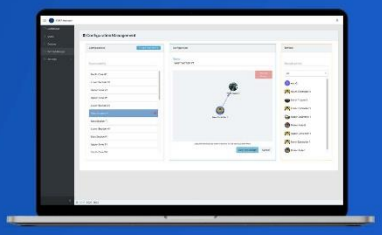
FORT PRO SERIES

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



FORT Robotics, 2023, fortrobotics.com

Part number 400-0044

March 2023

Version 1.0 3/1/2023

FORT Robotics
1608 Walnut St floor 12
Philadelphia, PA 19103

Contents

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 full-stack solution 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 documentation for the FORT APIs at: https://support.fortrobotics.com/hc/en-us/categories/9353447729691-Developer-Portal (requires FORT Zendesk login credentials).

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.

Key Features

The **Safe Remote Control Pro** 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).
- Six proportional analog controls, 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 with 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 Appendix B: Safe Remote Control Pro Technical Specifications on page 74 for detailed technical specifications for the Safe Remote Control Pro.

The **Endpoint Controller** supports integration into a wide variety of simple, semi-autonomous, and very intelligent systems. Its flexible solid-state inputs and outputs support commonly used industrial control systems and safety field devices. 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 Appendix A: Endpoint Controller Technical Specifications on page 67 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.[1]

The following figure illustrates a basic configuration:

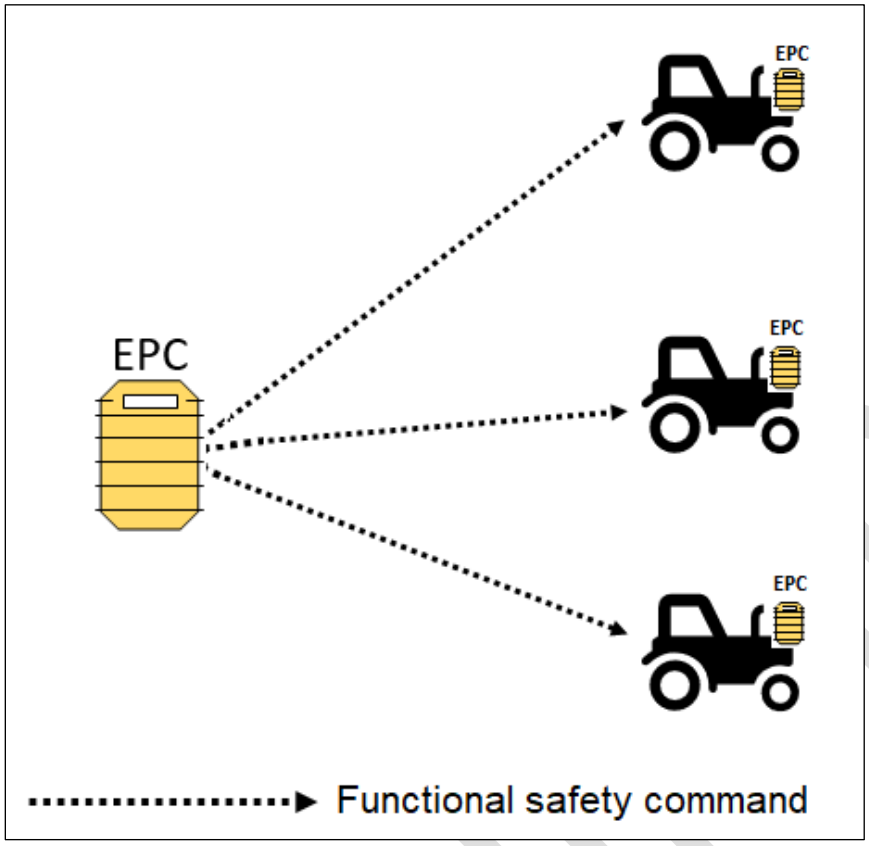


Figure 1 Basic Configuration

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.

[1] 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), or to a particular part of the equipment (to stop a robotic arm).

- 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. Chapter 2: Configurations and Use Cases on page 4 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 (Chapter 2: Configurations and Use Cases on page 4):
  - 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 20).
- **Wire** — Wire the inputs and outputs (Chapter 3: Installation — Wire and Mount EPC on page 23):
  - 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.

⚠ **IMPORTANT**: 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 at https://www.fortrobotics.com/start 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, and so on.

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 (https://support.fortrobotics.com/) to get help. Click **Sign up** to create a Zendesk account if you don't already have one.

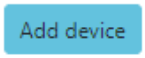
TO ADD DEVICES TO FORT MANAGER:

(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, 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** — 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** (page 7) — 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[2]) to send safety and control signals.
- **SRC Pro and EPC Hybrid Configuration** (page 13)— An Endpoint Controller and Safe Remote Control Pro are both able to communicate with multiple Endpoint Controllers (up to 30[2]). 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[2]) 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:

[2] For this release, an SRC Pro or SRC Pro Hybrid configuration allows only one EPC. Later releases allow up to 30 EPCs as stated.

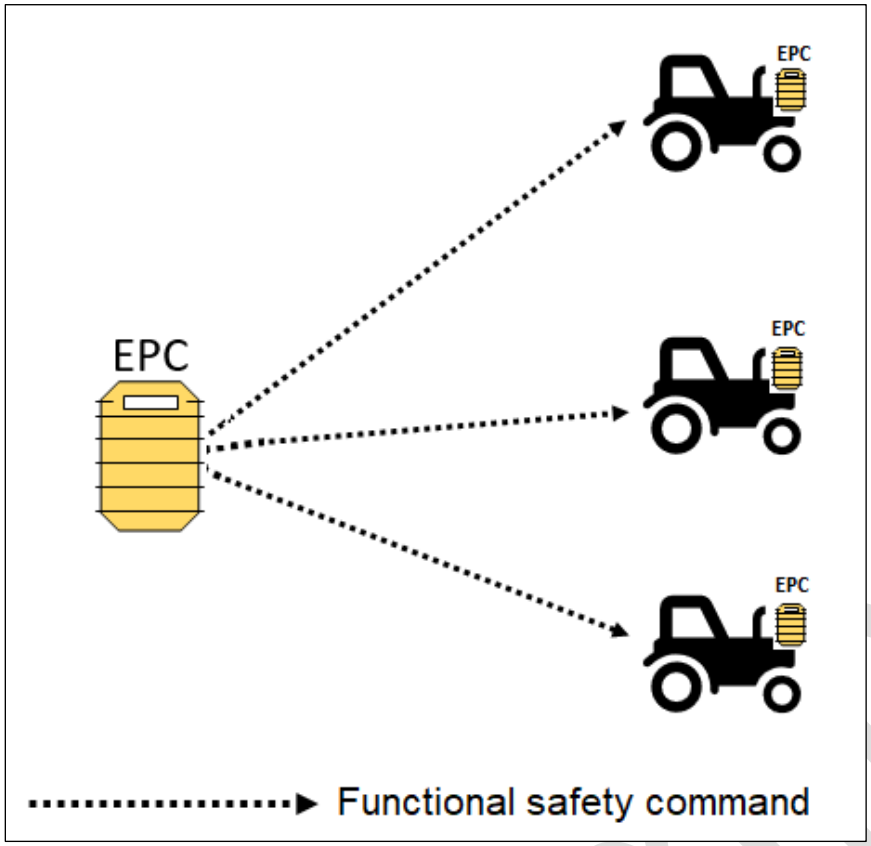


Figure 2 EPC to EPC Configuration

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

Table 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

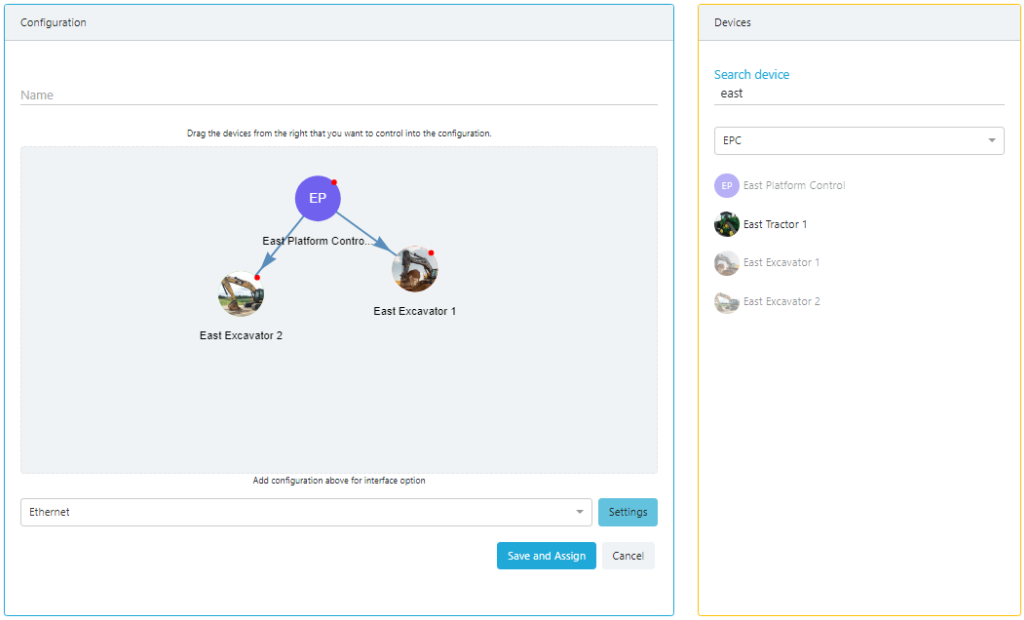
This procedure shows how to build a configuration that consists of one Endpoint Controller sender and up to 30 Endpoint Controller receivers.

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 username and password 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.
     - **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 (250 msec default).

⚠ **WARNING:** 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 EPC 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.

- **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

a. If you select a CAN mode, accept, or change the value in **CAN Bitrate** (250 kbit default).
b. 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 11 you have the option to change the CAN ID.

9. 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 the IP address for the device, for example: 192.168.1.2.
   - **Input1**, **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.
10. Click **OK** to save the settings for the sender; the green dot indicates that you have set required parameters.
11. 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 the IP address for the device, for example: 192.168.1.2.
    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.

       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.

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

12. Repeat the previous step to assign an IP address to every EPC receiver in the configuration (and optionally change the Node ID or address.
13. 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 Device Configuration onto an EPC and SRC Pro on page 20 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[3]). 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 unsupervised mode (see Machine Select on page 11).

[3] For this release, an SRC Pro configuration allows only one EPC. Later releases allow 30 EPCs as stated.

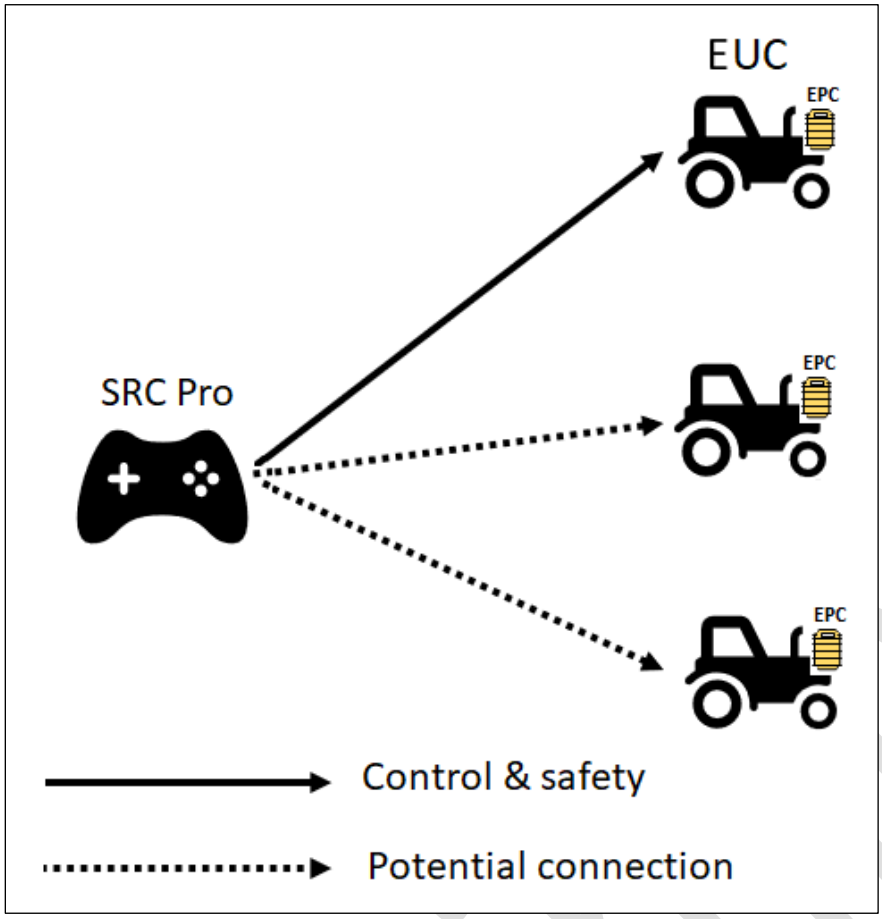


Figure 3 SRC Pro to EPC configuration

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

Table 2 SRC Pro to EPC configuration

Sender	Inputs	Receivers	Communication
SRC Pro	Integrated E-Stop switch	Up to 30[4] 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 (by picking from the list that is displayed on the LCD screen) and connect to one Endpoint Controller[4] at a time.

[4] For this release, only one EPC is allowed in an SRC Pro or SRC Pro Hybrid configuration. Later releases allow up to 30 EPCs as stated.

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 unsupervised 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, gyroscope measurements, 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.

Supervised mode works for both autonomous and non-autonomous machines. As shown in the following figure, you must connect Output 3 on each of the Endpoint Controllers (EPC) to the equipment under control (EUC).The section, Wiring Outputs on EPC Receivers on page 30 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 unsupervised mode. See Figure 5 for the wiring for machines that do require unsupervised mode.

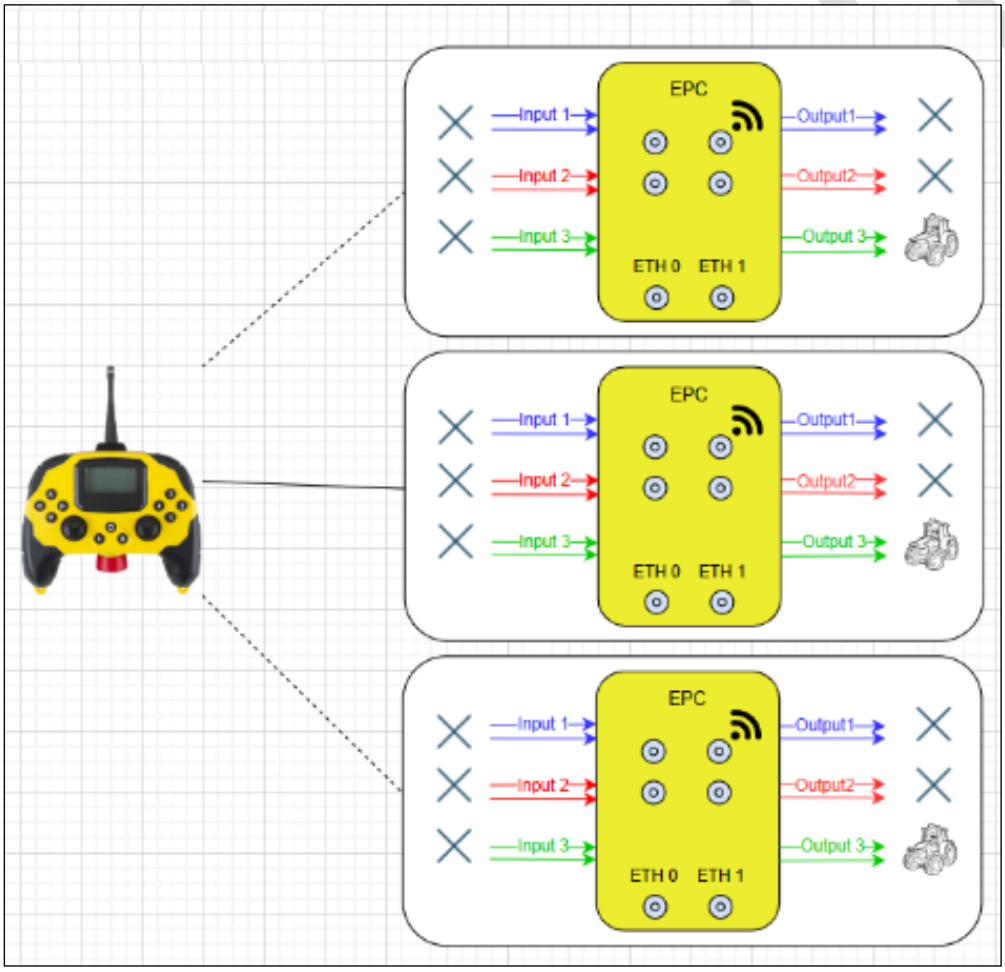


Figure 4 Machine Select Supervised Mode

Unsupervised mode is meant to be used with machines that have autonomous capability.

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 unsupervised.

In unsupervised 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; and the Endpoint Controller ignores 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.

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

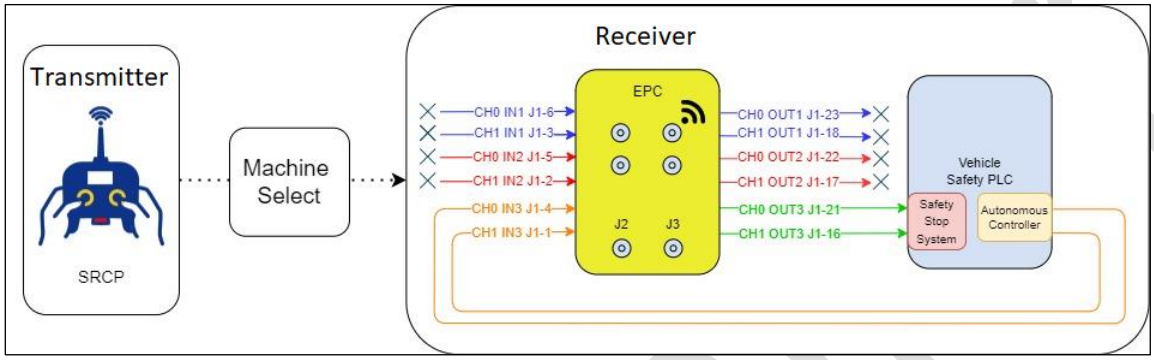


Figure 5 Input 3 Asserted on EPC Receiver

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.

The customer safety signal must be present before the mode switch to unsupervised mode, otherwise a safe state is triggered.

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[5] 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 18.

TO BUILD A CONFIGURATION WITH AN SRC PRO REMOTE:

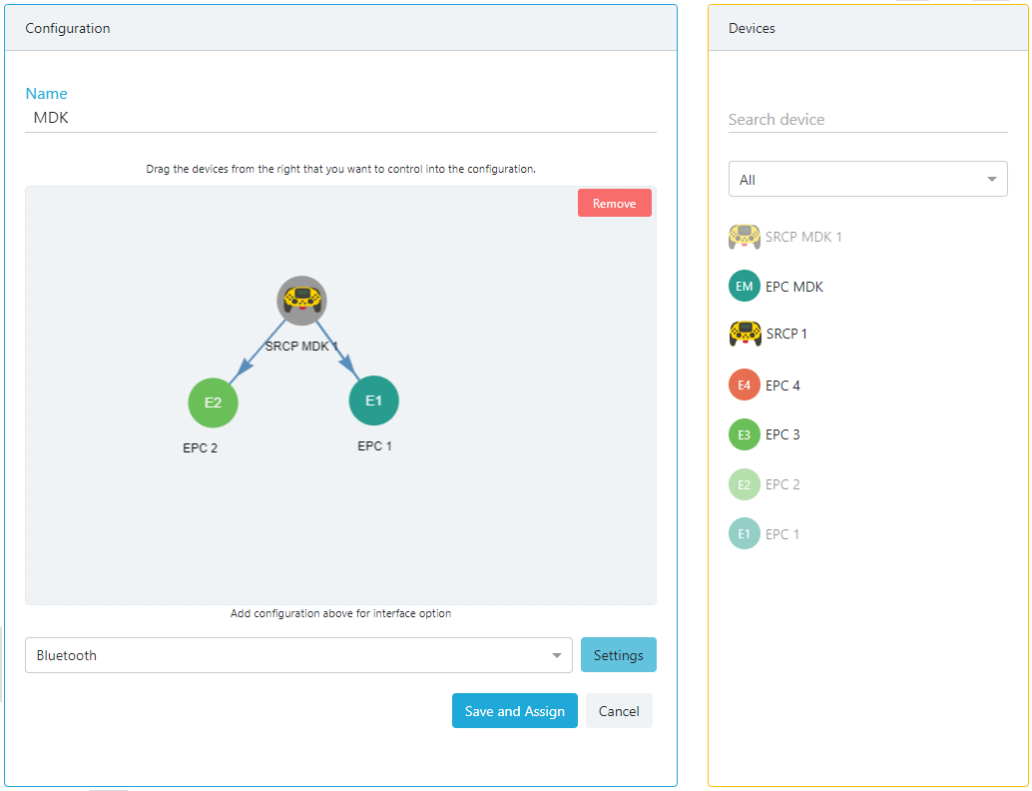
(Requires ConfigManager or Admin role.)

[5] For this release, an SRC Pro configuration allows only one EPC. Later releases allow 30 EPCs as stated.

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

> ⚠ **IMPORTANT:** For the initial GA release, do *not* add multiple EPCs to this configuration. This release supports one EPC only in an SRC Pro configuration. Later releases allow up to 30 EPCs as stated.



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 settings (if you selected ISM)
     - **ISM Network ID** Enter a numeric value between 1 and 128.
     - **ISM Transmission Power** Default is 5.
     - **ISM Transmission Channel** Default is 1.
   - **Safety Timeout:** Select a value for the safety communication timeout (250 msec default).

⚠ **WARNING:** 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 EPC 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.

- **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, or change the value.

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 the 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).
    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 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.

    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 Device Configuration onto an EPC and SRC Pro on page 20 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 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[6]) 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 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.

[6] For this release, an SRC Pro or SRC Pro Hybrid configuration allows one EPC only. Later releases allow 30 EPCs as stated.

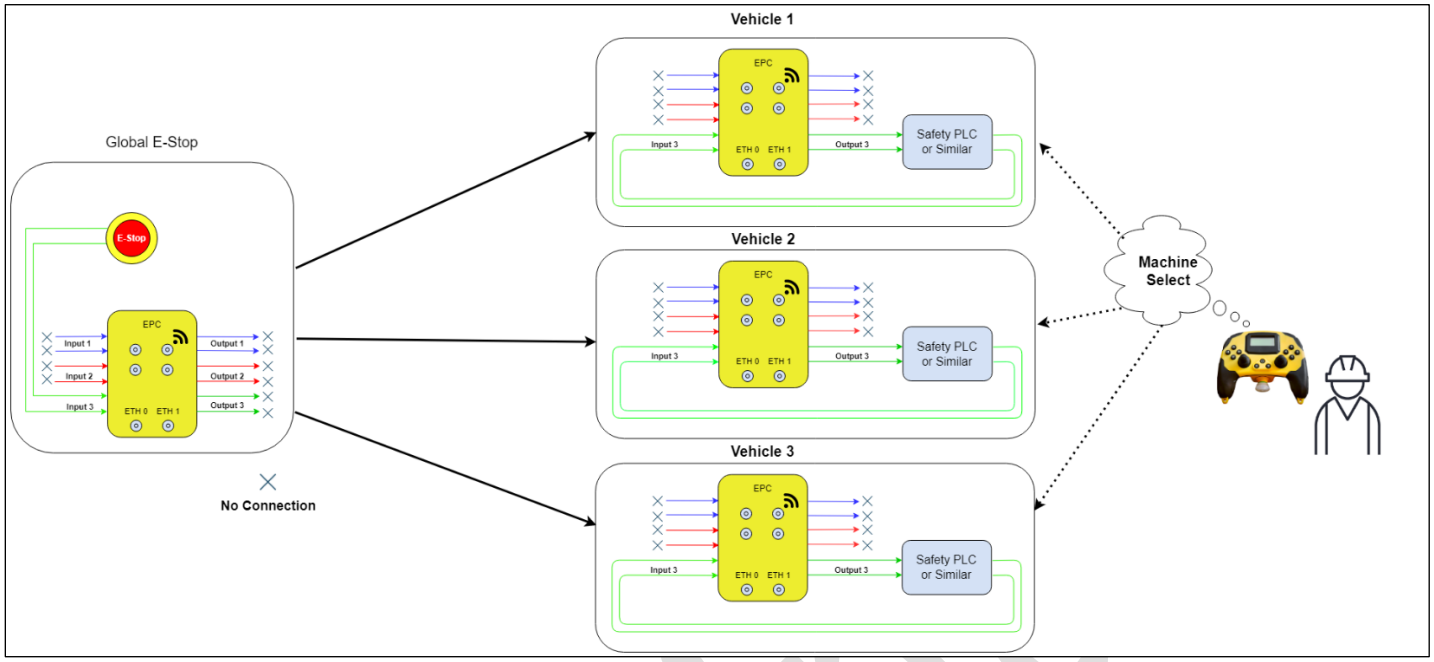


Figure 6 SRC Pro and EPC Hybrid Configuration

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[7] on the Endpoint Controller or the E-Stop button on the Safe Remote Control Pro turns off Output 3 on the receiver Endpoint Controller (and note that the Safe Remote Control Pro only affects the connected machine, 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 unsupervised mode, only pressing the global E-Stop[7] 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 3 SRC Pro and EPC Hybrid configuration

[7] 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.

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[8] 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[8] 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 Hybrid configuration.

BEFORE YOU BEGIN

This section assumes that you have already built and identified a configuration to use as the base for the Global E-Stop configuration. If not, follow the steps in Building an SRC Pro to EPC Configuration on page 13 to build a configuration with a Safe Remote Control Pro and up to 30[8] 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 username and password 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** 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.
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 13 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**.

[8] For this release, an SRC Pro or SRC Pro Hybrid configuration allows one EPC only. Later releases allow 30 EPCs as stated.

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

> ⚠ **IMPORTANT:** 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 Loading a Device Configuration onto an EPC and SRC Pro on page 20 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`).
  You should have received this file in a confirmation email package when you purchased your FORT devices —but if not, you can download it from FORT Manager (see Appendix D: FORT CLI Configuration Tool on page 85 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.
2. Connect your computer over Ethernet to port J2 on the EPC.
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.

   You are prompted to connect to FORT Manager and enter your email address:

   ```
   Connect to FORT Manager at https://app.fortrobotics.com/
   Enter User ID (email):
   ```

5. Type your FORT Manager email address and press **Enter**.
   You are prompted to enter your password:

```
Password:
```

6. Type your FORT Manager password and press **Enter**.
   You are prompted to enter the device serial number:

   ```
   Enter device serial number:
   ```

7. Type the serial number (found on the EPC device name place and also in FORT Manager on the Devices page) and press **Enter**.
8. Press **Enter** to load the configuration to the device.
   The tool finishes with the EPC by writing all the relevant configuration parameters.
9. Reboot the EPC.

Repeat this procedure for each Endpoint Controller in your configuration.

If your configuration has a Safe Remote Control Pro as the sender, complete the steps in the following procedure to load the configuration onto it.

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`).
  You should have received this file in a confirmation email package when you purchased your FORT devices —but if not, you can download it from FORT Manager (see Appendix D: FORT CLI Configuration Tool on page 85 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 the following command to launch the configuration tool for the SRC Pro:

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

   Where:

   `-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..

   You are prompted to connect to FORT Manager and enter your email address:

   ```
   Connect to FORT Manager at https://app.fortrobotics.com/
   Enter User ID (email):
   ```

5. Type your FORT Manager email address and press **Enter**.
   You are prompted to enter your password:

   ```
   Password:
   ```

6. Type your FORT Manager password and press **Enter**.
   You are prompted to enter the device serial number:

   ```
   Enter device serial number:
   ```

7. Type the serial number (found on the SRC Pro device and also in FORT Manager on the Devices page) and press **Enter**.
8. Press **Enter** to load the configuration to the device.
   The tool finishes with the SRC Pro by writing all the relevant configuration parameters.
9. Reboot the SRC Pro.

Once you complete the steps in Loading a Configuration onto an EPC on page 20 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.

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 I/O connector pinout (the same on a sender or receiver Endpoint Controller). The table after the figure lists the connectors for the integration cable used to connect devices to an Endpoint Controller (also used for both senders and receivers). Refer to this diagram and figure when wiring devices to an Endpoint Controller sender (Wiring Inputs on EPC Sender on page 27) or receiver (Wiring Outputs on EPC Receivers on page 30).

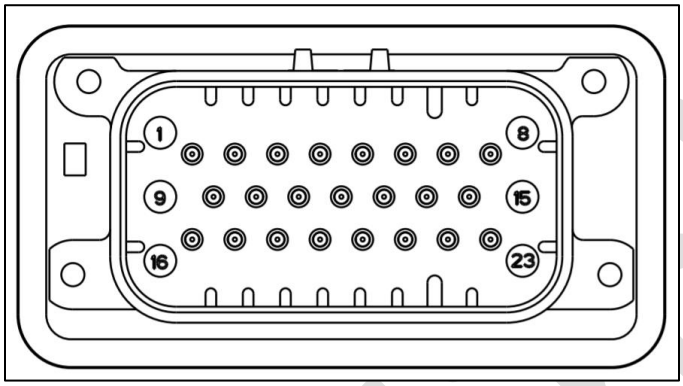


Figure 7: EPC I/O Connector Pinout (TE 1-776228-1)

> ⚠ **IMPORTANT:** In the following table, all wire colors apply to the FORT Part #100-0256 Integration Cable. All white cables have their pin number printed directly on the cable. The suggested mating connector to this port is a TE 770680-1.

Table 4: Connector pinouts

Pin #[9]	Name	Description	Wire Color FORT integration cable #100-0256[10]
1	IN5_CONN	Channel 1, Input 3	White
2	IN4_CONN	Channel 1, Input 2	White
3	IN3_CONN	Channel 1, Input 1	White

[9] Connector pinouts and signal descriptions are subject to change before release.
[10] Wire colors apply to the FORT Part #100-0256 integration cable.

Pin #[9]	Name	Description	Wire Color FORT integration cable #100-0256[10]
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[11]	PVin_RTN	Voltage Negative Polarity	White
8[11]	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 section 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 section after the table for wiring details.	
14[12]	PVin_IN	Voltage Positive Polarity	White
15[12]	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

[11] Connect Pins 7 & 8 together at the same place.
[12] 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:

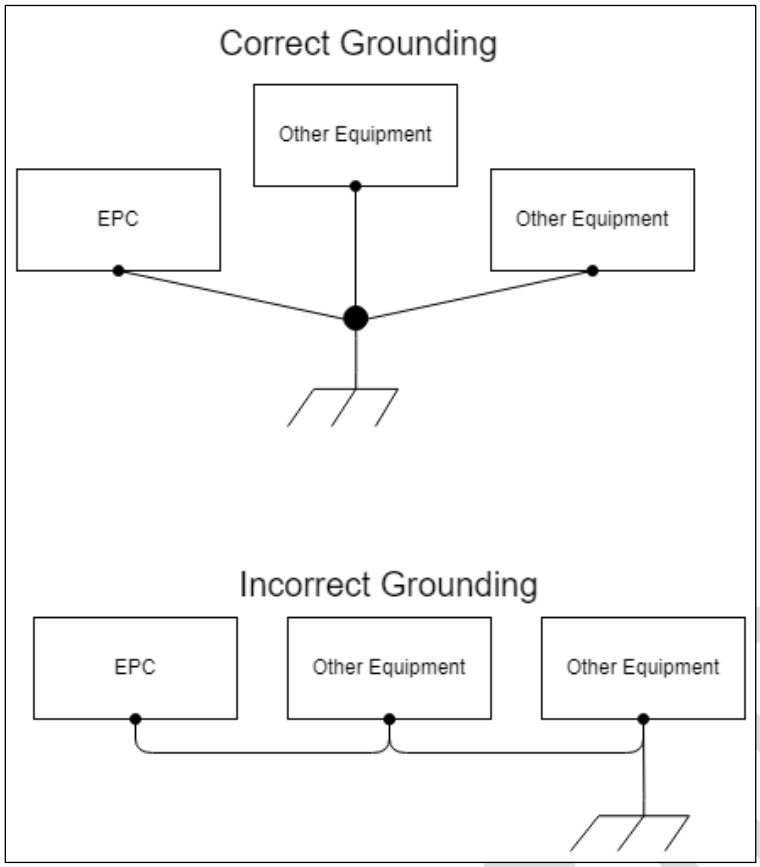


Figure 8 Correct and Incorrect Grounding Examples

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.

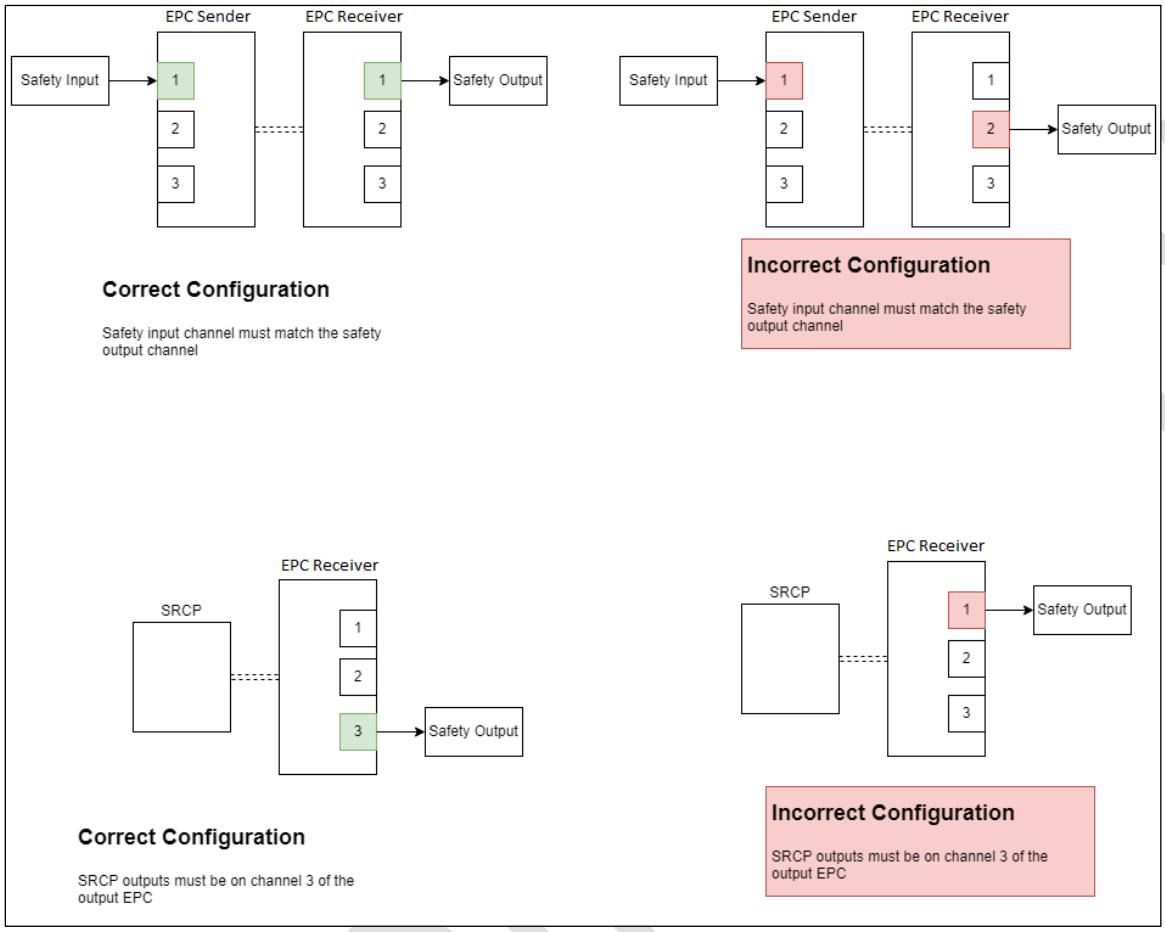


Figure 9 Correct and Incorrect Wiring Diagram

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.[13]

Refer to I/O Connector Pinout and Cable on page 23 for details of the EPC I/O connector and cable to use for connecting input devices to an Endpoint Controller sender.

[13] 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.

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.

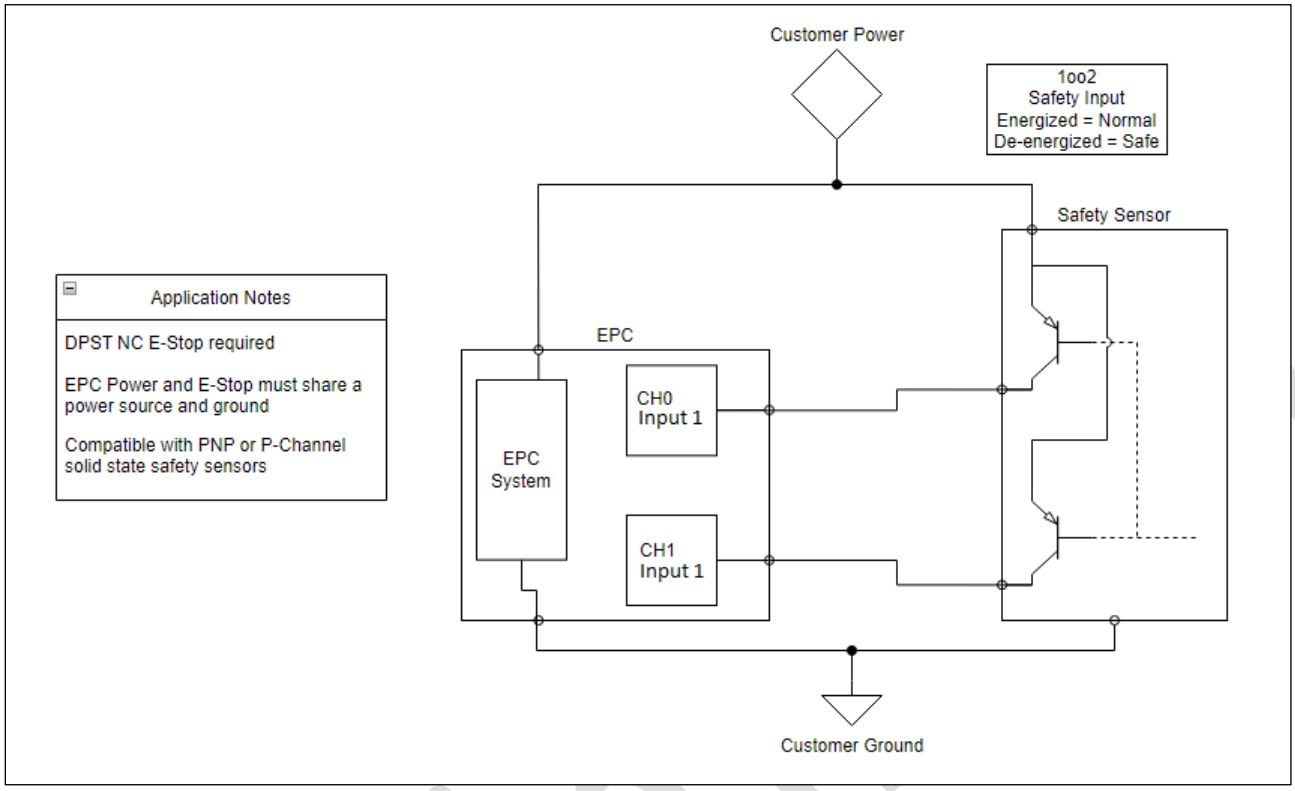


Figure 10: Solid State Device Wired to EPC

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.

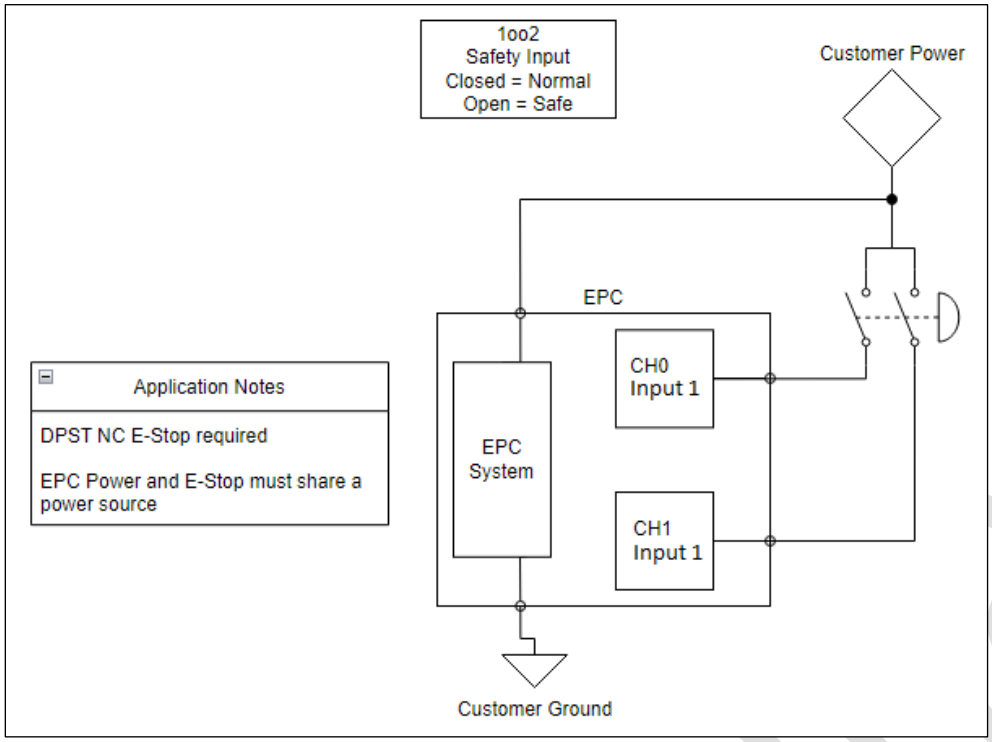


Figure 11: E-Stop Switch Wired to EPC

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 5 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.

Device	**Requirement**
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.

⚠ **IMPORTANT:** Each output on the EPC is designed with short circuit protection circuitry inside the EPC device. On the other hand, to satisfy applicable wiring codes and conditions, you are responsible for protection of field devices and wiring through appropriate fusing of the circuitry.

Figure 12 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:

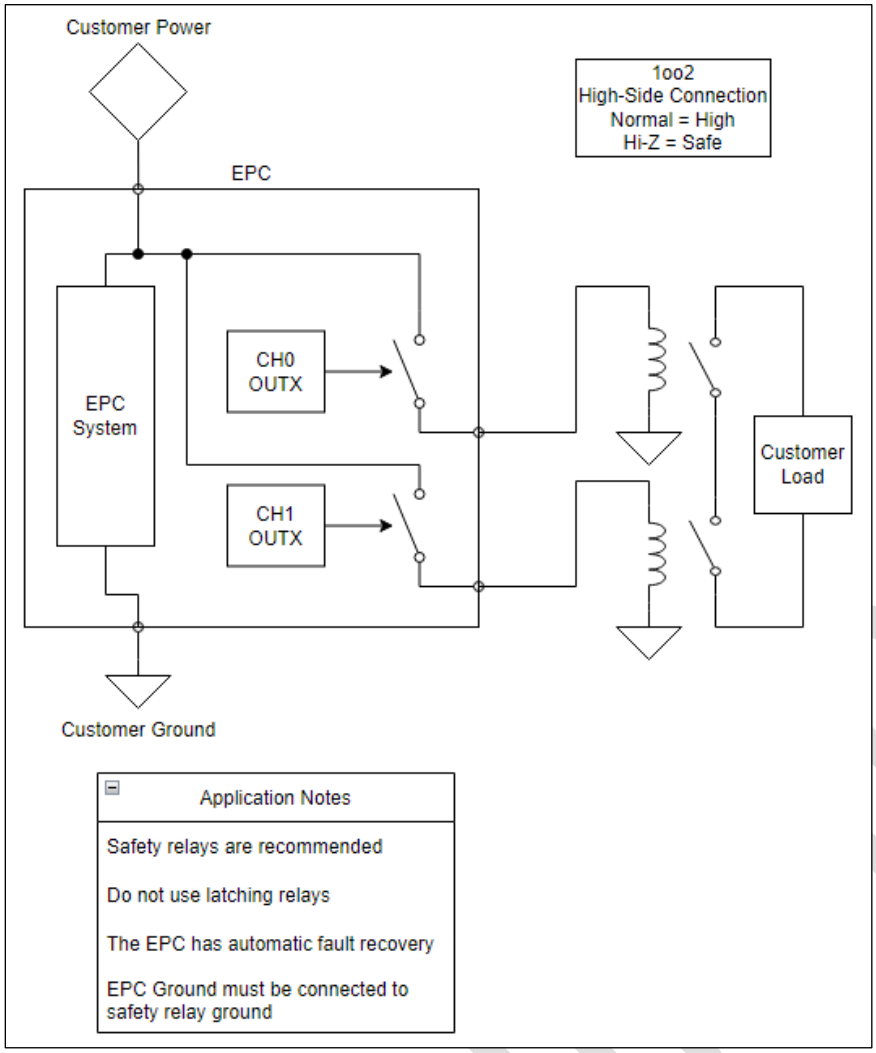


Figure 12: Output diagram

Note the following about this setup:

- You must connect EPC ground to safety relay ground.
- Do not use latching relays.
- 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.

Refer to I/O Connector Pinout and Cable on page 23 for details of the EPC I/O connector and cable to use for connecting an Endpoint Controller receiver to the EUC.

Table 6 Recommended and Tested Relays

Manufacturer	Model	Supply Voltage
Allen-Bradley	MSR127TP	24V

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

See Appendix E: Recommended Relays on page 87 for wiring diagrams for each of these relays.

Selecting Automatic or Manual Reset for Relays

An important 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 powerup 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., Estop 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., Estop 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.

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

Sample EPC-EPC Paired Configuration

Figure 13 demonstrates the wiring and communication between two Endpoint Controller devices, one configured as a sender and the other as a receiver. See Building a Configuration with an EPC Remote on page 7 for information on setting up a configuration with an Endpoint Controller as the sender (input controller).

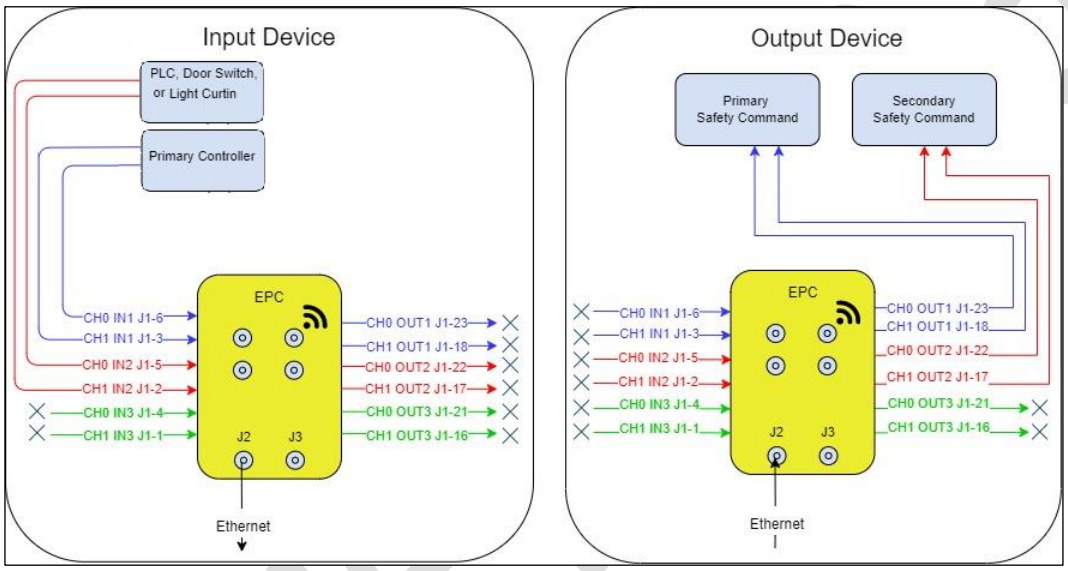


Figure 13: Sample EPC Paired Configuration with two Inputs

Mounting an EPC

An Endpoint Controller has four mounting holes to attach it to the equipment under control (EUC) as shown in Figure 18: EPC-1001 Mechanical Drawing on page 68. We recommend using ¼-20 or M6 machine screws for mounting.

⚠ **WARNING:** 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 7: Antennas

	275-0002	**275-0080**	**275-0096**
			
Manufacturer Part #	ANT-868-CW-QW	ANT-916-CW-QW	ANT-W63-SPNF1
FORT Device	EPC 1001 & 1002, SRC Pro 1001 & 1002, SRC, VSC, WES	EPC, SRC Pro	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)

	275-0002	**275-0080**	**275-0096**
Peak Gain	1.1dBi	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.

The following figure illustrates ideal placement for the antenna: clear line of sight (LOS), not too high or too low, no metal between, pointed straight up (whip antenna), or pointed towards other devices (puck antenna)

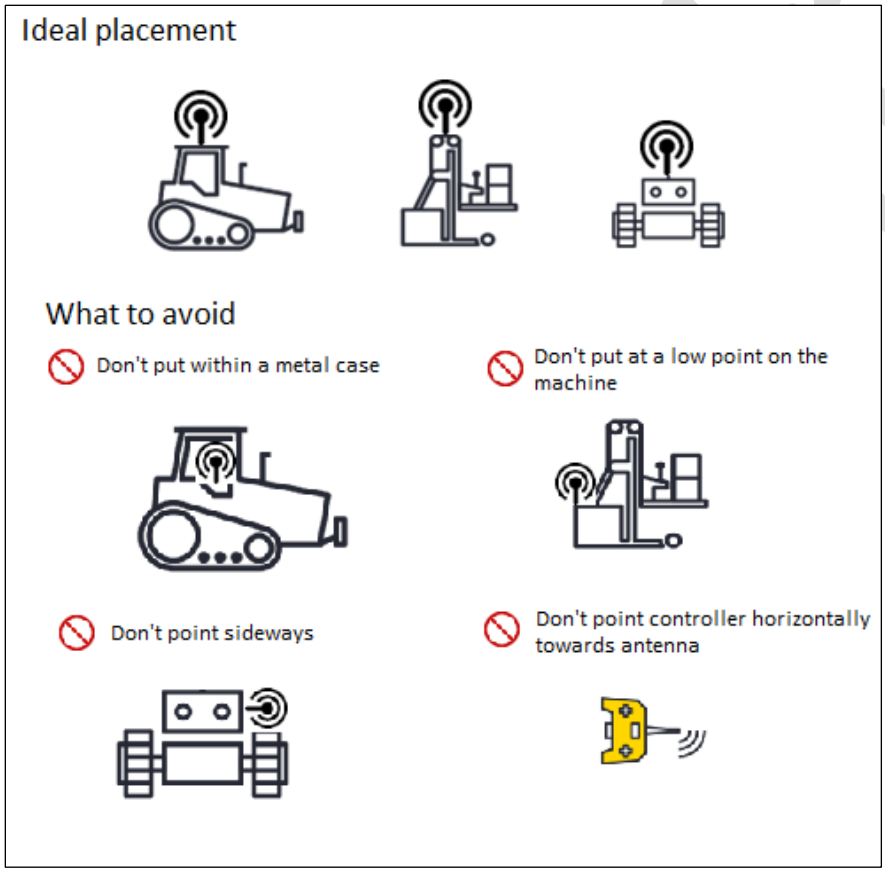


Figure 14: Antenna Placement

Attenuation from cable length and connection points

Every cable has a loss value of power based on input end, length of middle, and output end as shown in the following table:

Table 8 Antenna Attenuation

Input End	Middle Length	Output End	Attenuation
RP-SMA male	2 ft	RP-SMA male	TBD
RP-SMA male	20 ft	RP-SMA male	TBD
RP-SMA female	500mm	TNC female	TBD
RP-SMA female	1700mm	TNC female	TBD
RP-SMA female Bulkhead			TBD
U.FL	9 in	SMA	TBD

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

Table 9 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 15 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, if you push the power button the LCD screen turns on. In addition, once the motors engage, the device vibrates to indicate that it is ready to use.

When you push the power button to turn it off, the Safe Remote Control Pro is no longer sending valid safety messages to the connected Endpoint Controller, which goes to safe state after the timeout period is exceeded.

PAUSE BUTTON

Pressing the Pause button causes the Safe Remote Control Pro to enter pause mode. The Safe Remote Control Pro sends a safety message to the connected Endpoint Controller (if any) closing the relays and initiating a safe state. 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.

Modes

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

Supervised and Unsupervised Modes

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 unsupervised 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, gyroscope measurements, 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.

Supervised mode works for both autonomous and non-autonomous machines.

Unsupervised mode is meant to be used with machines that have autonomous capability.

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 unsupervised.

In unsupervised 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; and the Endpoint Controller ignores an E-Stop press on the Safe Remote Control Pro as well as not responding to joystick movements and button presses on the Safe Remote Control Pro.

See Figure 5 Input 3 Asserted on EPC Receiver on page 13 for an illustration of the wiring for machines with autonomous capability that require operation in unsupervised mode.

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.

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 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.

Connecting an 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[14] in the configuration independently of FORT Manager — this feature is called: *machine select*.

BEFORE YOU BEGIN

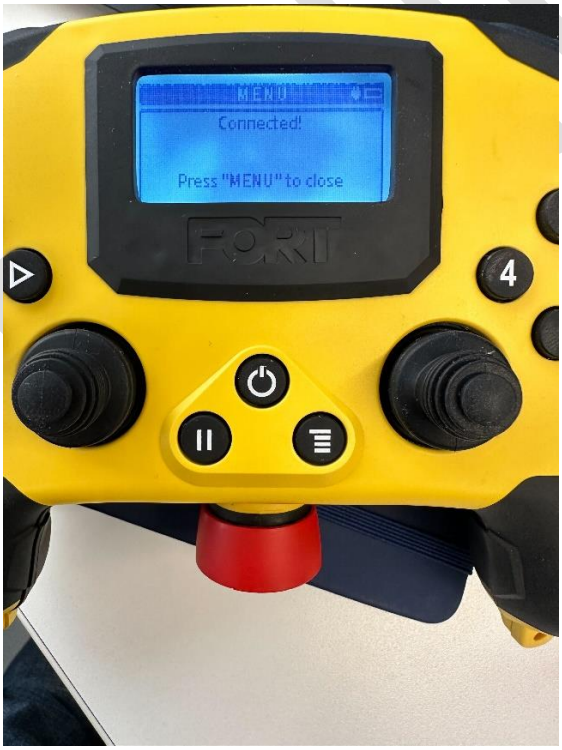
Make certain that both devices are powered up and in range of each other.

TO CONNECT AN SRC PRO TO AN EPC:

1. Power up both devices and keep them within range of each other.
2. On the SRC Pro LCD screen, navigate to the **Machine** tab.
   The screen shows a list of devices that you added to the configuration in FORT Manager.

[14] For this release, an SRC Pro or SRC Pro with Global E-Stop configuration allows one EPC only. You must still connect the SRC Pro to an EPC, as described in this section, but any SRC Pro configuration contains only one EPC.

3. Select the device to connect with.
4. Click **Connect**.
   The screen displays a confirmation code.
5. Use the number buttons to type the code to confirm the selection.
6. Wait for the connection to be established and when confirmed, press the **Menu** button to close the window.



After you confirm the connection, the EPC transitions to supervised mode. 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.

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

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.[15] 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.

The previously connected device remains in the mode it was set to (supervised or unsupervised). In unsupervised mode, the equipment under control remains powered up and running. On the other hand, if the state of the Endpoint Controller is supervised and you connect to a different Endpoint Controller, the first Endpoint Controller no longer receives a safety signal from the Safe Remote Control Pro and goes 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 Safe Remote Control Pro sets the mode of the Endpoint Controller to supervised. At any time after connecting to an Endpoint Controller in supervised mode you can change the mode of the Endpoint Controller to unsupervised.

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.

1. On the SRC Pro LCD screen, navigate to the **Machine** tab and select the connected machine.

[15] For this release, an SRC Pro or SRC Pro Hybrid configuration allows one EPC only, therefore connecting to a different EPC is not currently possible. Later releases allow up to 30 EPCs in an SRC Pro or SRC Pro Hybrid configuration.

2. Click **Change Mode**.
   The screen displays a confirmation code.
3. Use the number buttons to type the code to confirm the selection.
4. After the mode change is successful, press the **Menu** button to close the prompt.

   If you select the machine again on the **Machine** tab, the screen displays the mode. For example, if you began in supervised mode, the screen should show: **`Unsupervised Mode`**.

Chapter 5 CAN Application Support

The Endpoint Controller's CAN (Controller Area Network) application supports two industry standard protocols for CAN messages — CANopen (see next section) and J1939 (see J1939 Implementation on page 53)

CANopen Implementation

The CANopen protocol has two uses in terms of an SRC Pro - EPC integration:

- Transmit joystick and control button commands from the SRC Pro to your systems installed on the machine that the EPC is connected to.
- Optionally, transmit user-configured parameters such as engine temperature, fuel level, etc. from the machine to the SRC Pro to be displayed to the user on the LCD screen.

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 should have received an EDS file and sample program to dump CANopen traffic in a confirmation email package when you purchased your FORT devices —but if not. request it via our Customer Support Portal.

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

Table 10 CANopen

Description	Direction	Frequency
Joystick Data – Buttons (Table 11: TPDO1 Buttons, p.45)	Transmit	~16 Hz
Joystick Data - Thumbstick Axes (Table 12: TPDO2 Thumbstick Axes, p.48)	Transmit	~16 Hz
Joystick Data - Trigger Axes (Table 13: TPDO3 Trigger Axes, p.48)	Transmit	~16 Hz
EPC Heartbeat Message (Table 14 and Table 15 on page 49)	Transmit	5 Hz

Description	Direction	Frequency
SRC Pro Settings Message (Table 16 and Table 17 on page 50)	Receive	N/A
SRC Pro User Display Text Message (Table 19 on page 51)	Receive	N/A

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`)

Table 11: TPDO1 Buttons

Object Dictionary Index (hex)	Sub-Index	Bit	Name	Usage
60.00	01	00	memory x-axis	Unused - Fixed 0
60.00	01	01	memory y-axis	Unused - Fixed 0
60.00	01	02	memory z-axis	Unused - Fixed 0
60.00	01	03	ms	Unused
60.00	01	04	ms	Unused

Object Dictionary Index (hex)	Sub-Index	Bit	Name	Usage
60.00	01	05	ms	Unused
60.00	01	06	ms	Unused
60.00	01	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	b6	Unused
60.00	02	06	b7	Unused
60.00	02	07	b8	Unused
60.00	03	00	b9	1 Key
60.00	03	01	b10	2 Key

Object Dictionary Index (hex)	Sub-Index	Bit	Name	Usage
60.00	03	02	b11	3 Key
60.00	03	03	b12	4 Key
60.00	03	04	b13	Menu
60.00	03	05	b14	Unused
60.00	03	06	b15	Unused
60.00	03	07	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 12: 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 13: TPDO3 Trigger Axes

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

EPC Heartbeat 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 14 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 EPC heartbeat message format.

Table 15: EPC Heartbeat Message Format

Byte Offset	Size	Description	Value
0	2	Status Sequence ID	16-bit Unsigned Integer (little-endian) 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 - Unsupervised 0x33 - Not Applicable (EPC to EPC Pairing) **Bits 3:0 - SMCU0 Mode** 0000 - No Mode (Error State) 0001 - Supervised 0010 - Unsupervised 0011 - Not Applicable (EPC to EPC Pairing) **Bits 7:4 - SMCU1 Mode** 0000 - No Mode (Error State) 0001 - Supervised 0010 - Unsupervised 0011 - Not Applicable (EPC to EPC Pairing)
6	1	Output 2 Mode	Same as Output 1 Mode
7	1	Output 3 Mode	Same as Output 1 Mode

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. The following table shows the object dictionary for the SRC Pro Settings message.

Table 16: 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

The following table shows the SRC Pro Settings message format:

Table 17: 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 18: 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.

Table 19: 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

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.

Table 20: 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 21: 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.

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 via an on-device configuration parameter. Contact FORT support if you require a value other than the default.

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 should have received DBC file and sample program to dump J1939 traffic in a confirmation email package when you purchased your FORT devices —but if not. request it via our Customer Support Portal.

Table 22 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
65280	0xFF00	EPC Heartbeat - J1939 Proprietary Message	Transmit	5 Hz
65281	0xFF01	SRC Pro Settings Command - J1939 Proprietary Message	Receive	N/A
65282	0xFF02	User Display Text String - J1939 Proprietary Message	Receive	N/A

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 23 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 = Not Available	**Keypad** button **Left second** has been pressed. As per j1939 DA it is Joystick button 4
6	2 bits		**Keypad** button **Left third** has been pressed. As per j1939 DA it is Joystick button 3

Bytes	Bits	J1939 PGN 64982 Data field	Description
6	2 bits		**Keypad** button **Pause** has been pressed. As per j1939 DA it is Joystick button 2
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
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
7	2 bits		**Keypad** button **Left First** has been pressed As per j1939 DA it is Joystick button 5
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
8	2 bits		**Keypad** button **Right First** has been pressed As per j1939 DA it is Joystick button 10

Bytes	Bits	J1939 PGN 64982 Data field	Description
8	2 bits		**Keypad** button **Right Second** has been pressed As per j1939 DA it is Joystick button 9

Left Joystick - J1939 Extended Joystick Message 1

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

Table 24: 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

EPC Heartbeat - J1939 Custom Message

The Endpoint Controller transmits a heartbeat message to provide status for various Endpoint Controller functionality. It uses the TPD04 protocol to transmit the heartbeat message at a rate of every 5 Hz. The following table shows the heartbeat message format.

Table 25: EPC Heartbeat Message Format

Byte Offset	Size	Description	Value
0	2	Status Sequence ID	16-bit Unsigned Integer (little-endian) 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 - Unsupervised 0x33 - Not Applicable (EPC to EPC Pairing) **Bits 3:0 - SMCU0 Mode** 0000 - No Mode (Error State) 0001 - Supervised 0010 - Unsupervised 0011 - Not Applicable (EPC to EPC Pairing) **Bits 7:4 - SMCU1 Mode** 0000 - No Mode (Error State) 0001 - Supervised 0010 - Unsupervised 0011 - Not Applicable (EPC to EPC Pairing)
6	1	Output 2 Mode	Same as Output 1 Mode
7	1	Output 3 Mode	Same as Output 1 Mode

SRC Pro Settings - J1939 Custom Message

The Endpoint Controller supports receiving an SRC Pro Settings Message in order to change settings on a connected Safe Remote Control Pro.

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

The following table shows the SRC Pro Settings Message format:

Table 26: 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
5	3	Reserved for Future Use	

SRC Pro Setting Keys

The following table shows the SRC Pro Setting Keys

Table 27: 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 the 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 Message - J1939 Custom 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. To change the display mode of the Safe Remote Control Pro, the SRC Pro Settings Message can be used to set the display mode.

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 4 segments of 6 characters to build a 24-character string.

Table 28: 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 29: 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 second 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.

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 lifecycle, 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 lifecycle.

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 (man-in-the-middle attack) 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 using a certificate stored on the Secure Element.
- 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 at: https://www.fortrobotics.com/start.

Getting Around in FORT Manager

Use the items in the left-side Navigation pane or the clickable sections in the Dashboard to navigate in FORT Manager:

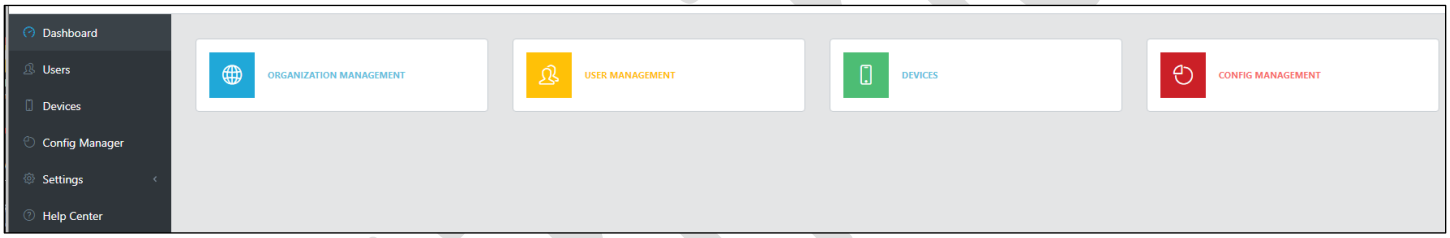


Figure 16 FORT Manager Dashboard

Note that the functions available in FORT Manager depend on the role assigned to the user who logs in, as well as whether they have full- or read-only permission. If you don't have any permission for a particular function (such as device management), it won't be visible on the dashboard nor in the navigation pane. If you have read-only permission, you can select it, for example Devices, and see a list of devices, but you can't add, delete, or modify a device.

The User Management section explains roles and permissions in more detail.

Organization Management

(Requires the Admin role)

Organization Management is available on the Dashboard or Settings in the navigation pane but only if you have the Admin role.

It allows you to provide details for your organization (name, phone, email, address, etc.) and choose a logo if desired.

NOTE: The ability to generate a code is a future enhancement that allows multiple organizations (for example, an OEM manufacturer and one of its customers) to share configurations. Although the code generator is functional, the rest of this feature has not been implemented.

User Management

(Requires Admin role)

User Management 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 permissions.
- ***ConfigManager*** — Create, edit, and delete configurations.
  Read-only view the Devices tab on the Devices page (but the Firmware tab is not visible).
- ***DeviceManager*** Create, edit, and delete devices.
  View the Config Management page (read-only).
  View the Firmware tab on the Devices page and download firmware files and the CLI tool.
- ***Operator*** Read-only permissions across FORT Manager but can't make changes and is not able to see the Users and Organization pages nor the Firmware tab on the Devices page.
  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 two-factor authentication for their own account and to view a list of their sessions.

To Add a User

(Requires Admin role)

1. Click **User Management** and click **Add user** in the upper right of the screen.
2. Type the email address for the user.
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. 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 in the Users page.

To Edit or Delete Roles for an Existing User

(Requires Admin role)

1. Click **User Management** and double click the user's name or click the edit icon in the **Action** column for the user.
2. Do either of the following:
   a. To add roles, select one or more roles in **Available Roles** and click the arrow icon to move them to **Assigned Roles**.
   b. To remove roles, select one or more roles in **Assigned Roles** and click the arrow icon to move them to **Available Roles**.
3. Click **Save** to save the new roles for the user.

To Delete an Existing User

(Requires Admin role)

1. Click **User Management** and click the delete icon in the **Action** column for the user.

   FORT Manager displays a warning message.

2. Click **Yes** to delete the user or **Cancel** to keep them.

Device Management

Device Management enables you to see and manage (with appropriate permissions) all of the devices in your organization. It also provides access to the Firmware tab, which enables you to download firmware update files and the CLI tool (to use for loading device configurations and making firmware updates).

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

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

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

To Add a Device

(Requires DeviceManager 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 **Next**.
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 EPCs attached to EUCs.

To Edit a Device

(Requires DeviceManager or Admin role)

1. Click **Devices** and double click the device name or 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 in Config Manager.

To Download Firmware Update Files or the CLI tool

(Requires DeviceManager or Admin role)

1. Click **Devices** and click the **Firmware** tab.
2. Click the download icon to the right of the file to download.

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
- Loading a Configuration onto an SRC Pro
- Updating EPC Firmware

- Updating SRC Pro Firmware

Configuration Management

Config Management enables you to see, as well as build or manage (with appropriate permissions) configurations for you organization. A configuration allows you to build out all of the wired or wireless pairings between your Pro Series devices.

All users can view the Config Manager page but only Admins and users with ConfigManager 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
- Building an SRC Pro to EPC Configuration
- Building a Hybrid Configuration

Settings

Allows an Admin user to set details about the organization, as well as for all users to augment security their security, and view sessions.

- *Organization* allows an Admin to enter or update details for the organization. Note that the organization Code is intended for future use.
- *Account* allows a user to enable multifactor authentication for their own account (through Google Authenticator).
- *Sessions* allows a user to view recent connections to the organization in FORT Manager.
- *Help Center* takes you to the FORT support site in a new browser window (requires a separate Zendesk account), where you can view detailed information about all FORT products and capabilities, as wells as useful tips, a knowledge base, the Developer Portal, and customer support ticket creation and management.

  You can access the Help Center on Zendesk at https://support.fortrobotics.com.

Chapter 8 Verification of Safety Systems

Before integrating an Endpoint Controller with your work environment, you must perform some basic safety tests to verify that the system is operating as expected in terms of safety.

You should develop a set of proof tests as part of your safety case. We can suggest some common tests, such as turning off power on a sender Endpoint Controller, disconnecting the radio, pressing the E-Stop, and so on, but these are just suggestions, and you need to develop specific tests for each of your configurations.

⚠ **IMPORTANT:** 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.).

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 (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 7 or Building an SPR Pro to EPC Configuration on page 13)

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.

Appendix A: Endpoint Controller Technical Specifications

This appendix provides the hardware specifications for the FORT devices.

EPC Mechanical Drawing

The following figure shows a mechanical drawing of the EPC 1000.

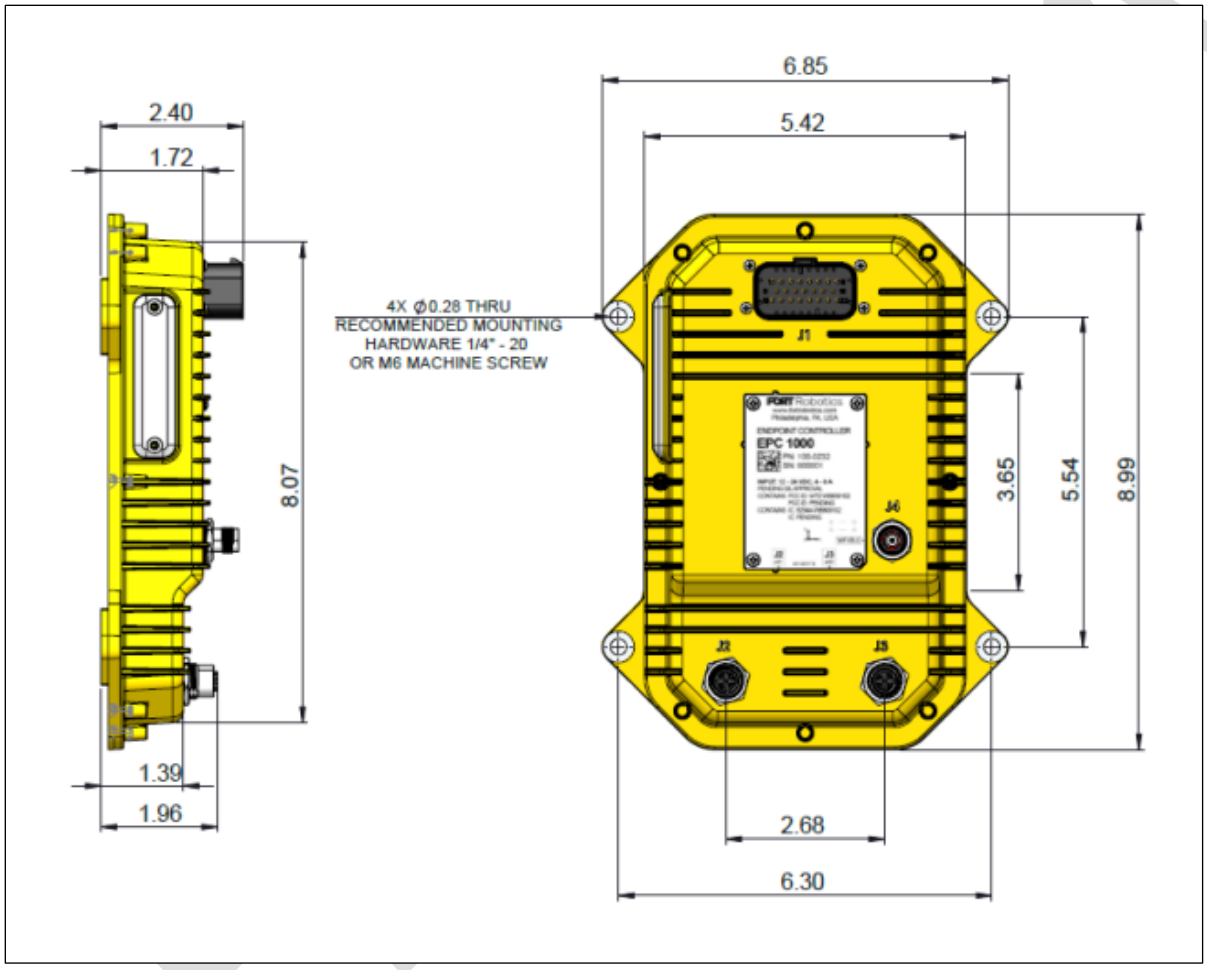


Figure 17 EPC-1000 Mechanical Drawing

The following figure shows a mechanical drawing of the EPC-1001.

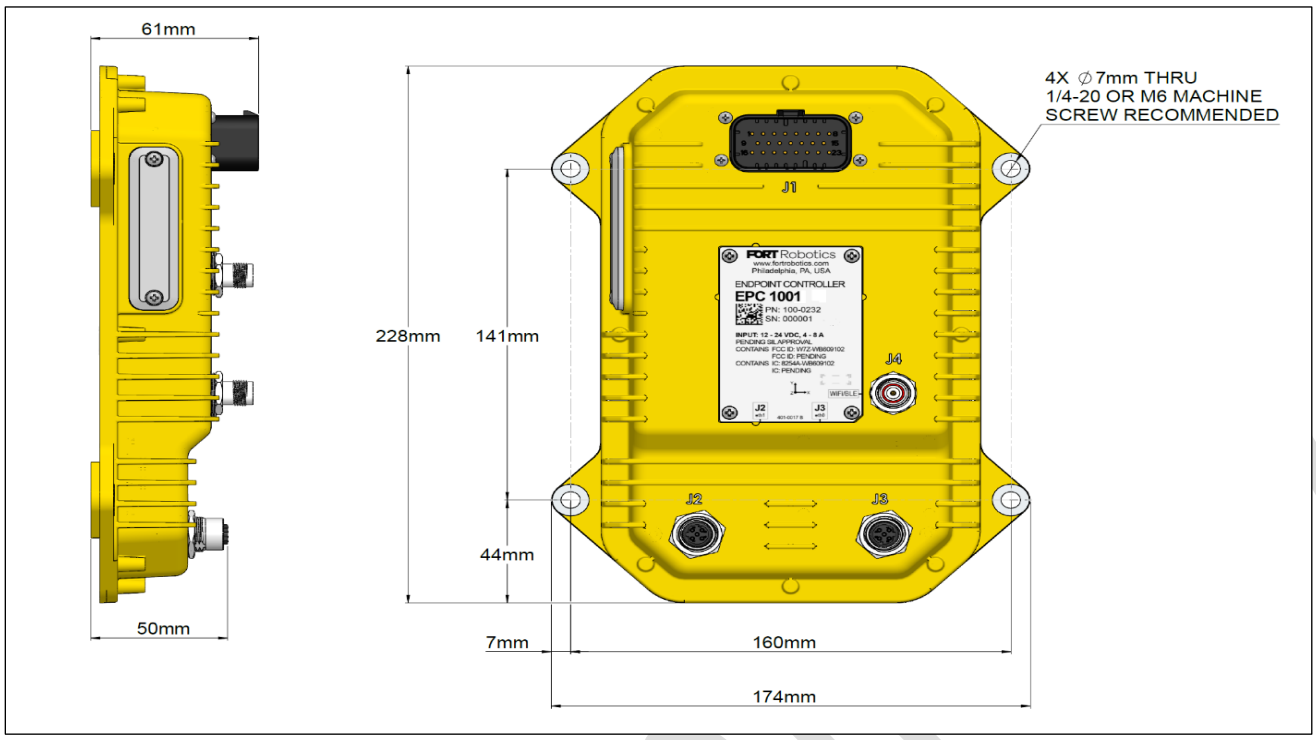


Figure 18: EPC-1001 Mechanical Drawing

The following picture shows the connectors on an EPC-1002.

Figure 19 EPC-1002 Backplate showing Connectors

Table 30 shows the recommended connectors for an Endpoint Controller device.

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

Table 30: Suggested EPC Connector Types

Connector Number	Suggested Mating Connector Type for EPC
J1	TE 770680-1.
J2	Ethernet M12 – D Type
J3	Ethernet M12 – D Type
J4	RP-TNC Plug (male) with center socket (female)
J5	RP-TNC Plug (male) with center socket (female)
Side Door	MICRO SD
Side Door	RECPT, MINI USB B
Side Door	MICRO-SIM CARD, 6 CONTACTS

Recommended and Absolute Maximum Ratings (EPC)

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

Table 31 EPC Recommended- and Absolute-Maximum Ratings[16]

Specification	Minimum	Typical	Maximum
PVin (12V operation)	9.6[17]	12	14.4
PVin (24V operation)	19.2[17]	24	28.8
PVin(V)	8	-	32
Input Voltage	0 V		Vin+0.7 V

[16] Stresses beyond those listed under *Minimum* and *Maximum* in the table may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated under *Minimum* and *Maximum* is not implied. Exposure to absolute-minimum or maximum-rated conditions for extended periods may affect device reliability.

[17] The supply source must provide enough current for the system to recognize a signal as 'high'. If the voltage supply drops 20% from nominal voltage (9.6 V for a 12 Volt battery or 19.2 V for a 24 volt battery) the system logs a safety fault.

Specification	Minimum	Typical	Maximum
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 32 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[18]	8VDC	12VDC (or 24VDC)	32VDC
Input state for logic OFF/LOW	0VDC	0 ~ 1VDC	Less Than 8VDC
Input Impedance		TBD	

Safety Output Specifications

The following table provides specifications for the safety outputs:

[18] This applies to 12 VDC and 24 VDC supplied EPC Equipment.

Table 33 Safety Output Specifications

Specification	Minimum	Typical	Maximum
PVin (12V operation)	9.6[19]	12	14.4
Output ON State	9.6V	12	14.4
On-state Voltage Drop			1.057 V
PVin (24V operation)	19.2[17]	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 uS	
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 34 (EPC) North America ISM Radio Specifications

Specification	Minimum	Typical	Maximum
Frequency	902 MHz		928 MHz
Bandwidth		600 kHz	

[19] The supply source must provide enough current for the system to recognize a signal as 'high'. If the voltage supply drops 20% from nominal voltage (9.6 V for a 12 Volt battery or 19.2 V for a 24 volt battery) the system logs a safety fault.

Specification	Minimum	Typical	Maximum
Channels		26	
Receive Sensitivity	TBD		
Modulation		2-GFSK	
Baud Rate		500 kbps	
Power (conducted RF output)	-19 dBm		27 dBm
EPC Part number	North America ISM radio is available in EPC model 1001		

European ISM Radio (EPC)

The following table provides specifications for the European ISM radio:

Table 35 European ISM Radio Specifications

Specification	Minimum	Typical	Maximum
Frequency	869.4 MHz		869.653 MHz
Bandwidth		250 kHz	
Channels		1	
Receive Sensitivity	TBD		
Modulation		2-GFSK	
Baud Rate		200 kbps	
Power (conducted RF output)	-15 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 36 BLE Radio Specifications

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

Specification	Minimum	Typical	Maximum
Receive Sensitivity	-99 dBm		

Ethernet Specifications

The following table provides Ethernet specifications:

Table 37 Ethernet Specifications

Specification	Minimum	Typical	Maximum
Speed		10/100Mbps	

Data Interfaces

The Endpoint Controller's integration interface is USB or CAN (Controller Area Network). CAN Application Support on page 44 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 the PVin. Maintain a single ground reference for all power and reverence voltages.

The following table provides specifications for the CAN interface

Table 38 CAN Bus Specifications

Specification	Minimum	Typical	Maximum
CAN H/L Voltage		TBD	
High Level input		TBD	
Low level input		TBD	
Driver output current		TBD	
Driver input current		TBD	
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

Appendix B: Safe Remote Control 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.

Figure 20 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 39 (SRC Pro) Absolute and Recommended Specifications

SPECIFICATION	MIN	TYPICAL	MAX
Vin(V)			
Current			

SPECIFICATION	MIN	TYPICAL	MAX
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			
Run Time (Bluetooth)			
Run Time (ISM)			

Table 40: Safe Remote Control Pro (SRC Pro) Technical Specifications (OLD)

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 41 (SRC Pro) North America ISM Radio Specifications

Specification	Minimum	Typical	Maximum
Frequency	902 MHz		928 MHz
Bandwidth		600 kHz	
Channels		26	
Receive Sensitivity	TBD		
Modulation		2-GFSK	

Specification	Minimum	Typical	Maximum
Baud Rate		500 kbps	
Power (conducted RF output)	-19 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 42 European ISM Radio Specifications

Specification	Minimum	Typical	Maximum
Frequency	869.4 MHz		869.653 MHz
Bandwidth		250 kHz	
Channels		1	
Receive Sensitivity	TBD		
Modulation		2-GFSK	
Baud Rate		200 kbps	
Power (conducted RF output)	-15 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 43 BLE Radio Specifications

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

Appendix C: Safety

This Appendix explains the safety related operations and methods used to achieve functional safety of the product designs for 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 Endpoint Controller is related to handling of the emergency stop (E-Stop) and similar safety device commands.

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.

The following sections of this chapter describe the operations inside the Endpoint Controller, including input, logic, and output, and explain in detail all valid use cases of an Endpoint Controller and its 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 an Ethernet 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).

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 with their own independent input circuitry, processing, output circuitry, and external monitoring (via a watchdog).

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:

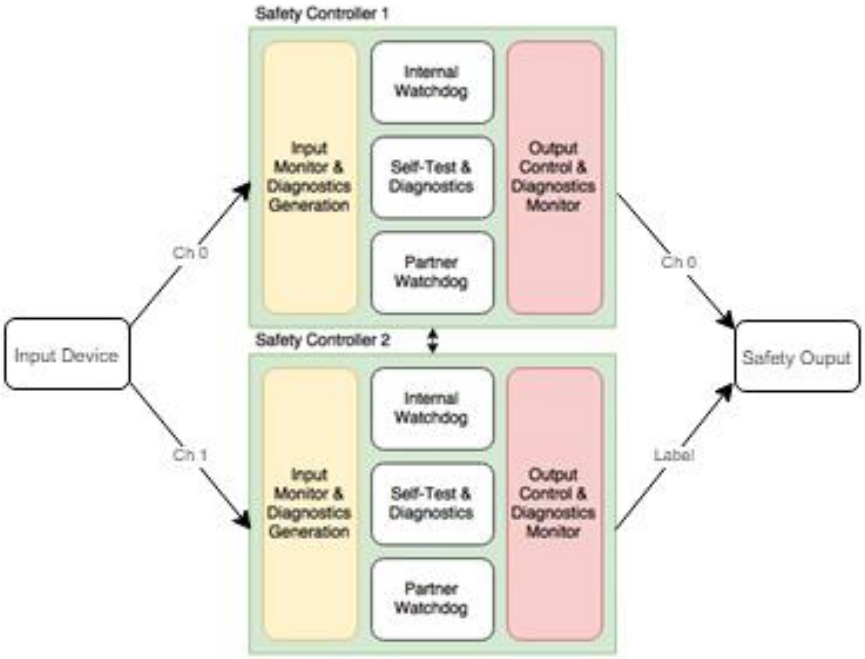


Figure 21: 1oo2 Safety Architecture

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**: sends a safety message to request safety from the remote device(s).
- A **receiving device**: 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** stops sending safety messages which triggers a timeout causing the receiving devices to turn off their output relays.

- A **receiving device** loses power to the outputs of the system which 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 req). The following diagram shows the flow of safety data and commands, from one Endpoint Controller (EPC) to another Endpoint Controller.

If the AMCU changes the content of a safety message because of an error, the receiving SMCU detects the change, considers the changed message invalid and does 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

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.

Virtual Inputs

Virtual Inputs are safety request messages, generated by the SMCUs of an Endpoint Controller or Safe Remote Control Pro, that are serially transmitted to the AMCU of the Endpoint Controller or Safe Remote Control 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:

Serial Communication with Application Processor (AMCU)

On a sender Endpoint Controller, 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 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 not safety relevant.

Serial Communication between the two Safety Processors (SMCU)

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.

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 (cyclic redundancy check) 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 every timeout period, otherwise the outputs will be turned off to put the EUC in a safe state.

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 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.

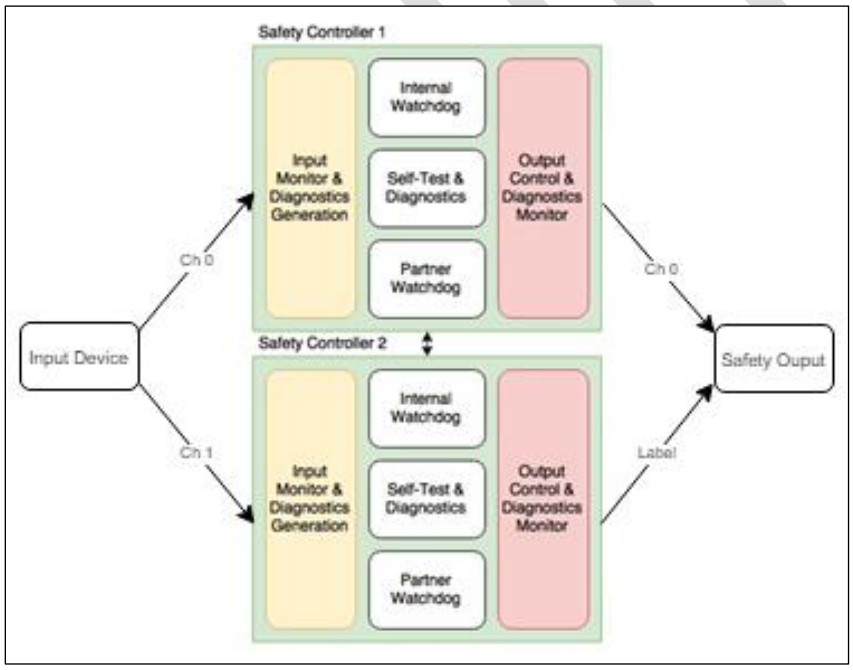


Figure 22: Redundant Architecture

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

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.

Physical Outputs

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 safety request messages generated by the SMCUs of an Endpoint Controller, 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), which 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 in the diagram) receives the safety request message and serially transmits it to its SMCU as shown in the following diagram:

Figure 23: Serial Communication

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

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 in Chapter 2). 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 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 Device Configuration onto an EPC and SRC Pro in Chapter 2). After each reset or powerup, 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.

⚠ **IMPORTANT:** 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

Hardware Metrics based on FMEDA

TBD

Mechanical and Electrical Safety

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.

The system has a mission time and proof test interval of 20 years (175200 hours).

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.

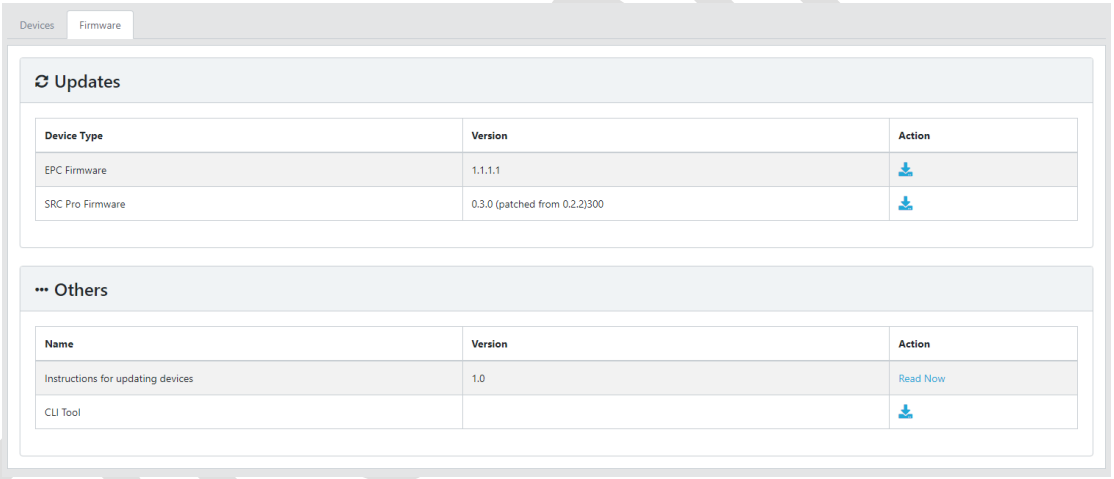
Downloading the Tool

You should have received the compressed archive file for the CLI tool (`fort-cli-cfg-<version>.tar.gz`) in a confirmation email package when you purchased your FORT devices —but if you no longer have access to it or want to be certain you have the most current version, you can download it from FORT Manager as follows.

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 the **Devices** tile at the top of the dashboard or **Devices** in the left navigation pane, and click the **Firmware** tab.



3. Click the download button for the 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. 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.

5. 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:

   ```
   $PATH (Enter)

   -bash: /home/user/.local/bin:/home/mkline/.local/bin:/usr/local/sbin: …
   ```

6. If `.local/bin` is not in your `$PATH`, add the following line to your `.bashrc` file:

   ```
   export PATH="$HOME/.local/bin:$PATH"
   ```

7. 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 20.
- Loading a Configuration onto an SRC Pro on page 21.
- Updating EPC Firmware on page 93.
- Updating SRC Pro Firmware on page 95

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 44 Recommended and Tested Relays

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

ALLEN-BRADLEY, MSR127TP

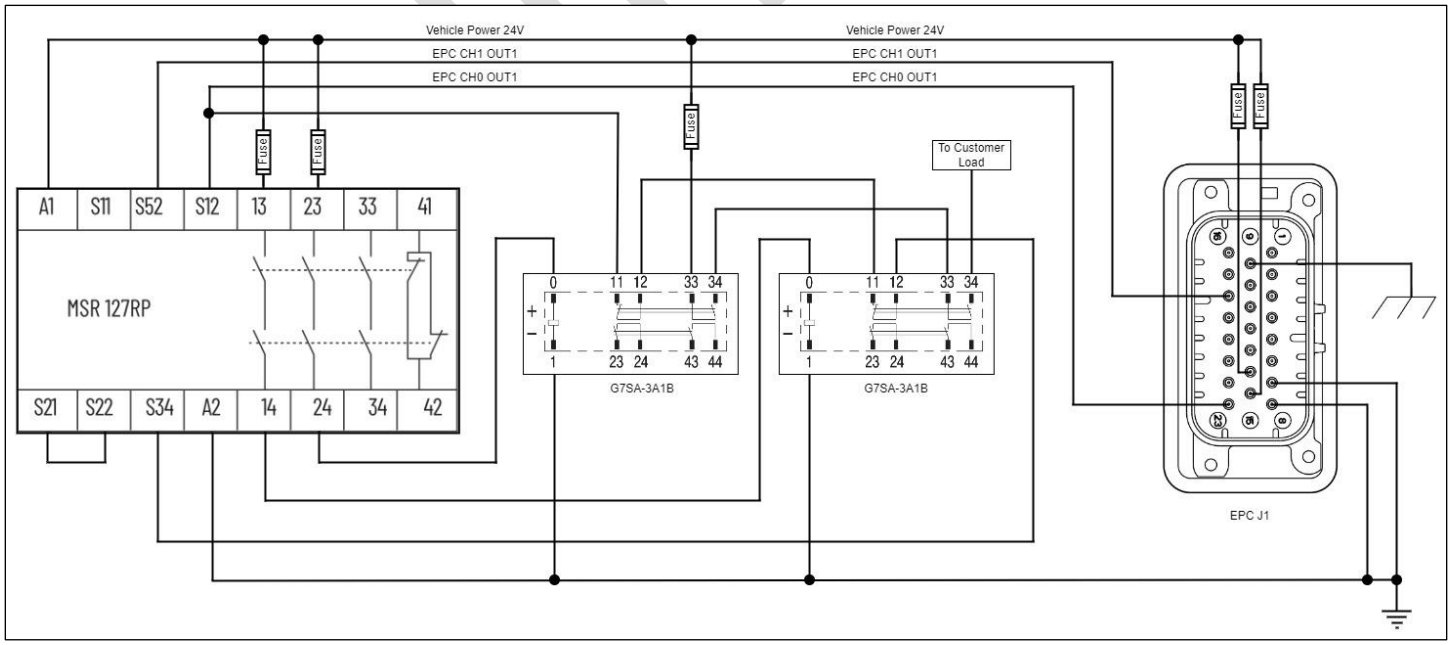


Figure 24 Allen-Bradley MSR127TP Relay Wiring Diagram

EATON ESR5-NV3-30

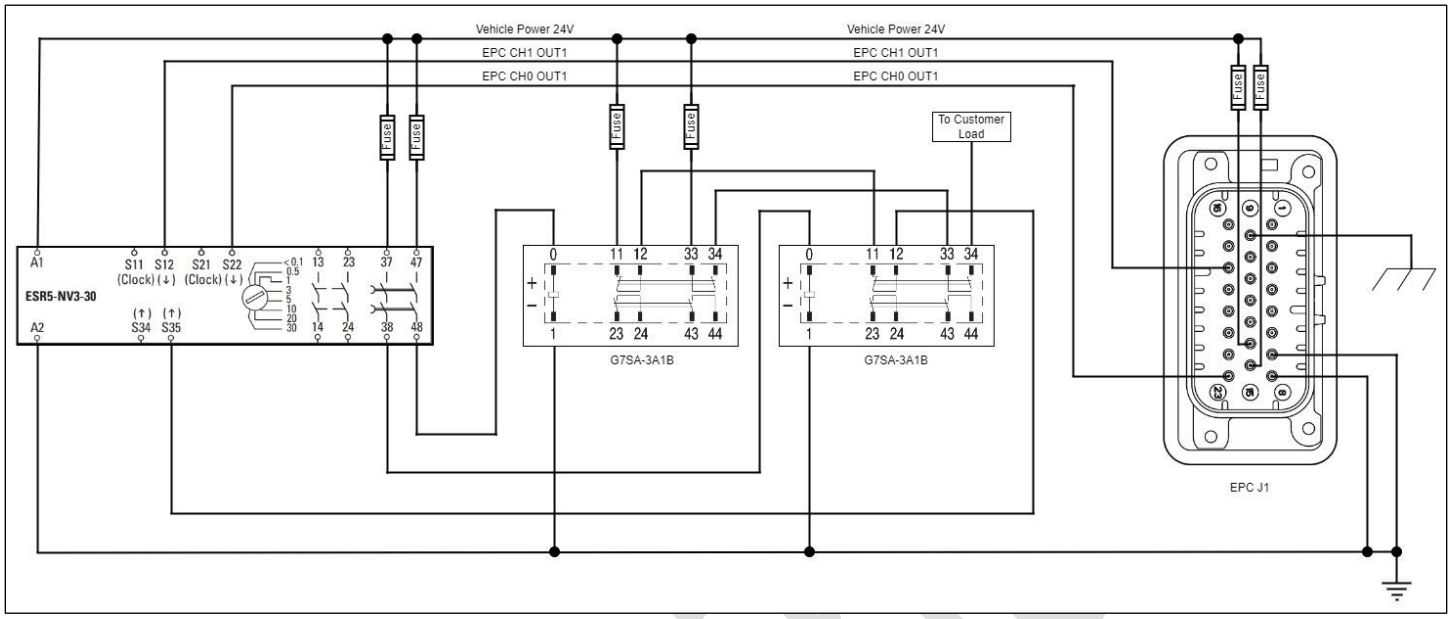


Figure 25 Eaton ESR5-NV3-30 Relay Wiring Diagram

PILZ 751104

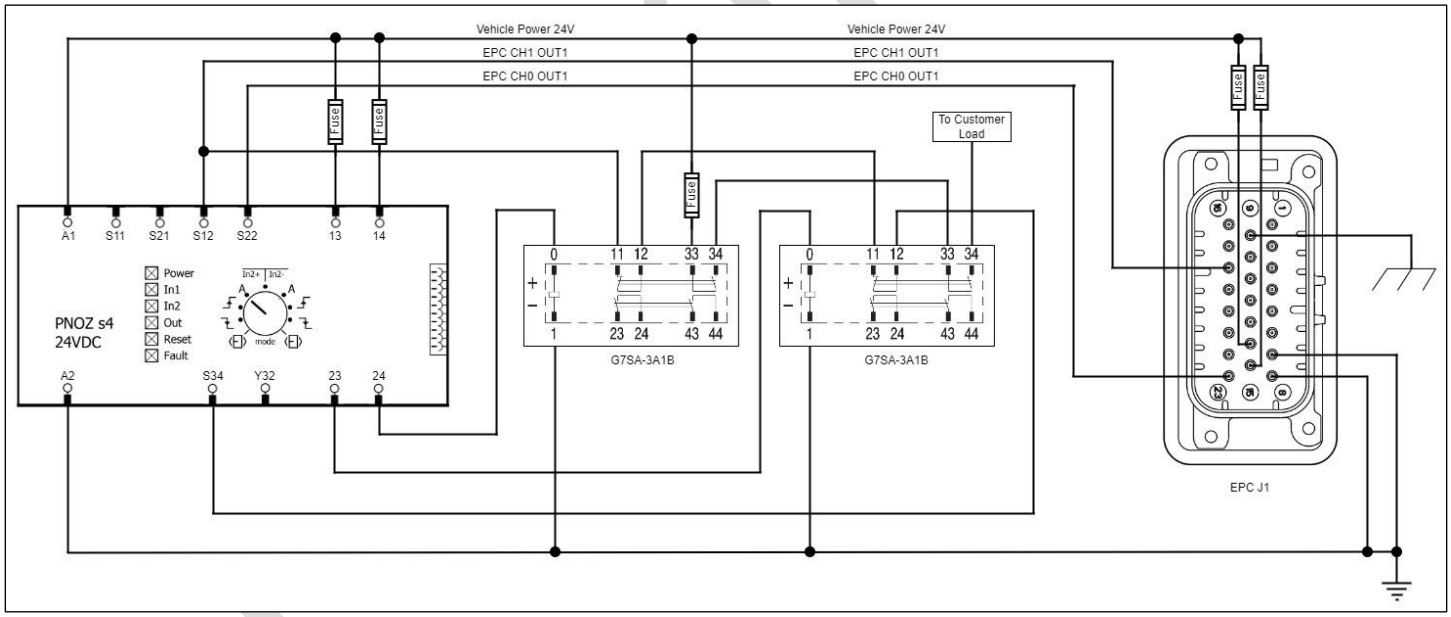


Figure 26 PILZ 7751104 Relay Wiring Diagram

IDEM SCR-3-1P-I

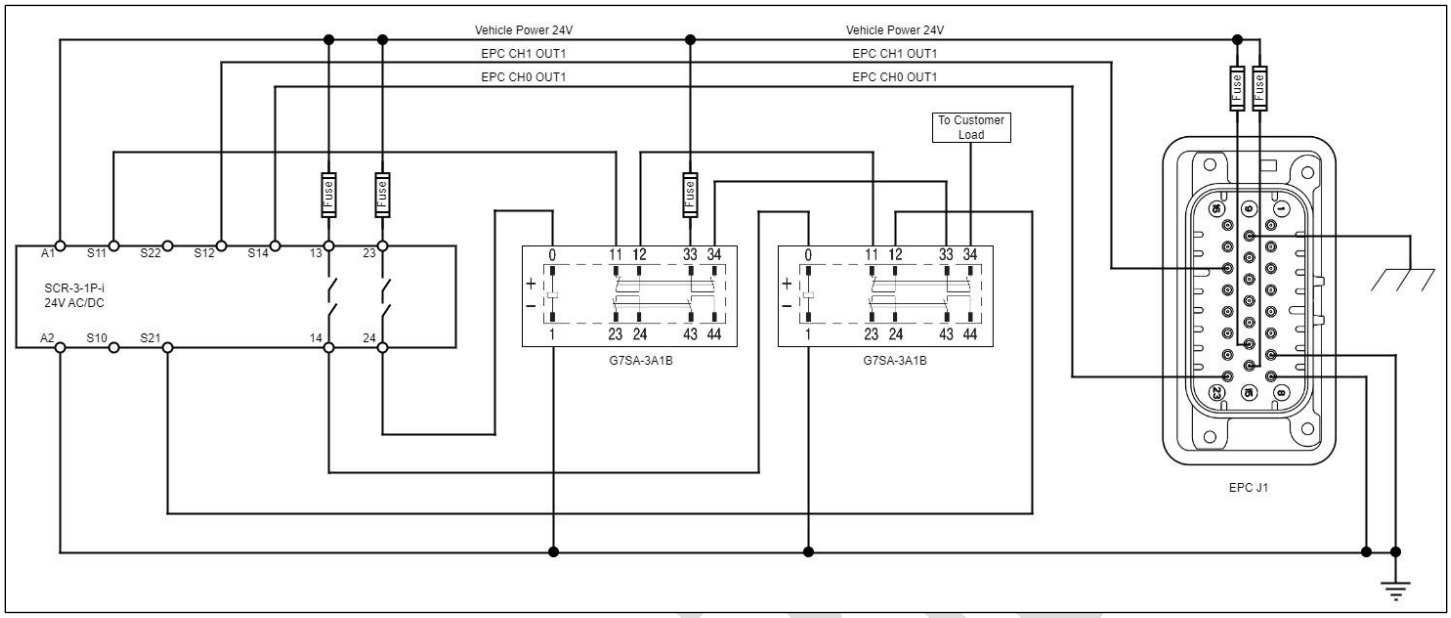


Figure 27 IDEM SCR-3-1P-I Relay Wiring Diagram

OMRON G7SA-3A1B

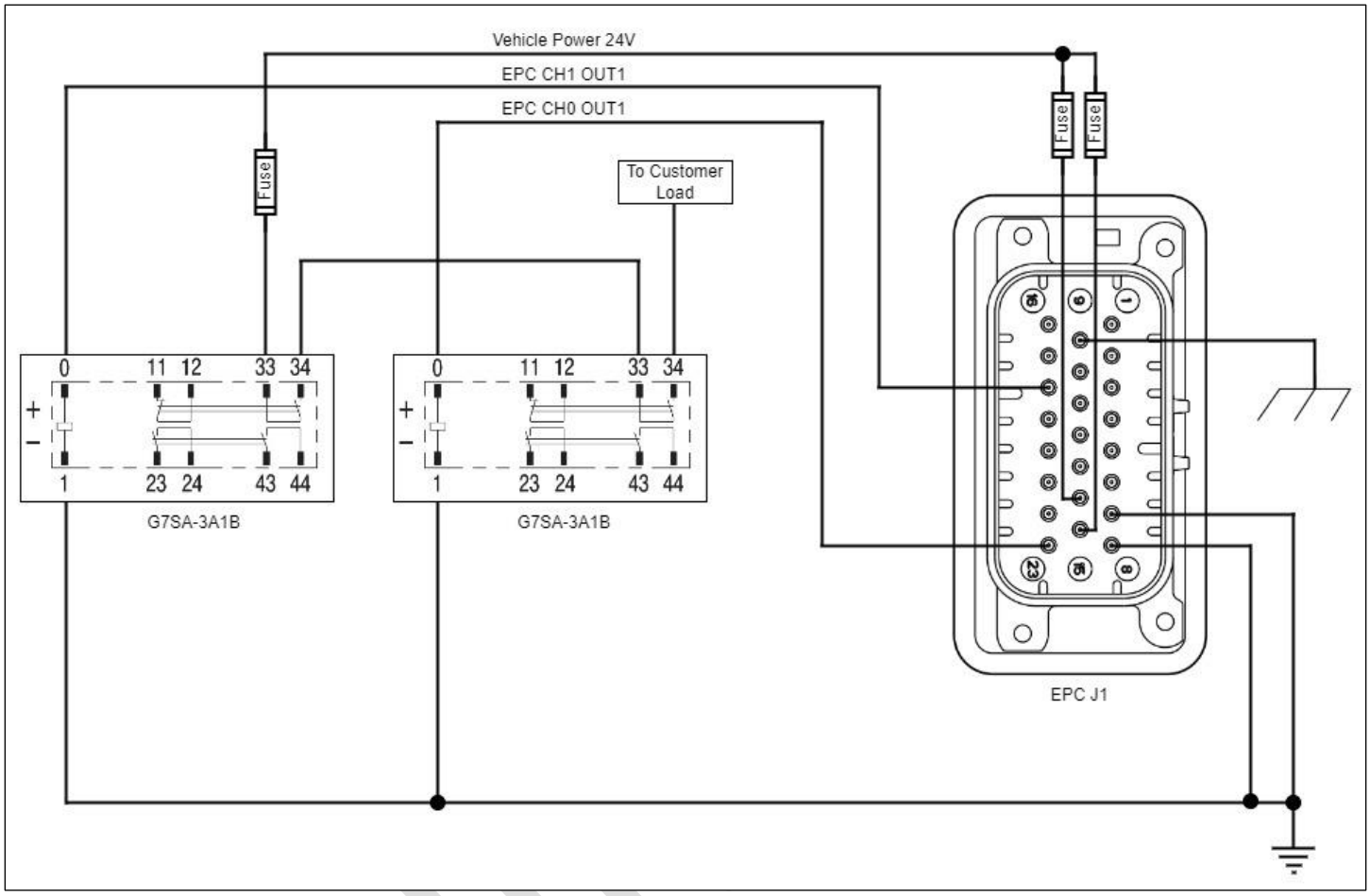


Figure 28 OMRON G7SA-3A1B Relay Wiring Diagram

PANASONIC SFS3-L-DC12V-D

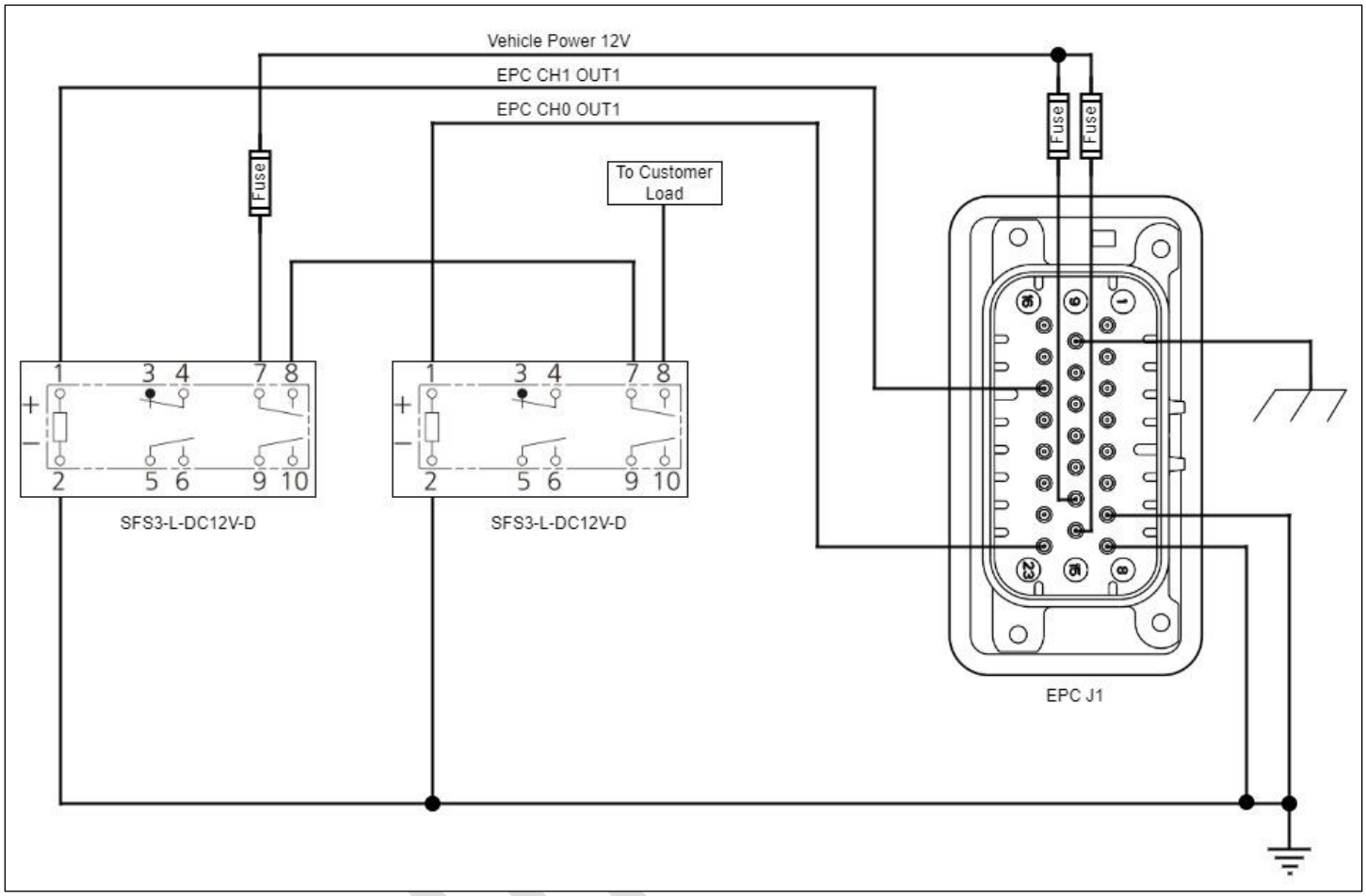


Figure 29 PANASONIC SFS3-L-DC12V-D Relay Wiring Diagram

Appendix F:Notifications and Certifications

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 handle a device that is damaged or fails for any reason, and how to update the firmware as necessary.

Device Failure

> ⚠ **WARNING:** 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 Building and Loading a Configuration on page 3.

Updating EPC Firmware

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

> 💡 **NOTE:** 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 (https://support.fortrobotics.com/) 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 should have received this file in a confirmation email package when you purchased your FORT devices —but if

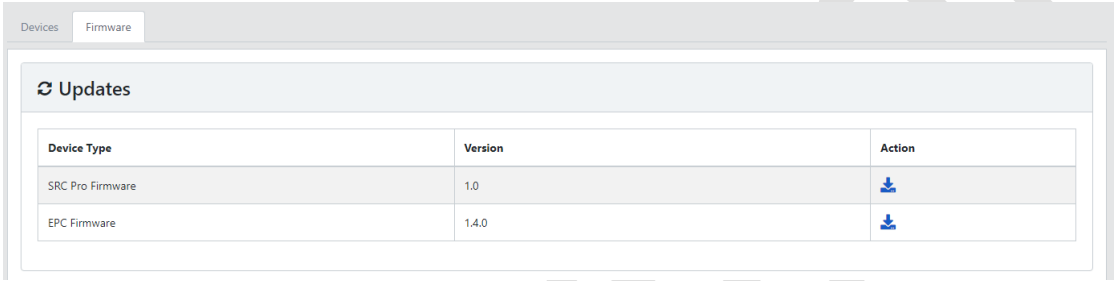
not, you can download an archive package that contains it from FORT Manager (see the first procedure that follows these bullets for instructions on downloading and extracting the file).

- Latest FORT CLI Configuration Tool (`fort-cli-cfg`).
  You should have received a compressed file with the tool (`fort-cli-cfg-<version>.tar.gz`) in a confirmation email package when you purchased your FORT devices —but if not, you can download it from FORT Manager (see Appendix D: FORT CLI Configuration Tool on page 85 for more information, including installation instructions for the tool).

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 the **Devices** tile at the top of the dashboard or **Devices** in the left navigation pane, and click the **Firmware** tab.



3. Click the download button in the **Action** column for **EPC Firmware**.

   FORT Manager downloads the product update file to the Downloads folder on your computer.

4. 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 your Linux computer to the EPC J2 port using an M12-RJ45 cable.
2. 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.

3) Use the arrow keys to navigate to **Device Firmware Update** and press **Enter**.
4) Use the arrow keys to navigate to **Firmware Update** and press **Enter**.
5) 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.

6) Use the arrow keys to navigate to **Device reboot** and press **Enter** to reboot the device.

Updating SRC Pro Firmware

All Safe Remote Control Pros come with the latest firmware preinstalled. 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. 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 (https://support.fortrobotics.com/) to get help.

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

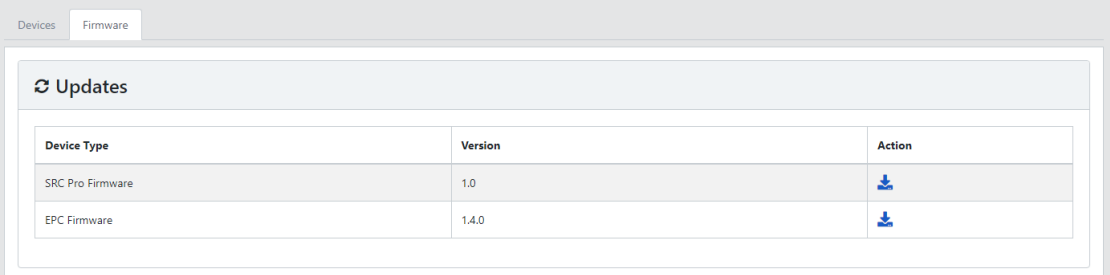
REQUIRED ITEMS

- Linux computer running Ubuntu 20.04 with ethernet networking capability or a Windows machine.
- Firmware upgrade file for the SRC Pro.
  You should have received this file in a confirmation email package when you purchased your FORT devices —but if not, you can download an archive package that contains it from FORT Manager (see the first procedure that follows these bullets for instructions on downloading and extracting the file).
- Latest FORT CLI Configuration Tool (`fort-cli-cfg`).
  You should have received a compressed file with the tool (`fort-cli-cfg-<version>.tar.gz`) in a confirmation email package when you purchased your FORT devices —but if not, you can download it from FORT Manager (see Appendix D: FORT CLI Configuration Tool on page 85 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 the **Devices** tile at the top of the dashboard or **Devices** in the left navigation pane, and click the **Firmware** tab.



3. Click the download button in the **Action** column for **SRC Pro Firmware**.

   FORT Manager downloads the firmware update file to the Downloads folder on your computer.

5. Copy the file (`flashlayouts-stm32mp15-epc-<vers>.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\ flashlayouts-stm32mp15-epc-<vers>.tar.gz <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:

   ```
   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 **Firmware Update** and press **Enter**.
5) Type the path to the update file and press **Enter**, for example:

   ```
   ./ flashlayouts-stm32mp15-epc-<vers>.tar.gz
   ```

   Note that the update process may take up to three minutes to complete.

6) Use the arrow keys to navigate to **Device reboot** and press **Enter** to reboot the device.

Troubleshooting

⚠ **WARNING:** 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.

The FORT system logs and timestamps all faults and safety mechanism faults that occur. You can access log files through the configuration tool.

Appendix H: Revision History

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)[20]	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.
J (GA release candidate)	2/10/23	Incorporated edits from multiple reviews. Added Chapter 4 about SRC Pro. Rewrote introduction. Rewrote procedures for loading configurations.

[20] 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 (https://www.fortrobotics.com/guardian). Guardian allows you to get firmware and software updates, extended support, and warranty coverage beyond the limited one-year hardware warranty term.