstructions, turning off the Safe Remote Control Pro, or anything else that prevents communication between the devices.

During normal operation, a receiver Endpoint Controller expects to receive at least one valid safety message from the sender Endpoint Controller within the (user-configurable) timeout period or else it enters the safe state (turns off its outputs). If the Endpoint Controller stops receiving valid messages because of communication loss (or any other reason), once the timeout period is exceeded, the safety processor on the Endpoint Controller opens the safety relays to initiate the E-Stop command.

While performing safety tests on your Pro Series devices, verify that communication loss isn't affecting the performance of your equipment or causing unsafe operation. You can experiment with different values for the timeout while testing — 250 ms (default value), 500 ms, 750 ms, or 1000 (1 sec) — to address any issues you find. You set the timeout value in FORT Manager when building a configuration. See "Building an EPC to EPC Configuration" on page 2-2 or "Building an SRC Pro to EPC Configuration" on page 2-9.

A higher value, which makes the Endpoint Controller less sensitive to communication loss, means that if an Endpoint Controller loses communication with its sender, the EUC will run for a longer period before stopping automatically. On the other hand, a lower timeout value, which reduces the risk of the EUC running without connection to the safety controller, increases the sensitivity to communication loss.

⚠ **WARNING:** Once you put your system into production, we strongly recommend that you keep the default value (250 msec). If you consider changing the value, do so only after consulting with your system safety manager.

Updating EPC Firmware

All Endpoint Controllers come with the latest firmware preinstalled at the time of shipment. FORT releases periodic updates to the Endpoint Controller firmware for performance, safety, and security reasons.

⚠ **IMPORTANT:** Non-safety critical firmware updates are only available to customers whose device has an active Guardian subscription. Guardian allows you to get firmware and software updates, extended support, and warranty coverage beyond the limited one-year hardware warranty term.

FORT Customer Support notifies all customers through email regarding relevant firmware updates. The email includes an attachment with the firmware upgrade file, which is also available for download in FORT Manager. If you are not sure whether your firmware is up to date, or if you are eligible for updates, fill out a request on the Support Portal to get help.

This section shows how to update firmware on an Endpoint Controller in the field. It assumes default IP values; replace with your own as needed.

REQUIRED ITEMS

- Linux computer running Ubuntu 20.04 with Ethernet networking capability
  Use M12-RJ45 cable if connecting directly to the EPC (e.g., ASI-M12-RJ45-11101).
- Firmware upgrade file for the EPC.
  You can download an archive package that contains the latest version from FORT Manager (the procedure that immediately follows these bullets provides instructions for downloading and extracting the file).
- Latest FORT CLI Configuration Tool (`fort_cli_cfg`).
  If you don't already have this tool, you can download it from FORT Manager. See "FORT CLI Configuration Tool" on page D-1 for more information, including installation instructions for the tool.
- The 23-pin connector and cable and a power supply for the EPC. The mating connector to the EPC connector port is a TE 770680-1 and the cable is the FORT #100-0256 Integration Cable. See "I/O Connector Pinout and Cable".

TO DOWNLOAD EPC FIRMWARE UPGRADE FILE

(Requires DeviceManager or Admin role.)

1. Launch FORT Manager and enter your username and password when prompted.
2. Click **Firmware** in the left navigation pane to open the Firmware page.
3. Click the **Download** button in the **Action** column for **Endpoint Control (EPC)**.
   FORT Manager downloads the product update file to the Downloads folder on your computer.
4. (Optional, this step is required only if you are running FORT Manager in a browser on a different computer than your Linux computer, for example, on a Windows machine. If you are running FORT Manager on a Linux machine, you can skip this step.)
   Copy the file (`epc-prod-update-<vers>.tar.zst`) from a directory on your Windows machine to the home directory on your Linux computer by using the secure copy command (`scp`):

a. Open a terminal on a Windows machine.
b. Type the following (replace the values in brackets with your values):

```
scp C:\<myDir>\epc-prod-update-<vers>.tar.zst <user>@<ipaddress>:/home/<user>
```

Go to the next procedure to install the firmware file.

TO INSTALL THE EPC FIRMWARE UPDATE FILE

(Requires Admin or Operator role)

1. Connect the 23-pin connector to EPC and boot it up by applying power to `PVin_IN` (pins 14 & 15).
2. Connect your Linux computer to the EPC J2 port using an M12-RJ45 cable.
3. Open a terminal and execute the FORT CLI Configuration Tool:

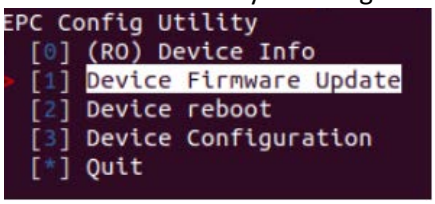
```
fort_cli_cfg -e 192.168.3.10 -m
```

Where:

`-e 192.168.3.10`
Specifies The EPC's IP address (default value, yours might be different).

`-m (--menu)`
Specifies the interactive menu option for the configuration tool.

4. Use the arrow keys to navigate to **Device Firmware Update** and press **Enter**.



5. Use the arrow keys to navigate to **Firmware Update** and press **Enter**.
6. Type the path to the update file and press **Enter**, for example:

```
./epc-prod-update-1014.tar.zst
```

Note that the update process may take up to three minutes to complete.
7. Use the arrow keys to navigate to **Device reboot** and press **Enter** to reboot the device.

To verify that the device firmware was updated successfully, do the following with the Linux computer still connected to the EPC:

1. Run the configuration tool again with the menu option:

```
fort_cli_cfg -e 192.168.3.10 -m
```

2. Use the arrow keys to navigate to **(RO) Device Info** and press **Enter**.
3. Use the arrow keys to navigate to **Version Info** and press **Enter**.

Updating SRC Pro Firmware

All Safe Remote Control Pros come with the latest firmware preinstalled at the time of shipment. FORT releases periodic updates to the Safe Remote Control Pro firmware for performance, safety, and security reasons.

⚠ **IMPORTANT:** Non-safety critical firmware updates are only available to customers whose device has an active Guardian subscription. Guardian allows you to get firmware and software updates, extended support, and warranty coverage beyond the limited one-year hardware warranty term.

FORT Customer Support notifies all customers through email regarding relevant firmware updates. The email includes an attachment with the firmware upgrade file. The file is also available for download in FORT Manager as described in the following procedure. If you are not sure whether your firmware is up to date, or if you are eligible for updates, fill out a request on the Support Portal to get help.

This section shows how to update firmware on a Safe Remote Control Pro in the field.

REQUIRED ITEMS

- Linux computer running Ubuntu 20.04 with Ethernet networking capability or a Windows machine.
  Use M12-RJ45 cable to connect directly to the SRC Pro (e.g., ASI-M12-RJ45-11101).
- Firmware upgrade file for the SRC Pro.
  You can download an archive package that contains the latest version from FORT Manager (the procedure that immediately follows these bullets provides instructions for downloading and extracting the file).
- Latest FORT CLI Configuration Tool (`fort_cli_cfg`).
  If you don't already have this tool, you can download it from FORT Manager. See "FORT CLI Configuration Tool" on page D-1 for more information, including installation instructions for the tool.

TO DOWNLOAD THE SRC PRO FIRMWARE UPGRADE FILE

(Requires DeviceManager or Admin role.)

1. Launch FORT Manager and enter your username and password when prompted.
2. Click **Firmware** in the left navigation pane to open the Firmware page.
3. Click the **Download** button in the **Action** column for **Safe Remote Control Pro (SRC)**.
   FORT Manager downloads the firmware update file to the Downloads folder on your computer. The file is in a compressed format but note that you *don't* need to uncompress it to install it.
4. (Optional, this step is required only if you are running FORT Manager in a browser on a different computer than your Linux computer, for example, on a Windows machine. If you are running FORT Manager on a Linux machine, you can skip this step.)
   Copy the file from a directory on your Windows machine to the home directory on your Linux computer by using the secure copy command (`scp`):
   a. Open a terminal on a Windows machine.
   b. Type the following (replace the values in brackets with your values):
   `scp C:\<myDir>\<device_firmware_file> <user>@<ipaddress>:/home/<user>`

Go to the next procedure to install the firmware file.

TO UPGRADE THE SRC PRO FIRMWARE:

(Requires Admin or Operator role)

1. Connect the USB port on the SRC Pro to your Linux computer.
2. Open a terminal and execute the FORT CLI Configuration Tool:
   Note that you need execute permission to `/dev/ttyACM0`.

```
fort_cli_cfg -n /dev/ttyACM0 -m
```

Where:

`-n (nxp) /dev/ttyACM0`
: Specifies an SRC Pro device and identifies the USB port in use; your port could be different.

`-m (--menu)`
: Specifies the interactive menu option for the configuration tool

3. Use the arrow keys to navigate to **Device Firmware Update** and press **Enter**.
4. Use the arrow keys to navigate to **Update From Bundle** and press **Enter**.
5. Type the path to the SRC Pro update bundle and press **Enter**, for example:

   `./<device_firmware_file>.zst`

   The device firmware file is in a compressed format, but you don't need to uncompress it.
   Note that the update process may take up to three minutes to complete.
6. Use the arrow keys to navigate to the main menu, select **Device reboot** and press **Enter** to reboot the device.

Calibrating Axis

The SRC Pro joysticks are calibrated at the factory, however, if you observe that the fingersticks and thumbsticks are not operating properly, follow the steps in these procedures to verify that the axis values are correct and to recalibrate them if necessary.

To Verify Calibration

1. Power on the SRC Pro, press the **Menu** button, and navigate to the **Settings** tab.
2. Press the down arrow key to scroll to and select **Axis Values**.
3. Press **1** and navigate to the **Calibration** tab.
4. Move each individual fingerstick and thumbstick around its full range of motion.

   Each axis should read 0 when the fingerstick or thumbstick is centered and the full range should be from -2048 to 2047.
5. Press **1** to exit the menu.

If the values you see are *not* correct, follow the steps in the next procedure to recalibrate your device.

To Recalibrate the SRC Pro

1. Power on the SRC Pro and press the **Menu** button.
2. Press the down arrow key to scroll to and select **Calibrate Axis**.
3. Press **1**.
4. Follow the on screen instructions to move each individual fingerstick and thumbstick around its full range of motion Up, Down, Left, Right).

   The screen displays an indicator of the current position and the full range that it has reached so far. You can press 2 at any point to exit the menu without applying the new calibration settings.
5. Let go of all fingersticks and thumbsticks when complete and press **1** to select the **Finish** option and accept the new calibration settings.
6. Press **1** or **2** to close.

7. Press the down arrow to scroll to and select **Axis Values** to verify the new calibration settings.
8. Move each individual fingerstick and thumbstick around its full range of motion.

   Each axis should read 0 when the fingerstick or thumbstick is centered and the full range should be from -2048 to 2047.
9. Press **1** to exit the menu.

Troubleshooting

> ⚠ **CAUTION:** The EPC and SRC Pro have no user-serviceable parts. Do not attempt to make any changes or repairs to these devices. If you have maintenance or repair questions fill out a request on the customer support portal: https://support.fortrobotics.com/.

If a device is not functioning properly, for any reason, we recommend discontinuing use and rebooting it to see if that corrects the problem. If it doesn't, fill out a request on the customer support portal: https://support.fortrobotics.com/ to address the issue.

APPENDIX H Revision History

The manual version corresponds to the product version[1]. The latest version is available on the customer support site.

This section describes the major updates in each release.

October 2023 Release

The *1.6.0* release introduces a new versioning scheme in which the version number of the book matches the product version number. For the current manual, which covers both EPC 1.6.0 and SRC Pro 4.6.2, we've chosen to use the EPC version number. In the future, we plan to release manuals that are targeted at a single product.

The *1.6.0* release *includes* the following major changes:

- The "FORT Manager" chapter has been updated with information about FORT Manager 2.0, the current *version*.
- The "CAN Application Support" chapter has been updated with new messages for EPC 1.6.0.

September 2023 Release

The 2023-08-28 release supports the GA releases of both the EPC and SRC Pro and includes the following *major* changes:

- Changed the style of page numbering and figure and table numbering to *Chapter-#* (*Appendix-#*), for example, pages in Chapter 3 are 3-1, 3-2, etc. and in Appendix B are B-1, B-2, etc. and figures and tables are Figure 3-1, Table 3-1, etc.
- Added a table of figures and a table of tables.

August 2023 Release

The 2023-08-28 release supports the GA releases of both the EPC and SRC Pro and includes the following major changes:

- Changed date format from *MM-DD-YYYY* to the international standard (ISO 8601) for dates (*YYYY-MM-DD*). The change is reflected in the manual version as well, which corresponds to the date.
- Clarified "Diagnostic Test Intervals", specifically in reference to the short to battery test.

1. The EPC version (1.6.*x*) for this release.

July 2023, Release

- Standardized alerts as could cause injury or death, could cause equipment damage, or is important not to miss. Added explanation in new front matter: "About this Guide" on page iii.
- Updated instructions for connecting an SRC Pro to an EPC in "Connecting the SRC Pro to an EPC" on page 4-3.
- Updated explanation of machine-select process and wiring in "Machine Select" on page 2-6.
- Updated "SRC Pro Mechanical drawing" on page B-2 and "SRC Pro Features" on page 4-1.
- Filled in details in multiple spec tables.

June 2023, Release

The release has the following major changes:

- Documented new ISM Transmission Channel settings in "Building an SRC Pro to EPC Configuration" on page 2-9.
- Updated process for "Updating SRC Pro Firmware" on page G-5.
- Added "Calibrating Axis" on page G-7.
- Added FMEDA summary for SRC Pro: "FMEDA Summary (SRC Pro)" on page C-13.
- Removed *Preliminary* watermark.
- Removed footnotes describing limit of one EPC in an SRC Pro or hybrid configuration. Limit is 30 as stated in the manual.

April 11, 2023, Release

The 4/11/2023 version has the following major changes:

- Page number total now includes prefatory pages (Title, Copyright, and TOC pages) so page numbers match the page number of the PDF file.
- Updated images for the SRC Pro and EPC.
- Documented new ISM settings (Low, Medium, High) in "Building an SRC Pro to EPC Configuration" on page 2-9.
- Added a section about "Proof Testing" on page G-2.
- Added information about connecting the J3 connector in "Loading a Configuration onto an EPC" on page 2-15 and "Connecting EPCs to a network" on page 2-18.
- Added a section on "Care and Handling" on page G-1.
- Removed the chapter "Verification of Safety Systems" and moved the material to "Product Maintenance" on page G-1.
- Rewrote the section "I/O Connector Pinout and Cable" on page 3-1 to be clear that the information in the table is about the connector signals, not about the cable.

- Rewrote instructions for using the CLI tool to update firmware, including information on using FORT Manager to download the tool and the firmware. Added the appendix: "FORT CLI Configuration Tool" that describes how to download and install the CLI tool.
- Added a section with the FMEDA summary for the EPC ("FMEDA Summary (EPC)" on page C-11) and the SRC Pro ("FMEDA Summary (SRC Pro)" on page C-13).
- Added a section about the "Diagnostic Test Intervals" on page C-13.

March 1, 2023, Release

The March 1, 2023, Release has the following major changes:

- Incorporated edits from multiple reviews.
- Added Chapter 4 about SRC Pro.
- Rewrote introduction.
- Rewrote procedures for loading configurations.
- Added chapter about using FORT Manager.

Pre-releases

Version	Date	Changes
A	11/30/2020	Initial Release
B	12/23/2020	Revise Figure 3 and Figure 4
C	1/13/2021	Remove Orderable Parts Tables, Revised Installation section
D	2/1/2021	Correct typo of CAN Hi pin in pinout table
E	7/14/2021	Revision History moved to top of doc, Added CANopen Implementation Section
F	5/27/22	Complete overhaul, new organization, new title, new sections, new style (removed numbering in heads), FORT Manager & CLI tool configuration info, etc.
G	6/14/22	Added Title page from product marketing, formatted document for two-sided printing (even and odd pages), fixed branding issues, added firmware update instructions. Removed 'Draft' watermark.
H (*draft*)	8/17/22	Added Configurations and Safety (draft) sections. Rewrote and expanded intro. Wrote section about safe state and normal state. Added Security section outline.
I (draft)[a]	1/13/23	Changed Heading 1s to Chapter – Appendix format. Added some details to Chapter 6 Security. Reorganized and simplified Chapter 3 Configurations. Rewrote Safety chapter. Added multiple figures and rewrote text for Chapter 3 Installation.

a. Part number 400-0044 (https://hri.aligni.com/part/405102).

APPENDIX I *Warranty*

You can view the End-User Agreement here: https://fortrobotics.com/end-user-agreement/.

You can view the OEM Supply and License Agreement here: https://fortrobotics.com/oem-agreement/.

We provide non-safety critical firmware updates to customers whose device has an active Guardian subscription. Guardian allows you to get firmware and software updates, extended support, and warranty coverage beyond the limited one-year hardware warranty term.