

FORT Robotics Pro Series User Guide

Preface

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

Document part number: 400-0044

Copyright © 2025, 2026 by FORT Robotics, Inc

All rights reserved.

FORT Robotics is a trademark of FORT Robotics.

Proprietary Information Notification:

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

Chapter 1. Introduction

This chapter introduces the Pro Series devices and FORT Manager, explains how a wireless safety signal moves your equipment between its normal state and its safe state, and outlines the plan, wire, and configure sequence you follow to set a system up.

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

The Pro Series includes:

- **Endpoint Controller (EPC)** — A mountable sender and receiver that can execute trusted commands over Bluetooth low energy, Long-Range Bluetooth, Wi-Fi, Ethernet, and ISM Radio. It can be used as a sender, to send safety signals to other FORT devices, such as NSC Pros or other Endpoint Controllers, or as a receiver, wired into a machine for control and safety functions sent by another FORT device. Which radios are available depends on the model; see [Device Models and Communication Methods](#) (on page 51). For more information on the EPC, see [EPC Technical Specifications](#) (on page 142).
- **Safe Remote Control Pro (SRC Pro)** —Used as a sender to wirelessly connect to an EPC or NSCP, it provides both wireless E-Stop and remote operator control of a machine at a safe distance. Which radios are available depends on the model ; see [Device Models and Communication Methods](#) (on page 51). For more information on the SRCP, see [SRC Pro Technical Specifications](#) (on page 168). For more information on which models FORT Manager supports, see [SRC Pro Models and Support Status](#) (on page 171).
- **Wireless E-Stop Pro (WES Pro)** A handheld sender that sends a wireless E-Stop command to connected machines ¹ with the push of a button. See [WES Pro Technical Specifications](#) (on page 173) for detailed technical specifications.
- **Nano Safety Controller Pro (NSC Pro)** — An embedded board with a small form factor, used as a receiver, that allows OEM developers to build emergency stop (E-Stop) functionality directly into their machines without requiring bolt-on hardware. The NSC Pro controls a machine (known as the EUC, or equipment under control) by receiving safety signals from a mobile or stationary sender with which it is paired.
- **FORT Manager** — A cloud-based platform that provides device registration, configuration, management and updates, and management of users. Managing users means that FORT Manager holds account information for the people in your organization. For more information, see [Personal Data in FORT Manager](#) (on page 227). You can reach FORT Manager three ways:

¹ A WES Pro can pair with one receiver only. The receiver can be an EPC or an NSC Pro. Consult the [Release notes](#) for information specific to the version of the product that you are using.

- The [FORT Manager Web App](#), which provides a UI for building configurations. The web app presents six pages in the left navigation pane — **Dashboard**, **Devices**, **Configurations**, **Firmware**, **Users**, and **Organization**. For more information, see [What You See in FORT Manager](#) (on page 7).
- The FORT Manager Desktop App, which you download from the web app. It provides additional functionality not found in the web app, including the ability to load configurations and firmware without an internet connection.
- The FORT API, which provides programmatic access to configuration management. For more information, see [FORT Manager API Reference Guide](#).

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.

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.
- A receiver wired to each EUC.
- A remote controller (an EPC, SRC Pro, or WES Pro) that communicates wirelessly with the receivers attached to the EUCs to send safety signals, and in the case of the SRC Pro, safety and control signals.

The following figure illustrates a basic configuration with an EPC sender and three EPC receivers:

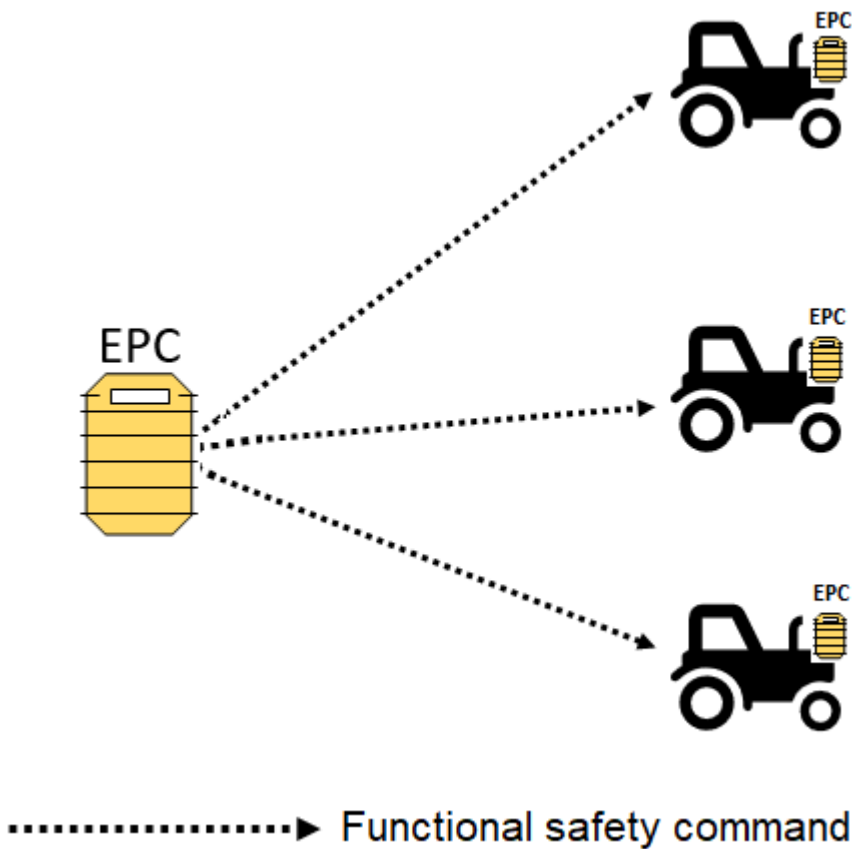


Figure 1: Basic Configuration

The basic operational philosophy of the system 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 a receiver is monitoring an area and a worker opens a guard or reaches into a hazardous area, which causes the receiver to initiate the safe state.
- The system detects an automatic diagnostic fault and initiates the safe state.

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

System Setup Process

The following steps walk you through setting up your Pro Series devices—from initial planning to final system testing—to ensure safe and reliable communication between components and safe operation of your equipment.

Note:

Although we show Plan as the first step, this manual assumes you’ve already determined how many devices you need and have purchased them. Similarly, while Wire appears before Configure, the order is flexible—teams may wire and configure in parallel.

That said, wiring and configuration are interdependent. For example, if you assign an E-Stop Switch to EPC Input 1, you must wire an E-Stop Switch—not a light curtain—to that input. You don’t need to follow a strict sequence, but when you’re ready to test the system, wiring and configuration must align.

- **Plan** — Determine the type of configuration to build. [Configurations and Use Cases](#) (on page 50) 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.
- **Wire** — Wire the inputs and outputs ([Wire and Mount Endpoint Controller](#) (on page 10))
 - If the transmitter device (sender) is an EPC, wire the inputs to an E-Stop type device or to a Solid State Safety Device (SSD); see [Wiring EPC Sender](#) (on page 10).
 - If the transmitter is an SRC Pro or WES Pro, no wiring is necessary because the E-Stop is built into it.
 - Wire the EPC output(s) to the EUC; see [Wiring EPC Receivers](#) (on page 10).
- **Configure** — Build a logical configuration using the FORT Manager Web App, the FORT Manager Desktop App, or the FORT API .

If you haven’t done so already, you can follow the instructions in the [Getting Started Guide](#) to log in to FORT Manager, set up an account, and register your devices. You can also:

- Set up your organization, manage user accounts, and assign roles. Adding someone to your organization stores their account information in FORT Manager. For more information, see [Personal Data in FORT Manager](#) (on page 227).
- Add devices to a configuration and set device and network parameters, including communication channels, timeout value, and types of inputs.
- View current configurations and device utilization.
- View support tickets.
- Update firmware as necessary.

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, email a request to support@fortrobotics.com to get help.

- **Load** —Load a configuration onto each device ([Loading a Configuration onto Your Devices](#) (on page 79)).
- **Test** — Verify that the system performs as expected before deploying it. For example, pressing an E-Stop button stops the EUC, walking in front of a light curtain slows or stops the EUC, and so on. Be certain that a safety expert verifies that the system is operating in accordance with your safety plan.



Warning:

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

FORT Manager enables you to build secure and functionally safe device configurations, through the web app, the desktop app, or the FORT API. Additionally, FORT Manager enables you (or someone in your organization) to perform the following tasks:

- Set up your organization, manage user accounts, and assign roles.
- Add devices to a configuration and set device and network parameters, including communication channels, timeout value, and types of inputs.
- View current configurations and device utilization.
- View support tickets.
- Update firmware as necessary.

What You See in FORT Manager

FORT Manager does not offer every organization the same set of features. FORT enables features for particular organizations, so a control described in this guide may not be present in your FORT Manager, and a feature announced in the release notes may not be enabled for you yet.

This is separate from the other reasons a control may be absent. A control can also be missing because of the type of configuration you are building, the model of the device you selected, or the role your account holds. For more information, see [Device Models and Communication Methods](#) (on page 51) for what each device model supports.

Note:

If this guide describes a control that you cannot find, and neither your configuration type, your device model, nor your role explains it, the feature may not be enabled for your organization.

FORT Manager Dashboard Page

The **Dashboard** is the page FORT Manager opens on. It has four areas.

- Notifications Row

- A single collapsible row at the top of the page, with a badge showing the number of unread notifications. Expand it to read them and dismiss them individually. Firmware releases are not announced here; they appear in the firmware release table.
- Firmware Release Table
 - The current published version for each device type, with a **New** badge against any version published since you last looked. For the full list and the downloads, go to the **Firmware** page.
- Stat Cards
 - Counts of devices, configurations, and users in your organization. Each card also shows a sub-metric — for example the number of invitations still pending — and opens the matching page filtered to that subset.
- Device Utilization Chart
 - How many of your registered devices belong to a configuration and how many are registered-only. A registered-only device is one FORT Manager knows about that belongs to no configuration. It cannot communicate with any other FORT device until it is added to one and that configuration is loaded onto it.

To raise a support request, click **Submit Request** on the Dashboard.

Device Status

FORT Manager reports two independent things about a device. They answer different questions.

Where It Appears	Values	What It Tells You
Status column, Devices page	Online / Offline / Pending	Whether FORT Manager is currently in contact with the device. It says nothing about which configuration the device holds.
Configuration view, Configurations page	Ready to Deploy / Deployed	Whether the configuration you are looking at has been applied to that device. It says nothing about whether the device is reachable now.

Important:

A device can be **Online** and still be running a configuration you have since changed. Neither badge is a substitute for reading the device itself. For more information, see [Confirming Configurations After You Reconnect](#).

FORT Manager Screens

The FORT Manager web app presents six pages in the left navigation pane. Procedures in this guide refer to them by name.

- **Dashboard**
 - The landing page: a notifications row, a firmware release table, stat cards for devices, configurations and users, and a device utilization chart. For more information, see [The Dashboard Page](#) (on page 7).
- **Devices**
 - Every device registered to your organization, with its model, registration date and status. Use it to find a serial number or a model number, to filter a fleet by model type, and to open a device's detail view.
- **Configurations**
 - Where you build, review, deploy, and modify configurations. For more information, see [Building a Configuration](#) (on page 68).
- **Firmware**
 - The published firmware version for each device type, and the **Downloads** card for the Desktop App, the CLI Configuration Tool, and the FORT SDK. For more information, see [The Firmware Page](#) (on page 199).
- **Users**
 - The people in your organization and the role each one holds. For more information, see [Personal Data in FORT Manager](#) (on page 227).
- **Organization**
 - Your organization's details and its API keys. For more information, see [API Key Expiry](#) (on page 228).

Opening a device from the **Devices** page shows its detail view, which has four tabs: **Info**, **History**, **Logs**, and **Health**.

Chapter 2. Wire and Mount Endpoint Controller

This chapter explains how to wire an Endpoint Controller as a sender or as a receiver — safety devices, power, ground, relays, Ethernet, and CAN — and how to place its antennas and mount it on your equipment.

Wiring EPC Sender

Note:

When wiring safety devices to an EPC sender, refer to [EPC I/O Connector Pinout and Cable](#) (on page 142), which lists each of the EPC's connector signals.

Use the J1 connector on the EPC to wire the EPC to safety devices and a power source.



CAUTION:

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

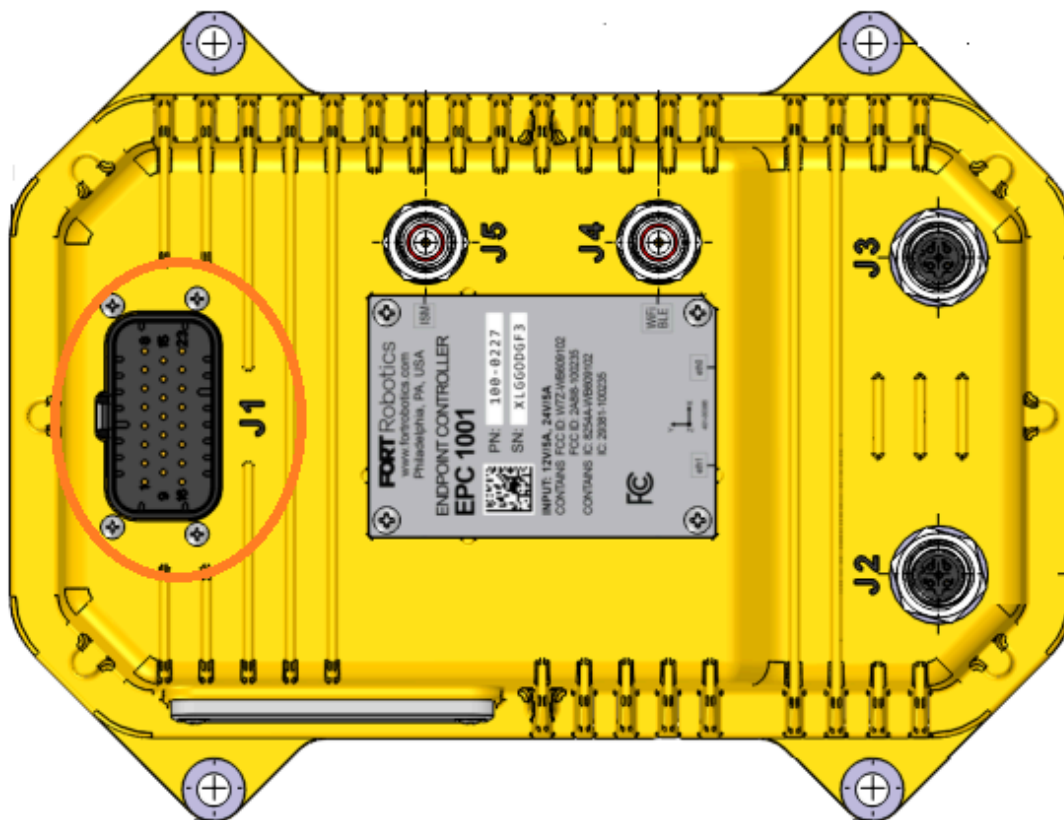


Figure 2: Fig. 2 EPC J1 Port

Before you begin, have on hand:

- A TE 770680-1 connector, the recommended mating connector to the EPC's 23 pin port (J1).
- A FORT #100-0256 Integration Cable to wire safety devices and power to the EPC.
- The safety device(s) to wire to the EPC. See [Input Safety Devices](#) (on page 14) for guidelines in selecting a safety device to use with an EPC.
- A 12 V or 24 V power source for the EPC.

Wiring Safety Devices and Power to EPC Sender

Refer to the figures: [Solid State Device Wired to EPC](#) (on page 12) and [E-Stop Switch Wired to EPC](#) (on page 13) to see wiring diagrams of safety sensors and E-Stops wired to an EPC.

You can connect either of the following types of devices to an EPC sender:

- **An E-Stop type switch**, which is a mechanical switch (internally contains two redundant switches).
 - Switches remain closed until someone pushes the E-Stop button, at which point the internal switches open.
 - A DPST NC (double-pole single-throw, normally closed) E-Stop is required so that both switches activate at the same time.
- **A solid state safety device.**
 - A DPST NC (double-pole single-throw, normally closed) safety sensor is required so that both switches activate at the same time.
 - You can use a PNP or P-Channel solid state safety sensor.

Note:

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.

**CAUTION:**

Ensure that your power supply is either 12 V or 24 V.

The EPC power and the safety devices must share ground reference.

For each safety input, you must use redundant connections.

To wire safety devices and power to the EPC:**Note:**

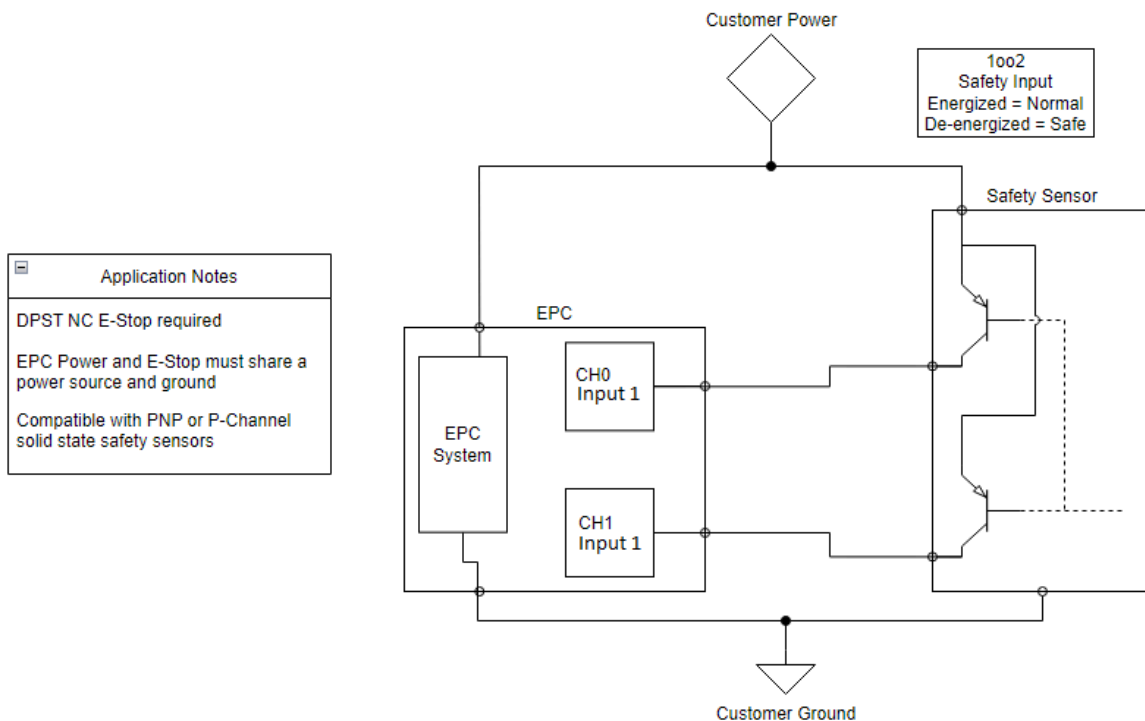
Make sure that the Device Safety I/O Settings in FORT Manager match the inputs that you are wiring here.

In most configurations you can wire Input 1, Input 2, or both. In a Two-to-One configuration with a WES Pro and an EPC, the configuration's **Output to Control** setting determines which single input is used – Input

1 for Output #1, Input 2 for Output #2 — and the other is grayed out in FORT Manager. Wire only the input your configuration uses. For more information, see [Choosing Which Output the Senders Control](#).

1. Attach the TE 770680-1 connector and FORT #100-0256 Integration Cable to the J1 port on the EPC.
2. Connect pin 3 (Channel 1, Input 1) and pin 6 (Channel 0, Input 1) to the safety device.
3. Connect pin 2 (Channel 1, Input 2) and pin 5 (Channel 0, Input 2) to the safety device.
4. Connect Pins 7 & 8 (PVin_RTN) to the negative polarity terminal of the power supply.
5. Connect Pins 14 & 15 (PVin_IN) to the positive polarity terminal of the power supply.
6. Connect Pin 9 (CH_GND) to ground. Connect to common power supply if earth ground is not available. See [Grounding an EPC](#) (on page 13) for more information.
7. Connect the safety device to a common power supply and ground (see following two figures).

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 EPC sender.



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

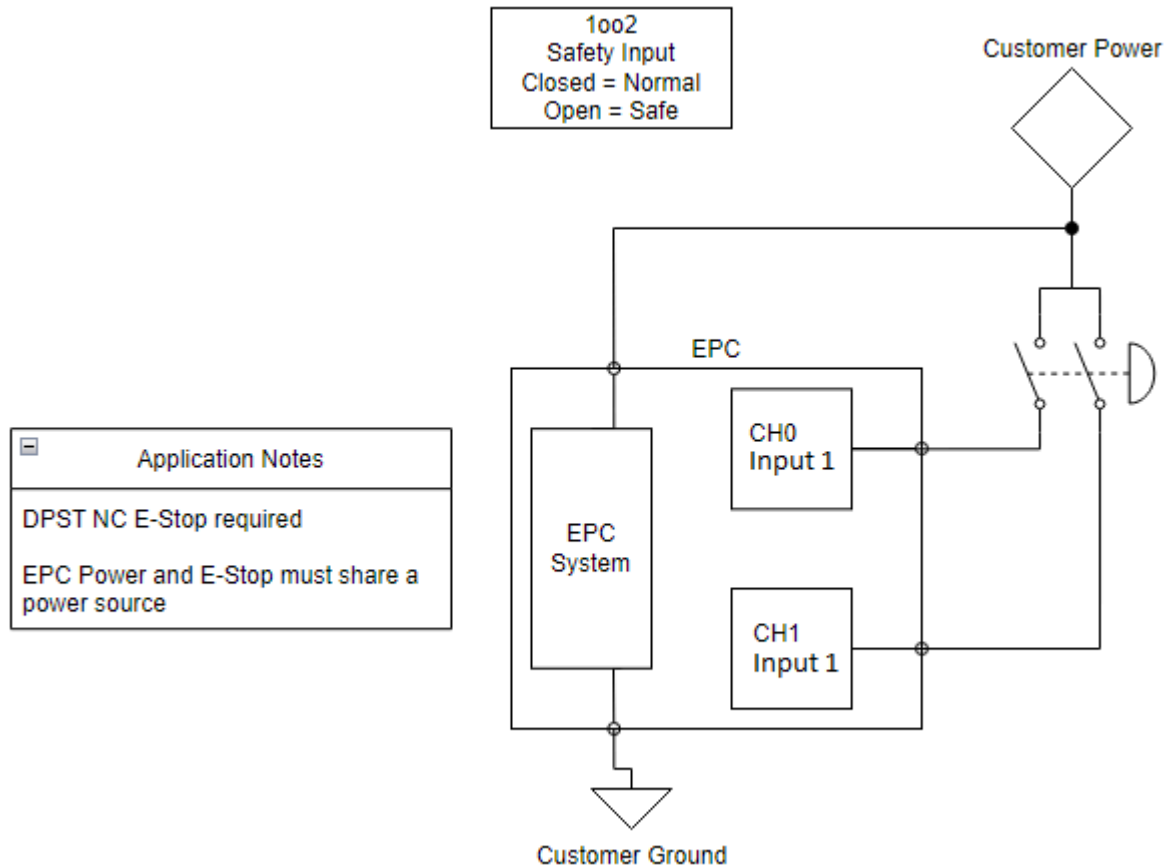


Figure 4: Fig. 4 E-Stop Switch Wired to EPC

Grounding an EPC

Note:

Connect Pin 9 CH_GND to power supply common if an earth ground is not available.

Be certain that there is only one path for return current between the host and receiving nodes. 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. Ensure that you ground unused pins in connectors and unused wires in cables at a single point on the connector. Ground unused wires at alternate ends to nearby ground pins.

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

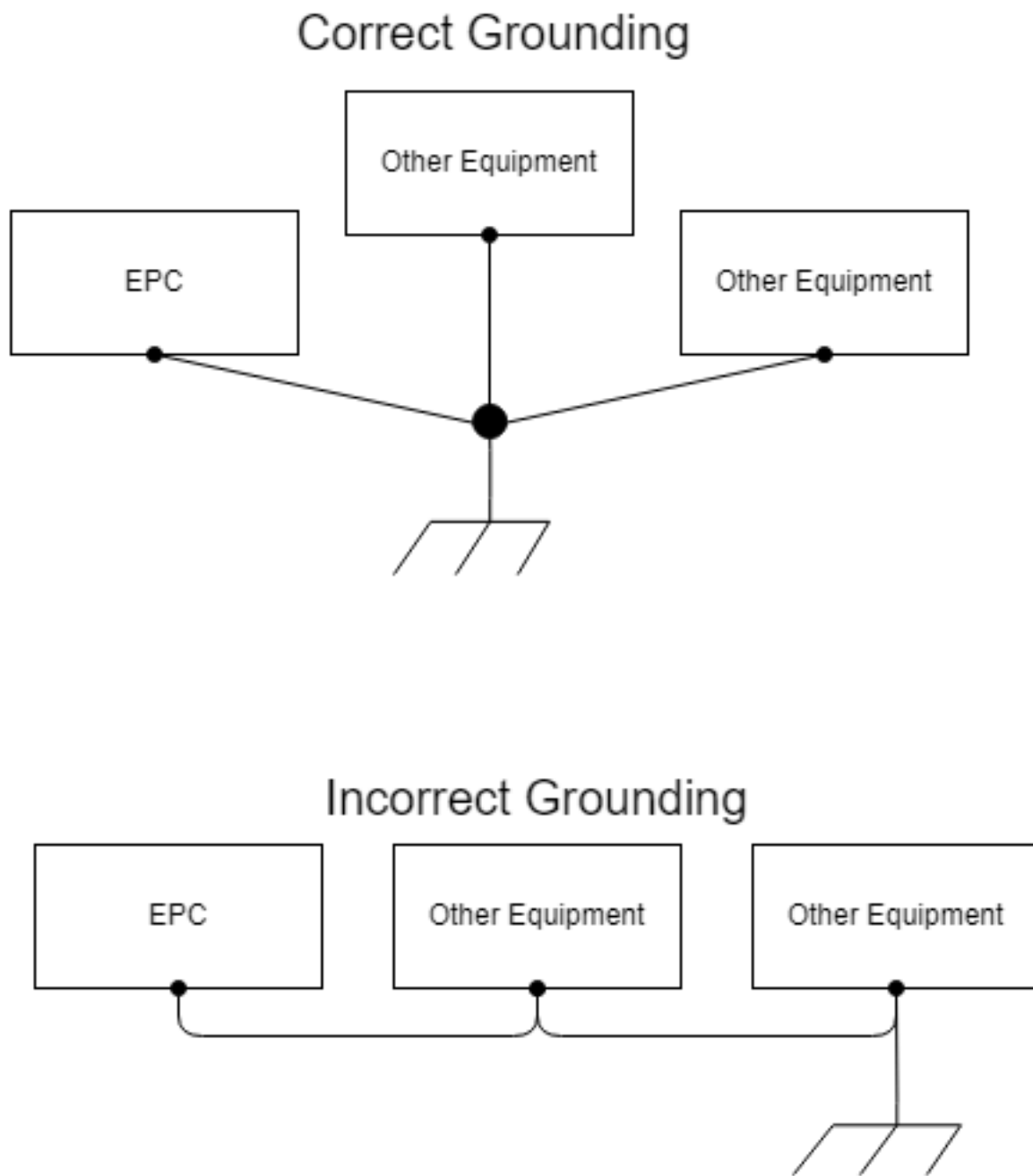


Figure 5: Fig. 5 Examples of Correct and Incorrect Grounding

Input Safety Devices

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

Table 1: Table 1 Requirements for Devices Connected to EPC Inputs

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

Note:

How a sender's safety inputs are assigned depends on the configuration. In some configurations the assignment is fixed and FORT Manager offers no options – this applies to the EPC sender in an [SRC Pro with Global E-Stop Configuration](#) (on page 65) and in a [Two-to-One over Long-Range Bluetooth](#) (on page 59). In others you choose it – in a [Two-to-One with a WES Pro and an EPC](#) (on page 61), the EPC sender's Input 1 is configurable and is the input that stops the machine.

Before wiring a sender, check which input its configuration uses.

Connecting an EPC Sender to Ethernet

If you plan to use Ethernet for communication, connect the J3 port to your Ethernet gateway using an M12 - D cable:

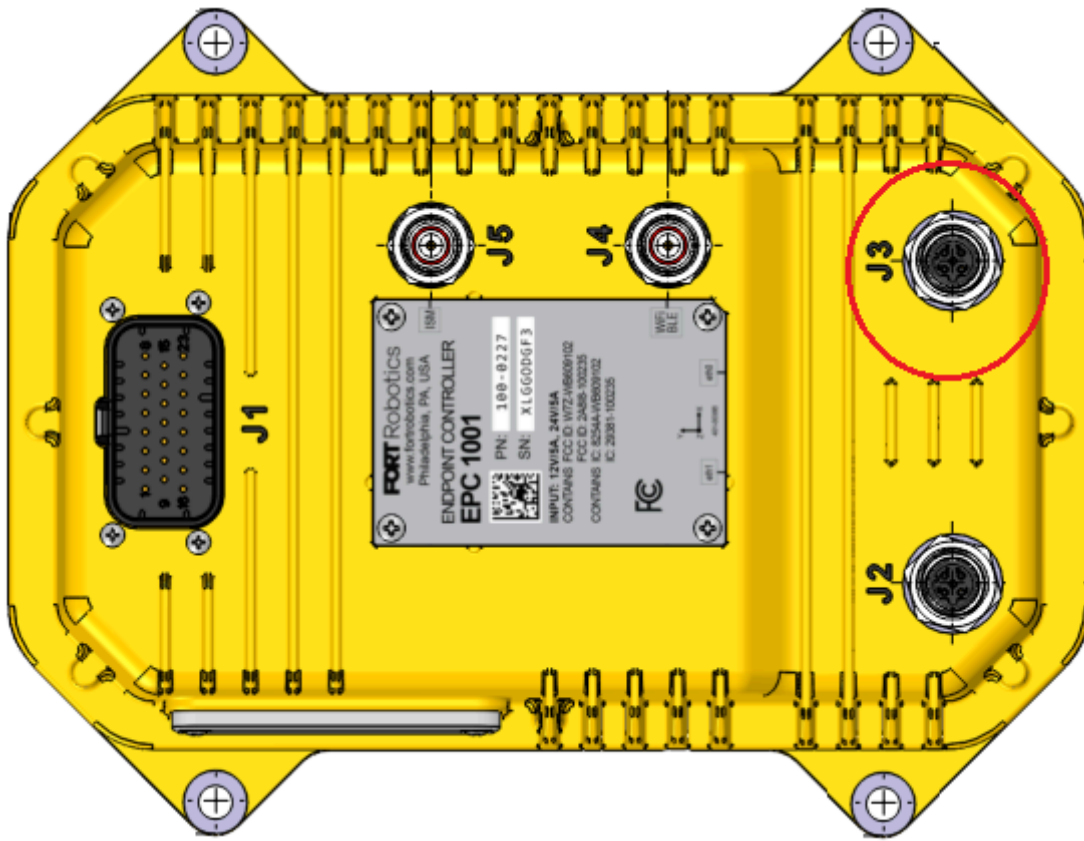


Figure 6: Fig. 6 EPC J3 Port

Placing an ISM Radio Antenna on EPC Sender

If you plan to use ISM Radio for communication, you must place an antenna on the J5 quick disconnect antenna port.

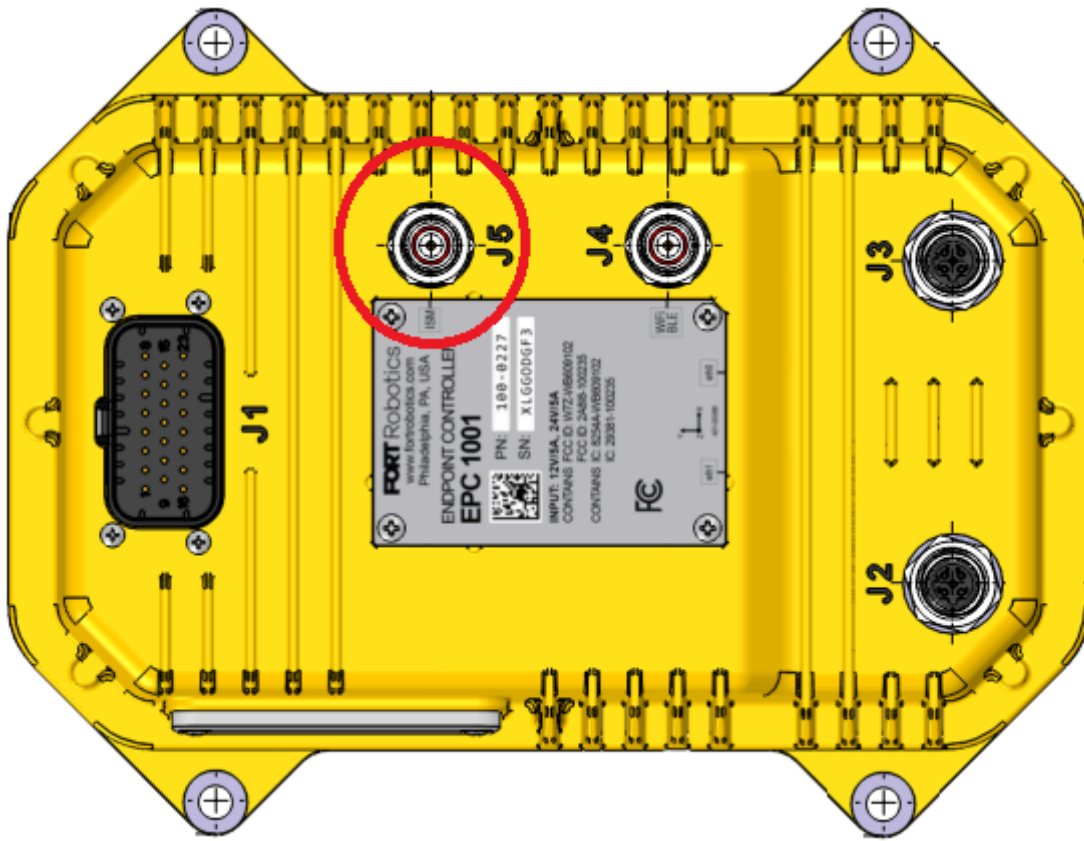


Figure 7: Fig. 7 EPC J5 Antenna Port



CAUTION:

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

Operating an ISM radio without an antenna installed could damage the unit.

Use grommets when routing the antenna cable through enclosures.

Important:

[Antennas](#) (on page 193) provides a list of FORT recommended antennas, but you may use your own antenna if you so choose. Be certain that it meets the standards for antennas listed in [Notifications and Certifications](#) (on page 218).

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

Placing a WiFi / BLE Antenna on EPC Sender

If you plan to use Wi-Fi or BLE for communication, you must place an antenna on the J4 quick disconnect antenna port.

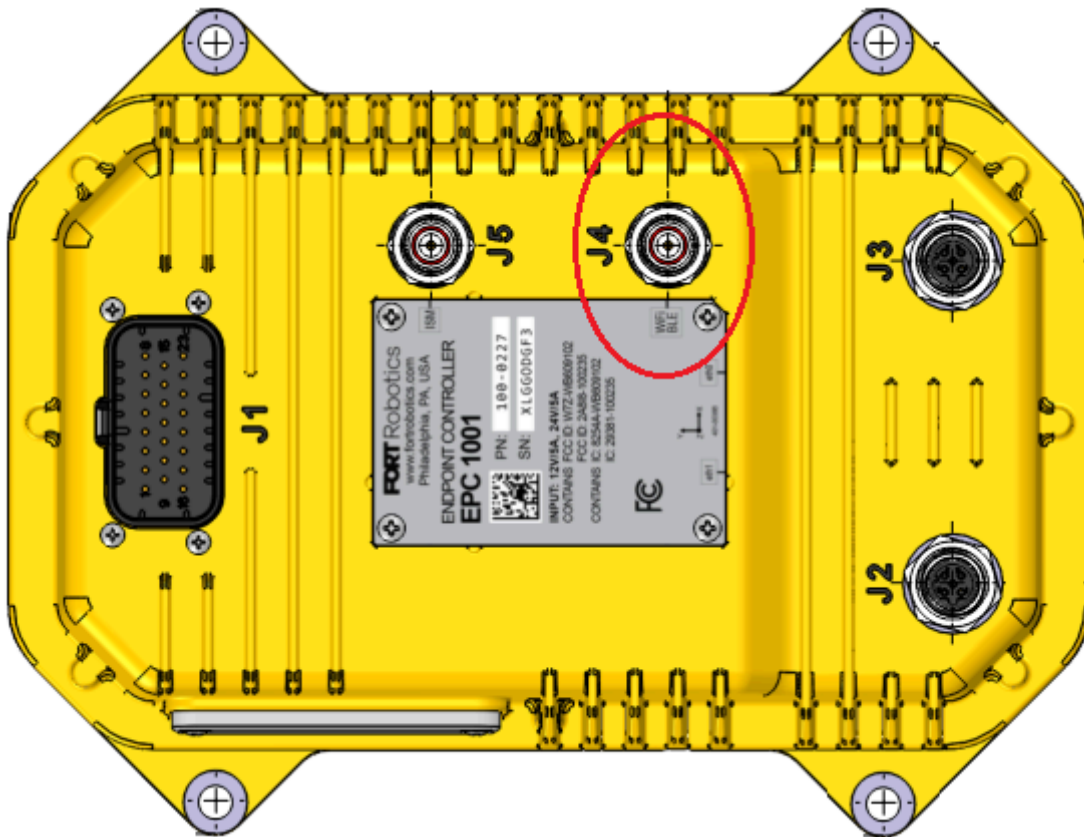


Figure 8: Fig. 8 EPC J4 Antenna Port



CAUTION:

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

Use grommets when routing the antenna cable through enclosures.

Important:

[Antennas](#) (on page 193) provides a list of FORT recommended antennas, but you may use your own antenna if you so choose. Be certain that it meets the standards for antennas listed in [Notifications and Certifications](#) (on page 218).

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

Wiring EPC Receivers

Important:

When wiring an EPC receiver to your equipment (equipment under control, or EUC), refer to [EPC I/O Connector Pinout and Cable](#) (on page 142), which lists each of the EPC's connector signals.

Use the J1 connector on the EPC to wire the EPC to the EUC, a power source, and optionally to a CAN bus.

**CAUTION:**

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

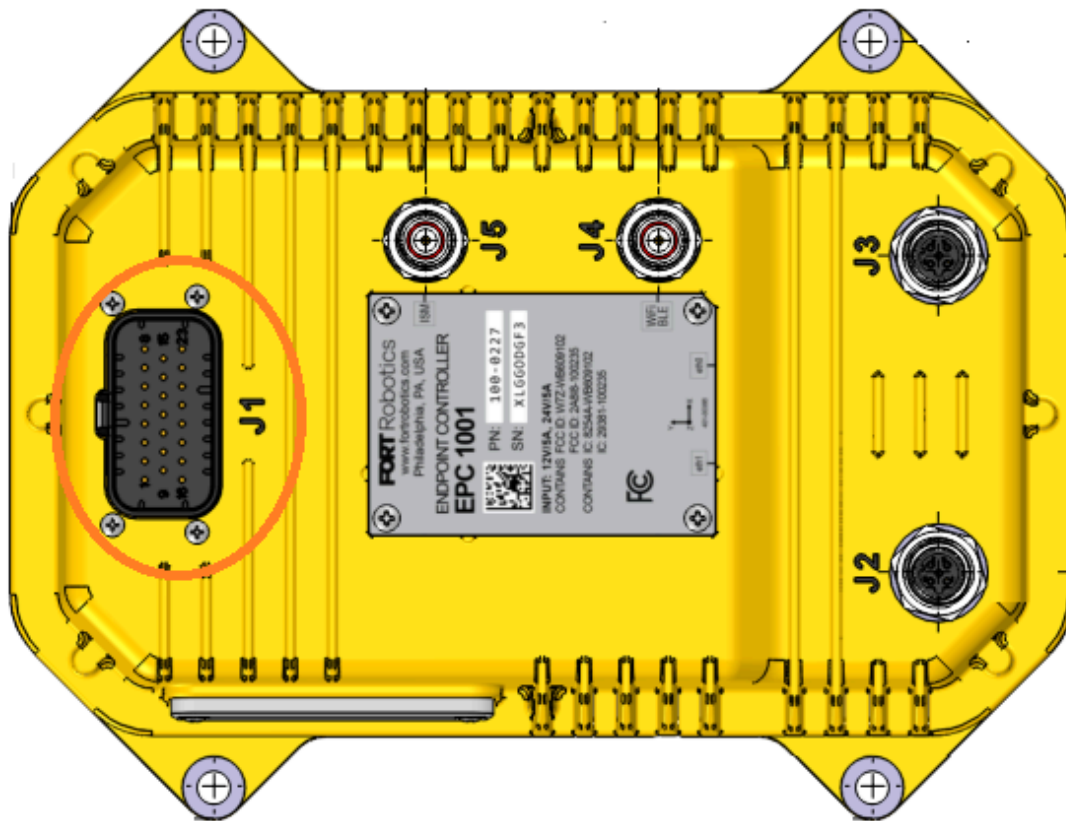


Figure 9: Fig. 9 EPC J1 Port

Before you begin, have on hand:

- A TE 770680-1 connector, the recommended mating connector to the EPC's 23 pin port.
- A FORT #100-0256 Integration Cable to wire the EPC to your equipment.
- The relays to attach to the EUC. See [EPC Recommended and Tested Relays](#) (on page 23) for a list.

**Warning:**

Do **not** use latching relays because the contactors of a latching relay will not open after power is removed from the coil, thereby creating an unsafe situation.

We highly recommend that you use relays that require manual reset, not relays that reset automatically; see [Selecting Automatic or Manual Reset for Relays](#) (on page 25).

Wiring EPC Receivers with EPC or WES Pro Sender

This section explains how to wire an EPC receiver in a configuration with an EPC or WES Pro sender. See [Wiring Receivers with an SRC Pro Sender](#) (on page 23) if the sender includes an SRC Pro.

For each EPC safety 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 EPC keeps the output on to keep the relays closed. On the other hand, if safety is requested, the EPC 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.

Refer to the figure: [EPC Safety Output Diagram](#) (on page 22) to see a wiring diagram of one EPC output connected to two relays in series to control the power supply of the EUC.

Note:

The type of sender in your configuration determines which outputs you can wire on the EPC *receiver*:

- In a configuration with an EPC *sender*, you can wire Output 1, Output 2, or both on the EPC *receiver*.
- In a configuration with a WES Pro sender, you can wire either Output 1 or Output 2, but *not* both on the EPC *receiver*.

Make certain that the outputs specified in FORT Manager match the wiring you are doing here.

To wire safety outputs on an EPC receiver to your equipment:

1. Attach the TE 770680-1 connector and FORT #100-0256 Integration Cable to the J1 port on the EPC.
2. For Output 1, connect pin 18 (Channel 1, Output 1) and pin 23 (Channel 0, Output 1) to the safety device.
3. For Output 2, connect pin 17 (Channel 1, Output 2) and pin 22 (Channel 0, Output 2) to the safety device.

Output 3 is reserved for use in a configuration with an SRC Pro.

4. Connect Pins 7 & 8 (PVin_RTN) to the negative polarity terminal of the EUC power supply.
5. Connect Pins 14 & 15 (PVin_IN) to the positive polarity terminal of the EUC power supply.
6. Connect Pin 9 (CH_GND) to ground. Connect to common power supply if earth ground is not available such as in a moving vehicle. See [Grounding Receiver EPCs](#) (on page 26) for more information.
7. Connect the safety device to common power supply and ground (see following two figures).



CAUTION:

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

The following figure shows an example of the two channels (CH0 and CH1) of one Endpoint Controller (EPC) output connected to two relays in series to control the power supply of the EUC:

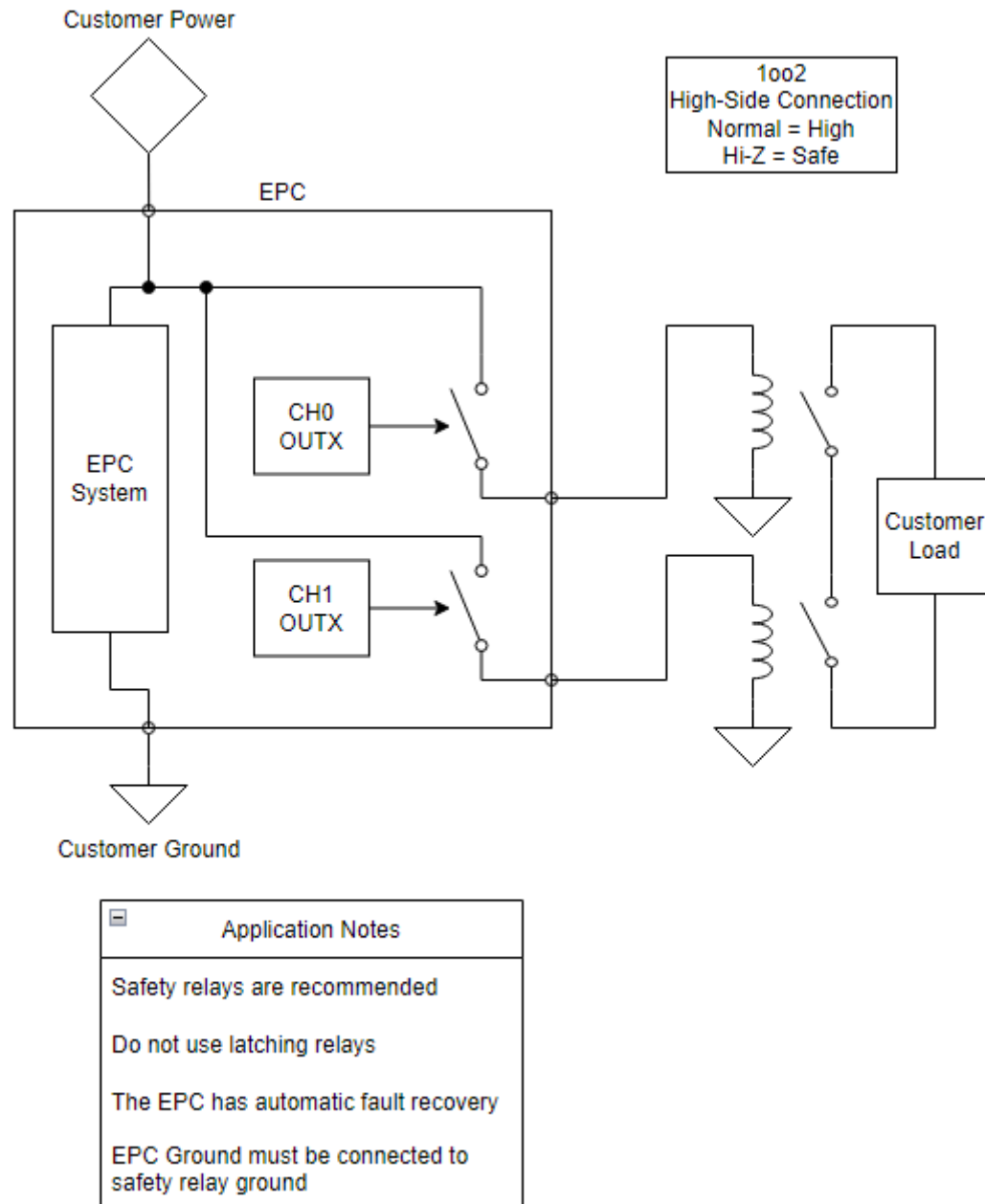


Figure 10: Fig. 10 EPC Safety Output Diagram

Note the following about this setup:

- You must connect the EPC ground to the safety relay ground.
- The EPC 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.

The EPC utilizes OSSD test pulses to detect shorts, so the downstream safety input must be able to filter out these pulses. See [OSSD Pulses](#) (on page 190) for detailed information on how Pro series receivers use OSSD pulses.



Warning:

Do **not** use latching relays because the contactors of a latching relay will not open after power is removed from the coil, thereby creating an unsafe situation.

We highly recommend that you use relays that require manual reset, not relays that reset automatically; see [Selecting Automatic or Manual Reset for Relays](#) (on page 25).

Table 2: Table 2 EPC Recommended and Tested Relays

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

See [Recommended Relays](#) (on page 181) for wiring diagrams for each of these relays.

Wiring Receivers with an SRC Pro Sender

How you wire an EPC receiver in a configuration with an SRC Pro sender depends on whether the EUC has autonomous capability.

Note:

The information in this section applies to any configuration that includes an SRC Pro sender and has EPC receivers:

- Machine Select configuration (SRC Pro sender and EPC receiver(s)).
- SRC Pro with Global E-Stop Configuration (SRC Pro and EPC sender with EPC receiver(s)).
- Two-to-One Configuration (SRC Pro and WES Pro sender with EPC receiver).

Wiring an EPC to an EUC Without Autonomous Capability

A machine that does not have autonomous capability can operate in supervised mode only.

As shown in the following figure, you must connect Output 3 on each of the EPCs to the equipment under control (EUC). [Wiring EPC Receivers with EPC or WES Pro Sender](#) (on page 20) 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 EPC keeps the output on to keep the relays' contactors closed. On the other hand, if safety is requested, the EPC 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 have autonomous capability. See [Wiring an EPC to use with Machines With Autonomous Capability](#) (on page 25) for the wiring for machines that do require autonomous operation.

Note:

Although the figure shows a single SRC Pro sender, the wiring for the EPC's would be the same if an EPC or WES Pro were added as senders.

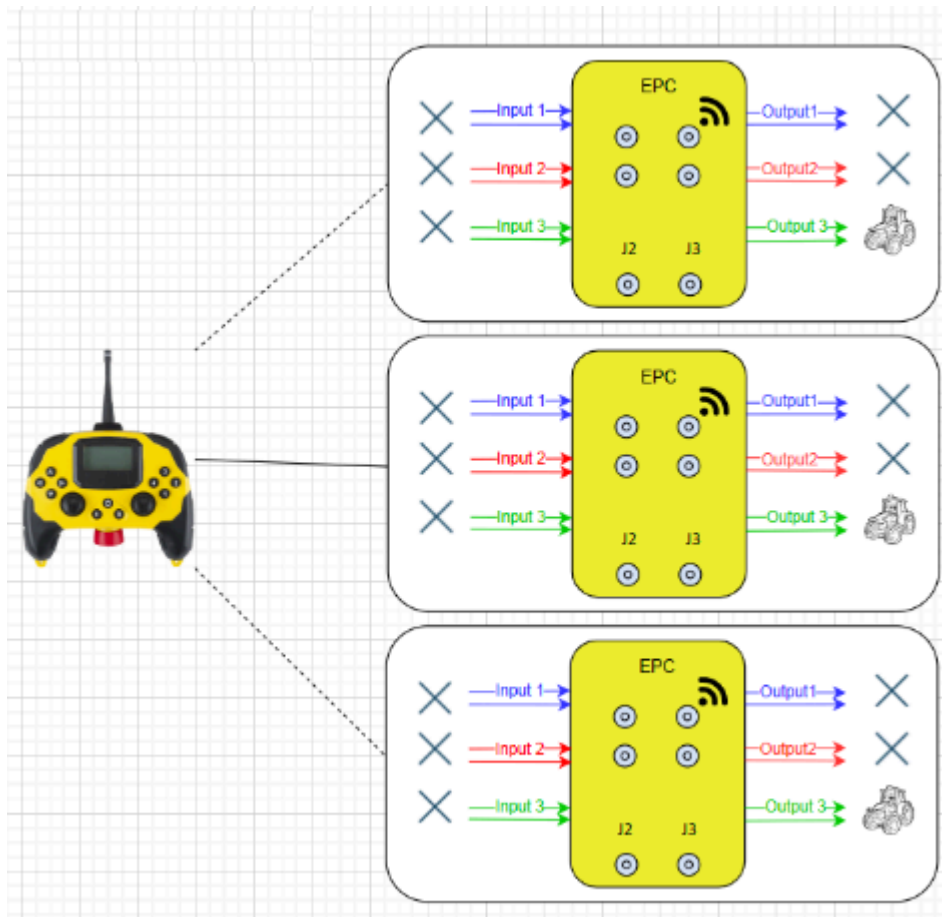


Figure 11: Fig. 11 Machine Select Supervised Mode

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

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

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

Wiring an EPC to use with Machines With Autonomous Capability

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

Note:

Although the figure shows a single SRC Pro sender, the wiring for the EPC's would be the same if an EPC or WES Pro were added as senders.

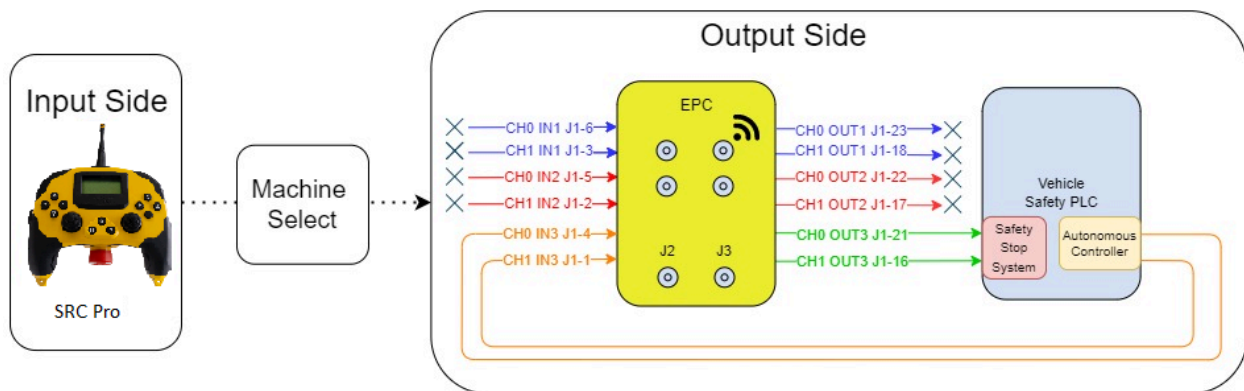


Figure 12: Fig. 12 Input 3 Asserted on EPC Receiver

As long as the customer safety signal to Input 3 on the EPC remains in the normal state (high), the machine remains powered up and running. If the customer safety signal to the EPC changes out of the normal state, the EPC automatically switches to safe mode, turning off Output 3, and breaking the power connection to the EUC. Machines such as this can operate in supervised or unsupervised mode. In fact, when first connected to an SRC Pro, they are always in supervised mode.

Selecting Automatic or Manual Reset for Relays

When designing and implementing the safety circuit downstream from the EPC, including the safety relays, be certain to reference ISO 13850, which defines the core principles for designing and implementing an emergency stop (E-stop) function on machinery, and ISO 13849-1, which defines how to design and validate safety-related parts of control systems on machinery.

Important:

We highly recommend that for an EPC's output you attach relays that require manual reset, not relays that reset automatically. If you choose to use relays that reset automatically, be certain that your safety system prevents a hazardous situation from occurring when relays reset automatically.

**Warning:**

Do **not** connect latching relays to EPC outputs because the contactors of a latching relay will not open after power is removed from the coil, thereby creating an unsafe situation.

Grounding Receiver EPCs**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. 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. Ensure that you ground unused pins in connectors and unused wires in cables at a single point on the connector. Ground unused wires at alternate ends to nearby ground pins.

In addition, if you require a pull down resistor in order to make the output signal go to ground when an E-Stop is triggered, we recommend using a 1.6k ohm resistor to pull the output pins (16, 17, 18, 21, 22, and 23, depending on which ones are used) to ground.

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

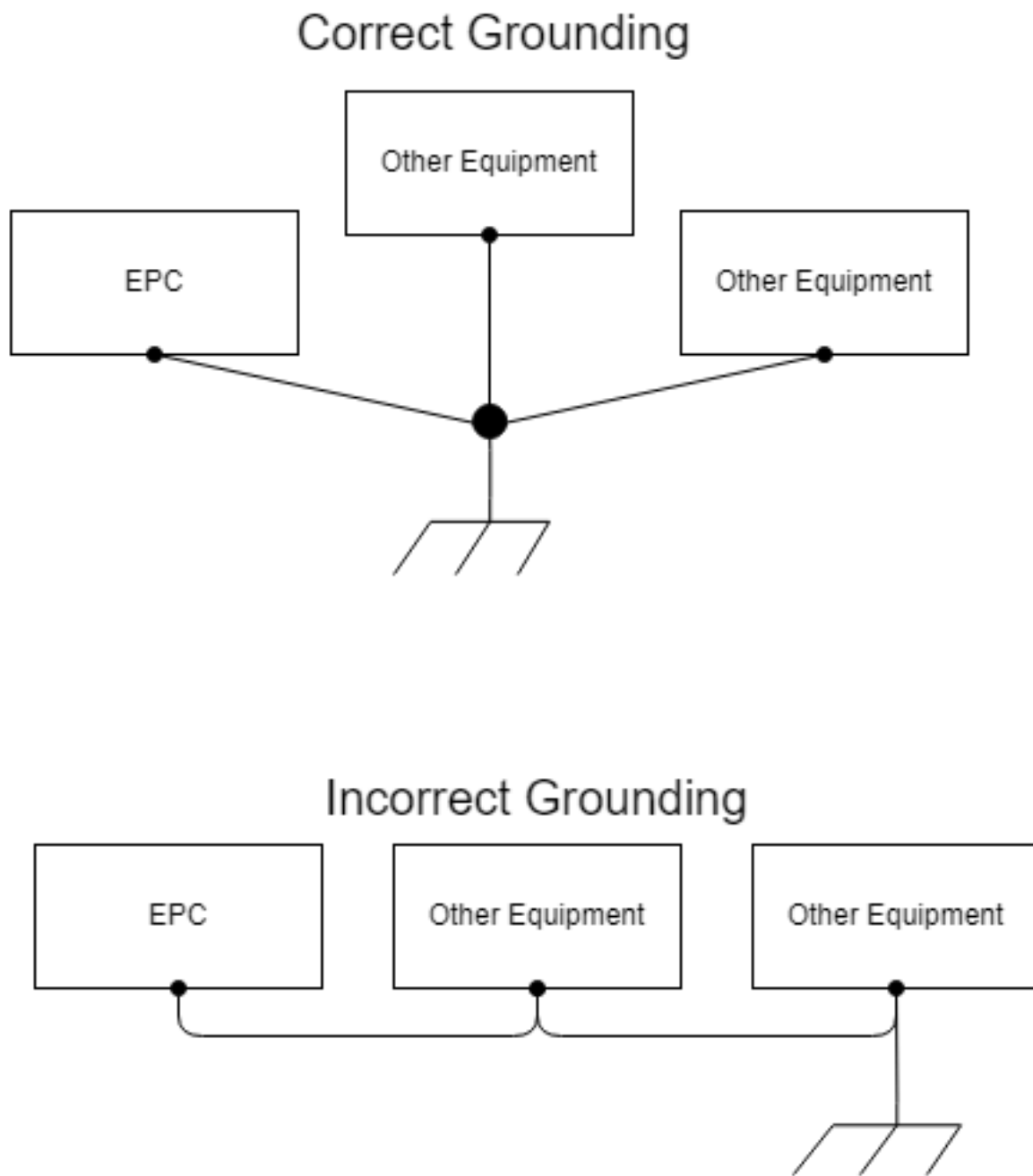


Figure 13: Fig. 13 Examples of Correct and Incorrect Grounding

Engine Cranking (EPC)

If you attach the EPC to an ignition circuit, be aware that engine cranking can drop the voltage below 8 V (on a 12 V system) causing the EPC to turn off the outputs and triggering a safe state. In addition, cranking may drop the voltage low enough that the EPC temporarily stops functioning and resets. You should assess whether this behavior is a safety issue for your application. It may not be. For example, if the EPC doesn't power up until after the equipment is running, cranking the engine shouldn't affect the

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

Connecting an EPC Receiver to Ethernet

If you plan to use Ethernet for communication, connect the J3 port to your Ethernet gateway using an M12 - D cable:

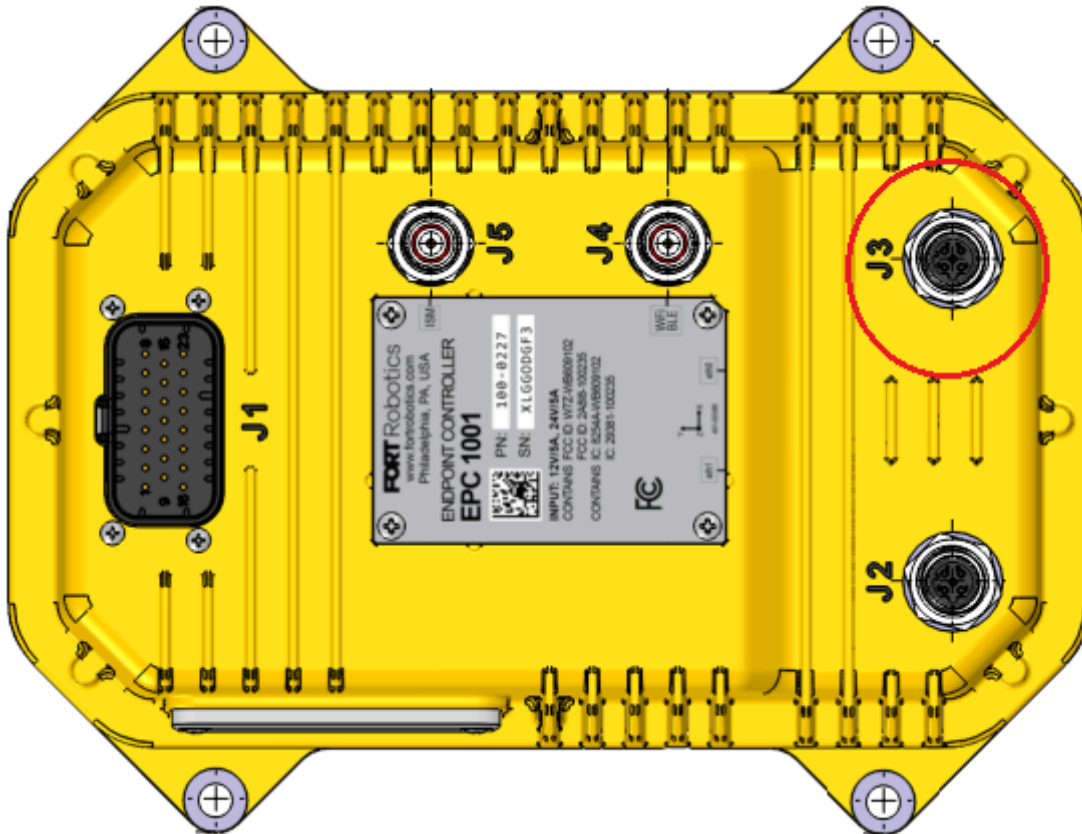


Figure 14: Fig. 14 EPC J3 Port

CAN Interface

If you are using CAN, which is optional, connect the CAN bus from the EPC to the EUC (CAN1_L and CAN1_H, pins 11 and 12,).

Important:

Termination resistors are important for reliable CAN bus communication. The EPC integration cable does not come with any termination inside the cable. You may need a 120 ohm termination resistor if one isn't already present in the CAN network.

If you require shielding, wire CAN1_SHIELD (pin 13) to the EUC.

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, which 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.

Placing an ISM Radio Antenna on EPC Receiver

If you plan to use ISM Radio for communication, you must place an antenna on the J5 quick disconnect antenna port.

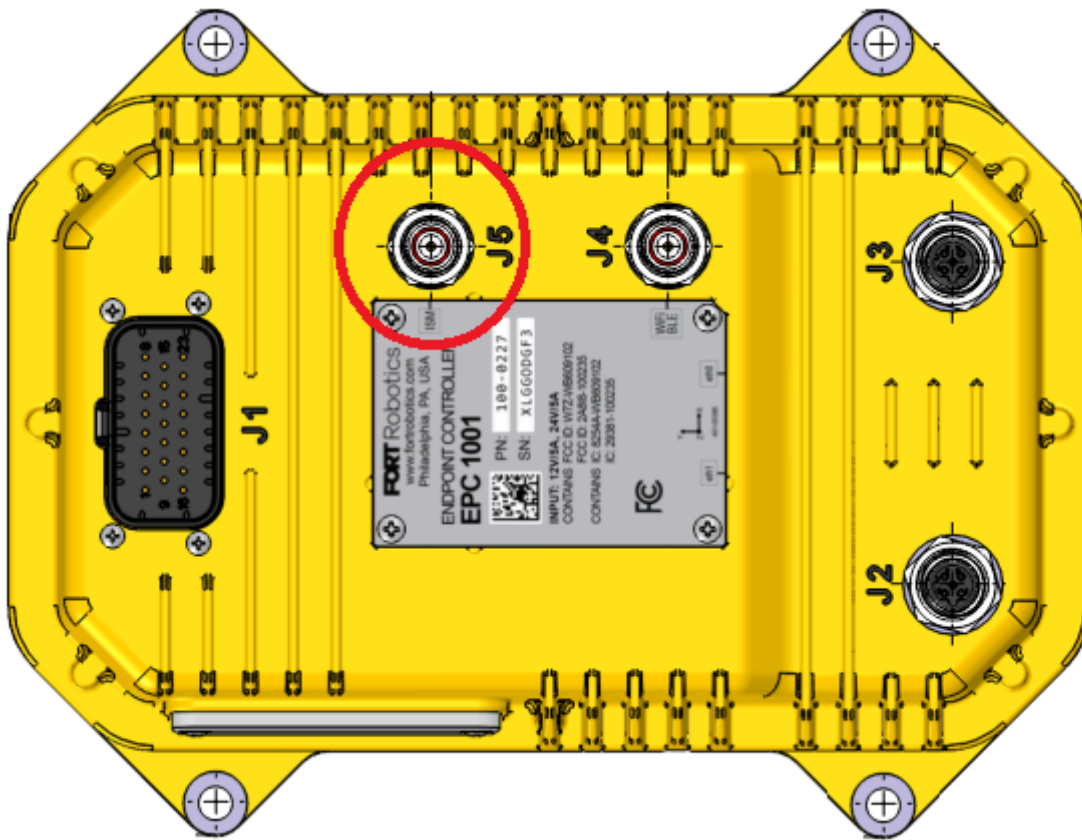


Figure 15: Fig. 15 EPC J5 Antenna Port



CAUTION:

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

Operating an ISM radio without an antenna installed could damage the unit.

Use grommets when routing the antenna cable through enclosures.

Important:

[Antennas](#) (on page 193) provides a list of FORT recommended antennas, but you may use your own antenna if you so choose. Be certain that it meets the standards for antennas listed in [Notifications and Certifications](#) (on page 218).

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

Placing a WiFi / BLE Antenna on EPC Receiver

If you plan to use Wi-Fi or BLE for communication, you must place an antenna on the J4 quick disconnect antenna port.

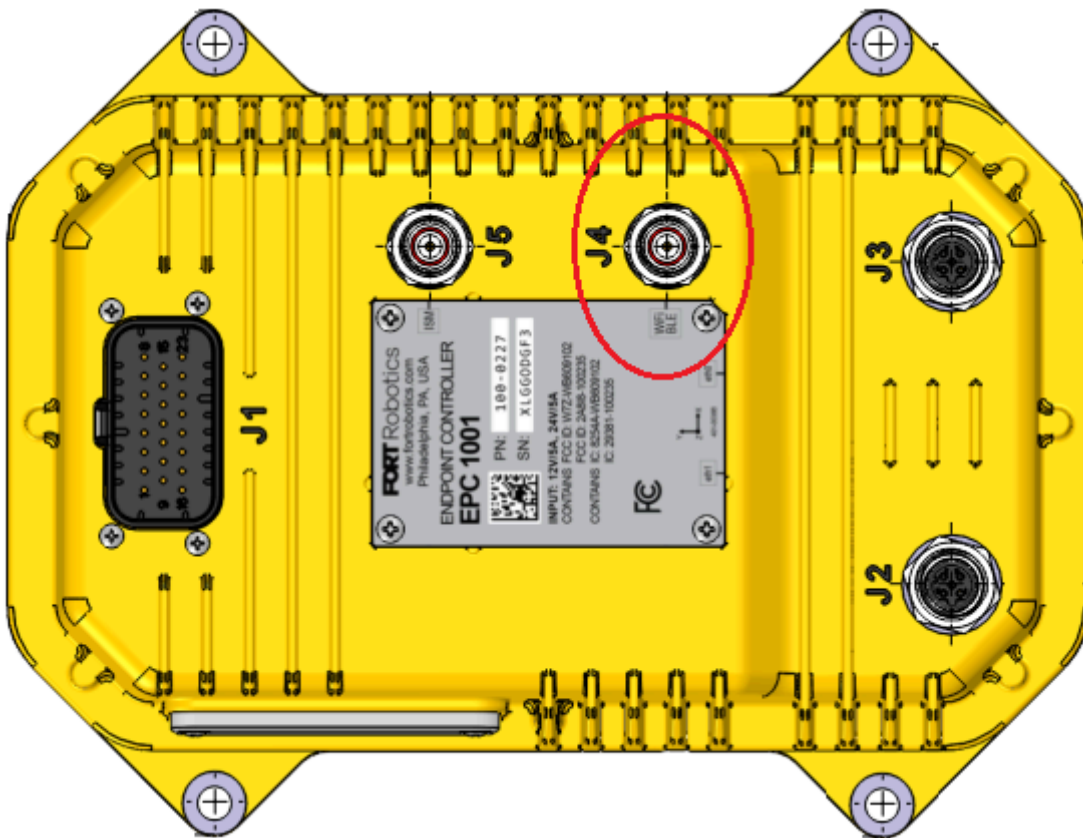


Figure 16: Fig. 16 EPC J4 Antenna Port



CAUTION:

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

Use grommets when routing the antenna cable through enclosures.

Note:

[Antennas](#) (on page 193) provides a list of FORT recommended antennas, but you may use your own antenna if you so choose. Be certain that it meets the standards for antennas listed in [Notifications and Certifications](#) (on page 218).

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

Mounting an EPC

An Endpoint Controller has four mounting holes to attach it to the equipment under control, EUC (receiver), or your chosen structure (sender) as shown in the following figure. We recommend using ¼-20 or M6 machine screws for mounting.

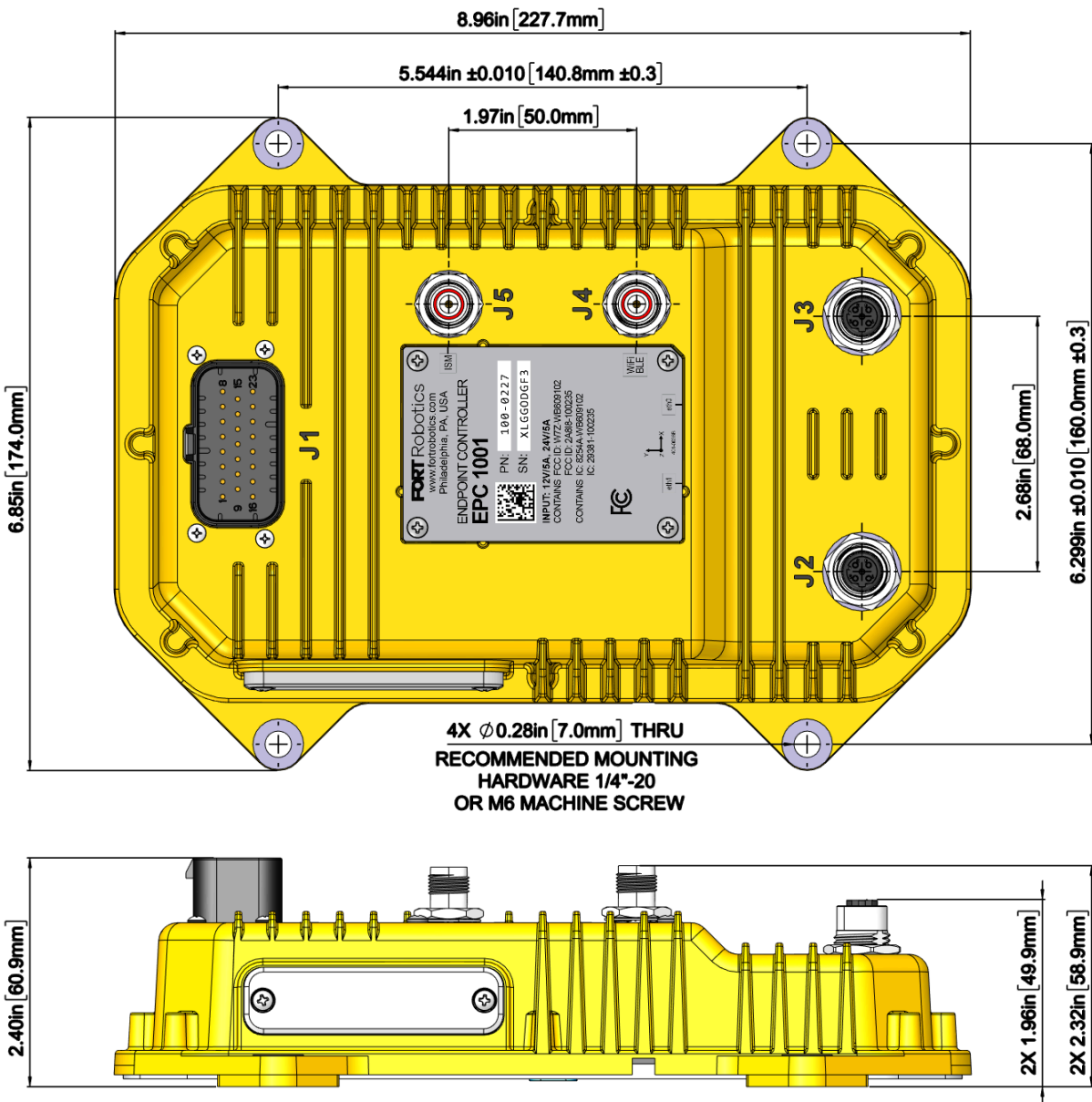


Figure 17: Fig. 17 EPC-1001 Mechanical Drawing



CAUTION:

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

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

Chapter 3. Wire and Mount Nano Safety Controller Pro

This chapter explains how a Nano Safety Controller Pro's inputs and outputs relate to each other, how to wire the board to your equipment for either a wireless radio or an IP network, and how to select an antenna and embed the board in your machine.

Before jumping to the actual procedures, we recommend that you read the material in the following sections:

- [Relationship of Inputs and Outputs](#) (on page 33), which explains the differences different relationships between the inputs and outputs depending on the type of sender and on whether your system is configured for CAT0 (Immediate Stop) or CAT1 (Controlled Stop).
- [Understanding NSC Pro Safety Output Wiring](#) (on page 35), which explains the use of safety relays connected to NSC Pro outputs.

When you're ready to wire up your devices, we provide separate procedures depending on the type of your configuration:

- [Wiring an NSC Pro for a Wireless Radio \(SRC Pro, WES Pro, EPC\)](#) (on page 37) explains how to wire the NSC Pro to your equipment for any type of sender when communicating via ISM or Bluetooth.
- [Setting up an NSC Pro for IP Networking \(EPC Sender\)](#) (on page 40) explains how to wire the NSC Pro to your equipment when communicating via Wi-Fi or Ethernet. Because the NSC Pro does not come with a Wi-Fi modem or wired Ethernet adapter, extra hardware and instructions are necessary to support this configuration.

Relationship of Inputs and Outputs

FORT Manager enables you to configure an NSC Pro receiver with one of two shutdown options, CAT0 immediately shuts down any corresponding outputs on the receiver, or CAT1 which provides a phased output, as follows:

- **CAT0 configuration** – The type of sender determines the specific behavior:
 - An **EPC** sender defines a one-to-one correspondence between the inputs on the EPC and each output of all receivers in the configuration. Input 1 of the sender controls Output 1 of the receiver and Input 2 of the sender controls Output 2 of the receiver. Applying the E-Stop immediately turns off the corresponding output on the receiver.
 - For an **SRC Pro** sender the built-in E-Stop button is pre-defined to control Output 2 of the receiver; applying the E-Stop immediately turns off Output 2 of the corresponding receiver.
 - For a **WES Pro** sender the built-in E-Stop button is pre-defined to control Output 1 of the receiver; applying the E-Stop immediately turns off Output 1 of the corresponding receiver.

Note:

The assignments above are the defaults for a configuration with a single sender. In a Two-to-One configuration that offers an Output to Control setting, that setting determines which output both senders act on, and it overrides these defaults. For more information, see [Choosing Which Output the Senders Control](#) (on page 62).

- **Two senders on one receiver**

In a Two-to-One configuration, both senders act on the same output of the receiver. Where the configuration offers an **Output to Control** setting, that setting determines which output — and it overrides the per-sender defaults described above.

Table 3: Output Controlled in a Two-to-One Configuration (CAT0)

Output to Control	WES Pro	EPC sender	Receiver output used
Output #1	Built-in E-Stop	Input 1	Output 1
Output #2	Built-in E-Stop	Input 2	Output 2

The EPC sender's usable input tracks the output you select: Input 1 for Output #1, Input 2 for Output #2. The input that does not match is grayed out in FORT Manager and has no effect. For more information, see [Choosing Which Output the Senders Control](#) (on page 62).

Important:

The output stays off while either sender is requesting a stop. Releasing the E-Stop on one sender does not turn the output back on if the other sender is still stopping it.

- **CAT1 configuration** – For all types of senders, allows a phased shutdown of the equipment:
 - Applying the E-Stop immediately turns off Output 1 of the receiver and after a user-defined delay (up to 30 seconds, configured by you in 0.1 sec increments in FORT Manager) turns off Output 2 of the receiver.
 - When the E-Stop request is removed, both outputs (Output1 and Output2) turn on at the same time, i.e., there is no delay between them during reactivation.

For more information see [Understanding Stop Categories for Machinery Stopping Functions](#).

The following diagram illustrates these relationships.

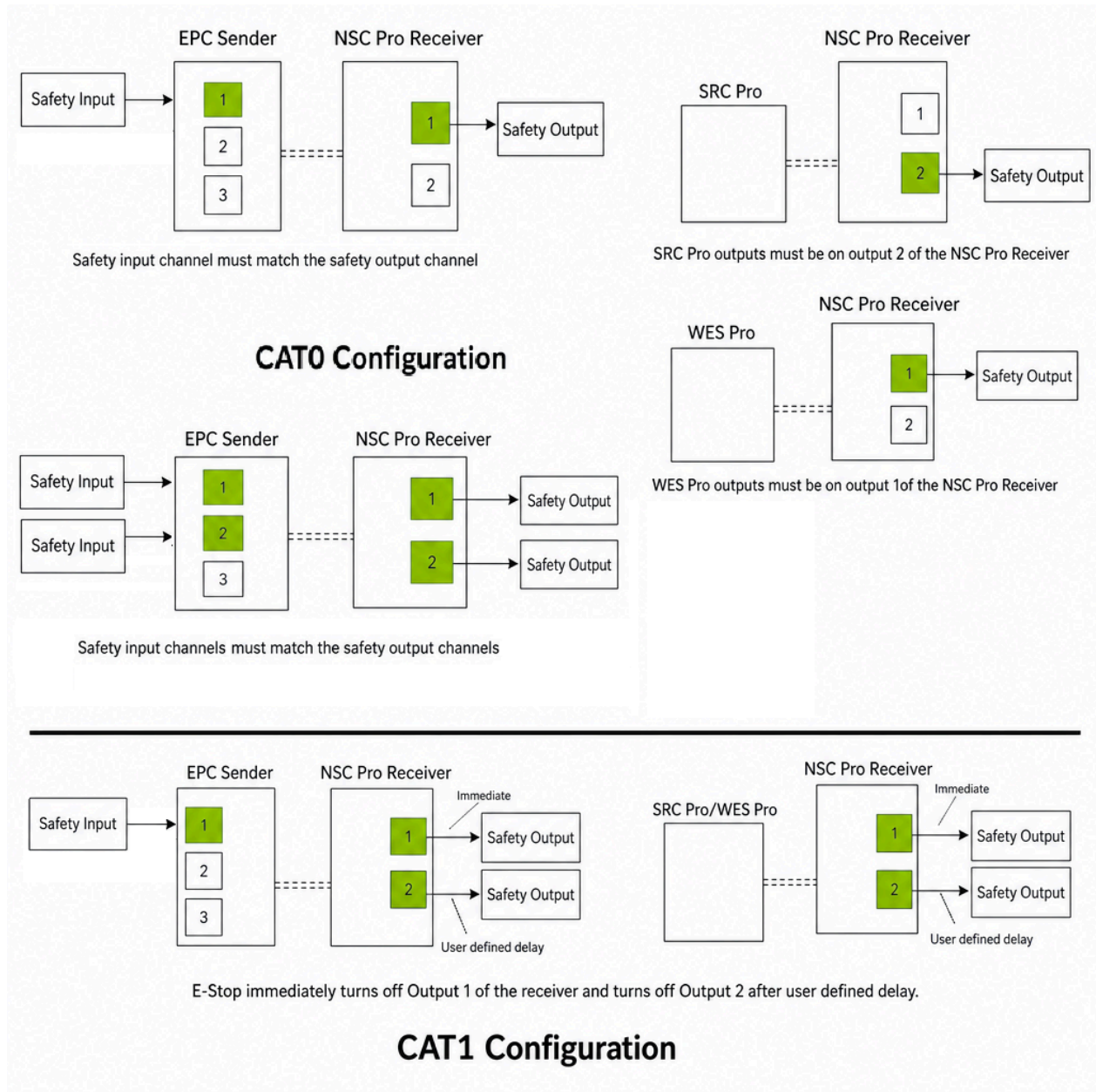


Figure 18: Fig. 18 Examples of CAT0 and CAT1 Wiring Diagrams

Understanding NSC Pro Safety Output Wiring

For each NSC safety 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 NSC keeps the output on to keep the relays closed. On the other hand, if safety is requested, the NSC 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 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:

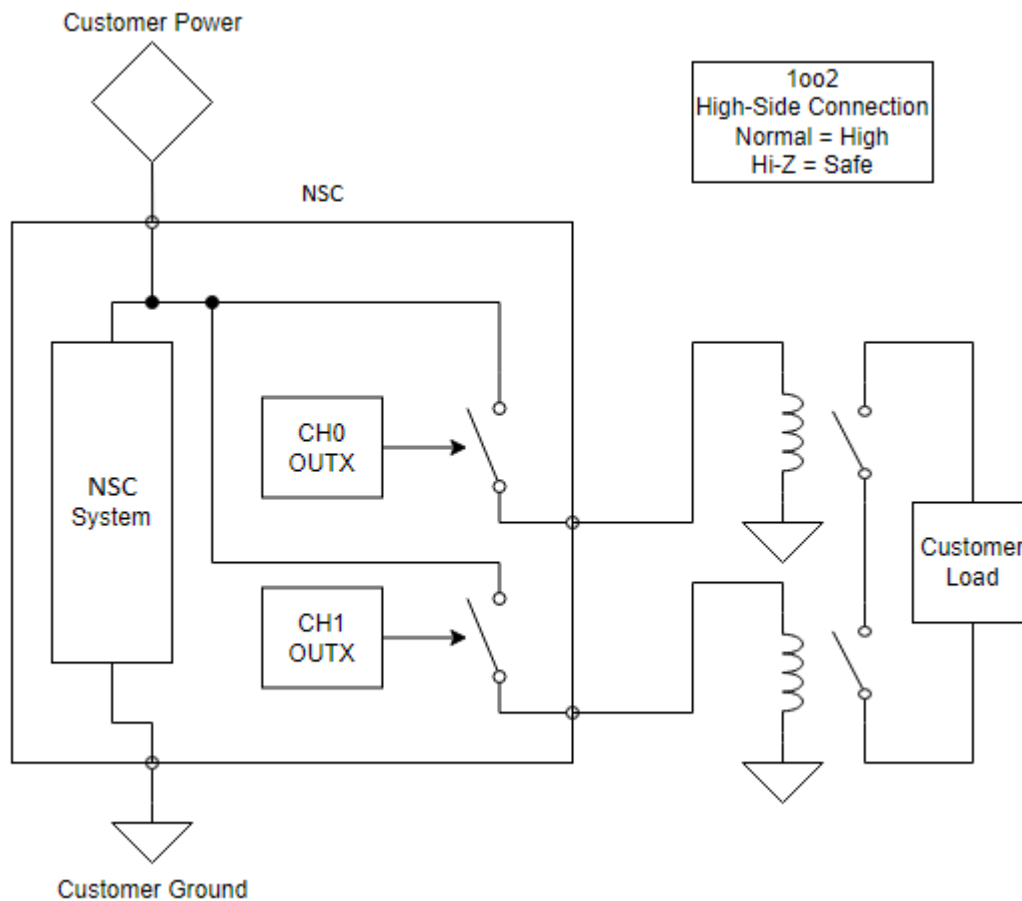


Figure 19: Fig. 19 NSC Safety Output Diagram

Note the following about this setup:

- You must connect the NSC ground to the safety relay ground.
- The NSC 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 and verify that it is compatible with OSSD.

The NSC Pro utilizes OSSD test pulses to detect shorts, so the downstream safety input must be able to filter out these pulses. See [OSSD Pulses](#) (on page 190) for detailed information on how Pro series receivers use OSSD pulses, including how to turn them off for NSC Pro devices.

Table 3 NSC Recommended and Tested Relays

Manufacturer	Model	Supply Voltage
TE	V23047-A1005-A501	5

Manufacturer	Model	Supply Voltage
TE	V23047-A1012-A501	12
PANASONIC	SFS3-L-DC12V-D	12
OMRON	G7SA-3A1B DC12	12

See [Recommended Relays](#) (on page 181) for wiring diagrams for each of these relays.

Selecting Automatic or Manual Reset for Relays (NSC Pro)

When designing and implementing the safety circuit downstream from the NSC Pro, including the safety relays, be certain to reference ISO 13850, which defines the core principles for designing and implementing an emergency stop (E-stop) function on machinery, and ISO 13849-1, which defines how to design and validate safety-related parts of control systems on machinery.

Important:

We highly recommend that for an NSC Pro's output you attach relays that require manual reset, not relays that reset automatically. If you choose to use relays that reset automatically, be certain that your safety system prevents a hazardous situation from occurring when relays reset automatically.



Warning:

Do **not** connect latching relays to NSC Pro outputs because the contactors of a latching relay will not open after power is removed from the coil, thereby creating an unsafe situation.

Wiring an NSC Pro for a Wireless Radio (SRC Pro, WES Pro, EPC)

This section shows how to wire an NSC Pro to your equipment for any type of sender when communicating over a wireless radio — ISM, Bluetooth, or Long-Range Bluetooth. The wiring is the same for all three.

If your devices will communicate via Wi-Fi or Ethernet, see the instructions in [Setting up an NSC Pro for IP Networking \(EPC Sender\)](#) (on page 40).

Note:

For all of the following wiring procedures, refer to [NSC PRO 80-Pin I/O Connector Pinout](#) (on page 152), which lists each of the NSC Pro's connector signals.



Warning:

Electrostatic Discharge (ESD) Handling

The NSC Pro can be damaged by electrostatic discharge (ESD). To reduce the risk of ESD damage while installing an NSC Pro, take the following precautions:

- Wear a grounded ESD wrist strap when handling the device.
- Work on an ESD-safe mat or grounded surface.

- Avoid touching exposed connector pins or internal circuitry.
- Maintain ambient humidity above 30% when possible.
- Discharge static by touching grounded metal before handling the device.
- Store the controller in anti-static packaging when not installed.

Required Items

Before you begin, have on hand your FORT devices and your equipment to control (EUCs), as well as:

- A TE 5-5179180-3 80-pin receptacle connector that you mate with the TE 5177986-3 80-pin connector plug on the secondary side of the board to wire the NSC Pro to the EUC, to a power source, etc.
- An integration cable.
- The relays to attach to the EUC. See [NSC Pro Recommended Relays](#) (on page 181).
- A configuration that you built in FORT Manager.

Verify whether the configuration is CAT0 (Immediate Stop) or CAT1 (Controlled Stop).

Important:

The type of *sender* in your configuration and whether you specify CAT0 or CAT1 determine which outputs you can wire on the NSC Pro receiver:

- For **CAT0** (Immediate Stop) configurations:
 - For an EPC sender, you may wire Output 1 only, or wire both Output 1 and Output 2. You cannot wire only Output 2, because Output 1 is the primary safety output.
 - For an SRC Pro sender, you must wire Output 2 only.
 - For a WES Pro sender, you must wire Output 1 only.
- For **CAT1** (Controlled Stop) configurations with any type of sender, the NSC Pro uses two independent safety outputs to support a controlled stop followed by power removal. Therefore you must wire both NSC Pro outputs, as follows:
 - Output 1 always performs the immediate shutdown portion of the stop.
 - Output 2 always performs the phased (delayed) shutdown portion of the stop.

This allows you to remove power immediately from one part of the EUC (via Output 1) while allowing another part (via Output 2) to complete a controlled stop before power is removed.

Be sure that the wiring matches the configuration selected in FORT Manager, including whether the system is set for CAT0 or CAT1 behavior.

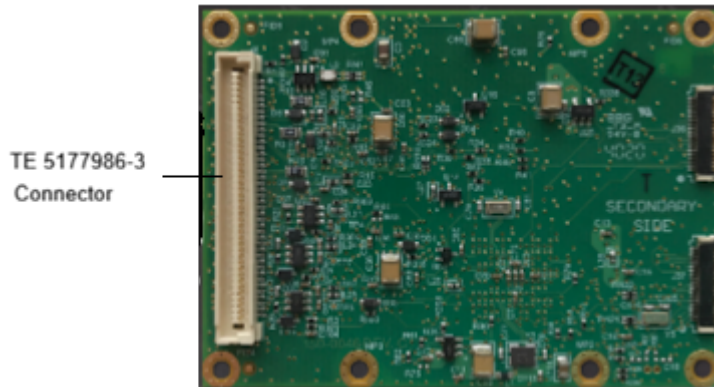


Figure 20: Fig. 20 TE 5177986-3 connector on Secondary Side

To Wire the NSC Pro to the EUC

To begin, attach the TE 5-5179180-3 80-pin receptacle connector to the TE 5177986-3 80-pin connector plug on the secondary side of the board.

1. Connect pins 10 & 12 (PVIN) to the main power supply on the EUC.²
2. Connect grounding pins, 8, 23, 46, 69, and 79 together at the same place (common power supply in the likely case that earth ground is not available).

See [Grounding an NSC Pro](#) (on page 46) for details.

3. If you are using CAN, connect the CAN bus on the NSC Pro to the EUC (CAN0, pins 24 and 26,).

Using the CAN bus is optional and if you are using the serial connection, you can't use CAN.

Important:

Termination resistors are important for reliable CAN bus communication. The NSC Pro integration cable does not come with any termination inside the cable. You may need a 120 ohm termination resistor if one isn't already present in the CAN network.

4. If you are using a serial bus for diagnostics, connect one of the serial ports on the NSC Pro to the EUC (UART0, Pins 50 & 54, or UART1, pins 58 and 62).

Using the serial port is optional, and if you are using CAN, you can't use the serial port to connect to the EUC.

5. For Output 1, connect pin 55 (Channel 0 Output 1) and pin 57 (Channel 1, Output 1) to the safety relay.
6. For Output 2 (if using), connect pin 78 (Channel 0, Output 2) and pin 80 (Channel 0, Output 2) to the safety relay.
7. Make the USB port available for configuring the NSC Pro by connecting pins 2 and 4 for data & pin 6 for power to the USB port on the NSC Pro.

² See [Engine Cranking \(NSC Pro\)](#) (on page 47) for possible issues with connecting the NSC to an ignition circuit for power.

Note that without power (from pin 6) the NSC Pro will not detect the USB connection.

Be certain to tie the ground from the USB source to the same common ground as the main power supply.

8. Optionally, to wire external LEDs to show the power, connection, and operational status of the NSC Pro:
 - a. Wire pins 5, 7, & 9.
 - b. Connect pin 18 to pull 3.3 V output (max current 50mA) from the onboard power supply to power the LEDs.
9. To provide a backup battery (3-3.3 V DC), for example to keep a clock running (which is required to guarantee that you get accurate time stamps from NSC Pro logs):
 - a. Wire pin 48.
 - b. Use Pin 46 to ground the battery to the same ground as the main power supply.

If you aren't providing a battery, tie pin 48 to pin 18 (P3V3_OUT).



CAUTION:

Each output on the NSC is designed with short circuit protection circuitry inside the NSC device. However, drawing more than 750 mA must be avoided since it won't activate short circuit protection and could potentially damage the device. To satisfy applicable wiring codes and conditions, you are responsible for protection of field devices and wiring through appropriate fusing of the circuitry (see [Recommended Relays](#) (on page 181) for details about fuse size and diodes to use).

Setting up an NSC Pro for IP Networking (EPC Sender)

This section applies only when the NSC Pro communicates over Wi-Fi or Ethernet. If your configuration uses a wireless radio — ISM, Bluetooth, or LRBLE — you do not need the additional hardware or the FORT SDK described here. For more information, see [Wiring an NSC Pro for a Wireless Radio \(SRC Pro, WES Pro, EPC\)](#) (on page 37).

The NSC Pro does not come with a Wi-Fi modem or wired Ethernet adapter. To support using Wi-Fi or Ethernet from a FORT sending device, such as an EPC, we supply the FORT SDK, an IP to UART bridge that converts the IP traffic/stream from the sending device to serial traffic that can be read by the NSC Pro. Each machine on which you've embedded an NSC Pro requires that you supply a Linux computer with the Ubuntu OS running the FORT SDK, networked to the sending device via Ethernet or Wi-Fi, and connected to the NSC Pro via Serial and USB.

The following figure illustrates the communication between the EPC and the NSC Pro (through the IP to UART bridge on the Linux computer) as well as the connections between the NSC Pro and the EUC.

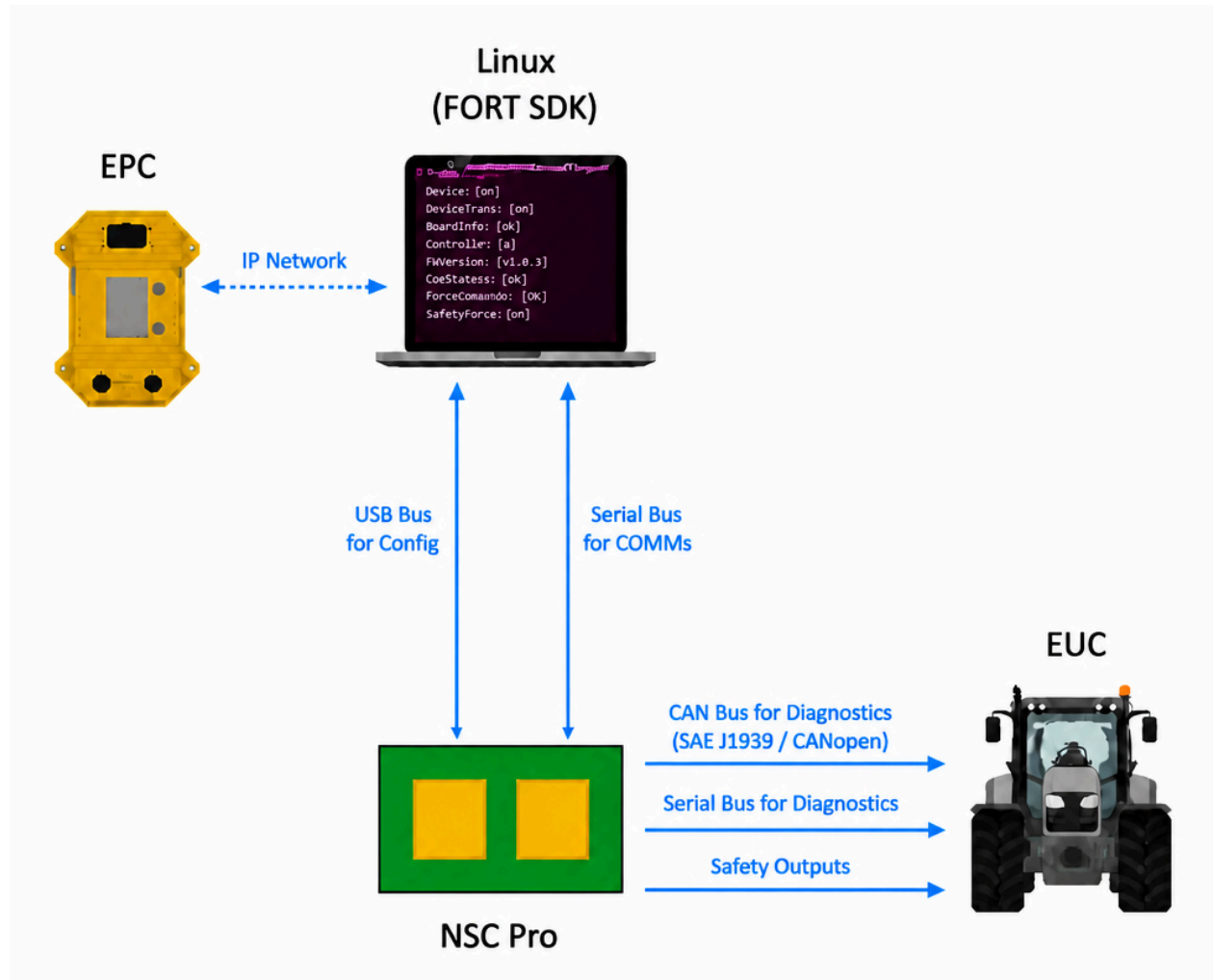


Figure 21: Fig. 21 NSC Pro Communications

Install and Run the FORT SDK

This section provides procedures for downloading, installing, and running the FORT SDK Pro on your Linux machine.

Required Items

- Linux computer running Ubuntu with Ethernet networking capability (required for using the CLI Configuration Tool and the SDK)
- FORT CLI Configuration Tool, `fort_cli_cfg` (find latest version on Firmware tab of FORT Manager).
- FORT SDK Tool, `fort-agent-pro` (find latest version on Firmware tab of FORT Manager).

To Download and Install the FORT SDK

(Requires FORT Manager DeviceManager or Admin role.)

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

FORT Manager downloads a Debian package: `fort-sdk_<version>_amd64.deb` to the Downloads folder on your computer.

1. In a terminal on the Linux machine, use `apt` to install the local version of the FORT SDK from the directory in which you saved it to the Linux host machine:

```
aptinstall ./fort-sdk_<version>_amd64.deb
```

1. Add yourself to the `dialout` user group so you won't need `sudo` permission when using the `fort-sdk` tool to access the serial device:

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

1. Restart the terminal.
2. To verify that the tool has been successfully installed and that you can run it, type the following command in a terminal window:

```
fort-agent-pro -version
```

If you see the current version displayed, the tool is ready to use.

Important:

Set the IP address of the Linux machine to that of the NSC Pro in the FORT Manager configuration.

To Run the FORT SDK Tool

1. In a terminal on the Linux host machine, navigate to the directory in which you installed the application.
2. Launch the tool with the following parameters:

```
fort-agent-pro -s<safety_serial_path> -c<config_serial_path>
```

The paths will appear as shown in the following example if the NSC Pro is connected to the Linux computer:

```
fort-agent-pro -s/dev/serial/by-id/usb-FTDI_Dual_RS232-HS-if01-port0 -c/dev/serial/by-id/usb-FORT_Robotics__Inc._NSC_Pro_NOTSET-if00
```

Important:

To ensure that the FORT SDK is always running on the Linux computer, you can implement it as a service that launches whenever the Linux machine restarts; see [Implement FORT SDK as a Service](#) (on page 195).

Wiring an NSC Pro for IP Networking

Note:

For all of the following wiring procedures, refer to [NSC PRO 80-Pin I/O Connector Pinout](#) (on page 152), which lists each of the NSC Pro's connector signals. In addition, refer to [Fig. 21 NSC Pro Communications](#) (on page 40) for a visual representation of the relationships between the EPC, Linux computer (FORT SDK host), NSC Pro, and the EUC.



Warning:

Electrostatic Discharge (ESD) Handling

The NSC Pro can be damaged by electrostatic discharge (ESD). To reduce the risk of ESD damage while installing an NSC Pro, take the following precautions:

- Wear a grounded ESD wrist strap when handling the device.
- Work on an ESD-safe mat or grounded surface.
- Avoid touching exposed connector pins or internal circuitry.
- Maintain ambient humidity above 30% when possible.
- Discharge static by touching grounded metal before handling the device.
- Store the controller in anti-static packaging when not installed.

Required Items

Before you begin, have on hand:

- A Linux computer running Ubuntu and the FORT SDK, or on which you will install and run the SDK.
- A TE 5-5179180-3 80-pin receptacle connector that you mate with the TE 5177986-3 80-pin connector plug on the secondary side of the board to wire the NSC Pro to the EUC, a power source, the Linux computer, etc (see figure).
- An integration cable.
- The relays to attach to the EUC. See [NSC Pro Recommended Relays](#) (on page 181).

Important:

The type of *sender* in your configuration and whether you specify CAT0 or CAT1 determine which outputs you can wire on the NSC Pro receiver:

- For **CAT0** (Immediate Stop) configurations:
 - For an EPC sender, you may wire Output 1 only, or wire both Output 1 and Output 2. You cannot wire only Output 2, because Output 1 is the primary safety output.
 - For an SRC Pro sender, you must wire Output 2 only.
 - For a WES Pro sender, you must wire Output 1 only.
- For **CAT1** (Controlled Stop) configurations with any type of sender, the NSC Pro uses two independent safety outputs to support a controlled stop followed by power removal. Therefore you must wire both NSC Pro outputs, as follows:
 - Output 1 always performs the immediate shutdown portion of the stop.
 - Output 2 always performs the phased (delayed) shutdown portion of the stop.

This allows you to remove power immediately from one part of the EUC (via Output 1) while allowing another part (via Output 2) to complete a controlled stop before power is removed.

Be sure that the wiring matches the configuration selected in FORT Manager, including whether the system is set for CAT0 or CAT1 behavior.

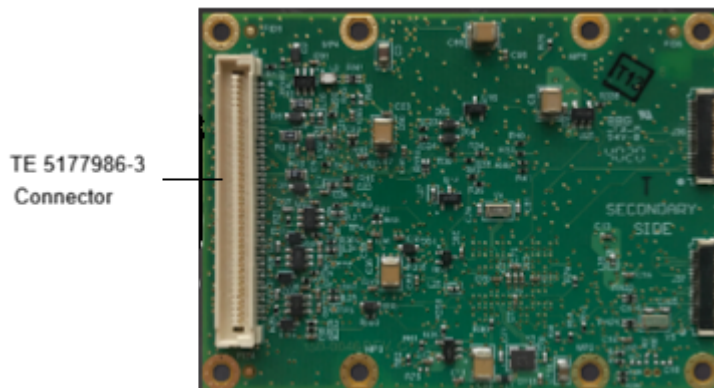


Figure 22: Fig. 22 TE 5177986-3 connector on (Secondary) Side

To Wire the NSC Pro to the Host Computer and to the EUC:

1. Attach the TE 5-5179180-3 80-pin receptacle connector to the TE 5177986-3 80-pin connector plug on the secondary side of the board.
2. **Connect the NSC Pro to the host computer:**

- a. Connect the USB port on the NSC Pro (using pins 2 and 4 for data & pin 6 for power) to a USB port on the host computer.

The USB connection enables you to configure the NSC Pro. Note that without power (from pin 6) the NSC Pro will not detect the USB connection.

- b. Connect serial port `Serial0` on the NSC Pro (IP to UART bridge, pins 50 & 54) or `Serial1` (IP to UART bridge, pins 58 & 62) to a serial port on the host computer.

This connection enables the FORT SDK, running on the host computer, to convert IP traffic from the sending device to serial traffic that can be read by the NSC Pro.

3. Connect pins 10 & 12 (PVIN) to the main power supply on the EUC.³
4. Connect grounding pins, 8, 23, 46, 69, and 79 together at the same place (common power supply in the likely case that earth ground is not available).

See [Grounding an NSC Pro](#) (on page 46) for details.

5. If you are using CAN, connect the CAN bus from the NSC Pro to the EUC (CAN0, pins 24 and 26,).

Using the CAN bus is optional and if you are using the serial connection for the data output interface between the NSC Pro and the EUC, you can't use CAN.

Important:

Termination resistors are important for reliable CAN bus communication. The NSC Pro integration cable does not come with any termination inside the cable. You may need a 120 ohm termination resistor if one isn't already present in the CAN network.

6. If you are using a serial bus for diagnostics, connect the other serial port on the NSC Pro (whichever one is *not* connected to the SDK on the Linux computer) to the EUC (UART 0, pins 50 & 54, or UART1, pins 58 & 62).

Using the serial port is optional, and if you are using CAN, you can't use the serial port to connect to the EUC.

7. For Output 1, connect pin 55 (Channel 0 Output 1) and pin 57 (Channel 1, Output 1) to the safety relay.
8. For Output 2 (if using), connect pin 78 (Channel 0, Output 2) and pin 80 (Channel 0, Output 2) to the safety relay.
9. **Optionally, to wire external LEDs to show the power, connection, and operational status of the NSC Pro:**
 - a. Wire pins 5, 7, & 9.
 - b. Connect pin 18 to pull 3.3 V output (max current 50mA) from the onboard power supply to power the LEDs.
10. **Optionally, to provide a backup battery (3-3.3 V DC), for example to keep a clock running:**
 - a. Wire pin 48.
 - b. Use Pin 46 to ground the battery to the same ground as the main power supply.

If you aren't providing a battery, tie pin 48 to pin 18 (P3V3_OUT).



CAUTION:

Each output on the NSC is designed with short circuit protection circuitry inside the NSC device. However, drawing more than 750 mA must be avoided since it won't activate short circuit

³ See [Engine Cranking \(NSC Pro\)](#) (on page 47) for possible issues with connecting the NSC to an ignition circuit for power.

protection and could potentially damage the device. To satisfy applicable wiring codes and conditions, you are responsible for protection of field devices and wiring through appropriate fusing of the circuitry (see [Recommended Relays](#) (on page 181) for details about fuse size and diodes to use).

Grounding an NSC Pro

Note:

Connect all ground (GND) pins together and 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. 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.

In addition, if you require a pull down resistor in order to make the output signal go to ground when an E-Stop is triggered, we recommend using a 1.6k ohm resistor to pull the output pins (55 and 57, and 78 and 80 if used) to ground.

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

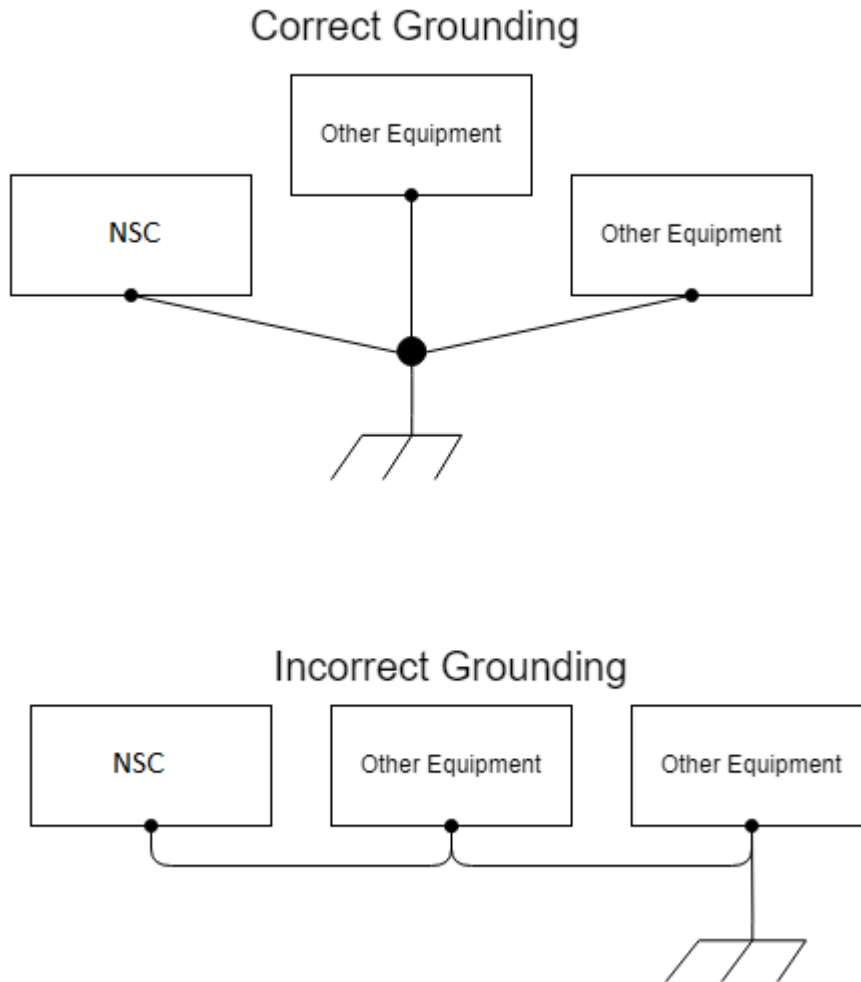


Figure 23: Fig. 23 Examples of Correct and Incorrect Grounding

Engine Cranking (NSC Pro)

If you attach the NSC Pro to an ignition circuit, be aware that engine cranking can drop the voltage below 4.5 V causing the NSC Pro to turn off the outputs and triggering a safe state. In addition, cranking may drop the voltage low enough that the NSC Pro temporarily stops functioning and resets.

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

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

Embedding an NSC Pro

When embedding the Nano Safety Controller Pro in your equipment, keep in mind the clearances shown in the following table:

Table 4 NSC Pro Board Clearances

Board	Dimension
Primary side of board clearance	4 mm
Secondary side of board clearance	5 mm
Secondary side of board standoff	9 mm
Primary side of board with ISM clearance	20.1 mm

See [Mechanical Drawings NSC Pro and ISM Radio](#) (on page 152) for NSC Pro and ISM measurements.

Environmental Considerations

Important:

Be certain that you install the NSC Pro in a location that prevents:

- Exposure to condensing or splashing water.
- Temperatures beyond rated operating and storage ranges (see [Specifications](#) (on page 152)).
- Dust, pollution and other particle contaminants (IEC 60950-1 pollution degree 2).
- Electrostatic discharge.

You should validate through testing that the installation method is appropriate for the application.

Selecting and Placing an Antenna

FORT offers a variety of antenna options to support the wireless communication method you will be using. The antennas for the Nano Safety Controller Pro are accessories that you need to select prior to purchase. The antennas for the Safe Remote Control Pro are built into the device so you must select one prior to purchase.

Note:

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 4: Table 5 Antennas NSC Pro

FORT Device	SRC Pro to NSC Pro via ISM 868	SRC Pro to NSC Pro via ISM 900	EPC to NSC Pro via Wi-Fi or Ethernet	EPC to NSC Pro via ISM 900
Antenna Type	Whip Straight	Whip Straight	Provided via equipment (EUC)	Whip Straight
Usage	ISM EU Bands	ISM NA Bands	Wi-Fi; Ethernet	ISM NA Bands

FORT Device	SRC Pro to NSC Pro via ISM 868	SRC Pro to NSC Pro via ISM 900	EPC to NSC Pro via Wi-Fi or Ethernet	EPC to NSC Pro via ISM 900
Frequency Range	750–950MHz	865-965MHz	2.4 - 2.5GHz (5.1 to 5.9GHz pending tests)	865-965MHz
Peak Gain	1.1 dBi	1.8 dBi	4.5dBi @ 5.1-5.9Ghz band and 7.2dBi in the 2.4 to 2.5Ghz band	1.8 dBi
Ideal Placement	Elevated; pointed straight up; clear LOS	Elevated; pointed straight up; clear LOS	Elevated; pointed straight up; clear LOS	Elevated; pointed straight up; clear LOS

Use grommets when routing the antenna cable through enclosures.



CAUTION:

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

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

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

Table 5: Table 6 Rules for using Approved Antennas

Device	FCC ID (US)	IC (Canada)	CE (Europe)
NSC Pro EPC 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. Configurations and Use Cases

This chapter describes the configurations you can build — one-to-one, one-to-many, machine select, and two-to-one — explains which device models and communication methods each one requires, and shows how to build and modify a configuration in FORT Manager or through the FORT API.

After you register your FORT Pro Series devices, you can add them to a configuration. You can build configurations in the FORT Manager Web App, in the FORT Manager Desktop App, or through the FORT API.

A configuration allows you to: ⁴

- Add devices to a network enabling them to communicate with each other.
- Configure device settings.
- Select the method for device communication.
- Designate the type of sender for the configuration (EPC, WES Pro, SRC Pro).
- Designate the type of receivers for the configuration (EPC, NSC Pro).
- Configure the inputs on the sender.

The following table shows the various configurations that you can build with Pro Series devices:

Table 6: Table 7 Configurations

Configuration Type	Sender:Receivers ⁵	Definition
One-to-One (1:1) (on page 53)	EPC : EPC; EPC : NSC Pro; WES Pro : EPC; WES Pro : NSC Pro SRC Pro : EPC; SRC Pro : NSC Pro	One sender connected to one receiver.

⁴ Not all of these functions are available for every type of configuration, for every device model, or to every organization. For example, you don't configure inputs on an SRC Pro or WES Pro; the method of communication may be predetermined by the device model so it can't be set in FORT Manager; and some features are enabled for particular organizations. For more information, see [What You See in FORT Manager](#) (on page 7).

⁵ Consult the [Release notes](#) for information specific to the version of the product that you are using regarding the type and number of devices that can be paired together.

Configuration Type	Sender:Receivers ⁵	Definition
One-to-Many (1:many) (on page 54)	EPC : many EPCs EPC : many NSC Pros	One sender that is capable of sending an E-Stop to all receivers in the configuration at once.
Machine Select (on page 56)	SRC Pro : many EPCs SRC Pro : many NSC Pros	One sender that recognizes multiple receivers but can connect to and control one receiver at a time.
Two-to-One (2:1) (on page 57)	SRC Pro & WES Pro : 1 EPC SRC Pro & EPC : 1 EPC (ISM and Bluetooth) SRC Pro & EPC : 1 EPC (LRBLE) WES Pro & EPC : 1 NSC Pro (LRBLE) WES Pro & EPC : 1 EPC (LRBLE or Ethernet) <i>LRBLE combinations require mdoel 1003.</i>	Two senders, each able to send a safety signal to the connected receiver.
SRC Pro with Global E-Stop (on page 65)	SRC Pro & EPC : many EPCs (up to 30)	One SRC Pro that recognizes multiple receivers but can connect to and control one receiver at a time, plus an E-Stop that can send a safety signal to all receivers at once.

Device Models and Communication Methods

Not every device can use every communication method. The radio is built into the device, so the model you own determines which methods are available to it, and therefore which configurations it can join.

The following table lists the models that FORT Manager supports. A model that has reached end of support is not listed, even if the device is still in service. For more information, see [SRC Pro Models and Support Status](#) (on page 171).

⁵ Consult the [Release notes](#) for information specific to the version of the product that you are using regarding the type and number of devices that can be paired together.

Table 7: Communication Methods by Device Model

Communication Method	EPC	SRC Pro	WES Pro	NSC Pro
ISM 900 MHz (North America)	EPC 1001	SRC Pro 1001	—	NSC Pro 1001
ISM 868 MHz (Europe)	EPC 1002	SRC Pro 1002	—	NSC Pro 1002
Bluetooth Low Energy (BLE)	EPC 1000, 1001, 1002	SRC Pro 1001, 1002	—	—
Long-Range Bluetooth (LRBLE)	EPC 1003	SRC Pro 1003	WES Pro 1003	NSC Pro 1003
Wi-Fi	All EPC models	—	—	With additional hardware
Ethernet	All EPC models	—	—	With additional hardware

Important:

Every device in a configuration must support the communication method the configuration uses. A configuration that communicates over LRBLE can contain only model 1003 devices — senders and receivers alike.

Note:

Which interfaces FORT Manager offers you can be narrower than what the hardware supports, because some configurations restrict the choice. For example, in a 2:1 configuration with a WES Pro and an EPC, Wi-Fi is not offered for an EPC sender of model 1003. For more information, see [Settings in a WES Pro and EPC Configuration](#) (on page 73).

Note:

The NSC Pro has no built-in Wi-Fi modem or wired Ethernet adapter. Using an IP network with an NSC Pro requires additional hardware. For more information, see [Setting up an NSC Pro for IP Networking \(EPC Sender\)](#) (on page 40)

You can find a device's model number on its nameplate, in a handheld's onscreen menu, or in FORT Manager on the Devices page. For the radio specifications of each model, see

- [EPC Technical Specifications](#) (on page 142)
- [SRC Pro Technical Specifications](#) (on page 168)
- [WES Pro Technical Specifications](#) (on page 173)

Note:

Antennas are matched to the radio, not only to the device. When you select an antenna, check it against the communication method you plan to use. For more information, see [Antennas](#) (on page 193).

You build these configurations in FORT Manager or through the FORT API, and you apply them from a computer connected to each device. You can find instructions for building any type of configuration in [Building a Configuration](#) (on page 68) and instructions for loading configurations onto your devices in [Loading a Configuration onto Your Devices](#) (on page 79).

One-to-One Configuration

In a One-to-One (1:1) configuration, you configure a single sender connected to a single receiver.

For the sender, you can use an SRC Pro, EPC, or WES Pro.

For the receiver, you can use either an EPC or an NSC Pro.

The following table shows details about a One-to-One configuration:

Table 8: Table 8 One-to-One Configurations

Sender	Receiver	Communication
EPC	EPC	Ethernet, Wi-Fi, BLE, LRBLE
EPC	NSC Pro	ISM 900 and 868, LRBLE (model 1003 only)
WES Pro	EPC	LRBLE
WES Pro	NSC Pro	LRBLE
SRC Pro	EPC	ISM, Bluetooth, LRBLE
SRC Pro	NSC Pro	ISM

Note:

For which radios each device model carries, see [Device Models and Communication Methods](#) (on page 51).

The following figure shows possible One-to-One configurations:

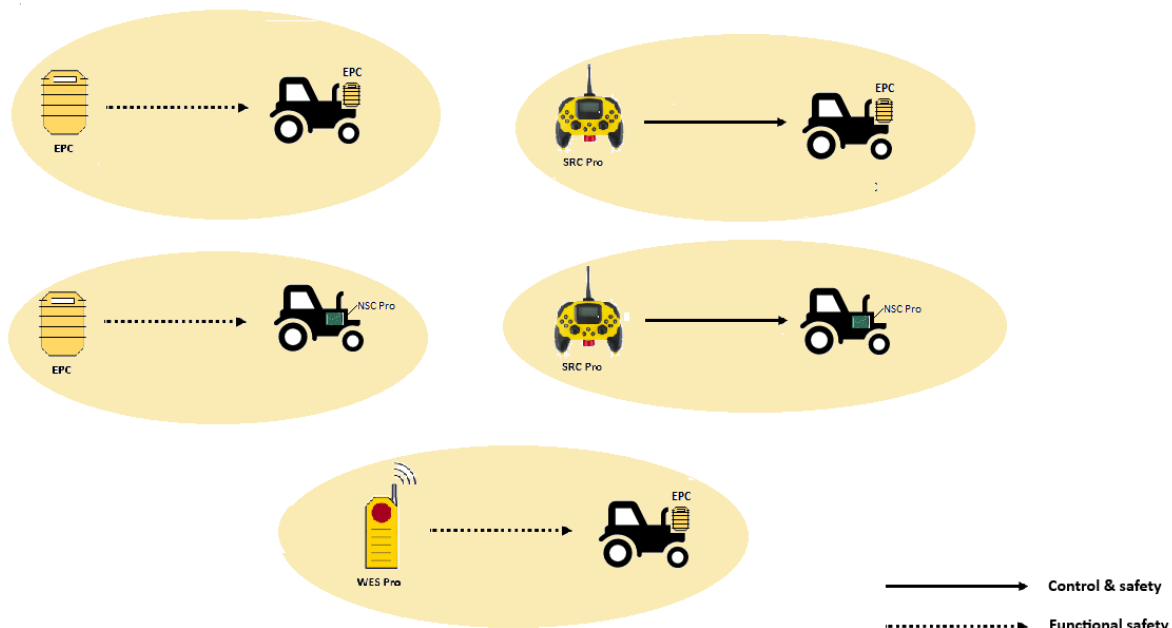


Figure 24: Fig. 24 Possible One-to-One Configurations

Note:

If your configuration connects devices through Ethernet, and your network contains complex message routing and firewall rules, you may need to set up UDP port allocation rules to ensure that data packets move seamlessly back and forth between your devices over an Ethernet network. See [UDP Port Allocation for Ethernet Connections](#) (on page 67).

One-to-Many Configuration

In a One-to-Many (1: many) configuration, a single EPC sender is connected to and able to send a safety signal to multiple EPCs or NSC Pros at once.

Important:

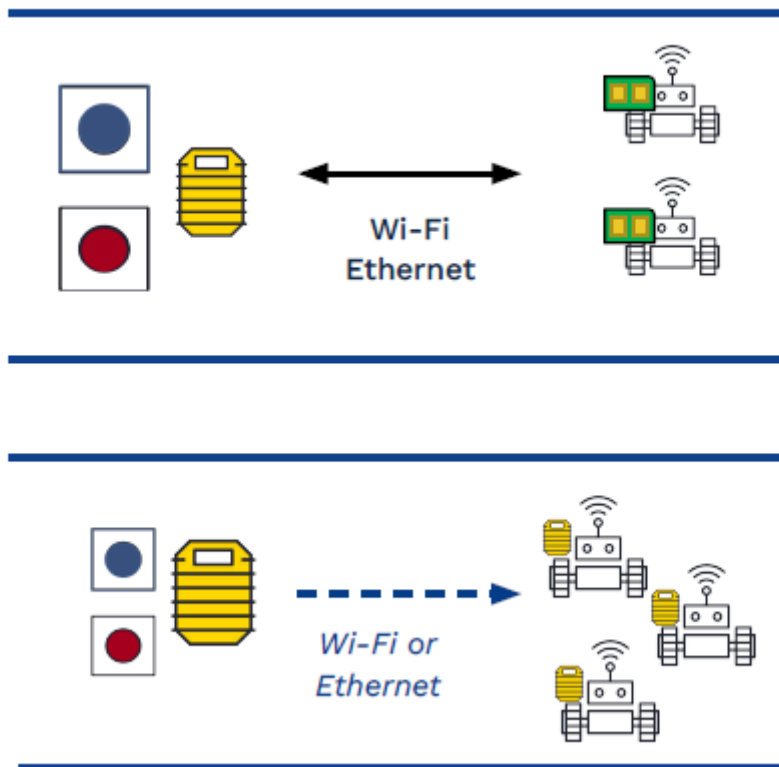
You cannot mix and match the receivers – they must be all EPCs or all NSC Pros.

The following table shows details about a One-to-One configuration:

Table 9: Table 9 One-to-Many Configurations

Sender	Receiver ⁶	Communication
EPC	Multiple EPCs (up to 30)	Ethernet, Wi-Fi
EPC	Multiple NSC Pros (up to 30)	ISM 900 and 868

The following figure illustrates two possible One-to-Many configurations:

**Figure 25: Fig. 25 One-to-Many Configurations****Note:**

If your configuration connects devices through Ethernet, and your network contains complex message routing and firewall rules, you may need to set up UDP port allocation rules to ensure that data packets move seamlessly back and forth between your devices over an Ethernet network. See [UDP Port Allocation for Ethernet Connections](#) (on page 67).

⁶ Consult the [Release notes](#) for information specific to the version of the product that you are using regarding the type and number of devices that can be paired together.

Machine Select Configuration

In a Machine Select Configuration, one SRC Pro recognizes multiple receivers (all EPCs or all NSC Pros, not a mix) but can connect to and control only one at a time. For example, an equipment operator can connect to a machine in the yard with an SRC Pro, maneuver it out to a work area, place it in *unsupervised* mode and go back to the yard to pick up a different machine. The machine can continue to run safely in *unsupervised* mode (assuming it has autonomous capabilities) while disconnected from the SRC Pro. See the discussion that follows in [Supervised and Unsupervised Mode](#) (on page 56).

The following table shows details about a Machine Select Configuration:

Table 10: Table 10 Machine Select Configurations

Sender	Receiver ⁷	Communication
SRC Pro	Multiple EPCs (up to 30) with unsupervised mode capability.	ISM 900, ISM 868 BLE, LRBLE
SRC Pro	Multiple NSC Pros (up to 30) <i>without</i> unsupervised mode capability.	ISM 900 and 868

Supervised and Unsupervised Mode

When the user selects a machine and successfully connects to the receiver (EPC or NSC Pro) on that machine, the receiver 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 EPC or NSC Pro and is sending input data such as joystick movements, safety messages, etc. to the selected machine. If an operator pushes the E-Stop button, the EPC or NSC Pro enters the safe state. If the Safe Remote Control Pro stops communicating with the EPC or NSC Pro, resulting in a timeout, the EPC or NSC Pro enters the safe state.

Unsupervised mode is meant to be used with machines that have autonomous capability. For example, after taking a machine out of the yard to a work area, an operator can put it in unsupervised mode and it can continue to run safely while disconnected from the SRC Pro. The operator can go back to the yard with the SRC Pro, connect to a different machine, and bring it out to the work area.

Note:

If a machine is not equipped for autonomous capability, switching into unsupervised mode causes a safe state.

⁷ Consult the [Release notes](#) for information specific to the version of the product that you are using regarding the type and number of devices that can be paired together.

Important:

Unsupervised mode is only available for EUCs with EPC receivers, not for those with NSC Pro receivers. When an SRC Pro stops communicating with an NSC Pro (from an E-Stop signal or loss of communication), the machine is inoperable until the SRC Pro reconnects with the NSC Pro receiver. Putting an NSC Pro into unsupervised mode cause a safe state.

In unsupervised mode, the SRC Pro and the EPC are not communicating with each other, so the SRC Pro is not sending safety or control information to the EPC. Rather, the EPC that is attached to the equipment is responsible for monitoring the customer supplied safety signal, and if that signal changes out of the normal state, the EPC enters the safe state and breaks the circuit to the equipment under control. For wiring details, see [Wiring Receivers with an SRC Pro Sender](#) (on page 10).

**Warning:**

Make certain that your equipment operators are aware of the following points about operating equipment in unsupervised mode:

- Pushing the E-Stop button on the SRC Pro has no effect because the EPC ignores an E-Stop command in unsupervised mode.
- Be certain that the equipment is able to operate safely without need of the E-Stop button, as pushing it will have no effect and it may not be quick, easy, or even possible to change the mode of the EPC back to supervised for a number of reasons, including the following:
 - The equipment with the EPC is out of range of the SRC Pro.
 - The SRC Pro has run out of battery.
 - The SRC Pro is damaged or unresponsive.

See [Building a Configuration](#) (on page 68) for details of using FORT Manager to build a configuration.

Two-to-One Configuration

A Two-to-One (2:1) configuration has two senders and one receiver, which allows either of two people to send an E-Stop signal to the receiver and the EUC. The possible combinations are as follows:

- SRC Pro and WES Pro senders with one EPC, communicating over LRBLE.
- SRC Pro and EPC senders with an EPC, communicating over ISM or Bluetooth.
- SRC Pro and EPC senders with an EPC, communicating over LRBLE. This combination requires model 1003 for all three devices. For more information, see [Two-to-One over Long-Range Bluetooth](#) (on page 59)
- WES Pro and EPC senders with one NSC Pro, communicating over LRBLE. For more information, see [Two-to-One with a WES Pro and an EPC](#) (on page 61).
- WES Pro and EPC senders with one EPC, communicating over LRBLE, with the option of Ethernet for the EPC sender. For more information, see [Two-to-One with a WES Pro and an EPC](#) (on page 61).

For example, in a configuration with an SRC Pro and a WES Pro or an SRC Pro and an EPC, the equipment operator could control the machine with an SRC Pro and push the E-Stop at any time to resolve a safety issue. At the same time, another person could observe the operation from a different vantage point and press the E-Stop on the WES Pro or on the EPC sender if they see a safety issue.

In a different scenario, the equipment operator uses the SRC Pro to drive the equipment to a work area and then puts the EPC attached to the equipment under control (EUC) in unsupervised mode. In this case, the SRC Pro does not control movement of the EUC nor will pressing the E-Stop affect the EUC. However, the secondary controller, a WES Pro or EPC, can still send an E-Stop signal to the EPC receiver attached to the EUC.

The following figure illustrates a Two-to-One configuration with SRC Pro and WES Pro senders.

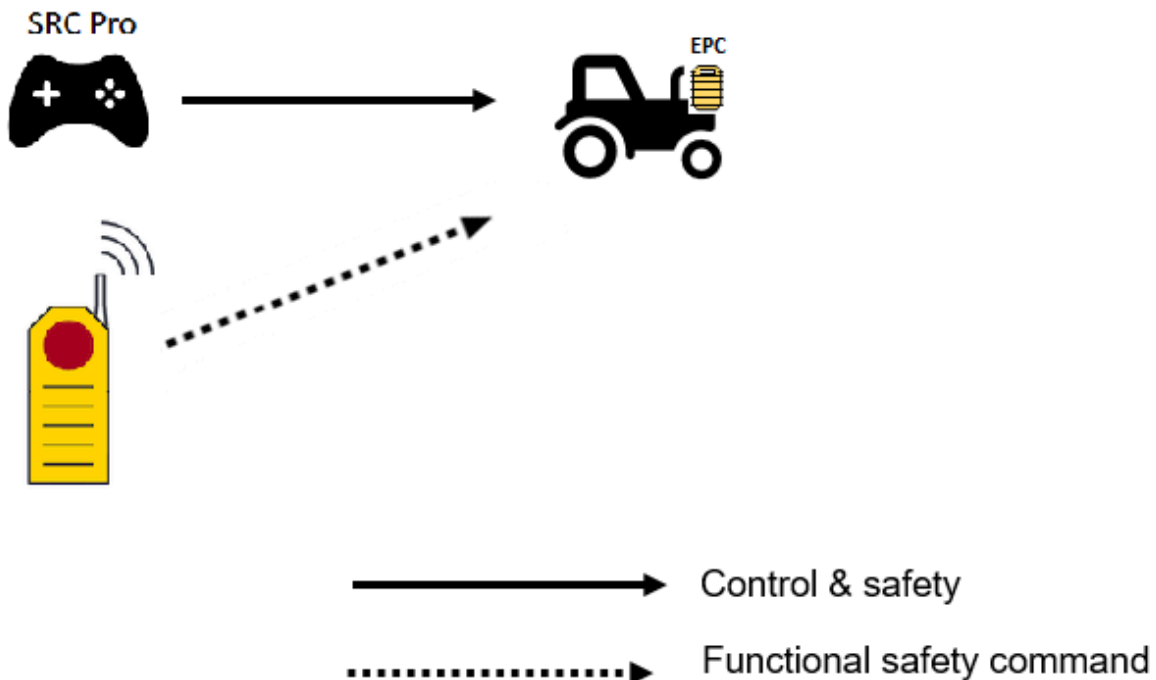


Figure 26: Fig. 26 SRC Pro and WES Pro to EPC Configuration

The following table shows details about a Two-to-One configuration:

Table 11: Table 11 Two-to-One Configuration

Sender	Receivers ⁸	Communication	Device Models
SRC Pro and WES Pro	One EPC	LRBLE	SRC Pro 1003, WES Pro 1003, EPC 1003
SRC Pro and EPC	One EPC	ISM, Bluetooth	Any model carrying the radio you select
SRC Pro and EPC	One EPC	LRBLE	SRC Pro 1003, WES Pro 1003, EPC 1003 (both the sender and the receiver)
WES Pro and EPC	One NSC Pro	LRBLE	WES Pro 1003, EPC 1003, NSC Pro 1003
WES Pro and EPC	One EPC	LRBLE, Ethernet	WES Pro 1003, EPC 1003

Note:

A 2:1 configuration supports exactly one receiver. In a configuration that communicates over LRBLE, adding a second receiver changes the configuration – the additional receivers communicate over Ethernet and the configuration is no longer LRBLE throughout. For more information, see [Two-to-One over Long-Range Bluetooth](#) (on page 59) and [Two-to-One with a WES Pro and an EPC](#) (on page 61).

For which radios each device model carries, see [Device Models and Communication Methods](#) (on page 51)

Two-to-One over Long-Range Bluetooth

In this configuration an SRC Pro and an EPC both act as senders to a single EPC receiver, and all three communicate over Long-Range Bluetooth (LRBLE). It suits work areas where the operator needs to drive a machine at a distance while a second person retains independent authority to stop it, and where running Ethernet or an ISM radio to the E-Stop station is impractical.

What each device does

- SRC Pro sender (the controller)
 - Drives and maneuvers the equipment under control, and can send an E-Stop. This is the device the equipment operator holds.
- EPC sender (the secondary controller)

⁸ Consult the [Release notes](#) for information specific to the version of the product that you are using regarding the type and number of devices that can be paired together.

- Sends an E-Stop to the receiver. It does not control machine movement. Mount it where a supervisor can reach it — for example, overlooking the work area. It remains able to stop the machine when the SRC Pro is paired with and managing a different receiver.
- EPC receiver
 - Wired to the equipment under control. Accepts safety and control signals from the SRC Pro, and safety signals from the EPC sender.

Requirements

- All three devices must be model 1003. LRBLE is carried only by the SRC Pro 1003 and the EPC 1003. A device of any other model cannot join an LRBLE configuration. For more information, see [Device Models and Communication Methods](#) (on page 51).
- *Exactly one receiver.* A 2:1 configuration over LRBLE supports a single EPC receiver. Adding a second receiver changes the configuration: the additional receivers communicate over Ethernet, and the configuration is no longer LRBLE throughout.
- *An antenna on each device.* For more information, see [Antennas](#) (on page 193).

Important:

The EPC sender communicates with the EPC receiver over LRBLE or Ethernet, not both. Which one applies is set on the **General** tab when you configure settings, and it determines what options you are offered at the device level. For more information, see [Settings in a 2L1 LRBLE Configuration](#) (on page 72).

Range and Placement

LRBLE has a usable range of roughly 100–300 m, depending on line of sight, antenna placement, and the environment. Both links in this configuration — SRC Pro to receiver, and EPC sender to receiver — are subject to that range independently.

Position the EPC sender so that the whole area the machine will work in stays within range of it. A supervisor's E-Stop is only useful where it can be received.



Warning:

Before putting this configuration into production, walk the boundaries of the work area and confirm that both senders maintain communication with the receiver throughout. Loss of communication for longer than the configured safety timeout causes the receiver to enter the safe state. For more information, see [Wireless Communication Loss](#) (on page 216)

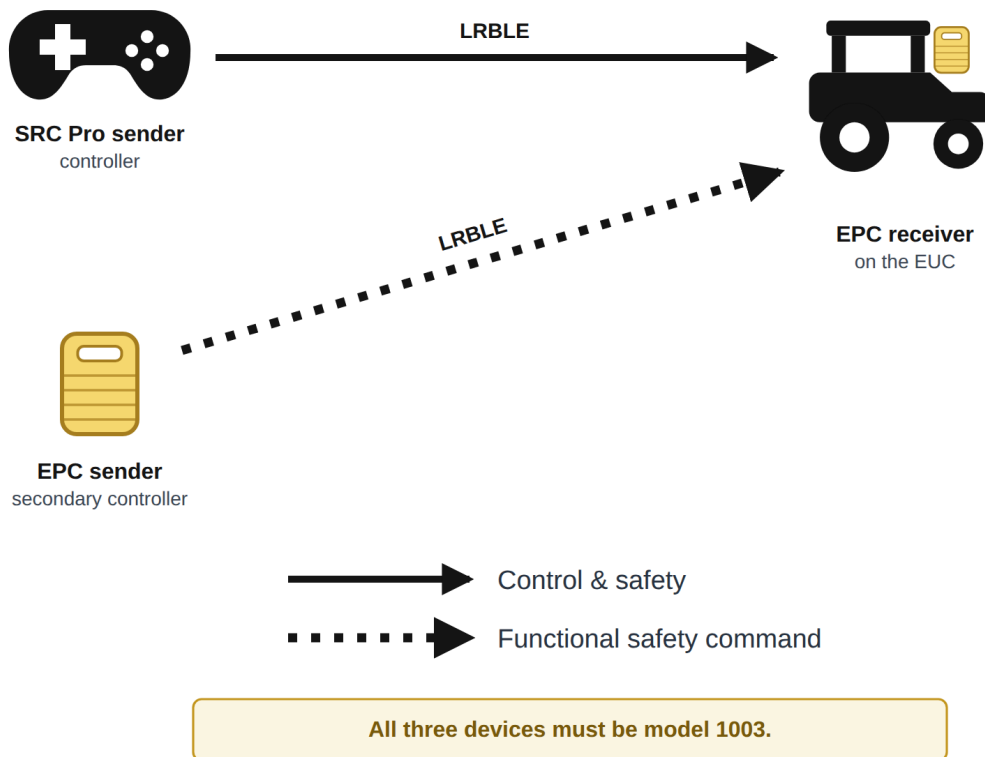


Figure 27: SRC Pro and EPC to EPC Configuration over LRBLE

Note:

The two operator scenarios described under [Two-to-One Configuration](#) (on page 57) apply to this configuration as well: a second person can observe from a different vantage point and press the E-Stop on the EPC sender, and the EPC sender can still stop the EUC when the receiver has been placed in unsupervised mode.

Two-to-One with a WES Pro and an EPC

In this configuration a handheld WES Pro and a fixed EPC both act as senders to a single receiver, and either one can stop the equipment. Unlike the other Two-to-One configurations, neither sender drives or maneuvers the machine — both exist only to stop it.

It suits deployments where each machine has a dedicated human minder who carries a stop device, and the facility also needs a stop that does not depend on any one person being present. A robot working alongside people, supervised one-to-one during an early rollout, is the case this configuration was built for.

What Each Device Does

- WES Pro sender

- A handheld E-Stop carried by the person supervising the machine. Pressing its E-Stop button stops the equipment.
- EPC sender
 - A fixed E-Stop station wired into the facility – for example at a doorway, a cell boundary, or a supervisor's station. An E-Stop device wired to its Input 1 stops the equipment. It does not control machine movement.
- Receiver
 - An NSC Pro embedded in the machine, or an EPC wired to it. It accepts a stop from either sender.

Both Senders Act on the Same Output

Both senders in this configuration act on the same output of the receiver, and you choose which one when you build the configuration. Set it with **Output to Control** on the **General** tab. For more information, see [Choosing Which Output the Senders Control](#) (on page 62).

Whichever output you choose, the receiver's other output is not used by this configuration.

Important:

Both senders stop the same output. You cannot assign the WES Pro and the EPC sender to different outputs so that each stops a different part of the machine. If your application needs independent outputs per sender, this configuration does not provide it.



Warning:

Because both senders act on the same output, the machine is stopped whenever either sender requests a stop, and it can only resume when neither is requesting one. Make certain that everyone operating the equipment understands that clearing the stop on one device does not restart the machine if the other device is still stopping it.

Choosing Which Output the Senders Control

Use **Output to Control** on the **General** tab to choose whether the senders drive Output 1 or Output 2 of the receiver. You can control one or the other, not both.

The choice applies to the whole configuration rather than to an individual device, so both senders act on the output you pick. Two things must then be wired to match it.

Wire the EPC sender's input to match

The EPC sender's usable input follows the output you selected. FORT Manager grays out the one that does not apply, and Input 3 is reserved and always grayed out.

Table 12: EPC Sender Input by Output Selection

Output to Control	Wire the E-Stop Device to	J1 pins on the sender	Grayed Out
Output #1	Input 1	6 (Channel 0) and 3 (Channel 1)	Input 2, Input 3
Output #2	Input 2	5 (Channel 0) and 2 (Channel 1)	Input 1, Input 3

Inputs are dual channel pairs in the same way outputs are. For more information, see [Wiring Safety Devices and Power to EPC Sender](#) (on page 11)

Wire the Receiver's Output Pins to Match

Each output is a dual-channel pair on the receiver's J1 connector — one pin from Channel 0 and one from Channel 1. Wire both pins of the pair for the output you selected.

Table 13: Output to J1 Connector Pins (EPC Receiver)

Output to Control	J1 Pins	Signals
Output #1	18 and 23	OUT3_CONN (Channel 1, Output 1) and OUT0_CONN (Channel 0, Output 1)
Output #2	17 and 22	OUT4_CONN (Channel 1, Output 2) and OUT1_CONN (Channel 0, Output 2)

For the full pinout, see [EPC I/O Connector Pinout and Cable](#) (on page 143).



Warning:

Wire both pins of the pair. Each output is a dual channel output, and connecting only one pin leaves you with a single channel where the safety function assumes two.



Warning:

If the output you selected in FORT Manager does not match the pins you wired, the equipment will not stop when a sender requests a stop. Verify the selection against the wiring before putting the configuration into production, and test a stop from each sender.

You cannot change the output later

Important:

The output a configuration controls is set when the configuration is created and cannot be changed afterwards. To use the other output, build a new configuration and load it onto your devices.

Building a configuration requires a connection to FORT Manager, so a wrong output selection cannot be corrected in the field.

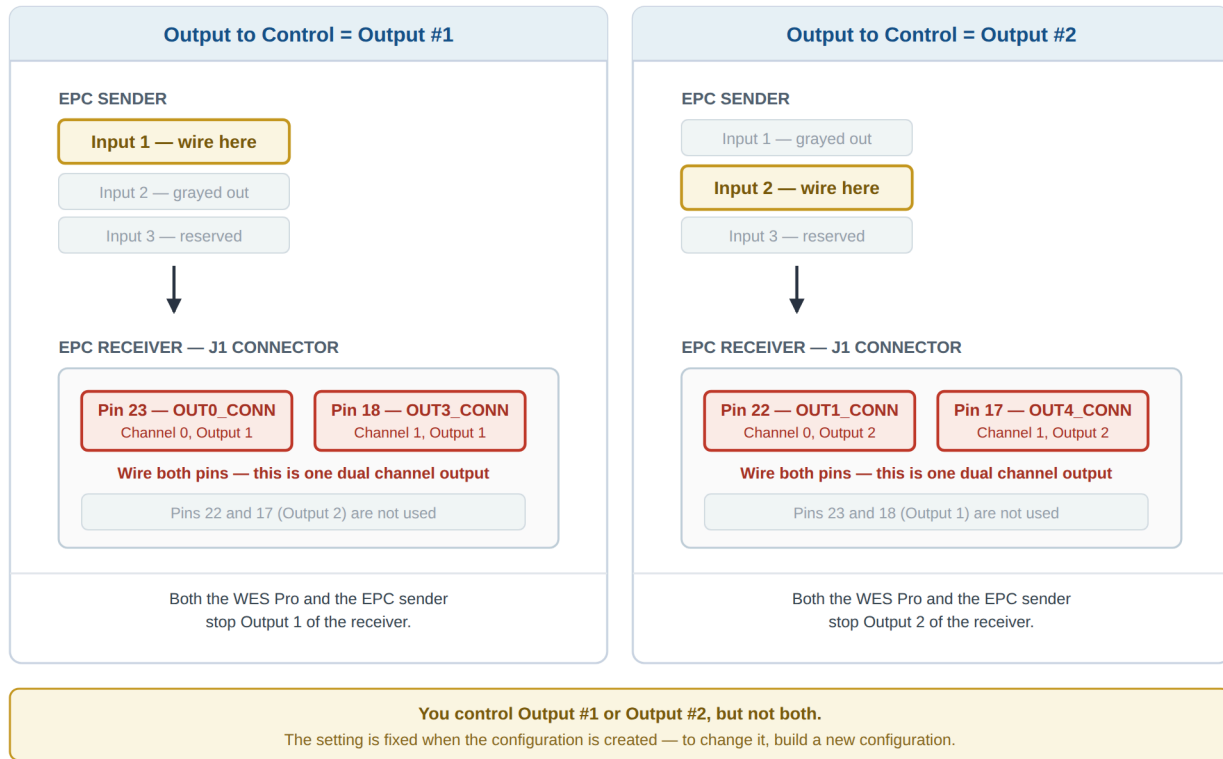


Figure 28: Output to Control

Requirements

- **All devices must be model 1003:** LRBLE is carried only by the WES Pro 1003, the EPC 1003, and the NSC Pro 1003. For more information, see [Device Models and Communication Methods](#) (on page 51).
- **Exactly one receiver:** A 2:1 configuration supports a single receiver.
- **An antenna on each device that needs one:** The WES Pro's antenna is built in; the EPC's and the NSC Pro's are accessories. For more information, see [Antennas](#) (on page 193).

Why LRBLE rather than an IP Network

The EPC sender can reach the receiver over LRBLE or over an IP network. LRBLE is the default and is usually the right choice for a pilot deployment, because it needs no connection to the customer's network: no switch ports, no addressing, and no involvement from the site's IT organization.

An IP network becomes worth the setup effort as a deployment grows — when many machines share infrastructure, or when the site already manages a network the devices can join. For more information on how to select the interface, see [Settings in a WES Pro and EPC Configuration](#) (on page 73).

Note:

If the receiver is an NSC Pro and you select Ethernet or Wi-Fi, the NSC Pro needs additional hardware, because it has no built-in Wi-Fi modem or wired Ethernet adapter. A LRBLE-only configuration needs none of that. For more information, see [Setting up an NSC Pro for IP Networking \(EPC Sender\)](#) (on page 40).

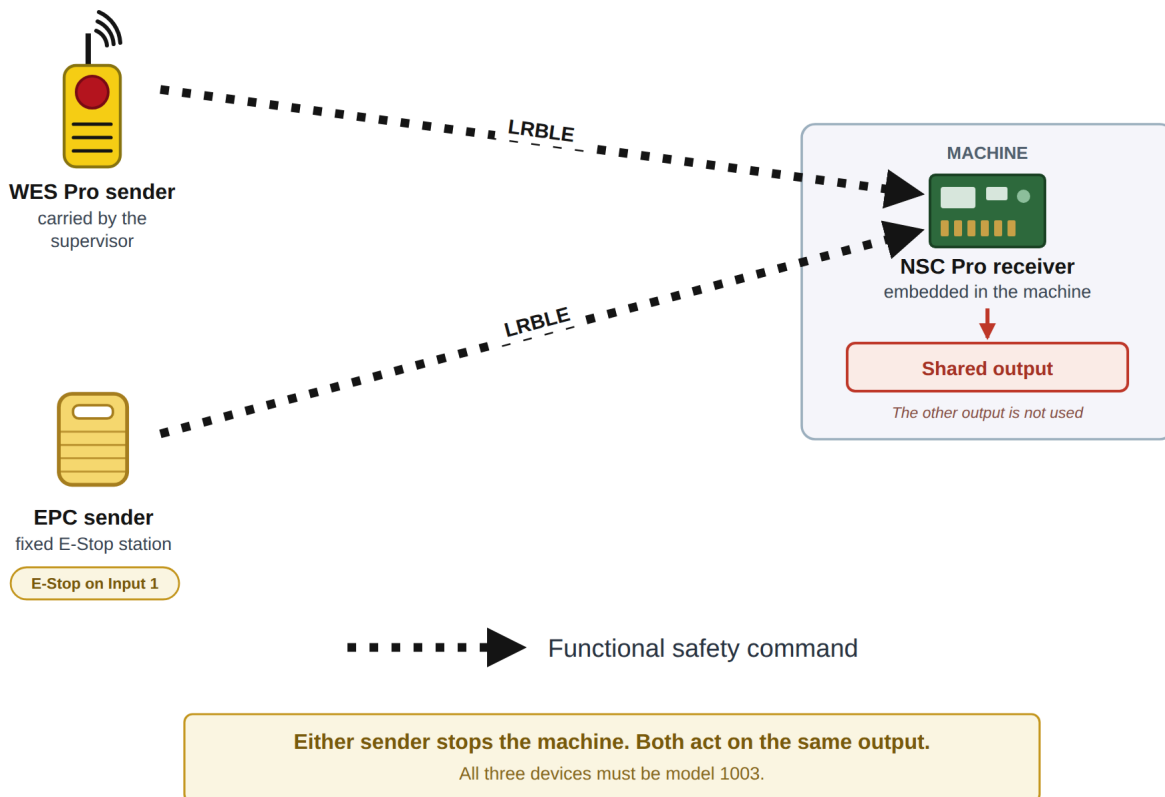


Figure 29: WES Pro and EPC to NSC Pro Configuration over LRBLE

SRC Pro with Global E-Stop Configuration

In an SRC Pro with Global E-Stop configuration, an SRC Pro recognizes multiple receivers but can connect to and control only one EPC at a time, and in addition, an EPC can send a safety signal to all receivers at once.

Note:

Currently, use of NSC Pro receivers in a Global E-Stop configuration is not supported.

The Safe Remote Control Pro can control and send safety signals to any one EPC receiver at a time and the EPC sender can send safety signals to all the EPC receivers 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 EPC 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 EPC is still connected to the machine that is operating autonomously, allowing a supervisor to press the E-Stop button on the sender EPC and stop the machine if necessary.

In practice you could place an EPC 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 EPC sender can send an E-Stop to every EPC that is connected to a vehicle and the Safe Remote Control Pro (using Machine Select) can connect to any one EPC at a time for safety and control functions.

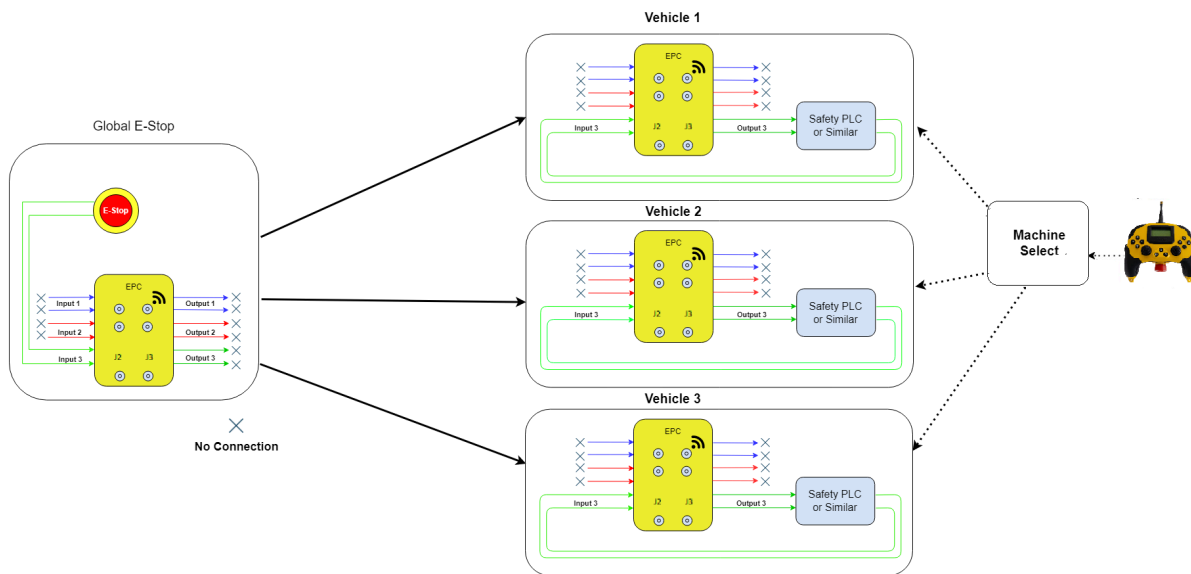


Figure 30: Fig. 27 SRC Pro with Global E-Stop Configuration

Note these points about this configuration:

- Inputs 1 and 2 are unused on the sender EPC (single EPC on the left of the figure).
- Outputs 1 and 2 are unused on the receiver EPCs (three EPCs on the right of the figure).

- When a Safe Remote Control Pro is connected to a receiver EPC in supervised mode, pressing either the global E-Stop on the EPC or the E-Stop button on the Safe Remote Control Pro turns off Output 3 on the receiver EPC (also note that the Safe Remote Control Pro affects the connected machine only, whereas the global E-Stop shuts off Output 3 on all devices).
- When a Safe Remote Control Pro is connected to a receiver EPC in unsupervised mode, only pressing the global E-Stop1 on the EPC will turn off Output 3 on the receiver EPCs. 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 14: Table 12 SRC Pro and EPC Hybrid configuration

Sender	Receivers	Communication
One SRC Pro and one EPC	Up to 30 receivers (EPCs) 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

See the next section for steps you may need to take if your configuration connects devices through Ethernet, and your network contains complex message routing and firewall rules.

UDP Port Allocation for Ethernet Connections

If your configuration connects devices through Ethernet, and your network contains complex message routing and firewall rules, you may need to set up UDP port allocation rules to ensure that data packets move seamlessly back and forth between your devices over an Ethernet network. This section does not apply to configurations that communicate only over LRBLE, ISM, or Bluetooth.

In a configuration with an EPC sender and EPC receivers, a receiver EPC makes requests to the sender at destination port 5683 (~2/sec).

In response, the sender sends data packets to the receiver (every 40 ms) to at least two randomly chosen UDP destination ports but using fixed port 5683. The destination ports change with the power cycle and may also change after an indeterminate amount of time elapses.

Because the destination ports of the safety packets are not fixed, you must set firewall filtering and port forwarding rules to use source port 5683 for sending safety packets (for example on the gateway serving the receiver EPC).

To configure firewall rules, issue the following two commands in a terminal:

```
iptables -A INPUT -s 192.168.1.1 -p udp --sport 5683 -j ACCEPT
iptables -A PREROUTING -t nat -p udp --sport 5683 -j DNAT --to 192.168.2.2
```

where:

- 192.168.2.1 is the IP address of the sender EPC in its subnet.
- 192.168.2.2 is the IP address of the receiver EPC in its subnet.

Here is a brief summary of what these commands do:

- The rule implemented by the first command allows incoming UDP packets from IP address 192.168.1.1 originating from source port 5683 to pass through the firewall.
- The rule implemented by the second command redirects UDP packets with source port 5683 to the IP address 192.168.2.2 by modifying their destination address.

Building a Configuration

Use the FORT Manager Web App, the FORT Manager Desktop App, or the FORT API to build a configuration. These instructions are applicable to all types of configurations.

Note:

The procedures in this section describe the FORT Manager Web App. To build configurations programmatically – for example, to generate a set of configurations for field testing – see [#unique_3/unique_3_Connect_42_building-config-with-fort-api](#).

Before you Begin

Make sure that:

- You've created a FORT Manager account and added your devices to FORT Manager.
- You know what kind of configuration you plan to build (refer to the [Configurations table](#) (on page 50)).
- You know which communication method the configuration will use, and you have confirmed that every device you plan to add supports it. Configurations that use LRBLE require model 1003 throughout. For more information, see [Device Models and Communication Methods](#) (on page 51).
- You know the details of your IP network:
 - If using Ethernet, the gateway address, range of available IP addresses, netmask, and optional DNS server.
 - If using Wi-Fi, network name and password, gateway address, range of available IP addresses, netmask, and optional DNS server.
 - If you are using the FORT API, you have created an API key in FORT Manager and you know your organization ID.
- If using CAN, which protocol – CANopen or J1939. Both are disabled by default. Which protocols are available depends on the receiver in your configuration:
 - An EPC receiver supports J1939 and CANopen.

- An NSC Pro receiver supports J1939 only. For more information, see [Data Interfaces \(NSC Pro\)](#) (on page 163)

To Create a Configuration and Add Devices

(Requires the FORT Manager ConfigManager or Admin role.)

Note:

The following instructions are complete as far as creating a configuration and adding devices to it. The FORT Manager interface is intelligent and provides prompts and warnings to guide you through the process of adding devices, and adjusts the available options based on choices you make and on the features enabled for your organization. For more information, see [What You See in FORT Manager](#) (on page 7).

1. Navigate to the [FORT Manager Web App](#) and enter your credentials when prompted.
2. Click **Configurations** in the left navigation pane.
3. Click **New Setup**.
4. On the **Setup Details** page, select *one* of the following:
 - **use SRCP as my controller**
 - **use EPC as my controller**
 - **use WESP as my controller**
 - a. If you are using a single sender, click **Continue** to accept the default of no secondary sender.
 - b. If you want to have an SRC Pro as well as an EPC sender, select **use SRCP as my controller**, then select **Yes** for an EPC secondary controller. For more information, see [Two-to-One over Long-Range Bluetooth](#) (on page 59).
 - c. If you want to have WES Pro as well as SRC Pro senders, select **use WESP as my controller**, then select **Yes** for SRCP as a secondary controller.
 - d. If you want to have a WES Pro as well as an EPC sender, select **use WESP as my controller**, then select **Yes** for an EPC secondary controller. For more information, see [Two-to-One with a WES Pro and an EPC](#) (on page 61).
5. In **Setup Name**, type a name to identify your configuration and click **Continue**.
6. On the **Select Sender** page, select a device to use from the list to use as a sender and click **Continue**.

Note:

A device that has reached end of support does not appear in the device list, and cannot be added to a new configuration. This does not mean the device has failed. For more information, see [SRC Pro Models and Support Status](#) (on page 171).

7. Optionally, select the second controller (if you chose this configuration in Step 4) and click **Continue**.
8. On the **Select Receiver(s)** page, select receivers from the list and click **Review Setup**.

Important:

To build a 2:1 configuration that communicates over LRBLE:

- Every device must be model 1003 — for an SRC Pro and EPC pairing, the SRC Pro sender, the EPC sender and the EPC receiver; for a WES Pro and EPC pairing, the WES Pro, the EPC sender and the receiver. Devices that do not carry an LRBLE radio cannot be added to the configuration. For more information, see [Device Models and Communication Methods](#) (on page 51).
- Select exactly one receiver. In a WES Pro and EPC configuration, the receiver can be an NSC Pro or an EPC. If you select more than one receiver, the additional receivers communicate over Ethernet and the configuration is no longer LRBLE throughout.

FORT Manager displays the sender(s) and receiver(s) in the configuration and displays the following message to alert you if settings are incomplete:

**CAUTION:**

This configuration is incomplete. Go to the settings page to add missing info.

Go to the next procedure to configure settings.

To Configure Settings**Note:**

The instructions for configuring settings will get you started but are not comprehensive. If you need help with any particular setting, click the info icon # next to it to see more information. Keep these points in mind when setting parameters:

- FORT Manager displays the **Warning** symbol # next to the Settings menu, as well as next to the General or Devices tabs on the Settings menu if any settings need to be configured.
- Required fields are highlighted.
- When you choose a particular setting, such as Wi-Fi, additional fields appear or are highlighted; for example, if you select Wi-Fi for communication, you are prompted to enter a network name and password, if you select Ethernet, you are prompted for an IP address, etc.

1. Click **Settings** to configure settings for the new configuration.
2. Click **General** to configure settings that apply to all devices in the configuration.

In a configuration with two senders, FORT Manager lists a communication interface for each sender separately. The interface you select here determines which settings you are offered at the device level.

Table 15: Communication Interfaces in a 2:1 SRC Pro and EPC Configuration

Sender Pair	Sender	Available Interfaces
SRC Pro and EPC	SRC Pro sender	Long Range Bluetooth

Sender Pair	Sender	Available Interfaces
SRC Pro and EPC	EPC sender	Long Range Bluetooth, Ethernet
WES Pro and EPC	WES Pro sender	Long Range Bluetooth
WES Pro and EPC	EPC sender	Long Range Bluetooth (default); Ethernet if the EPC is model 1003; Ethernet and Wi-Fi if the EPC model is 1000, 1001, or 1002.

The interface you select for the EPC sender determines which settings you are offered at the device level. For more information on the SRC Pro pairing, see [Settings in a 2:1 LRBLE Configuration](#) (on page 72). For more information on the WES Pro pairing, see [Settings in a WES Pro and EPC Configuration](#) (on page 73).

Note:

For all configurations, you must specify a safety timeout, which specifies the maximum amount of time that the sender and receivers are not communicating before a fault occurs to initiate the safe state. Before putting your configuration into production, you should test various timeouts to find the optimal setting. For more information, see [Wireless Communication Loss](#) (on page 205).

Also set on the **General** tab:

- **Output to Control** — Output 1 or Output 2 of the receiver. Both senders act on the output you select; you cannot control both. This setting cannot be changed after the configuration is created. For more information, see [Choosing Which Output the Senders Control](#) (on page 62).
- **CAN Mode** — Disabled, J1939, or CANopen. Which protocols are offered depends on the receiver: a configuration with an EPC receiver supports J1939 and CANopen, and a configuration with an NSC Pro receiver supports J1939 only. For more information, see [Data Interfaces \(NSC Pro\)](#) (on page 163).
- **Safety Timeout** — the maximum time the senders and receiver are not communicating before a fault occurs and the safe state is initiated.

Note:

Before putting your configuration into production, test various timeouts to find the optimal setting. With two independent senders, confirm the timeout behaves correctly for each of them. For more information, see [Wireless Communication Loss](#) (on page 216).

3. Click **Save** to save the general settings.
4. Click **Devices** and select a device from the drop-down list to configure settings specific to each device.

FORT Manager displays the **Warning** symbol # next to any device that requires you to configure settings.

5. Click **Save** when you've completed configuration of all devices.

Once you've built a configuration, you must load it onto each device in the configuration for it to take effect (see [Loading a Configuration onto Your Devices](#) (on page 79)).

Settings in a 2:1 LRBLE Configuration

When both senders in a 2:1 configuration communicate over Long-Range Bluetooth, some device-level settings are fixed by that choice and are not offered for editing. This section explains what changes and why.

The EPC sender's interface is set on the General tab

When you select Long Range Bluetooth for the EPC sender on the General tab, Ethernet is no longer offered as an interface option at the device level for that device.

Important:

To change the EPC sender from LRBLE to Ethernet, return to the **General** tab and change the interface there. You cannot change it from the device-level settings.

Safety I/O on the EPC sender

How FORT Manager treats the EPC sender's safety inputs depends on the configuration:

Table 16: EPC Sender Safety Input Behavior by Configuration

Configuration	Safety Input Behavior
SRC Pro with Global E-Stop Configuration (on page 65)	Inputs 1 and 2 are unused. The E-Stop acts on Output 3 of the receivers.
Two-to-One over Long-Range Bluetooth (on page 59) (SRC Pro and EPC over LRBLE)	No safety I/O options are offered; the assignment is fixed by the configuration.
Two-to-One with a WES Pro and an EPC (on page 61) (WES Pro and EPC)	Follows the Output to Control selection: Input 1 is configurable for Output #1, Input 2 for Output #2. The other is grayed out. Input 3 is reserved and always grayed out. For more information, see Choosing Which Output the Senders Control (on page 62).

Important:

Wiring and configuration must align. Wire the E-Stop device on the EPC sender to the input that the configuration actually uses — this differs between configurations. For more information, see [Wiring Safety Devices and Power to EPC Sender](#) (on page 11).

CAN and IP network settings

- *CAN*— If CAN is not enabled, no additional device-level settings are required for this configuration.
- *IP network* — IP network settings appear at the device level for both the EPC sender and the EPC receiver only when Ethernet is selected. In an LRBLE-throughout configuration there is no IP network to configure.

Note:

If you select Ethernet for the EPC sender, the configuration behaves as any other Ethernet configuration: IP network settings appear at both EPCs, and you may need to set UDP port allocation rules. For more information, see [UDP Port Allocation for Ethernet Connections](#) (on page 67)

Settings in a WES Pro and EPC Configuration

After you set the communication interfaces on the **General** tab, click **Devices** and select each device in turn. The settings you are offered depend on the device's role and on the interface you selected.

EPC Sender

Table 17: EPC Sender Settings

Settings	Behavior
Interface	Read-only. Shows the value you selected on the General tab. To change it, return to the General tab.
IP Network Settings	Appears only when the interface is Ethernet or Wi-Fi.
Input 1	Configurable when Output to Control is set to Output #1. Otherwise grayed out.
Input 2	Configurable when Output to Control is set to Output #2. Otherwise grayed out.
Input 3	Reserved. Always shown grayed out.

Important:

Wire the E-Stop device on the EPC sender to the input that matches your **Output to Control** selection — Input 1 for Output #1, Input 2 for Output #2. The other input does nothing. For more information, see [Choosing Which Output the Senders Control](#) (on page 62) and [Wiring Safety Devices and Power to EPC Sender](#) (on page 11).

WES Pro Sender

The WES Pro has a built-in E-Stop button and no configurable inputs, so it has no device-level safety I/O settings. Its interface is Long Range Bluetooth.

NSC Pro Receiver

Table 18: NSC Pro Receiver Settings

Setting	Behavior
Interface	Read-only. Shows the value you selected on the General tab.
IP Network Settings	Appears only when the interface is Ethernet or Wi-Fi. The NSC Pro needs additional hardware for either. For more information, see Setting up an NSC Pro for IP Networking (EPC Sender) (on page 40).
CAN Node ID	Appears when J1939 is enabled on the General tab.
Stop Category	CAT0 (Immediate Stop) or CAT1 (Controlled Stop). CAT1 adds a delay you configure, after which Output 2 also turns off. For more information, see Relationship of Inputs and Outputs (on page 33).
OSSD	A toggle. OSSD test pulses are enabled by default and detect shorts on the safety outputs. For more information, see OSSD Pulses (on page 190).

Important:

If you turn OSSD off, your safety circuit loses the short detection those pulses provide. Turn it off only if a downstream device cannot tolerate the pulses and you have another means of detecting a short. For more information, see [Potential side effects of OSSD pulses](#) (on page 191).

EPC Receiver

Table 19: EPC Receiver Settings

Setting	Behavior
Interface	Read-only. Shows the value you selected on the General tab.
IP Network Settings	Appears only when the interface is Ethernet or Wi-Fi.

Setting	Behavior
CAN Node ID	Appears when J1939 or CANopen is enabled on the General tab.

Note:

When the configuration uses LRBLE and CAN is disabled, the EPC receiver has no settings to configure and FORT Manager does not list it under **Devices**. The receiver is still part of the configuration and you must still load the configuration onto it. For more information, see [Loading a Configuration onto Your Devices](#) (on page 79).

Note:

If CAN is not enabled, no further device-level settings are required for an LRBLE-only configuration.

Modifying a Deployed Configuration

If you add or remove devices from a *deployed* configuration, you must take some steps to be certain that the correct configuration is deployed to all devices and that all receivers are communicating with the correct transmitter(s).

Note:

If you remove a device from a configuration that has not been loaded to its devices, there are no safety issues. A configuration has no effect on any device until it's been loaded (deployed) to one or more of the devices in the configuration.

Removing a Receiver from a Deployed Configuration

When you remove a *receiver* from a deployed configuration, you must ensure that it is no longer listening to the transmitters remaining in the configuration. For example, suppose that you remove from service a tractor with an attached EPC or NSC Pro receiver. Then you remove the receiver from the configuration. At this point, you might think that the receiver is no longer powering the tractor. However, although you modified the configuration, the device itself still contains the old configuration, and as long as it's powered on, it continues to listen to any transmitters for which it was programmed to listen.

When you remove one or more receivers from a configuration, you are prompted as follows:

```
The following receiver(s) from the configuration have been removed:
[Receiver IDs]. These receiver(s) will continue to listen to the
transmitter(s) in the configuration. To prevent unsafe conditions, perform
ANY of the following actions on the removed receiver(s):

- Remove the receiver(s) from the machine or disconnect from power
- Apply a blank configuration to the receiver(s)
- Add the receiver(s) to a new configuration and reconfigure them
```

You can ignore this message if you haven't loaded the configuration to any devices yet.

If you don't intend to use the device(s) again, you can remove them from the machine or disconnect them from power.

On the other hand, if you anticipate a need to reuse the receiver in the future, but don't yet have a new configuration ready, you can apply a blank configuration to the device(s):

To Apply a Blank Configuration

1. In FORT Manager, after you remove a device, tether it to the computer that is running FORT Manager.
2. Click the link **Apply Blank Config** that pops up.

The info pane for the device opens.

3. Click the **Update** link to apply a blank configuration to the device.

The device now indicates that it has a blank configuration. Even if powered on, the device is unable to communicate with any other FORT device.

The device that you removed is now available to add to another configuration whenever you choose to do so. The receiver will keep its outputs low, meaning the robot or machine will remain in an unpowered state, until the receiver is flashed with a new, non-blank configuration and pairs with a transmitting device.

Note:

It's a best practice to redeploy the configuration to the transmitter when you remove a receiver, though not strictly necessary. It is *not* necessary to redeploy the configuration to the remaining receivers since nothing has changed for them. However, FORT Manager will show all devices as **Ready to Deploy** rather than **Deployed**, and if you want FORT Manager to display the correct deployment status, you must redeploy to every device in the configuration (see [To Redeploy a Configuration](#) (on page 77)). The status column on the **Devices** page is not affected by this issue; it reports reachability, not deployment (see [Device Status](#) (on page 8)).

Removing a Transmitter from a Deployed Configuration

When you remove a transmitter from a deployed configuration, and replace it with a new one, you must deploy the configuration to the new transmitter and redeploy it to all the receivers in the configuration (see [To Redeploy a Configuration](#) (on page 77)). You don't have to do anything special to the transmitter you removed. You can store it or reuse it in a different configuration.

Adding a Receiver to a Deployed Configuration

When you add a receiver to a One-to-Many configuration (an EPC sender with EPC or NSC Pro receivers), you must deploy the configuration to the new receiver.

Note:

You don't need to redeploy the configuration to the original receivers in the configuration, however FORT Manager will show all devices as *Ready to Deploy* rather than *Deployed*. If you want FORT Manager to

display the correct status, you must redeploy to every device in the configuration (see [To Redeploy a Configuration](#) (on page 77)). This is a known issue that is slated to be fixed with an upcoming release.

When you add a receiver to a Machine-Select Configuration (an SRC Pro sender with multiple potential EPC or NSC Pro receivers), or an SRC Pro with Global E-Stop Configuration (an SRC Pro and EPC transmitter with EPC receivers) you must deploy the configuration to the new receiver and to the SRC Pro transmitter.

Note:

You don't need to redeploy the configuration to the original receivers in the configuration, however FORT Manager will show all devices as *Ready to Deploy* rather than *Deployed*. If you want FORT Manager to display the correct status, you must redeploy to every device in the configuration (see [To Redeploy a Configuration](#) (on page 77)). This is a known issue that is slated to be fixed with an upcoming release.

To Redeploy a Configuration

You can redeploy a configuration with the FORT Manager Desktop App.

The following procedure outlines the procedure to redeploy a configuration using the FORT Manager Desktop App:

1. In FORT Manager Desktop, select one of the devices and click **Tether**.

The application displays information about the device, including the name of the configuration to which the device belongs.

2. Click **Update** next to the configuration name to upload the configuration to the device.

The application shows that the configuration has been updated and automatically untethers the device. You can unplug the device from the computer unless you have a firmware update to apply as well.

Repeat this procedure for every device in the configuration.

If you are using the CLI tool for configuration, see [Loading a Configuration onto Your Devices](#) (on page 79).

Bulk Actions on the Devices Page

The **Devices** page lets you select several devices with the row checkboxes and then assign, export, or delete them together. Assign and export are convenience operations. Bulk delete is not.



Warning:

Deleting a device that belongs to a deployed configuration has the same effect as removing it from that configuration, and the same safety consequence: the device still holds the configuration it was loaded with, and while it is powered on it continues to listen to the transmitters it was programmed to listen to. Deleting it from FORT Manager does not change what the hardware does.

Before you bulk delete, for every receiver in the selection perform ANY of the actions listed in [Removing a Receiver from a Deployed Configuration](#) (on page 75): remove the receiver from

the machine or disconnect it from power, apply a blank configuration to it, or add it to a new configuration and reconfigure it.

Note:

A device can belong to more than one configuration. Deleting it removes it from all of them. Check every configuration the device is a member of before you delete. For more information, see [Multiple Configurations for a Device](#).

Export writes the selected rows to a file and changes nothing on the devices.

Chapter 5. Loading a Configuration Onto Your Devices

This chapter explains how to load a configuration onto your devices once you have built it, using either the FORT Manager Desktop App or a FORT command-line tool, and helps you choose between them.

After you build a configuration, or make changes to an existing configuration, you need to load it onto your devices. There are two ways to do this:

Table 20: Ways to Load a Configuration

	FORT Manager Desktop App	FORT CLI v2	
Internet Connection Required	No, if you download in advance	No, once configuration files are downloaded.	
Use case	You want a UI, and you are working with one configuration at a time.	You are on a Linux computer with connectivity to FORT Manager and want a command-line workflow, or you need the interactive device menu.	

Important:

To initially create a new device configuration, internet connectivity is required.

We provide separate instructions for:

- [Loading a Configuration with the Desktop App](#) (on page 79)
- [Loading a Configuration with the CLI Tool](#) (on page 81)

Loading a Configuration with the Desktop App

This section shows how to load a configuration onto any FORT device (EPC, NSC Pro, SRC Pro, WES Pro) by using the Desktop App.

Required Items:

- A configuration that you built in FORT Manager.
- Windows or Linux computer running with Ethernet networking capability (required for using the FORT Manager Desktop App).
- Cables to connect your device to the computer:

- EPC — M12-RJ45 cable (e.g., ASI-M12-RJ45-11101)
- NSC Pro — USB-A to USB-C
- SRC Pro — USB-A to mini USB-B; SRC Pro 1003 has a USB-C port.
- WES Pro — Docking station
- FORT Manager Desktop App. Download the latest version from the **Downloads** card on the **Firmware** page of the FORT Manager Web App, or from [GitHub](#)).
- The FORT device and any connected machines are in a safe state to be configured.

To Load a Configuration with the Desktop App

1. Launch the FORT Manager Desktop App on your computer.
2. Boot up or power on your device.
3. Connect your computer to the device:
 - For an EPC, connect over Ethernet to port J2 on the EPC using the M12-RJ45 cable.
 - For an NSC Pro, SRC Pro, or WES Pro, connect via USB.

The application displays a message that it has detected a device for tethering. If multiple devices are connected to the computer, the application displays a list of devices to choose from.

4. Select the device and click **Tether**.

The application displays information about the device including the name of the configuration to which the device belongs.

- a. If FORT Manager doesn't auto detect the device, click **Tether a Device** and select the type of device:
 - For an EPC, enter the IP address.
 - For other devices, enter the COM port, generally **COM3**.
- b. Click **Connect**.

5. Click **Update** next to the configuration name to upload the configuration to the device.

The application shows that the configuration has been updated and automatically untethers the device. You can unplug the device from the computer unless you have a firmware update to apply as well.

Repeat this procedure for every device in the configuration.

To Download a Configuration for Offline Loading using the FORT Manager Desktop App

One of the advantages of the desktop app is that you can use it without an internet connection. If you plan to load configurations or make firmware updates when the internet is not available, you can download the firmware and configurations when connected to the internet and store them in the app for later retrieval.

1. Launch the FORT Manager Desktop App on your computer.
2. Click **Configurations**.

3. Select the configuration to download.
4. Click **Download Configuration**.

The Download Status changes to *Downloaded*.

Repeat for any other configurations that you plan to upload when offline.

Note:

Downloaded files are stored inside the application, not in your computer's file system.

Loading a Configuration with the CLI Tool

This section shows how to load (deploy) a configuration onto any FORT device (EPC, NSC Pro, SRC Pro, WES Pro) by using the CLI tool `fort_cli_cfg`.

Important:

The CLI command `fort_cli_cfg -w` retrieves the configuration from FORT Manager at the time you run it, and prompts you to confirm a code in a browser. It requires a working connection to FORT Manager and cannot be completed offline.

Required Items:

- A configuration that you built in FORT Manager.
- Linux computer running Ubuntu 20.04 with Ethernet networking capability.
- A working connection to FORT Manager, and your FORT Manager credentials.
- Cables to connect your device to the computer:
 - EPC — M12-RJ45 cable (e.g., ASI-M12-RJ45-11101)
 - NSC Pro — USB-A to USB-C
 - SRC Pro — USB-A to mini USB-B
 - WES Pro — Docking station
- Latest FORT CLI Configuration Tool (`fort_cli_cfg`). If you don't already have it, download it from FORT Manager and install it on your Linux machine per the instructions in [FORT CLI Configuration Tool](#) (on page 177).
- The FORT devices and any connected machines are in a safe state to be configured.

To Load a Configuration with CLI Tool

1. Boot up or power on your device.
2. Connect your computer to the device:
 - For an EPC, we recommend that you connect over Ethernet to port J2 on the EPC using the M12-RJ45 cable, which always connects to 192.168.3.10. If you connect over Ethernet to port J3, specify the last IP address you configured for the EPC.
 - For an NSC Pro, SRC Pro, or WES Pro, connect via USB. Note that WES Pro requires the docking station.

3. In a Linux environment, open a Terminal window and run one of following commands:

- a. To upload a single configuration from FORT Manager to an EPC when connected to J2 (if connected to J3, specify the last IP address you configured for the EPC):

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

- b. To upload a single configuration from FORT Manager to an NSC Pro, SRC Pro, or WES Pro (your serial interface, `tttyACM0` could be different):

```
$ fort_cli_cfg -w --n /dev/tttyACM0
```

Note that you need execute permissions to `/dev/tttyACM0`, or whichever virtual port you are using for the device.

If you receive a permission error, complete the next two sub steps; otherwise continue to Step 4:

- a. Run the following command to add yourself to the dialout group:

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

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

The CLI tool returns a code. The browser opens a window that asks you to confirm that the displayed code matches that in the CLI tool.

4. Press **Enter** to confirm that the codes match.
5. If you aren't already authenticated, enter your FORT Manager username and password to authenticate to FORT Manager.
6. Return to the CLI tool where you are prompted to enter the device serial number:
7. Type the serial number and press **Enter**.

You can find the serial number on the device nameplate, in a handheld's onscreen menu, or in FORT Manager on the **Devices** page. On the **Devices** page, narrow a large fleet with the model-type chips above the table, or search by device name.

8. Press ****Enter**** to load the configuration to the device.

The tool finishes with the device by writing all the relevant configuration parameters.

9. Reboot the EPC.

Repeat this procedure for each Device in your configuration.

Next Steps

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

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

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

Chapter 6. Using an SRC Pro

This chapter describes the Safe Remote Control Pro's joysticks, buttons, and operating modes, explains how to connect it to an Endpoint Controller and move it to a different one, and lists the alerts and error messages it displays.

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.

Operating Your Equipment Safely with SRC Pro

This chapter has warnings and cautions throughout for how to use the SRC Pro safely in specific situations, such as when charging it or turning it off and on. Keep the following warnings in mind as well:



Warning:

Do not use the E-STOP button to pick up, hold, or carry the SRC Pro. Doing so may damage the E-STOP button and create an unsafe operating scenario.



Warning:

If the E-STOP button breaks, gets damaged, stuck, or is hard to operate, immediately press the power button to turn the device off and contact FORT's customer support.

Do not turn the device back on again until you have been asked by FORT's customer support to do so.

SRC Pro Features

The following figure highlights the Safe Remote Control Pro Features:



Figure 31: Fig. 28 SRC Pro Features

Important:

Avoid operating an SRC Pro near magnets. The SRC Pro relies on Hall Effect joysticks, which use magnetic fields and non-contact sensors to detect movement. Exposure to external magnets can interfere with these sensors, potentially causing erratic joystick behavior or inaccurate control responses.

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

Push the power button to turn the SRC Pro on or off. When you turn it on, the LCD screen lights up when it is ready to use. Inserting the charging cable into the mini USB port also turns the SRC Pro on if it is connected to a power supply.

When you push the power button to turn it off, if the SRC Pro is connected to a receiver, it stops sending valid safety messages, which:

- Causes the connected device to go to the safe state after the timeout period is exceeded if the device is in *supervised* mode.
- Allows the machine to run autonomously if the device is in unsupervised mode.

Note:

To reboot the device, push and hold the power button (for 8 seconds or more) and release it when the screen flashes.

Pause Button

Press the **Pause** button (two vertical lines) to enter Pause Mode, and press it again to exit Pause Mode. See [Pause Mode](#) (on page 86) for details.

Modes

This section explains the different modes for the Safe Remote Control Pro. See [Changing the Mode of the EPC](#) (on page 89) for information about supervised and unsupervised modes which apply to a connected EPC.

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 mode 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

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

Note:

If you push the **Menu** button to exit a menu before connecting to a device, the screen indicates Radio OFF.

You don't need to do anything explicit to turn the radio on. As soon as you initiate pairing with a receiver, the SRC Pro radio starts transmitting.

Idle Timeout

When you are not using the SRC Pro, there are some situations in which the battery can drain:

- You take a break, put it down for an extended time and it continues to run, draining the battery
- You are done with the device for the day and put it in a holder on the machine so that it charges as the vehicle charges. However, once the vehicle finishes charging, it shuts down, but if the SRC Pro remains on, it will drain power.

To mitigate this issue, the SRC Pro provides a menu setting that allows you to specify an Idle Shutdown Timeout, an amount of time, after which the SRC Pro automatically shuts off if it's idle.

To set the Idle Time Value:

1. a. Push the four-bar settings button.
2. Navigate to **Settings**.
3. Select **Idle Shutdown Timeout** and set to OFF or a value between 1 - 20 (minutes) in the dropdown menu.

Idle Shutdown activates if both of the following are true:

- The transmitter's Idle Shutdown Timeout is set to a non-zero value.
- All of the following have been true for the duration of the Idle Shutdown Timeout value: - The transmitter is not connected to any receiver. - The transmitter is not moving. - The transmitter is not connected to a USB power source; or it is connected to a USB power source, but is not uploading or downloading data over the USB connection.

Important:

If a device is actively connected to a receiver, even if it hasn't been moved for the Idle Timeout period, it won't go into Idle Shutdown; it will stay on and connected to the receiver.

Low-Power Charge Mode

If an SRCP that's connected to USB power (for charging or otherwise) is shut down, manually or via Idle Shutdown timeout, it will go to *Low-Power Charge Mode* rather than fully shutting off. In this mode, the SRC Pro will display the battery state while also locking out other functions to conserve battery power and speed up charging.

Connecting the SRC Pro to an EPC

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

Before You Begin

Make certain that:

- Both devices are powered up and in range of each other.
- You understand how Machine Select works and the difference between supervised and unsupervised modes ([Machine Select Configuration](#) (on page 50)).

Briefly, supervised means that the SRC Pro is sending joystick movements and safety data to the machine, whereas unsupervised means that the machine is operating independently with its own safety mechanism, and with no communication with the SRC Pro. When you first connect to an EPC, the mode is always supervised. You can change the mode at any time after connecting ([Changing the Mode of the EPC](#) (on page 89)).

To Connect an SRC Pro to an EPC:**Note:**

This procedure applies to both connecting to an EPC for the first time and connecting to a different EPC when already connected to an EPC.

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

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

The SRC Pro displays a warning screen indicating that the E-Stop button has been pressed.

3. Press the **Menu** button to exit the E-Stop activated screen.
4. On the SRC Pro LCD screen, use the arrow keys to navigate to the Machine tab.

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

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

The screen displays a confirmation code.

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

If you change your mind, you can press the **Menu** button to quit and return to the selection menu.

Note that pressing an incorrect number sequence also returns you to the selection menu.

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

At this point, the SRC Pro has transitioned to supervised mode. If the connection attempt fails, you can repeat the connection process.

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

You can now 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.

Note:

If the connection with a receiver is lost, the bottom row of the SRC Pro display window shows: RadioDisconnected.

Connecting an SRC Pro to a different EPC

You can change the device that an SRC Pro is connected to at any time.

Note:

There is no procedure to disconnect the SRC Pro from an EPC to which it is connected. The SRC Pro can be connected to only one EPC at a time, so connecting to a new EPC effectively disconnects from the old device. To connect to a new device, follow the connection procedure in the previous section.

Although you cannot explicitly deselect a connected device, in a one-to-one configuration, powering off the connected device is functionally equivalent to deselecting it.

Note the following about the previously connected device:

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

Changing the Mode of the EPC

Whenever you connect a Safe Remote Control Pro to an EPC, the SRC Pro sets the mode of the EPC to supervised. At any time after connecting to an EPC in supervised mode you can change its mode to unsupervised if the machine has autonomous capability and has been wired appropriately.

In unsupervised mode, the SRC Pro and the EPC are not communicating with each other, so the SRC Pro is not sending safety or control information to the EPC. Rather, the EPC that is attached to the equipment is responsible for monitoring the customer supplied safety signal, and if that signal changes out of the

normal state, the EPC enters the safe state and breaks the circuit to the equipment under control. For wiring details, see [Wiring Receivers with an SRC Pro Sender](#) (on page 10).



Warning:

Make certain that you are aware of the following points about operating equipment in unsupervised mode:

- Pushing the E-Stop button on the SRC Pro has no effect because the EPC ignores an E-Stop command when in unsupervised mode.
- Be certain that the equipment is able to operate safely without need of the E-Stop button, as pushing it will have no effect and it may not be quick or easy to change the mode of the EPC back to supervised for a number of reasons, including the following:
 - The equipment with the EPC is out of range of the SRC Pro.
 - The SRC Pro has run out of battery.
 - The SRC Pro is damaged or unresponsive.

To Change the Mode:

Make certain that:

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



CAUTION:

If you are changing the mode from supervised to unsupervised, be certain that the EPC is connected to a machine with autonomous capability and that it has been wired appropriately for unsupervised mode. If the machine does not have autonomous capability, and has not been wired appropriately, the EPC will transition to safe state when you change the mode to unsupervised.

See [Wiring an EPC to use with Machines With Autonomous Capability](#) (on page 10) for details.

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

The screen displays a confirmation code and a prompt to change to *Autonomous* or *Supervised* (opposite of the current mode).

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

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

4. Wait for the connection to be established and when confirmed, press **1** to close the window.
5. After the mode change is successful, press the **Menu** button to close the prompt.

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

Viewing the Connection Status

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

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

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

Turning the SRC Pro Off and Back On

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

After you turn the SRC Pro back on, machines that were in unsupervised mode will continue to operate in unsupervised mode, but the display will show these machines as blank. If the SRC Pro was connected to a machine in supervised mode, it will no longer have a connection unless you reestablish one. The display mode for that machine will be blank until you reconnect.

Note:

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

Turning the EPC Off and Back On

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

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

Note:

The displayed mode on the SRC Pro only indicates the mode that the user set the EPC to. It does not reflect the actual state of the EPC. For example: you set the mode of the EPC on Machine-1 to unsupervised and then use the SRC Pro to connect to Machine-2. Later, Machine-1 moves out of range

of the SRC Pro, or it is turned off, but since the SRC Pro doesn't have communication with that EPC, it continues to show the mode as unsupervised (indicated by **AUTO**).

Alerts and Error Messages

This section lists some SRC Pro error messages and how to resolve them.

- **Joystick Jammed** — Indicates a button was pressed during power on.
 - To resolve, power cycle the SRC Pro (Press and hold the power button for 8 or more seconds and release it when the screen flashes).
- **Keypad Jammed** — Indicates that a keypad button was pressed when the SRC Pro was powering on.
 - To resolve, power cycle the SRC Pro (Press and hold the power button for 8 or more seconds and release it when the screen flashes).
- **Radio Off** — Indicates that the SRC Pro radio is not broadcasting because it is not connected to a receiver.
 - No action is required. As soon as you initiate pairing between the SRC Pro and a receiver, the radio turns on and begins transmitting.

Note:

If the SRC Pro shows an error that is not listed here, or behaves in a way this guide does not explain, retrieve its logs before you contact support. For more information, see [Using Logs](#) (on page 206).

Chapter 7. Using a WES Pro

This chapter describes the WES Pro's E-Stop button, menu screen, and alerts, and explains how to charge it, replace its battery, connect it to a receiver, and store it safely between uses.

This chapter describes the features of the WES Pro and explains how to connect a WES Pro to a receiver.

Operating Your Equipment Safely with WES Pro

This chapter has warnings and cautions throughout for how to use the WES Pro safely in specific situations, such as when charging it or turning it off and on. Keep the following warnings in mind as well:



Warning:

Whenever approaching equipment for inspection or maintenance, press the E-Stop to be certain that the equipment is in a safe state and won't start operating unexpectedly. In addition, power off the machine via its power source, and follow relevant lock-out-tag-out procedures, to minimize the risk of energy-related hazards during maintenance.

Once you disengage the E-Stop, the connected device will operate normally. Be certain that the connected machine is safe to operate before disengaging the E-Stop.



Warning:

Do not use the E-STOP button to pick up, hold, or carry the WES Pro. Doing so may damage the E-STOP button and create an unsafe operating scenario.



Warning:

If the E-STOP button breaks, is damaged, stuck, or hard to operate, immediately press the power button to turn the device off and contact FORT's customer support.

Do not turn the device back on again until you have been asked by FORT's customer support to do so.

Charging the WES Pro

The WES Pro is powered by a rechargeable battery and is shipped with a docking station and a power supply and cable for charging the device.



Figure 32: Fig. 29 Docking Station Charger

The WES Pro provides a haptic indicator (vibrates) when the battery charge drops to 10%, as well as a different vibration pattern if the device shuts off because of low battery.

To Charge the Device



Warning:

Always charge the device where the dock is not exposed to dust or moisture. If the dock is wet, towel it off before charging the device.

1. Plug the power supply into an outlet.

2. Turn the docking station over and insert the USB-C connector into the port on the underside of the docking station:



Figure 33: Fig. 30 Docking Station Underside

3. As a precaution, press the E-Stop button on the WES Pro before inserting it into the dock.
4. Push the WES Pro into the docking station until it clicks in place.



Figure 34: Fig. 31 WES Pro in Docking Station

The WES Pro turns on (if off) and the indicator light on the docking station shows that it is charging. The LCD screen also shows the charge percentage for the battery.

5. Remove the WES Pro from the docking station when it's sufficiently charged.

Note:

When you place a WES Pro in the dock, it automatically powers on. To prevent it from reconnecting to a receiver, potentially triggering the equipment under control (EUC) to operate, the system keeps the receiver in a safe state until you explicitly disengage the E-Stop. If you haven't pressed the E-Stop, the WES Pro displays a message: **"Press the E-STOP to Enable WES Pro."** that remains on until you engage the E-Stop. To reconnect to a receiver, press the E-Stop, then disengage it. If the E-Stop is engaged, the message does not appear.

6. If you haven't engaged the E-Stop, press it now and proceed to the next step (or if it's engaged, just go to the next step).
7. **When it's safe to do so**, disengage the E-Stop by turning the button clockwise until it snaps out, which allows the EUC to operate normally. If the WES Pro is connected to a receiver and in range of it, when you disengage the E-Stop, the EUC powers on.

Replacing the Battery



CAUTION:

If the battery needs replacement, contact [customer support](#) and request service. Do **not** attempt to replace the battery yourself. The WES Pro has no user-serviceable parts, including the battery.

WES Pro Features and Operation

The following figure highlights the WES Pro features:



Figure 35: Fig. 32 WES Pro Features

Turn WES Pro On or Off

Push the power button (located on the bottom of the device) to turn the WES Pro on or off. When you turn it on, the LCD screen lights up and the device vibrates when it is ready to use. Inserting the device into the docking station also turns it on if the docking station is connected to a power supply.



CAUTION:

We recommend that you press the E-Stop button before powering the WES Pro on or off. However, the WES Pro has a built-in mechanism to prevent it from automatically reconnecting to a receiver when turning on, potentially triggering the EUC to operate unsafely. If the E-Stop button is *not* engaged when you turn the WES Pro on, the system prompts you to press the E-Stop button and keeps the receiver in a safe state until you first press the E-Stop button and then disengage it.

When you push the power button to turn it off, the WES Pro stops sending valid safety messages, which causes any connected device to go to the safe state after the timeout period is exceeded.

Note:

To reboot the device, push and hold the power button (for 8 seconds or more) and release it when the screen dims.

Connecting the WES Pro to a Receiver

There is no explicit procedure to connect a WES Pro to receivers. Once the configuration to which the devices belong has been uploaded⁹, the devices begin communicating with each other if they are turned on and in range of each other.

Note:

A WES Pro can be paired to an EPC or to an NSC Pro receiver.

In a Two-to-One configuration, the WES Pro shares its receiver with a second sender, and both act on the same output. The machine stays stopped while either device is requesting a stop, so releasing the E-Stop on the WES Pro does not restart the machine if the other sender is still stopping it. For more information, see [Two-to-One with a WES Pro and an EPC](#) (on page 61).

Which output the two senders share is set for the configuration and may be Output 1 or Output 2. For more information, see [Choosing Which Output the Senders Control](#) (on page 62)

Before You Begin

Make certain that you have uploaded the configuration to all devices ([Loading a Configuration onto Your Devices](#) (on page 79)).

To Connect a WES Pro to an EPC:

⁹ A WES Pro can pair with one receiver only. The receiver can be an EPC or an NSC Pro. Consult the [Release notes](#) for information specific to the version of the product that you are using.

1. As a safety precaution, press the E-Stop button.

When the devices connect, the E-Stop signal guarantees that the receiver is in a safe state and the equipment won't start operating unexpectedly.

2. Power up both devices and keep them within range of each other.

The WES Pro displays a message indicating that the E-Stop button has been pressed.

The WES Pro provides haptic feedback (vibrates) when it connects to the receiver.

3. Press # to exit the E-Stop activated screen.
4. You can press the **Menu** button # and click **Receiver Devices** to verify that the WES Pro has connected to the receiver.
5. **When it is safe to do so**, turn the E-Stop button clockwise until it pops out to release it.

At this point, the EUC should be operating normally.

E-Stop Button

Press the E-Stop button to send a safety command to a connected device or devices. The LCD will display the following alert: E-Stop triggered for all connected machines



Warning:

Once you disengage the E-Stop, the connected device will operate normally. Be certain that the connected machine is safe to operate before disengaging the E-Stop.

Turn the E-Stop button clockwise until it pops out to disengage the E-Stop command.

Press # to clear the alert.

WES Pro Menu Screen

Press the three-line **Menu** button # to access the WES Pro menus:

- Press the up and down arrows to navigate between menus and between menu items.
- Press # to open a menu or to change the setting for a menu item.
- Press the **Menu** button # to move back a level in the menu structure.

Note:

For some menus, you press # or the **Menu** button # to exit, in which case, the menu instructs you to do so.

The WES Pro provides the following menus:

- **Receiver devices —** Lists lists all receivers to which the WES Pro is able to connect¹⁰.

¹⁰ For this release, a WES Pro can pair with only one receiver. Consult the [Release notes](#) for information specific to the version of the product that you are using.

- **Device Attributes —**

Lists WES Pro device information, including:

- **Serial Number** - Shows the serial number for the device.
- **Firmware Version** - Shows the version of the firmware that is running on the device.
- **RSSI** - (Received Signal Strength Indicator) as perceived by the WES Pro.
- **Battery Information** - Shows the Volts and Amps for the battery.
- **Config Name** - Name of the configuration to which the device belongs.
- **MAC address** - Shows the MAC address of the device.

- **Device Settings —**

The settings menu allows you to customize the following settings:

- **Brightness** - Set the display to low, medium, or high.
- **Haptics** - Turn haptic responses on or off. The WES Pro provides three distinct vibration patterns to indicate device issues (low battery, communication loss, weak signal, etc.).
- **Motor Test** - Set the motor haptic response to Normal, Strong, or Pulse.
- **Button Test** - Allows you to verify that each of the buttons is responding when pressed.
- **Display Test** - Allows you to verify that each pixel of the display can be activated and deactivated.

Alerts

The WES Pro provides visual and haptic alerts:

- It vibrates to indicate low battery (below 10%).
- It vibrates if it shuts down due to low battery.
- It vibrates if it loses communication with a receiver.
- It vibrates to indicate a weak wireless signal.

- The LCD displays the following alert when an E-Stop is triggered: E-Stop triggered for all connected machines

When it's safe to do so, turn the E-Stop button clockwise until it pops out to disengage the E-Stop command. Once you disengage the E-Stop, the connected device(s) will operate normally.

Storing the WES Pro

If you plan to store the WES Pro for an extended period of time, we recommend doing so at the following temperatures to maximize battery life:

Table 21: Table 13 WES Pro Recommended Storage Temperatures

Period	Temperature
Up to one month	-20 °C to 50 °C
One to three months	-10 °C to 45 °C
Longer than three months	-10 °C to 35 °C

Chapter 8. CAN Application Support

This chapter describes how an EPC transmits joystick, control, and status data over CAN using the CANopen and J1939 protocols, documents the messages for each, and explains how to enable CAN and set its parameters in FORT Manager.

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

This chapter provides the following information:

- [CANopen Implementation](#) (on page 103) describes transmitting joystick data using the CANopen protocol.
- [J1939 Implementation](#) (on page 106) describes transmitting joystick data using the J1939 protocol.
- [SRC Pro Control Messages](#) (on page 114) describes control messages for both protocols.
- [Status Messages](#) (on page 117) describes status messages for both protocols.
- [Peer Connection Status](#) (on page 127) describes the message that reports whether each configured peer is currently connected.
- [Safety Event Messages](#) (on page 130) describes the messages that report safety state changes on the EPC.
- [Configuring CAN with FORT Manager](#) (on page 138) describes how to enable CAN and set optional parameters.

CANopen Implementation

This section shows how to send joystick data using CANopen.

When integrated with the SRC Pro, the EPC presents itself on the CANopen network as a CiA 301/401-1/401-2 compliant device.



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.

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

Table 22: Table 14 CANopen

Description	Direction	Frequency
Joystick Data – Buttons (See Table 6-2, “TPDO1 Buttons,” on page 6-3).	Transmit	~20 Hz (buttons actively pressed.) ~4 Hz (inactive & buttons not pressed)
Joystick Data - Thumbstick Axes (See Table 6-3, “TPDO2 Thumbstick Axes,” on page 6-3).	Transmit	~20 Hz
Joystick Data - Trigger Axes (See Table 6-4, “TPDO3 Trigger Axes,” on page 6-4).	Transmit	~20 Hz

Joystick and Button Data Representation

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

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

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

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

The following table shows the TPDO1 buttons.

Table 23: Table 15 TPDO1 Buttons

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

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

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

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

Table 24: Table 16 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 25: Table 17 TPD03 Trigger Axes

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

CANopen Limitations

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



Warning:

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

- The default bitrate of the CAN interface is 250000. You cannot adjust the bitrate through the CANopen NMT protocol but must do so by using FORT Manager or the FORT CLI Config Tool.
- The default device Node ID is 3. You cannot change the device address through the CANopen NMT functionality, but must do so by using FORT Manager, which lets you set the node ID for each device in a configuration. For more information, see [Configuring CAN with FORT Manager](#) (on page 138).

J1939 Implementation

The EPC's CAN application supports sending and receiving messages using the J1939 protocol. The EPC uses the Emotas J1939 stack to provide the full functionality of the J1939 protocol.



Warning:

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

At present, while the integration is intended to be compatible with a J1939 compliant network, the full capability set described in the standards is not yet implemented. You can find a sample DBC (Database Container) file to download on the Customer Support Portal in the Endpoint Controller article.

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

Table 26: Table 18 CAN J1939

PGN	PGN (Hex)	Description	Direction	Freq
	0xEEFF	Address Claiming	Transmit	

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

Address Claiming

Both the EPC and NSC-Pro support the standard J1939 address claiming procedure (PGN 0xEE00). This allows multiple J1939 devices on the same CAN bus to negotiate unique source addresses without manual configuration.

The FORT Manufacturer Code is **1262 (decimal)**.

Table 27: Table 19 J1939 Address Claiming Message

PGN	Description	Direction	Freq
0xEE00 (60928)	Address Claiming	Transmit	On startup and on address conflict

Note:

The EPC and NSC-Pro will first attempt to claim the source address configured in their configuration file. If another device on the bus contests that address, the standard J1939 arbitration procedure determines which device wins.

Address claiming is a standard J1939 mechanism. For details of the arbitration procedure, refer to SAE J1939-81 (Network Management).

The source address used at runtime is the address that was successfully claimed. It appears as the low byte of the 29-bit CAN ID on every transmitted message.

Valid J1939 source addresses run from 0x00 to 0xFD (253). Addresses 0xFE and 0xFF are reserved by the J1939 standard and are never used as source addresses by FORT devices.

J1939 Approved Source List

The EPC and NSC-Pro respond only to CAN messages whose J1939 source address appears in a configured approved source list. This provides a basic layer of filtering against unintended commands from other devices sharing the bus.

The approved source list is optionally provided as part of the device configuration file. An empty list means all source addresses are approved.

You can specify source addresses with FORT Manager (see [Configuring CAN with FORT Manager](#) (on page 138)).

Valid approved source addresses are **0 to 253 (decimal)**.

Note:

In J1939:

- Source address **254** is reserved as the NULL address (used during address claiming before an address is assigned).
- Source address **255** is reserved as the global address (broadcast).

The approved source list affects which incoming messages the device will act on — for example, SRC-Pro Settings Messages (PGN 0xFF01) and Display Text Messages (PGN 0xFF02). It does not affect address claiming behavior or the messages the device transmits.

Left Joystick - J1939 Basic Joystick Message

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

Table 28: Table 20 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

Bytes	Bits	J1939 PGN 64982 Data field	Description
	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

Bytes	Bits	J1939 PGN 64982 Data field	Description
	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	4 bits	Not used.	N/A
5	2 bits		Y-Axis Detent Position Status
5	2 bits		X-Axis Detent Position Status

Bytes	Bits	J1939 PGN 64982 Data field	Description
6	2 bits	00b: Button not pressed 01b: Button pressed 10b: Error Indicator 11b: NA	Keypad button Left North has been pressed. As per J1939 DA it is Joystick button 4 (up arrow)
6	2 bits		Keypad button Left West has been pressed. As per J1939 DA it is Joystick button 3 (left arrow)
6	2 bits		Keypad button Pause has been pressed. As per J1939 DA it is Joystick button 2
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 West has been pressed. As per J1939 DA it is Joystick button 8 (button 4 on device)
7	2 bits		Keypad button Menu has been pressed As per J1939 DA it is Joystick button 7

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

Left Joystick - J1939 Extended Joystick Message 1

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

Table 29: Table 21 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

Bytes	Bits	J1939 PGN 64983 Data field	Description
1/2	10 bits	The position of the joystick in the relative motion of travel from the neutral position. Position value of 0 is Neutral and position value 1000 (100%) is the end of linear zone. Value of 1022 indicates an error has occurred.	Z-Axis Position

Right Joystick - J1939 Basic Joystick Message 2

Same as Left Joystick - J1939 Basic Joystick Message 1.

Right Joystick - J1939 Extended Joystick Message 2

Same as Left Joystick - J1939 Extended Joystick Message 1.

SRC Pro Control Messages

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

Note:

The EPC filters messages to ensure that it does *not* incorrectly acknowledge IDs (CANopen) or PGNs (J1939) not meant for it.

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

Table 30: Table 22 RPDO1 (0x200 + Node ID) - SRC Pro Settings Message

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

Table 31: Table 23 RPDO2 (0x300 + Node ID) - User Display Text String

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

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

Table 32: Table 24 CAN J1939 SRC Pro Settings Message

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

Note:

You can change the default value by using [this procedure in FORT Manager](#) (on page 138) in case you have a crowded CAN bus with potential PGN conflicts on your system.

SRC Pro Settings Message

The EPC supports receiving an SRC Pro Settings message (from the equipment under control) to change settings on a connected Safe Remote Control Pro. This message is only supported for an EPC that is connected to a Safe Remote Control Pro.

**CAUTION:**

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

The following table shows the SRC Pro Settings message format:

Table 33: Table 25 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 34: Table 26 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 EPC supports receiving an SRC Pro user display text message (from the EUC) 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 EPC is connected to a Safe Remote Control Pro.

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

**CAUTION:**

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

Table 35: Table 27 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 36: Table 28 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.

Note:

Custom display text travels over the machine's CAN bus as an ordinary control message. Do not use it for a person's name or other personal data. For more information, see [Personal Data in FORT Manager](#) (on page 227).

Status Messages

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

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

Table 37: Table 29 TPD04: (0x480 + Node ID) - EPC Status Messages

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

The following table shows the PGN for J1939 status messages.

Table 38: Table 30 J1939 EPC Status Messages

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

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

Table 39: Table 31 Message Identifiers and Frequencies

Name	Identifier	Frequency	Notes
EPC Output Status 1	0	200 ms and on change of safety state	
EPC Connected Device Latency	1	1 sec	Not currently implemented. Always returns the value 0xFFFF.
SRC Pro System Status	2	1s normally; 10s if no data received from SRCP for >= 5 seconds	Enabled when SRC Pro is connected; in a 2:1 configuration, this message is enabled.
ISM Connection Status	3	1 sec	Enabled only if ISM is configured.

Name	Identifier	Frequency	Notes
WES Pro System Status	2	1s normally; 10s if no data received from WESP for >= 5 seconds	Enabled when WES Pro is connected; in a 2:1 configuration, SRC Pro System Status is enabled, <i>not</i> this message.
Radio Connection Status	3	1 sec	Enabled only if LRBLE is configured. In a 2:1 configuration, connection status will be for SRC Pro.

Note:**Table 31 Message Identifiers and Frequencies: Identifier Column**

The SRC Pro and WES Pro System Status messages have the same ID, as do the ISM Connection Status and Radio Connection Status messages. The EPC determines which message to send based on the connected device type or radio type. In a 2:1 configuration, the EPC sends the SRC Pro System Status message and the Radio Connection Status is for the SRC Pro.

EPC Output Status 1 Message

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

Table 40: Table 32 EPC Output Status 1

Byte Offset	Size	Description	Value
0	1	Message ID	Identifier for EPC Output Status 1 Message (on page 119) - 0x00
1	1	Status Sequence ID	8-bit Unsigned Integer that increments a sequence number to associate messages related to the EPC status to a single time

Byte Offset	Size	Description	Value
2	1	Output 1 State	Bits 3:0 - SMCU0 State Bits 7:4 - SMCU1 State 0000 - SAFETY_REQUESTED; cause is unspecified 0001 - SAFETY_NOT_REQUESTED 0010 - SAFETY_FAULT 0100 - Timeout; paired remote communication lost ¹¹ 1000 - Safety from input request
3	1	Output 2 State	Same as Output 1 State
4	1	Output 3 State	Same as Output 1 State
5	1	Mode	Bits 3:0 - SMCU0 State Bits 7:4 - SMCU1 State 0000 - No Mode (Error State) 0001 - Supervised 0010 - Autonomous (Unsupervised) 0011 - Not Applicable (EPC to NSC Pairing)
6	1	Reserved	Reserved for future use

¹¹ A timeout does not necessarily indicate that safety has been requested. For example, when you put an EPC in unsupervised mode (for a machine with autonomous capability), it is no longer communicating with the remote SRC Pro, which causes a CAN timeout signal. However, the machine itself is still operating safely as long as it's own safety system is functioning correctly, hence no CAN safety signal is sent. However, for a machine that is in supervised mode, losing communication with the remote device triggers both a *timeout* signal and a *safety requested* signal.

Byte Offset	Size	Description	Value
7	1	Reserved	Reserved for future use

EPC Connected Device Latency Message

Important:

This message was developed for future use but is not currently implemented for any FORT devices. It always returns the value 0xFFFF.

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

Table 41: Table 33 EPC Connected Device Latency

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

SRC Pro System Status Message

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

Note:

This message has the same identifier as the WES Pro System Status message. The EPC determines whether to send this message or the WES Pro message, based on which device is connected to the EPC. In a 2:1 configuration, it sends the SRC Pro message.

Table 42: Table 34 SRC Pro System Status

Byte Offset	Size	Description	Value
0	1	Message ID	Identifier for SRCP System Status message - 0x02
1	1	Status Sequence ID	Integer Incrementing sequence number to associate messages related to the SRCP System Status to a single time
2	1	USB Connected	Bit Meanings Bit 7: 1 = USB connected, 0 = USB disconnected Bit 6: 1 = USB charging, 0 = USB not charging Bits 5:0: Reserved
3	1	Battery Percentage	Battery Percentage from 0 (Decimal)% to 100 (Decimal)%

Byte Offset	Size	Description	Value
4	1	Mode	Mode Values: 0x04: Local Mode - Device is not yet paired. 0x06: Remote Mode - Device is paired, but not yet sending button/joystick state. 0x09: Operational Mode - Device is paired, and is sending button/joystick state. 0x0A: Menu mode - Device is in its menu. If connected, it continues to output the joystick message but with all values set to 0 to guarantee that no motion will occur. 0x0B: Pause mode - Device is paused. If connected, it continues to output the joystick message but with all values set to 0 to guarantee that no motion will occur.

Byte Offset	Size	Description	Value
5	1	Cause of Pause	Value to indicate the reason that the SRC Pro is in Pause mode Pause Cause Values: 0: None 1: Manual pause 2: Free fall 3: Orientation 4: Inactivity
6	1	Reserved	0xFF
7	1	No message	Bit Encoding Bit 7: 1 = No status messages received for >= 5 seconds, information may be out of date. Bits 6:0: Reserved

WES Pro System Status Message

This message is enabled only when a WES Pro is connected to the EPC. The rate (trigger) for this message is normally 1 second unless no data is received from the WES Pro for 5 seconds or more, in which case it is 10 seconds.

Note:

This message has the same identifier as the SRC Pro System Status message. The EPC determines whether to send this message or the SRC Pro message, based on which device is connected to the EPC. In a 2:1 configuration, it sends the SRC Pro message.

Table 43: Table 35 WES Pro System Status

Byte Offset	Size	Description	Value
0	1	Message ID	Identifier for WES Pro System Status message - 0x02
1	1	Reserved	0x0
2	1	USB Connected	Bit Meanings Bit 7: 1 = USB connected, 0 = USB disconnected Bit 6: 1 = USB charging, 0 = USB not charging Bits 5:0: Reserved
3	1	Battery Percentage	Battery Percentage from 0 (Decimal)% to 100 (Decimal)%
4	1	Reserved	0x0
5	1	Reserved	
6	1	Reserved	0x7F
7	1	Reserved	0x0

ISM Connection Status Message

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

Note:

This message has the same identifier as the Radio Connection Status message. The EPC determines whether to send this message or the Radio Connection message, based on the radio type.

Table 44: Table 36 ISM Connection Status

Byte Offset	Size	Description	Value
0	1	Message ID	Identifier for ISM Connection Status Message - 0x03

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

Radio Connection Status Message

The message rate (trigger) is 1 second, but only enabled when long range bluetooth (LRBLE) is configured.

Note:

This message has the same identifier as the ISM Connection Status message. The EPC determines whether to send this message or the ISM Connection message, based on the radio type.

In a 2:1 configuration, connection status reports the SRC Pro link. This is the case even when both senders communicate over LRBLE, as in a [Two-to-One over Long-Range Bluetooth](#) (on page 59): the RSSI value describes the SRC Pro's link to the receiver, not the EPC sender's link to the receiver.

Table 45: Table 37 Radio Connection Status

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

Peer Connection Status**Note:**

This message is only transmitted by EPC devices in an EPC-EPC 1:1 set-up. NSC-Pro does not support it.

Purpose

PeerConnectionStatus is a compact paged snapshot message that reports the connection state for a window of peer slots in a single 8-byte frame. It answers the question: *is each configured peer currently connected or disconnected?*

CAN Frame Identifier

Table 46: Table 38 Peer Connection Status Frame Identifier

Field	Value
J1939 PGN	0xFF05 (65285)
Priority	4
Source Address	Configured address (default 0x00)
29-bit CAN ID (with source 0x00)	0x18FF0500
CANopen TPDO	TPDO7 – COB-ID \$NODEID+0x780, OD object 0x3003
Direction	Transmit

Data source: the epc-peer-manager service tracks peer connectivity by monitoring CoAP heartbeats from remote peers and radio link state from the interface wrapper. The epc-can service subscribes to peer connection change events and encodes this message. Only configured peers (those in the peer list) are reported; unconfigured slots report Unknown_Unassigned.

Message Format

The message uses:

- Byte 0 for Peer_Offset (page index).
- 2 bits per peer slot in bytes 1 to 7.

Peer_Offset is a page index, not a raw peer number. The first reported peer slot in a frame is $28 \times \text{Peer_Offset} + 1$ (1-based).

With 7 data bytes available for peer states, each frame carries 28 peer states.

Table 47: Table 39 Peer Connection Status Format

Byte	Field	Description
0	Peer_Offset	Page index (0 = peers 1–28, 1 = peers 29–56, etc.)
1	Peer states [1–4]	2 bits per peer (4 peers per byte)
2	Peer states [5–8]	2 bits per peer

Byte	Field	Description
3	Peer states [9–12]	2 bits per peer
4	Peer states [13–16]	2 bits per peer
5	Peer states [17–20]	2 bits per peer
6	Peer states [21–24]	2 bits per peer
7	Peer states [25–28]	2 bits per peer

Each 2-bit peer state encodes:

- 0=Unknown_Unassigned – slot not configured in the peer list
- 1=Connected – peer is connected and heartbeating normally
- 2=Disconnected – peer was configured but is no longer responding
- 3=Reserved

Bit Layout Within Each Byte

Within each status byte (bytes 1–7):

- bits 1:0 = first peer in that group of four
- bits 3:2 = second peer
- bits 5:4 = third peer
- bits 7:6 = fourth peer

Example

If Peer_Offset=1, the frame reports peer slots 29 to 56.

Suppose the first four peers in that window are:

- peer 29 = Connected (01)
- peer 30 = Disconnected (10)
- peer 31 = Unknown/Unassigned (00)
- peer 32 = Connected (01)

Then byte 1 = 0b_01_00_10_01 = 0x49.

Page Ranges

Table 48: Table 40 Peer Connection Status Page Ranges

Peer_Offset	Peer slots reported
0	1 to 28
1	29 to 56

Peer_Offset	Peer slots reported
2	57 to 84

The maximum configured care list size is 32 peers, so in practice only one page (Peer_Offset=0) is needed in current deployments. The paged format exists to scale gracefully if the peer count increases.

Tradeoffs of the paged snapshot approach:

- Scales better to larger peer counts than a single frame per peer.
- Keeps a simple connected/disconnected snapshot concept.
- Requires multiple frames to build a full system view when more than 28 peers exist.
- Should be transmitted at a lower rate as peer count increases, since more messages are needed to refresh the full peer set.

Relationship to Safety Events

PeerConnectionStatus is a *snapshot* of the current connectivity picture. It does not describe *why* a peer disconnected or what safety state change occurred.

For richer information about peer safety state transitions, see [Safety Event Messages](#) (on page 130), which documents the Peer_Safety_Event message – J1939 PGN 0xFF03, CANopen TPDO5.

Safety Event Messages

Note:

Safety event messages are only transmitted by EPC devices in an EPC-EPC 1:1 set-up. NSC-Pro does not support them.

Two messages report safety state changes on the EPC. Both are available over J1939 and over CANopen; the table below gives the J1939 PGN for each, and the CAN frame table in each message's own section gives the CANopen TPDO.

Table 49: Table 41 Safety Event Messages

Message	PGN	29-bit CAN ID (source 0x00)	Purpose
Peer_Safety_Event	0xFF03 (65283)	0x08FF0300	Peer-related safety state from care list
Local_Safety_Event	0xFF04 (65284)	0x08FF0400	Local EPC safety detail from SMCU diagnostics

The split is intentional:

- Peer safety reporting stays simple – it only carries information the EPC actually knows from peer tracking and care list status.
- Local safety reporting carries richer SMCU diagnostic detail without overloading the peer message.

Data origin: the `smcu-mgmt-linux` service reads raw safety frames from SMCU 0 and SMCU 1 over serial, compares successive frames to detect changes, and publishes JSON safety events via ZMQ. The `epc-can` service subscribes to these events (via the CoAP service layer), encodes them into CAN frames, and transmits them on the bus. Events from SMCU 0 and SMCU 1 can be merged into a single frame using `Peer_Source_SMCU = 2 (Both)` when both SMCUs report the same change simultaneously.

Peer Safety Event

`Peer_Safety_Event` reports care list state changes for a specific peer slot.

The following table shows the CAN frame for this message:

Table 50: Table 42 Peer Safety Event CAN Frame

Field	Value
J1939 PGN	0xFF03 (65283)
Priority	2
29-bit CAN ID (source 0x00)	0x08FF0300
CANopen TPDO	TPDO5 – COB-ID \$NODEID+0x580, OD object 0x3001
Direction	Transmit

The following table shows the message layout for this message:

Table 51: Table 43 Peer Safety Event Layout

Byte	Signal	Type	Values / Meaning
0	Peer_Event_Counter	uint8	Increments for each peer safety event. Wraps at 255. Use to detect missed transitions.
1	Peer_Index	uint8	Care list slot index, 0-31.
2	Peer_Source_SMCU	uint8	0 = SMCU0 / 1 = SMCU1 / 2 = Both / 255 = Unknown
3	Peer_IO_Index	uint8	IO pair index on the peer.

Byte	Signal	Type	Values / Meaning
4	Peer_Current_State	uint8	0 = Care_List_Empty / 1 = Care_List_Ok / 2 = Care_List_Timeout / 3 = Care_List_Safety
5	Peer_Reserved_0	uint8	Reserved. Transmit zero.
6	Peer_Reserved_1	uint8	Reserved. Transmit zero.
7	Peer_Reserved_2	uint8	Reserved. Transmit zero.

Care List States

The Peer_Current_State field is derived from the SMCU's care list bitfield for the given peer slot. The simplified four-value enum used on CAN maps as follows:

Table 52: Table 44 Peer Current State Care List

Value	Name	Meaning
0	Care_List_Empty	This care list slot has no peer configured.
1	Care_List_Ok	The peer is configured, receiving messages within timeout, and not requesting safety.
2	Care_List_Timeout	The peer is configured but has not received all required messages within the timeout window.
3	Care_List_Safety	The peer is configured and receiving messages within timeout, but is requesting a safety state.

Examples

Peer timeout - care list slot 7 times out on SMCU 0:

Table 53: Table 45 Example of Timed-out Peer

Byte	Value (decimal)	Meaning
0	41	41st peer event sent
1	7	Peer index 7
2	0	SMCU 0
3	0	IO 0
4	2	Care_List_Timeout
5-7	0	Reserved

Peer requesting safety - same peer recovers from timeout but is now in safety:

Table 54: Table 46 Example of Peer Requesting Safety

Byte	Value (decimal)	Meaning
0	42	42nd peer event sent
1	7	Peer index 7
2	0	SMCU 0
3	0	IO 0
4	3	Care_List_Safety
5-7	0	Reserved

If a logger receives event counter 41 and then counter 43, it knows event 42 was missed and can flag that for review.

Local Safety Event

Local_Safety_Event reports local EPC safety state changes with SMCU-level detail.

The following table shows the CAN frame for this message:

Table 55: Table 47 Local Safety Event CAN Frame

Field	Value
J1939 PGN	0xFF04 (65284)
Priority	2
29-bit CAN ID (source 0x00)	0x08FF0400

Field	Value
CANopen TPDO	TPDO6 – COB-ID \$NODEID+0x680, OD object 0x3002
Direction	Transmit

The following table shows the message layout for this message:

Table 56: Table 48 Local Safety Event Layout

Byte	Signal	Type	Values / Meaning
0	Local_Event_Counter	uint8	Increments for each local safety event. Wraps at 255.
1	Local_Event_Type	uint8	Category of local change (see Event Types below).
2	Local_Source_SMCU	uint8	0 = SMCU0 / 1 = SMCU1 / 2 = Both / 255 = Unknown
3	Local_IO_Direction	uint8	0 = Input / 1 = Output / 2 = Both / 255 = Not Applicable
4	Local_IO_Index	uint8	IO pair index (0-2). 255 when not applicable to this event.
5	Local_Current_Safety_Status	uint8	Normalized safety summary bitfield (see below).
6-7	Local_Event_Code	uint16 (little-endian)	Exact SMCU cause value (see below).

Event Types

Table 57: Table 49 Event Types

Value	Name	Meaning
0	IO_State_Changed	The safety state of an IO pair changed.
1	IO_Cause_Changed	The cause of an IO pair's safety state changed without the state itself changing.
2	IO_State_And_Cause_Changed	Both the state and cause changed simultaneously.
3	Safe_State_1_Changed	The processor-level Safe State 1 cause changed (not tied to a specific IO pair).
4	Safe_State_2_Changed	The firmware/config-level Safe State 2 cause changed.
255	Reserved_Unknown	Reserved.

IO Direction

Local_IO_Direction identifies which side of the IO pair triggered the event:

- 0=Input - the event is tied to the input side of the IO pair
- 1=Output - the event is tied to the output side
- 2=Both - the event applies to both sides of the same IO index
- 255=NotApplicable - the event is not tied to a specific IO pair (use for Safe State 1/2 events)

IO Index

Local_IO_Index identifies which of the three SMCU IO pairs is involved (0, 1, or 2). Set to 255 when the event type is Safe_State_1_Changed or Safe_State_2_Changed.

Local Current Safety Summary

Local_Current_Safety_Summary is a normalized bitfield providing a quick summary of the current local safety status. It is intended for simple customer-facing logic without requiring decoding of the raw SMCU cause codes.

Table 58: Table 50 Local Current Safety Summary

Bit	Name	Meaning when set
0	Not_Requested_or_Output_Permitted	Safety is not currently requested, or output is permitted.
1	Fault_Present	A hardware fault is contributing to the safety state.
2	Timeout_Present	A care list timeout is contributing to the safety state.
3	Safety_Request_Present	An input safety request is contributing to the safety state.

Bits 4-7 are reserved and always zero.

Local Event Code

Local_Event_Code is a 16-bit little-endian value whose interpretation depends on

Local_Event_Type:

For IO events (types 0, 1, 2): it is the SMCU's outputSafeCause bitmask for the reported IO pair. Each bit indicates a specific cause:

Table 59: Table 51 Local Event Code

Bit	Name	Meaning
0	INPUT_REQUEST	The input side requested a safety state.
1	INPUT_FAULTY	The input side is detected as faulty.
2	CARE_TIMEOUT	A care list peer has not responded within the timeout window.
3	CARE_LATENCY	A care list peer's response latency exceeded the configured limit.
4	OUT_ON_FB_OFF	Output is commanded on but the feedback signal reads off.

Bit	Name	Meaning
5	OUT_OFF_FB_ON	Output is commanded off but the feedback signal reads on.
6	OSSD_FAILURE	Output circuit (OSSD) hardware failure.
7	PAIR_SMCU	The paired SMCU requested a safety state.
8	CUSTOMER_SUPPLY_VOLTAGE	Customer supply voltage dropped below 8 V.
9-15	Reserved	Reserved, always zero.

For Safe State 1 events (type 3): it is `lastSafeState1Cause`, a processor-level error code from the SMCU firmware.

For Safe State 2 events (type 4): it is `safeState2Cause`, a configuration or firmware error code from the SMCU.

Examples

IO safety request with timeout - input request, care timeout, and care latency on local output pair 2 from SMCU 0:

Table 60: Table 52 Example of IO Safety Request with Timeout

Byte	Value	Meaning
0	17	17th local event
1	2	IO_State_And_Cause_Changed
2	0	SMCU 0
3	1	Output direction
4	1	IO index 1 (output pair 2)
5	0x0C	Timeout_Present + Safety_Request_Present
6-7	0x000D	INPUT_REQUEST (bit 0) + CARE_TIMEOUT (bit 2) + CARE_LATENCY (bit 3)

Safe State 1 event - not tied to a specific IO pair:

Table 61: Table 53 Example of Safe State 1 Event

Byte	Value	Meaning
0	18	18th local event
1	3	Safe_State_1_Changed
2	0	SMCU 0
3	255	Not applicable
4	255	Not applicable
5	0x00	No IO summary for this event type
6-7	0x50A5	Exact Safe State 1 cause from SMCU firmware

Timing and Merge Behavior

epc-can uses a short merge window when deciding whether to combine events from SMCU 0 and SMCU 1 into a single frame with Peer_Source_SMCU = 2 (Both):

- **Peer Safety Event:** 600 ms merge window per IO slot per peer index. If SMCU 0 and SMCU 1 both report the same care list change for the same IO index within that window, one combined frame is emitted instead of two separate frames. Each IO index is tracked independently, so events on different IO slots do not interfere with each other.
- **Local Safety Event:** 200 ms merge window. The shorter window reflects that local state changes tend to be tightly synchronized between the two SMCUs.

If only one SMCU reports a change, or the two SMCUs report at different times outside the merge window, two separate frames are emitted – one with Peer_Source_SMCU=0 and one with Peer_Source_SMCU = 1.

Why the Split Is Useful

Separating peer and local safety into two messages gives integrators flexibility:

- Customers can filter peer and local traffic independently on their CAN tool.
- The peer message stays simple and easy to decode without SMCU internals knowledge.
- The local message can carry richer diagnostic detail for FORT support and analysis.
- Future growth of peer tracking and local diagnostics can happen independently.

Configuring CAN with FORT Manager

This section shows you how to use FORT Manager to enable CAN and set optional CAN parameters.

By default, CAN is disabled for communication between devices.

To Enable CAN and set Optional Parameters

1. Open FORT Manager and click **Configurations**.
2. Add your devices to the configuration (or select an existing configuration of interest).
3. Click **Settings > General** and in **CAN Mode** select *CANopen* or *J1939*.

All CAN parameters come with default values, however, you can change any of the following:

- **CAN Baudrate:** Select a value from the dropdown menu to set an optimal baudrate for your CAN bus.
- **SRCP User Display Text String PGN** and **SRCP Settings PGN** : (*J1939 only*) If you have a crowded CAN bus on your system and are worried about conflicting PGN values for these SRCP messages, you can change either or both of these values here. Select a value from the dropdown list; values are in the Proprietary B range, 0xFF00 - 0xFFFF.

If you change the default PGN value for either of these messages, you must edit the sample DBC file to match the PGN to the new value.

- **Source Addresses:** (*J1939 only*) Specify a comma-separated list of J1939 source addresses that are permitted to send messages to the EPC. To prevent unauthorized communication with the EPC, any addresses not on this list are ignored.

4. Click **Save**.

You can also change the numerical identifier for your EPC devices on the CAN network (which by default is set to 3 for all devices).

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. But you can assign different IDs to each device if you wish. The node ID applies to senders and receivers alike, on both CANopen and J1939.

Note:

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

5. In **Settings**, click the **Devices** tab and select a device from the **Devices** field.
6. In **CAN Node ID** type or select a number for the node ID (For CANopen, 1 - 127, for J1939, 1 - 253). Repeat for the sender as well as the receivers.
7. Repeat for each device to which to assign a new node ID, then click **Done**.

Chapter 9. UART Interface

This chapter documents the Nano Safety Controller Pro's UART serial interface – the message structure and the joystick and keypad message formats – and notes that a configuration can use serial or CAN messaging, but not both.

The Nano Safety Controller Pro provides a UART (Universal Asynchronous Receiver-Transmitter) interface for sending and receiving messages.

Note:

Although an NSC Pro supports both CAN and UART messaging, you cannot implement both in a configuration. When you build a configuration in FORT Manager, you can enable either CAN mode or serial mode (UART) for data transmission (or neither if you aren't planning to provide a data connection).

Serial Message Structure

The following table shows the structure of serial messages.

Table 62: Table 54 Serial Message Structure

Offset	Field	Length (Byte)	Description
0	Header	2	0x1001
2	Type	1	JOYSTICK = 0x50 KEYPAD = 0x51
3	Length	1	Data Length
4	Data	x	Per message type
message_length-2	Checksum	2	

Joystick Message

The following table shows details about the Joystick message.

Table 63: Table 55 Joystick Message

Field	Length	Description
Left X	16 bit	12bit signed ADC value Bit 13 data0K Max = 0x17FF, Center = 0x1000, Min = 0x1800

Field	Length	Description
Left Y	16 bit	See above
Left Z	16 bit	See above
Right X	16 bit	See above
Right Y	16 bit	See above
Right Z	16 bit	See above

Keypad Message

The following table provides details about the Keypad message.

Table 64: Table 56 Keypad Message

Field	Length	Description - Bitmap
Keypad Left	8 bit	[6-7]Down [4-5]Right [2-3]Up [0-1]Left
Keypad Center	8 bit	[6-7] [4-5]Menu [2-3]Power [0-1]Pause
Keypad Right	8 bit	[6-7]"1" [4-5]"2" [2-3]"3" [0-1]"4"

The button values for the keypad message are:

```
[0]Notset
[1]Set
[2]Error
[3]Unavailable
```

EPC Technical Specifications

This appendix provides the Endpoint Controller's hardware details: a mechanical drawing, the I/O connector pinout, electrical ratings, safety input and output specifications, and the radio, Wi-Fi, and Ethernet specifications for each EPC model.

EPC Mechanical Drawing

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

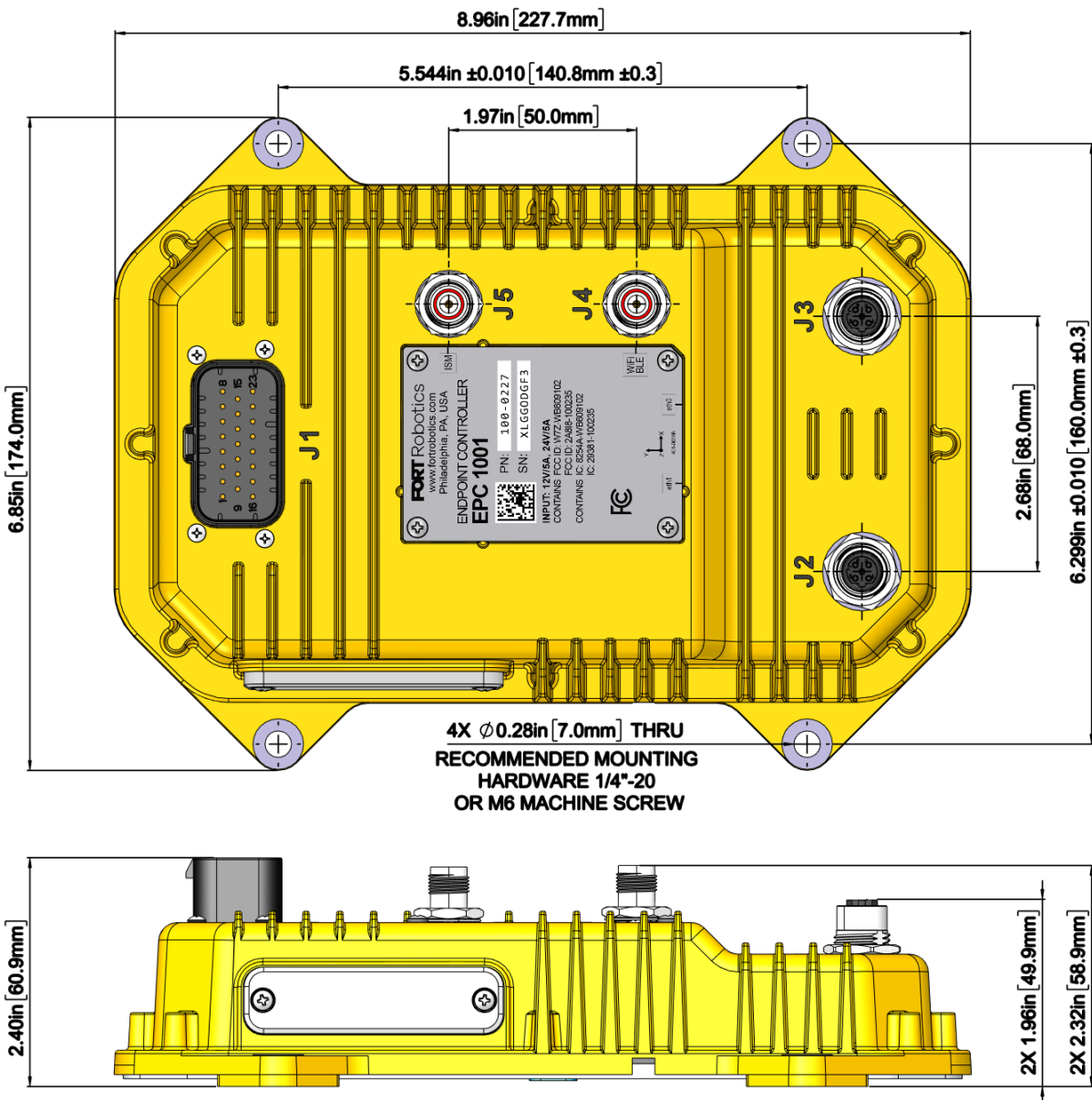


Figure 36: Fig. 33 EPC-1001 Mechanical Drawing

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

Table 65: Table 57 Suggested EPC Connector Types

Connector #	Suggested Mating Connector Type for EPC
J1	TE 770680-1.
J2	Ethernet M12 – D Type for management port connection. Connect to a port on a Linux or Windows machine to update firmware or load a configuration to the EPC.
J3	Ethernet M12 – D Type for connection to safety network.
J4	RP-TNC Plug (male) with center socket (female) quick disconnect antenna port for 2.4 GHz BLE & Wi-Fi antenna.
J5	RP-TNC Plug (male) with center socket (female) quick disconnect antenna port for 8xx and 9xx ISM antenna.

Note:

Connectors are designed to be hand tightened only. Use of a wrench or other tool will cause damage to the connector or cabling. The EPC has no user-serviceable parts. Do **not** attempt to open the device nor make any changes or repairs. If you have maintenance or repair questions email support@fortrobotics.com.

EPC I/O Connector Pinout and Cable

The following figure shows a diagram of the EPC's 23 pin I/O connector (the J1 connector on the Endpoint Controller).

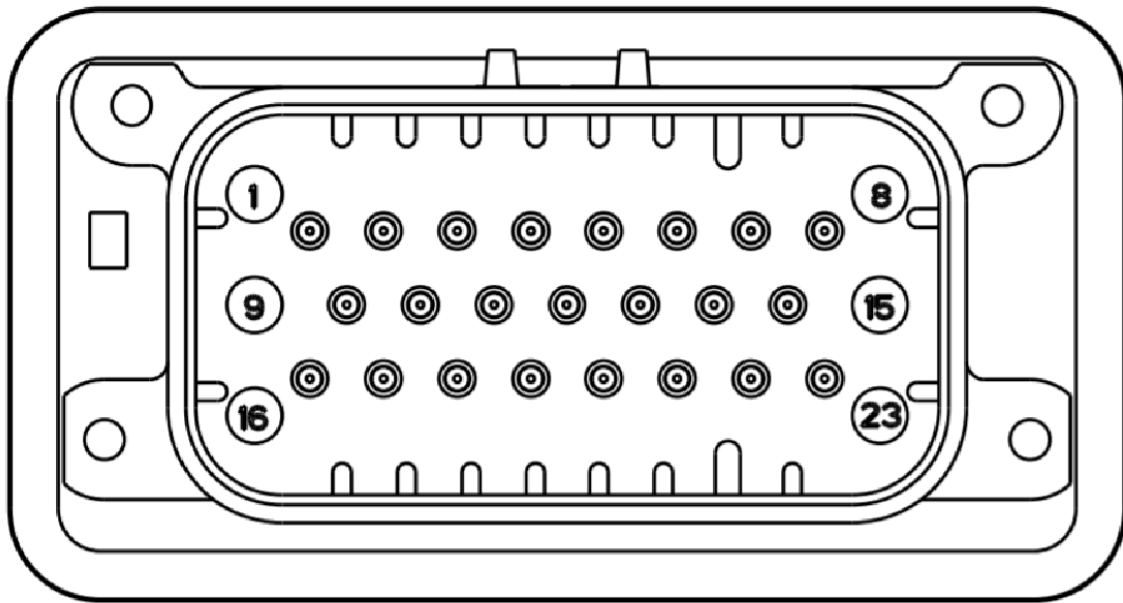


Figure 37: Fig. 34 EPC I/O Connector Pinout (TE 1-776228-1)

Note:

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

The following table describes each of the connector signals. Refer to the diagram and table when wiring devices to an Endpoint Controller sender ([Wiring EPC Sender](#) (on page 10)) or receiver ([Wiring EPC Receivers](#) (on page 10)).

Table 66: Table 58 EPC Connector pinout and signal descriptions

Pin #	Name	Description	Wire Color FORT integration
1	IN5_CONN	Channel 1, Input 3	White
2	IN4_CONN	Channel 1, Input 2	White
3	IN3_CONN	Channel 1, Input 1	White
4	IN2_CONN	Channel 0, Input 3	White
5	IN1_CONN	Channel 0, Input 2	White
6	IN0_CONN	Channel 0, Input 1	White

Pin #	Name	Description	Wire Color FORT integration
7	PVin_RTN	Voltage Negative Polarity	White
8	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 an EPC (on page 10) 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 CAN Interface (on page 10) if you require shielding for CAN.	
14	PVin_IN	Voltage Positive Polarity	White
15	PVin_IN	Voltage Positive Polarity	White
16	OUT5_CONN	Channel 1, Output 3	White
17	OUT4_CONN	Channel 1, Output 2	White
18	OUT3_CONN	Channel 1, Output 1	White
19	Reserved	Do not connect	
20	Reserved	Do not connect	
21	OUT2_CONN	Channel 0, Output 3	White

Pin #	Name	Description	Wire Color FORT integration
22	OUT1_CONN	Channel 0, Output 2	White
23	OUT0_CONN	Channel 0, Output 1	White

Note:

The outputs in the table above are dual channel pairs – each output uses one pin from Channel 0 and one from Channel 1:

- **Output 1** – pins 23 (Channel 0) and 18 (Channel 1)
- **Output 2** – pins 22 (Channel 0) and 17 (Channel 1)
- **Output 3** – pins 21 (Channel 0) and 16 (Channel 1)

In a configuration with an **Output to Control** setting, that setting determines which pair carries the safety signal. For more information, see [Choosing Which Output the Senders Control](#) (on page 62).

Important:

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

Recommended and Absolute Maximum Ratings (EPC)

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

Table 67: Table 59 EPC Recommended and Absolute Maximum

Specification	Minimum	Typical	Maximum
PVin (12V operation)	9.6	12	14.4
PVin (24V operation)	19.2	24	28.8
PVin (V)	8		32
Input Voltage	0 V		Vin+0.7 V
Current (not including output loads)	87 mA @32V		273 mA @8 V
Weight		878 g 1.9lb	
Ingress Protection		IP65	

Specification	Minimum	Typical	Maximum
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
Connectors		M12 Ethernet connectors (2); 23-pin main integration connector; RP-TNC antenna connectors (1 for BLE models, 2 for ISM models)	
Certification		SIL 3 Certified per IEC 61508	

Safety Input Specifications

The following table provides specifications for the safety inputs:

Table 68: Table 60 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	8VDC	12VDC (or 24VDC)	32VDC
Input state for logic OFF/LOW	0VDC	0 ~ 1VDC	Less Than 8VDC

Specification	Minimum	Typical	Maximum
Input Impedance		TBD	

Safety Output Specifications EPC

The following table provides specifications for the safety outputs:

Table 69: Table 61 Safety Output Specifications EPC

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

Wireless Radio Specifications (EPC)

You can purchase an Endpoint Controller with any of several different radios based on frequency requirements and local regulations. Prior to ordering and deployment, consult local regulations to ensure that you are obtaining an EPC with the proper radio.

North America ISM Radio (EPC)

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

Table 70: Table 62 (EPC) North America ISM Radio Specifications

Specification	Minimum	Typical	Maximum
Frequency	902 MHz		928 MHz
Bandwidth		600 kHz	
Channels		21	21
Receive Sensitivity		-100 dBm	
Modulation		2-GFSK	
Baud Rate		500 kbps	
Power (conducted RF output)	-10 dBm		23 dBm
EPC Part #	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 71: Table 63 European ISM Radio Specifications

Specification	Minimum	Typical	Maximum
Frequency	869.4 MHz		869.653 MHz
Bandwidth		250 kHz	
Channels		1	
Receive Sensitivity		-100 dBm	
Modulation		2-GFSK	
Baud Rate		200 kbps	
Power (conducted RF output)	-10 dBm		23 dBm
EPC Part #	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 72: Table 64 BLE Radio Specifications

Specification	Minimum	Typical	Maximum
BLE Version		5.1	
Baud Rate		1 Mbps	
Power (conducted RF output)			4 dBm
Receive Sensitivity	-99 dBm		
EPC Part #		EPC-1000, EPC-1001, EPC 1002	

The following table provides specifications for the Long-Range Bluetooth (LRBLE) radio, which is carried by the EPC1003 model only:

Table 73: Table 65 LRBLE Radio Specifications (EPC)

Specification	Description
BLE Long Range Version	5.0
Tx Power (conducted RF output)	17 dBm
Receive Sensitivity	-105 dBm
Range	100-300 m
EPC Part #	EPC 1003

Wi-Fi Specifications

The EPC supports 2.4 GHz and 5 GHz Wi-Fi (access point is not included). The following table provides specifications:

Table 74: Table 66 Wi-Fi Specifications (EPC)

Specification	Description
Max Power	20 dBm
Range	~50 m (customer coverage dependent)

Ethernet Specifications

The following table provides Ethernet specifications:

Table 75: Table 67 Ethernet Specifications

Specifications	Minimum	Typical	Maximum
Speed		10/100 Mbps	

Data Interfaces

The Endpoint Controller's integration interface is USB or CAN (Controller Area Network). "CANopen Implementation" on page 6-1 describes CAN communication specifications (data rates and protocol). Use the Endpoint Controller's dual safety outputs to prevent any motion of the equipment under control (EUC) when the Endpoint Controller receives an emergency stop from either the connected remote device or its wired emergency stop input. The emergency stop inputs are relative to P_{Vin}. Maintain a single ground reference for all power and reference voltages.

The following table provides specifications for the CAN interface.

Table 76: Table 68 CAN Bus Specifications

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

NSC Pro Technical Specifications

This appendix provides the Nano Safety Controller Pro's hardware details: mechanical drawings, the 80-pin connector pinout, electrical ratings, safety output and radio specifications, and the LED codes that report the board's status.

This appendix provides details of the Nano Safety Controller Pro hardware.

NSC Mechanical Overview

The following figures show top (primary side) and bottom (secondary) views of the NSC Pro:

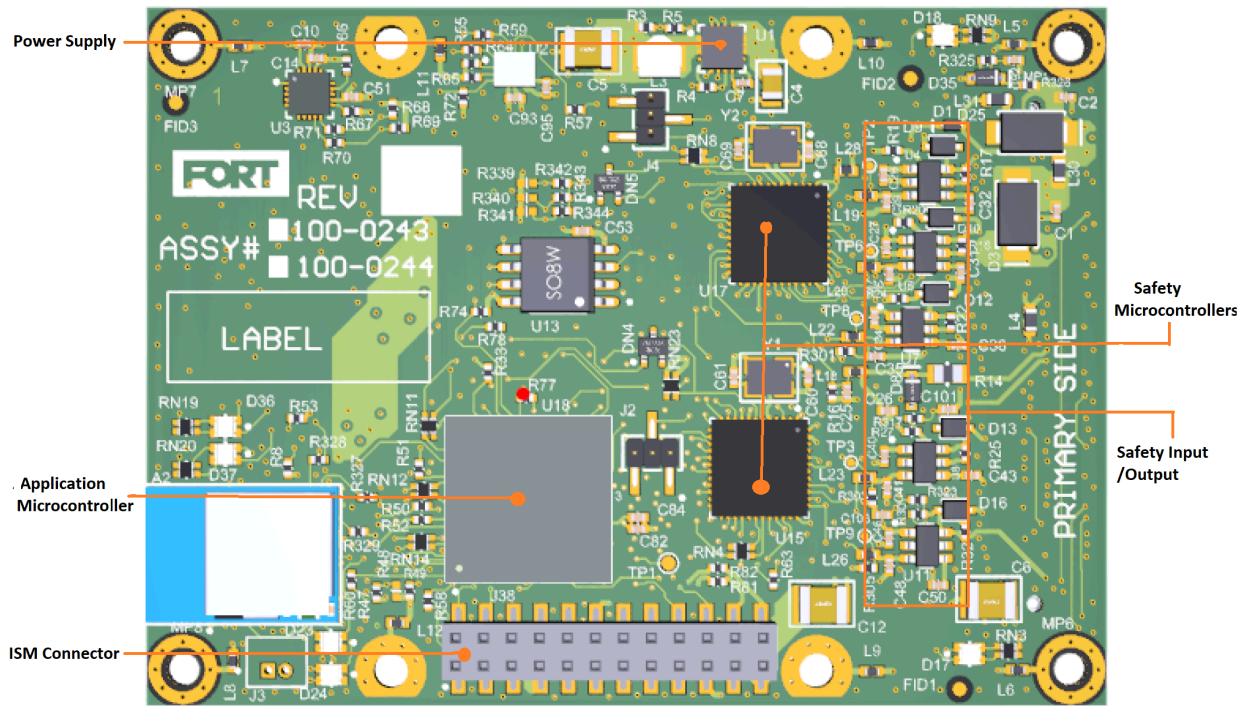


Figure 38: Fig. 35 NSC Pro Top (Primary) Side

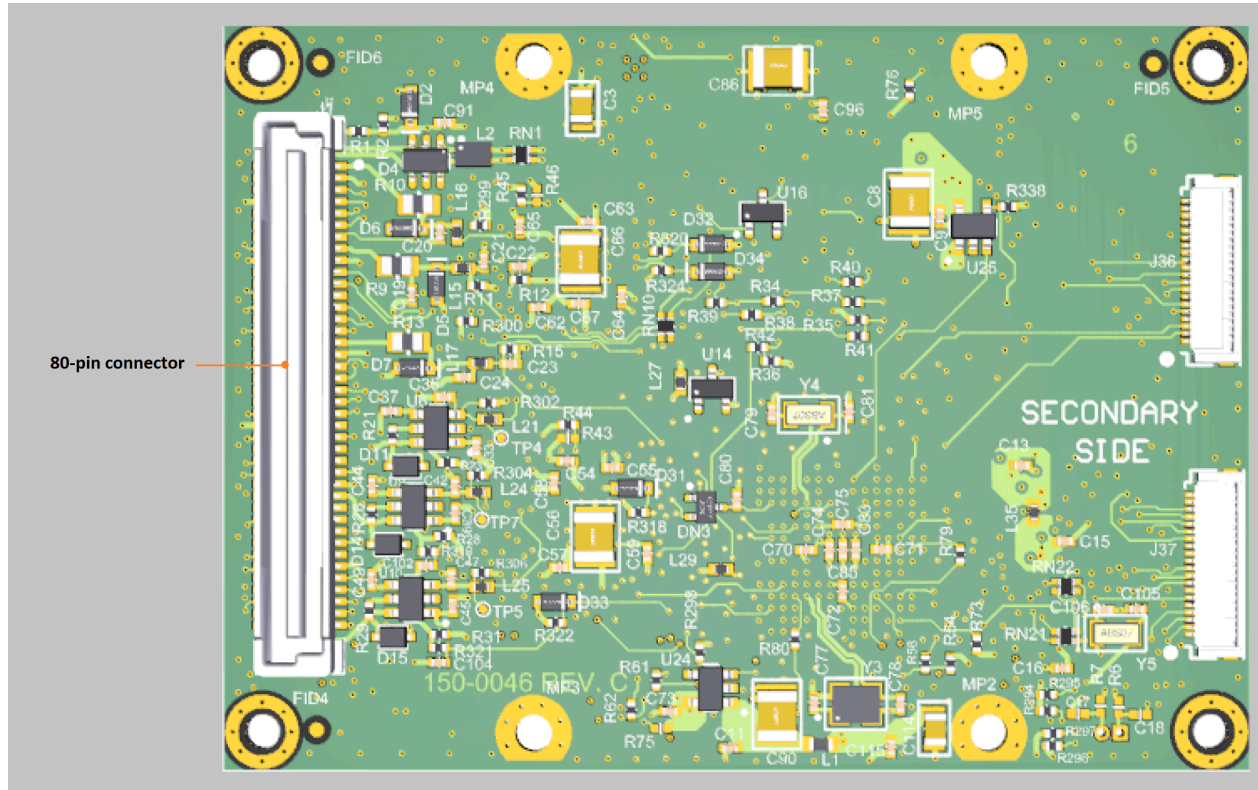


Figure 39: Fig. 36 NSC Pro Bottom (Secondary) Side

When embedding the Nano Safety Controller Pro in your equipment, keep in mind the following clearances:

- Primary side of board clearance 4 mm.
- Secondary side of board clearance > 5 mm
- Secondary side of board standoff = 9 mm
- Secondary side of board connector TE 5177986-3 (80-pin connector) – engages with TE 5-5179180-3 connector

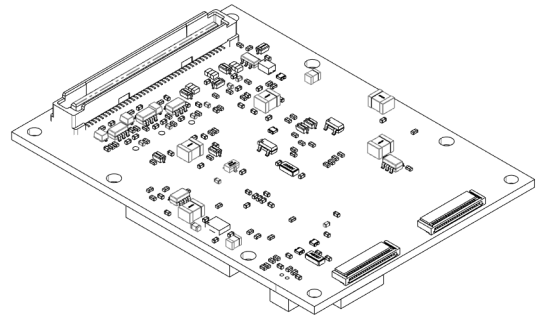
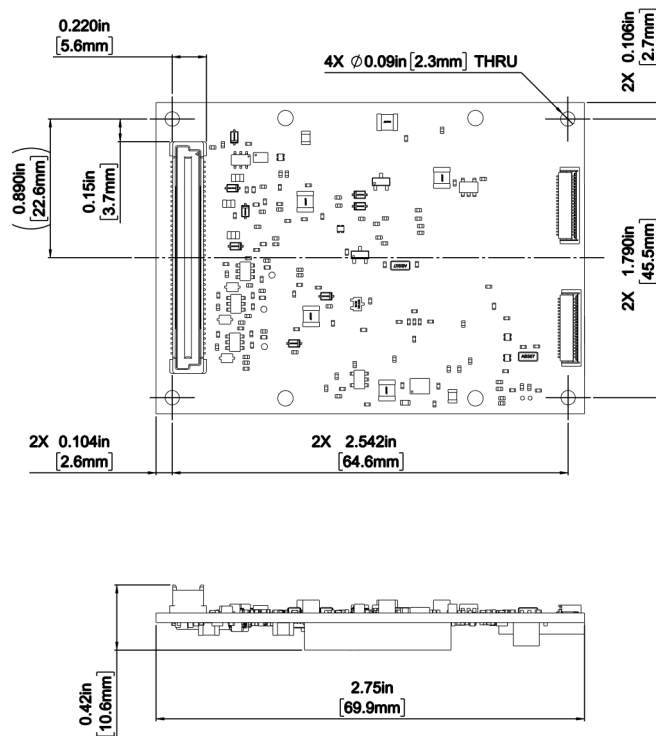
See [NSC PRO 80-Pin I/O Connector Pinout](#) (on page 156) for a description of the connector pins.

Note:

The two connectors on the right of the secondary side of the board, J36 and J37, are for FORT internal use only.

Mechanical Drawings NSC Pro and ISM Radio

The following figure shows a mechanical drawing of the Nano Safety Controller Pro (without the radio):



NANO SAFETY CONTROLLER PRO (NSCP) INTERFACE DIMENSIONS

ALL TOLERANCES ARE ± 0.005 [0.13mm]

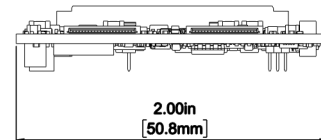
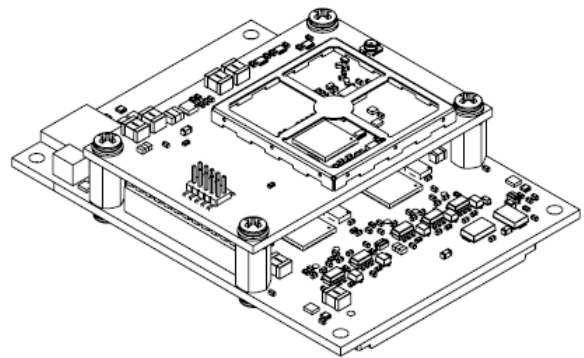
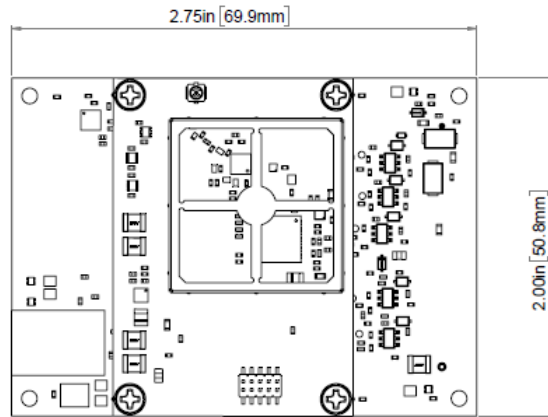


Figure 40: Fig. 37 NSC Pro Mechanical Drawing

The following figure shows a mechanical drawing of the NSC Pro with the ISM radio:



NSC Pro WITH ISM RADIO

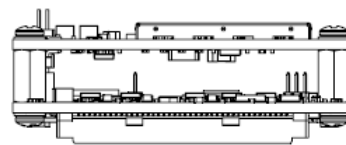
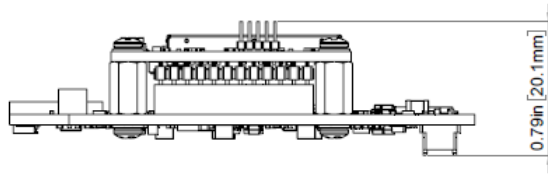


Figure 41: Fig. 38 NSC Pro with ISM Radio Mechanical Drawing

The following figure shows a mechanical drawing of the ISM radio for the NSC Pro:

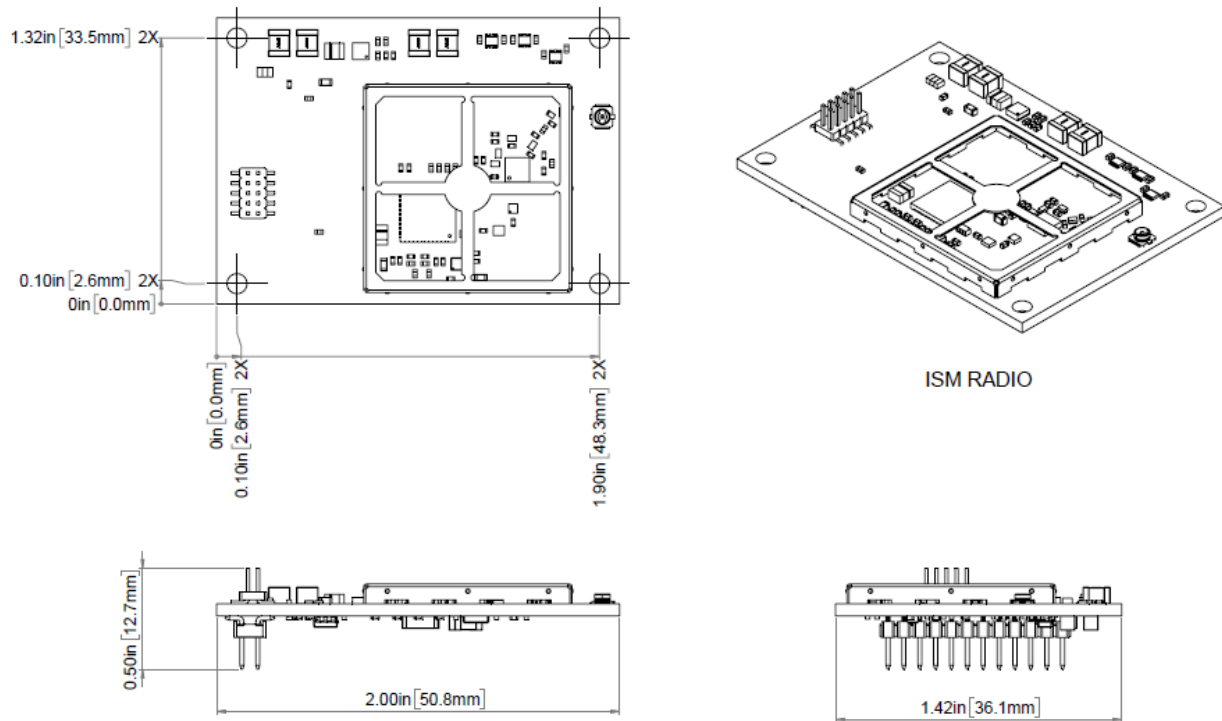


Figure 42: Fig. 39 ISM Radio Mechanical Drawing

NSC PRO 80-Pin I/O Connector Pinout

The following table describes each of the Nano Safety Controller Pro's connector signals. Refer to the table when embedding an NSC Pro receiver in the equipment to control.

Table 77: Table 69 NSC Pro Connector Pinout and Signal Descriptions

Pin #	Signal Name	Direction	Description
2 ¹²	USB_DN	I/O	USB differential pair negative

¹² You can use a USB connector (with pins 2 and 4) to configure and perform firmware updates to the NSC Pro. The NSC Pro, however, will not detect a USB connection unless USB Power is provided to the NSC Pro, that is, you've connected a device (through pin 6) that provides USB power. Note that the NSC Pro will still be powered by the supply with the higher voltage if the Main Power supply is also connected.

Pin #	Signal Name	Direction	Description
4 ¹³	USB_DP		USB differential pair positive
5	LED0_OUT	O	Power status GPO (general purpose output) that indicates whether the NSC is powered on.
6	PVIN_USB	I	USB Power input.
7	LED1_OUT	O	Connection status GPO that indicates whether the NSC Pro is connected to the sender over a radio interface (e.g. ISM). Note that this LED does not go high in an EPC to NSC Pro configuration.
8	GND	GND	Ground
9	LED2_OUT	O	Operational status GPO that indicates whether the NSC is fully operational (the firmware and configurations have loaded).
10	PVIN	I	Main power input
12	PVIN	I	Main power input

¹³ You can use a USB connector (with pins 2 and 4) to configure and perform firmware updates to the NSC Pro. The NSC Pro, however, will not detect a USB connection unless USB Power is provided to the NSC Pro, that is, you've connected a device (through pin 6) that provides USB power. Note that the NSC Pro will still be powered by the supply with the higher voltage if the Main Power supply is also connected.

Pin #	Signal Name	Direction	Description
18	P3V3_OUT	O	3.3 V output (max current 50mA) from the onboard power supply that you can use to run something small like an LED.
23	GND	GND	Ground
24	AP_CAN0_TX	O	AP CAN0 transmit
26	AP_CAN0_RX	I	AP CAN0 receive
46	GND	GND	Ground
48 ¹⁴	PVBAT	I	Customer supplied backup battery input (3-3.3 V DC); for example to keep a clock running when the NSC Pro is powered off. If you aren't using a battery tie this pin (PVBAT) to Pin 18 P3V3_OUT.
50 ¹⁵	FC0_TX	O	UART0 or IP to UART bridge Transmit
54	FC0_RX	I	UART0 or IP to UART bridge Receive
55	OUT1_CH0	O	Safety Output 1 Channel 0
57	OUT1_CH1	O	Safety Output 1 Channel 1

¹⁴ A battery backup is required to guarantee that you get accurate time stamps from NSC Pro logs.

¹⁵ You can use Pins 50 & 54 or 58 & 62 to connect to the Linux computer running the FORT SDK (UART to IP bridge) or to connect to a USB port on the EUC.

Pin #	Signal Name	Direction	Description
58 ¹⁶	FC9_TX	O	UART1 or IP to UART bridge transmit
62	FC9_RX	I	UART1 or IP to UART bridge receive
69	GND	GND	Ground
78	OUT2_CH0	O	Safety Output 2 Channel 0
79	EXPBOARD_DET	I	Tie to GND
80	OUT2_CH1	O	Safety Output 2 Channel 1

Connect a cable-mounted TE 5-5179180-3 (80-pin connector) receptacle to the board-mounted TE 5177986-3 plug on the secondary side of the board.

Specifications

The following table shows details about the Nano Safety Controller Pro.

Table 78: Table 70 NSC Specifications

Specification	Description
Device Form Factor	embedded receiver
Dimensions	50.8 mm x 69.9 mm x 10.4 mm (2.0" x 2.75" x 0.5")
Base Unit Weight	17 g (29 g with ISM radio)
Operating & Storage Temperature	-40°C to +85°C
Operating Voltage	4.5 to 13V DC input
Output Radio Transmission Power (conducted RF output)	ISM: -10 dBm to 27 dBm
Wired Interface	Serial (UART), CAN
CAN Supported Protocols	J1939 protocol
Connectors	Embedded board with 80-pin integration, IPEX antenna;

¹⁶ You can use Pins 50 & 54 or 58 & 62 to connect to the Linux computer running the FORT SDK (UART to IP bridge) or to connect to a USB port on the EUC.

Specification	Description
Input Voltage	12V nominal; 4.5 to 13V full range
Power Draw	0.1 - 0.3 W
Safety Outputs	2 dual channels
Safety Output Type	digital
Pairing	One EPC or one SRC Pro: (up to) 30 NSC Pros
Regulatory	FCC, IC, CE compliant (US)(CA)(EU)
Certification	E-Stop SIL3 rated per IEC 61508
Extended Warranty	Coming soon, talk to your sales rep

Recommended and Absolute Maximum Ratings

The following table shows the recommended and absolute maximum ratings for the Nano Safety Controller Pro.

Recommended Operating Conditions

The following table shows the recommended operating conditions for the Nano Safety Controller Pro.

Table 79: Table 71 Operating Conditions – Recommended and Absolute Maximum Ratings

Parameter	Minimum	Typical	Maximum
PVin (V)	4.5 V		13 V
PVin_USB	4.5 V	5 V	5.5 V
NSCP Current (not including output loads)	80 mA (serial comms)		650 mA (ISM max power)
Absolute Maximum Current at PVIN pins. Total input current is NSC Pro current plus output driving current.			1 A
Output Voltage	0		PVin
Output Driving Current (per channel)			230 mA

Parameter	Minimum	Typical	Maximum
Operational & Storage Temperature	-40 °C		85 °C

Safety Output Specifications

The following table provides specifications for the safety outputs:

Table 80: Table 72 Safety Output Specifications

Specification	Minimum	Typical	Maximum
PVin	4.5 V		13 V
Safety Outputs		Two dual channel outputs	
Output Type		Current Sourcing	
Current (per output channel)			230 mA
Output ON State	PVin (4.5 V)	PVin	PVin (13 V)
Output safe state	0 V	0 V	0 V
OSSD Pulse Width		300 µS	
OSSD Pulse Period		200 mS	

Wireless Radio Specifications

You can purchase a Nano Safety Controller Pro with any of several different radios based on frequency requirements and local regulations. Prior to ordering and deployment, consult local regulations to ensure that you are obtaining a device with the proper radio.

North America ISM Radio (NSC Pro)

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

Table 81: Table 73 (EPC) North America ISM Radio Specifications

Specification	Minimum	Typical	Maximum
Frequency	902 MHz		928 MHz
Bandwidth		600 kHz	
Channels		21	21

Specification	Minimum	Typical	Maximum
Receive Sensitivity		-100 dBm	
Modulation		2-GFSK	
Baud Rate		500 kbps	
Power (conducted RF output)	-10 dBm		27 dBm
NSC Pro Part number	North America ISM radio is available with NSC Pro model 1001		

European ISM Radio (NSC Pro)

The following table provides specifications for the European ISM radio:

Table 82: Table 74 European ISM Radio Specifications

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

Long-Range Bluetooth (LRBLE) Radio (NSC Pro)

The following table provides specifications for the Long-Range Bluetooth (LRBLE) radio, which is carried by the NSC Pro 1003 only:

Table 83: LRBLE Radio Specifications (NSC Pro)

Specification	Description
BLE Long Range Version	Version number
Tx Power (conducted RF output)	Conducted RF output, in dBm
Receive Sensitivity	Receive sensitivity, in dBm
Range	Usable range, in meters
NSC Pro Part Number	NSC Pro 1003

Data Interfaces (NSC Pro)

The NSC Pro's integration interface is CAN (Controller Area Network) or UART (Universal Asynchronous Receiver-Transmitter).

Important:

The NSC Pro does not have a built-in CAN transceiver so if you use CAN, you must purchase and install your own.

Note that the NSC Pro supports the J1939 protocol only. [J1939 Implementation](#) (on page 103) 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 P_{Vin}. Maintain a single ground reference for all power and reference voltages.

The following table provides specifications for the CAN interface:

Table 84: Table 75 CAN Bus Specifications

Specification	Minimum	Typical	Maximum
CAN TX High Level Output Voltage	3 V	3.3 V	
CAN TX Low Level Output Voltage	0 V	0.1 V	
CAN RX Positive Going Input Threshold		1.5 V	2.4 V
CAN RX Negative Going Input Threshold	0.6 V	1.2 V	

The following table provides specifications for the UART interface:

Table 85: Table 76 UART Specifications

Specification	Minimum	Typical	Maximum
CAN TX High Level Output Voltage	3 V	3.3 V	
CAN TX Low Level Output Voltage	0 V	0.1 V	
CAN RX Positive Going Input Threshold		1.5 V	2.4 V
CAN RX Negative Going Input Threshold	0.6 V	1.2 V	
UART RX Input Resistance	3 k Ω	5 k Ω	8 k Ω
UART Baud Rate		115200	

LED Diodes

The Nano Safety Controller Pro has four LED lights on the primary side of the board (as shown in the following figure) that are useful for testing (D36 and D37 for the application processor and D17 and D18 for the safety processor):

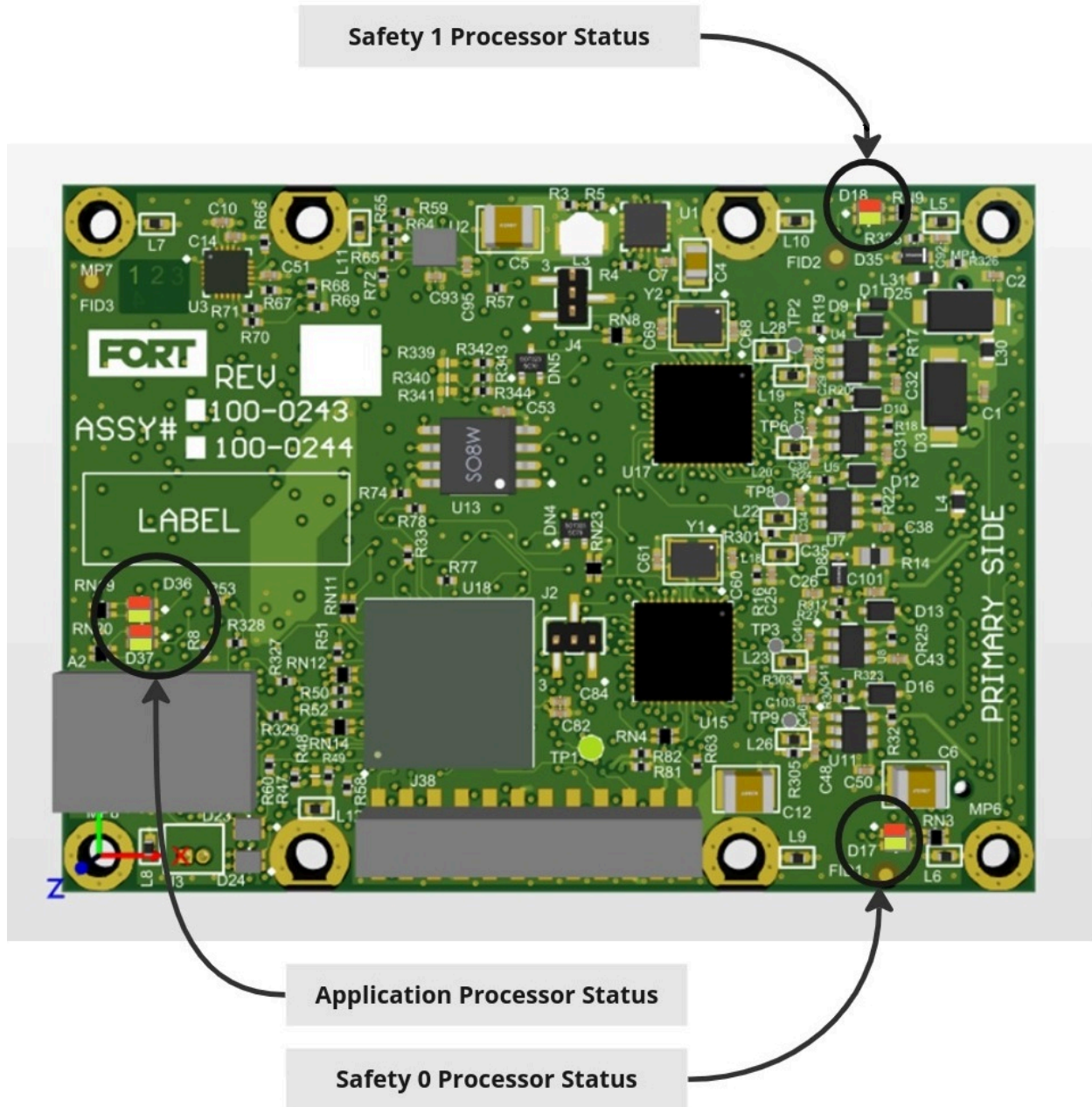


Figure 43: Fig. 40 NSC Pro LEDs

Application Processor Status During Secure Boot

When power is applied to the NSC Pro, the secure bootloader begins the boot process. The following table lists LED indicators controlled by the application processor bootloader during secure boot.

Table 86: Table 77 Application Processor Status during Secure boot

LED	Source	Indicates
D36 Red	Secure bootloader	On (red) when bootloader is executing.
D36 Green	Secure bootloader	On (green) when bootloader is launching application firmware.
D37 Red	Secure bootloader	On (red) during firmware update, and a flash sector erase is in progress.
D37 Green	Secure bootloader	On (green) during firmware update, and a flash sector write is in progress.

Application Processor Status During Normal Operation

When the application processor firmware is starting, all LED indicators are cleared. The following table lists LED indicators controlled by the application processor firmware during normal operation.

Table 87: Table 78 Application Processor Status Normal Operation

LED	Source	Indicates
D36 Red	Application firmware	Undefined (disable) in this context.
D36 Green	Application firmware	Undefined (disable) in this context.
D37 Red	Application firmware	Undefined (disable) in this context.
D37 Green	Application firmware	Blinks (green) at 2Hz when application processor is in normal operation.

Safety Processor Status During Normal Operation

The following table lists LED indicators controlled by the safety processor firmware during normal operation.

Table 88: Table 79 Safety Processor Status Normal Operation

LED	Source	Indicates
D17 Red	Application firmware	On (red) when safety outputs are asserted.
D17 Green	Application firmware	Blinks (green) at 1Hz when Safety Processor 0 is in run state.
D18 Red	Application firmware	On (red) when safety outputs are asserted.
D18 Green	Application firmware	Blinks (green) at 1Hz when Safety Processor 1 is in run state.

Note:

Don't confuse these LEDs on the board with the three GPO connectors (Pins 5, 7, and 9 on the 80 pin connector) that you can wire to external LEDs to provide status information (see [NSC PRO 80-Pin I/O Connector Pinout](#) (on page 156)). The LEDs are on the board and hence hidden after you embed the NSC Pro in your equipment, which makes them useful only for testing.

ISM Radio LEDs

The ISM radio board has three LEDs that are useful for testing.

Table 89: Table 80 ISM Radio Board LEDs

LED	Schematic	Indicates
D3 Green	LED_TX	Indicates TX (transmission) activity.
D3 Red	LED_TX	Indicates TX Error.
D4 Green	LED_RX	Indicates RX (reception) activity.
D4 Red	LED_RX	Indicates RX error (remains lit until error is cleared).
D5 Green	LED_STAT	Status heartbeat
D5 Red	LED_STAT	Status Error (remains lit until error is cleared).

SRC Pro Technical Specifications

This appendix provides the Safe Remote Control Pro's hardware details — mechanical drawing, electrical and battery ratings, and radio specifications — and lists which SRC Pro models FORT Manager still supports.

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 1001.

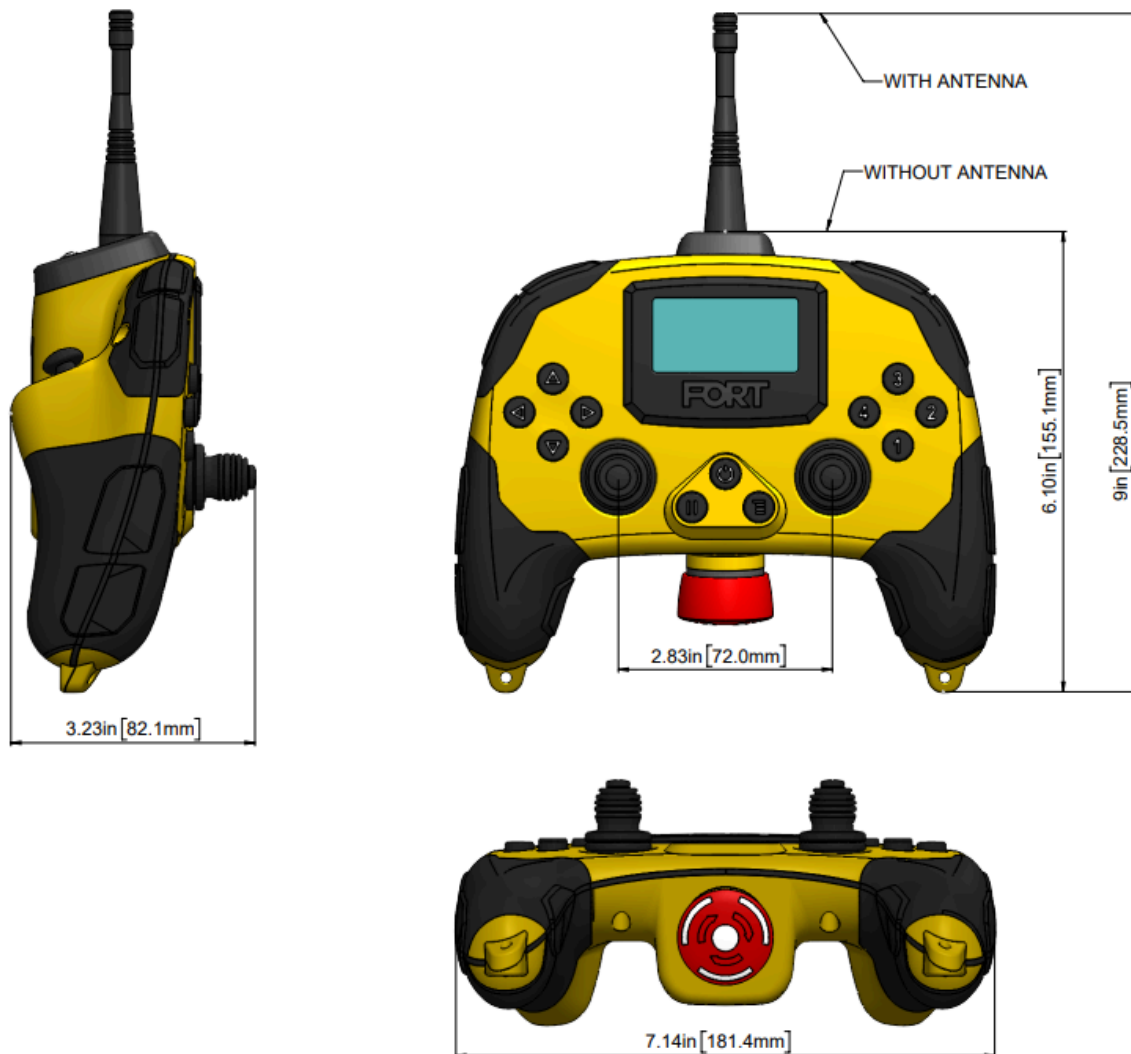


Figure 44: Fig. 41 SRC Pro Mechanical Drawing

Recommended and Absolute Maximum Ratings (SRC Pro)

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

Table 90: Table 81 SRC Pro Absolute and Recommended Specifications

Specification	Min	Typical	Max
Vin (V)		5 VDC (USB)	
Current		1.6 A	
Weight		726 g 1.6 lb	
Dimensions		181 mm x 155 mm x 83 mm 7.14" x 6.10" x 3.23"	
Ingress Protection		IP65	
E-Stop Button Impact Resistance Rating		IK07	
Operating and Storage Temperature (internally limited)	-20 °C		60 °C
Charging Temperature (internally limited)	0 °C		45 °C
Battery Type		Lithium Polymer	
Battery Size		4000 mAh	
Charge Time		4.5 hours	
Connectors		Mini-USB for models 1001 & 1002 USB-C for 1003	
Run Time (Bluetooth)	19 hours		22 hours
Run Time (ISM)	18 hours		21 hours
Certification		SIL 3 Certified per IEC 61508	

You can purchase an SRC Pro with any of several different radios based on frequency requirements and local regulations. Prior to ordering and deployment, consult local regulations to ensure that you are obtaining an SRC Pro with the proper radio.

North America ISM Radio (SRC Pro)

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

Table 91: Table 82 SRC Pro North America ISM Radio Specifications

Specification	Minimum	Typical	Maximum
Frequency	902 MHz		928 MHz
Bandwidth		600 kHz	
Channels		21	21
Receive Sensitivity		-100 dBm	
Modulation		2-GFSK	
Baud Rate		500 kbps	
Power (conducted RF output)	-10 dBm		23 dBm
SRC Pro Part number	SRC Pro 1001		

European ISM Radio (SRC Pro)

The following table provides specifications for the European ISM radio:

Table 92: Table 83 European ISM Radio Specifications

Specification	Minimum	Typical	Maximum
Frequency	869.4 MHz		869.653 MHz
Bandwidth		250 kHz	
Channels		1	1
Receive Sensitivity		-100 dBm	
Modulation		2-GFSK	
Baud Rate		200 kbps	
Power (conducted RF output)	-10 dBm		23 dBm
SRC Pro Part number	SRC Pro 1002		

Bluetooth Low Energy (BLE) Radio (SRC Pro)

The following table provides specifications for the BLE radio:

Table 93: Table 84 BLE Radio Specifications

Specification	Minimum	Typical	Maximum
BLE Version		5.1	
Baud Rate		1 Mbps	
Power (conducted RF output)			4 dBm
Receive Sensitivity	-99d dBm		
Part #		SRC Pro 1001, SRC Pro 1002	

The following table provides specifications for the Long-Range Bluetooth (LRBLE) radio, which is carried by the SRC Pro 1003 only:

Table 94: Table 85 LRBLE Radio Specifications (SRC Pro)

Specification	Description
BLE Long Range Version	5.0
Tx Power (conducted RF output)	+20 dBm
Receive Sensitivity	-105 dBm
Range	100-300 m
Part #	SRC Pro 1003

SRC Pro Models and Support Status

The following table lists the SRC Pro models and how each is supported in FORT Manager.

Table 95: SRC Pro Model Support Status

Model	Radio	Connector	Status in FORT Manager
SRC Pro 1000	The radio the 1000 carries.	The connector	End of support, September 30, 2026
SRC Pro 1001	North America ISM, and BLE	Mini-USB	Supported
SRC Pro 1002	European ISM, and BLE	Mini-USB	Supported

Model	Radio	Connector	Status in FORT Manager
SRC Pro 1003	Long-Range Bluetooth (LRBLE)	USB-C	Supported

End of Support for the SRC Pro 1000

FORT Robotics will discontinue the SRC Pro 1000 on September 30, 2026. Starting on September 30, 2026, FORT Manager will no longer support that model. Specifically, from that date you cannot:

- Register an SRC Pro 1000, including a replacement unit.
- Obtain a firmware update for an SRC Pro 1000.
- Create a new configuration that contains an SRC Pro 1000, or change an existing one.
- An end-of-support model also does not receive features added after its support ended. Device logging is one example: it arrives with a firmware update, and FORT publishes no further firmware for the SRC Pro 1000. For more information on what logging provides on supported models, see [Using Logs](#) (on page 206).

Important:

An SRC Pro 1000 that is already deployed keeps the configuration and the firmware it is running. It does not stop working on September 30, 2026, and its safety function is unchanged. What ends is the ability to change it from FORT Manager.

After the end of support date on September 30, 2026, the following will still continue:

- Covered repairs under the terms of the product warranty.

If you need continued configuration support or additional functionality, transition to the SRC Pro 1003, which adds Long-Range Bluetooth capability. For more information, see [Device Models and Communication Methods](#) (on page 51)

Note:

For the full notice, see [Placeholder for the SRCP1000 obsolescence bulletin](#)

WES Pro Technical Specifications

This appendix provides the Wireless E-Stop Pro's hardware details: a mechanical overview, weight and ingress ratings, battery and charging figures, operating and storage temperatures, and its Long-Range Bluetooth radio specifications.

This appendix provides details of the Wireless E-Stop Pro (WES Pro) hardware.

Mechanical Overview

The following figure shows front and bottom views of the WES Pro:



Figure 45: Fig. 42 WES Pro Front and Bottom

The following table shows details about the WES Pro.

Table 96: Table 86 WES Pro Specifications

Specification	Description
Device Form Factor	Wireless handheld sender
Dimensions	57 mm x 61 mm x 223 mm (2.24" x 2.38" x 8.78")
Weight	360 g (0.8 lb)
Operating Temperature	-20°C to +60°C (internally limited)
Storage Temperature	Up to one month: -20 °C to 50 °C One to three months: -10 °C to 45 °C Longer than three months: -10 °C to 35 °C
Charging Temperature (internally limited)	0 °C-45 °C
Operating Voltage	4.5 to 13V DC input
Vin (V)	5 VDC (USB) @1.6 A
Ingress Protection WES Pro	IP65
Ingress Protection Docking Station	IP30
Output Radio Transmission Power (conducted RF output)	ISM: -10 dBm to 27 dBm
Battery Type & Size	Lithium, 1.5 A
Charge Time	4 hours or less
Run Time	12 hours or more
Connectors	USB-C powered charging dock
Power Draw	100 mW
Safety Outputs	One dual channel digital output
Pairing	1 WES Pro to 1 EPC ¹⁷ or 1 WES Pro + 1 SRC Pro to 1 EPC
Regulatory	Pending FCC, IC, CE compliant (US)(CA)(EU)
Certification	E-Stop SIL 3 rated per IEC 61508

¹⁷ Be sure to check the the [Release notes](#) for information about the type and number of devices you can pair with a WES Pro that is specific to the version of the product you are using.

You can purchase a WES Pro with a long range Bluetooth radio.¹⁸

Long-Range Bluetooth Low Energy (LRBLE) Radio (WES Pro)

The following table provides specifications for the WES Pro BLE radio:

Table 97: Table 87 BLE Radio Specifications (WES Pro)

Specification	Description
BLE Long Range Version	5.0
Tx Power (conducted RF output)	+20 dBm
Receive Sensitivity	-105 dBm
Range	100-300 m
Part #	WES Pro 1003

Important:

We declare that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. This product can be used across EU member states.

¹⁸ Currently, the only radio available for the WES Pro is long range Bluetooth (LRBLE). Be sure to check the the [Release notes](#) for information about the type(s) of radios available for the WES Pro specific to the version of the product you are using.

FORT CLI Tools

This appendix describes the `fort_cli_cfg` tool, lists the commands it provides for listing devices and applying configurations and firmware, and explains how to install `fort_cli_cfg` on a Linux computer.

Table 98: FORT CLI Tool

Tool	Use Case	Works Offline	Download Location
<code>fort_cli_cfg</code>	Loading a configuration from FORT Manager, updating firmware, rebooting a device, and the interactive device menu.	No. Loading a configuration requires connectivity to FORT Manager.	The Downloads card on the Firmware page in FORT Manager. For more information, see Loading A Configuration with the CLI Tool (on page 81).

FORT CLI Configuration Tool

You can use the FORT CLI Configuration tool (`fort_cli_cfg`) on a Linux computer to:

- Load a configuration onto a FORT device.
- Update device firmware.
- Reboot a device.
- Spawn an interactive menu for a device.

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

Note:

`fort_cli_cfg` versions 3.8.0 and older used `pip` to install Python packages. Newer versions are standalone scripts installed directly into the system outside of `pip`. The next section provides current installation instructions. If you are installing a pre 3.8.1 version, use the [Legacy Installation instructions](#) (on page 179).

Download and Install the CLI Configuration Tool

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

- Linux computer running Debian 11 or 12, or Ubuntu 20, 22, or 24 with Ethernet networking capability.
- Latest FORT CLI Configuration Tool installation package (`fort_cli_cfg-<version>.zip`).
- The Python Package installer (`pip`) is installed in your environment. Only required if you have a previously installed version of the tool (3.8.0 or older) that you must uninstall.

To download & install fort_cli_cfg

1. Download the tool from FORT Manager:
 - a. Launch FORT Manager and enter your username and password when prompted.
 - b. Click **Firmware** in the left navigation pane.
 - c. In the **Downloads** card, click **CLI Tool** and note the version shown on the button (requires DeviceManager or Admin role).
 - d. FORT Manager downloads the file: `fort_cli_cfg-<version>.zip` to the Downloads folder on your computer.
2. Copy the installation package `fort_cli_cfg-<version>.zip` from the Downloads folder on your Windows or Linux computer (depending on which system you are running FORT Manager) to a location on your Linux computer.
3. If you have installed a previous version of the tool where `version#3.8.0`, you must uninstall the old version now before you can install the new one; open a terminal and enter the following command:

```
pip uninstall fort_cli_cfg
```

4. Open a new terminal on your Linux computer, navigate to the directory containing the installation package, and unzip it.
5. Run the installation script:

```
./install.sh
```

If the installation script fails, give it execution permissions with the following command:

```
chmod+x install.sh
```

6. When prompted, type **y** to add `~/ .local/bin/` to your PATH.

The installer copies `fort_cli_cfg` to `~/ .local/bin/` and makes it available system-wide if you answered yes to the prompt.

To verify installation:

```
fort_cli_cfg -\ -version
```

If you see the version displayed, the tool is ready to use.

To see a list of all options:

```
fort_cli_cfg -\ -help
```

To connect to an EPC device and access an interactive menu (Device Info, Reboot, etc.)

```
fort_cli_cfg -e192.168.3.10 -m
```

Your IP address may be different.

To connect to an NXP device (SRCPro, WESPro, NSCPro) and access an interactive menu (Device Info, Reboot, etc.)

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

Your serial interface (/dev/ttyACM0) may be different.

Note:

For convenience, if you don't specify a serial interface in the command, the CLI tool connects to the first FORT device it finds. Therefore, if you are connected to a single FORT (USB) device, you can simply run the following command to connect:

```
fort_cli_cfg -n
```

For step-by-step instructions on using this tool to load a configuration or update firmware, see:

- [Loading a Configuration with the CLI Tool](#) (on page 79).
- [Updating Firmware on Your Devices](#) (on page 199).

Important:

If you are installing **fort_cli_cfg version 3.8.0 or older**, use the **Legacy Installation** instructions below.

Legacy Installation – fort_cli_cfg versions 3.8.0 and Older

Note:

These instructions are for fort_cli_cfg versions 3.8.0 or older. For newer versions, see [Download and Install the CLI Configuration Tool](#) (on page 177).

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

- Linux computer running Ubuntu 20 with Ethernet networking capability.
- Latest FORT CLI Configuration Tool installation package (fort_cli_cfg-<version>.zip).
- The Python Package installer (pip) is installed in your environment.

1. Download the tool from FORT Manager:

- a. Launch FORT Manager and enter your username and password when prompted.
- b. Click **Firmware** in the left navigation pane.
- c. Click **Download CLI Tool Version: x.x.x** (requires DeviceManager or Admin role).

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

2. 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):

```
scpC:\\<myDir>\\fort_cli_cfg-<version>.tar.gzmuser1@<ipaddress>:/home/
<username>
```

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

```
pipinstall./fort_cli_cfg-<version>.tar.gz
```

5. Add yourself to the dialout user group so you won't need sudo permission when using the fort_cli_cfg tool to access the serial device:

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

6. Reboot your Linux machine .
7. To verify that the tool has been successfully installed and that you can run it, type the following command in a terminal window:

```
fort_cli_cfg-\\-version
```

If you see the version displayed, the tool is ready to use.

8. If you get a command not found error, verify that your \$PATH variable contains . local/bin, which is where pip installs applications. For example, in a terminal, type:

```
echo $PATH (Enter)
-bash: /home/user/. local/bin:/home/<username>/. local/bin:/usr/local/
sbin: ...
```

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

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

10. Restart the terminal.

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

```
fort_cli_cfg --help
```

Recommended Relays

This appendix lists the safety relays and diodes that FORT has tested with EPC and NSC Pro receivers, and provides a wiring diagram for each one to get you started.

This appendix describes the relays that we have tested for use with an EPC or NSC Pro receiver:

- [EPC Recommended Relays](#) (on page 181)
- [NSC Pro Recommended Relays](#) (on page 186)

EPC Recommended Relays

The sections that follow provide a wiring diagram for each relay that we have tested for use with an EPC receiver.

Important:

These wiring guides are intended as a *quick start* to assist you in wiring your FORT devices to your equipment, but are in no way a definitive guide to any of the relays. Be certain to consult the manufacturer's documentation for whichever relays you are using.

To satisfy applicable wiring codes and conditions, you are responsible for protection of field devices and wiring through appropriate fusing of the circuitry. You can fuse the EPC circuit in a number of different ways, but to determine the size of the fuse(s) you must account for:

- The EPC current, which is 87 mA@ 32V or 273 mA@ 8V (from the table in [Recommended and Absolute Maximum Ratings \(EPC\)](#) (on page 142)).
- The current per output channel (which you must measure as it varies based on your setup).
- The relay current (which you must measure as it varies based on your setup).

When testing your system, and before putting it into production, be certain to measure your actual current.

You **must** provide a flyback diode (external or built-in to the relay) to prevent reverse voltage (flyback) when the relay coils shutoff in response to a safety signal. The forward voltage of the diode should be standard (0.7 V), but the reverse breakdown voltage of the diode must be greater than the expected system voltage that will drive the relay coil. This diode should conduct in its forward-biased condition only (which occurs when the coil is suddenly de-energized in the case of the safety outputs of the system going from high to low).

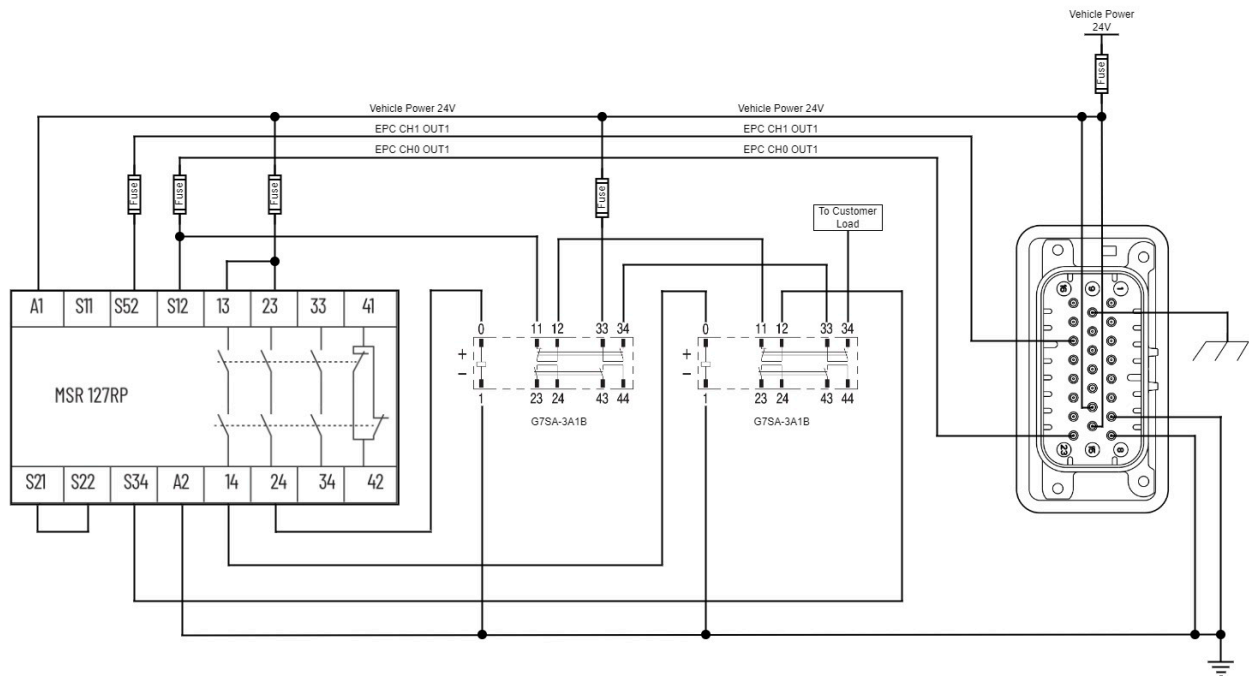
Note:

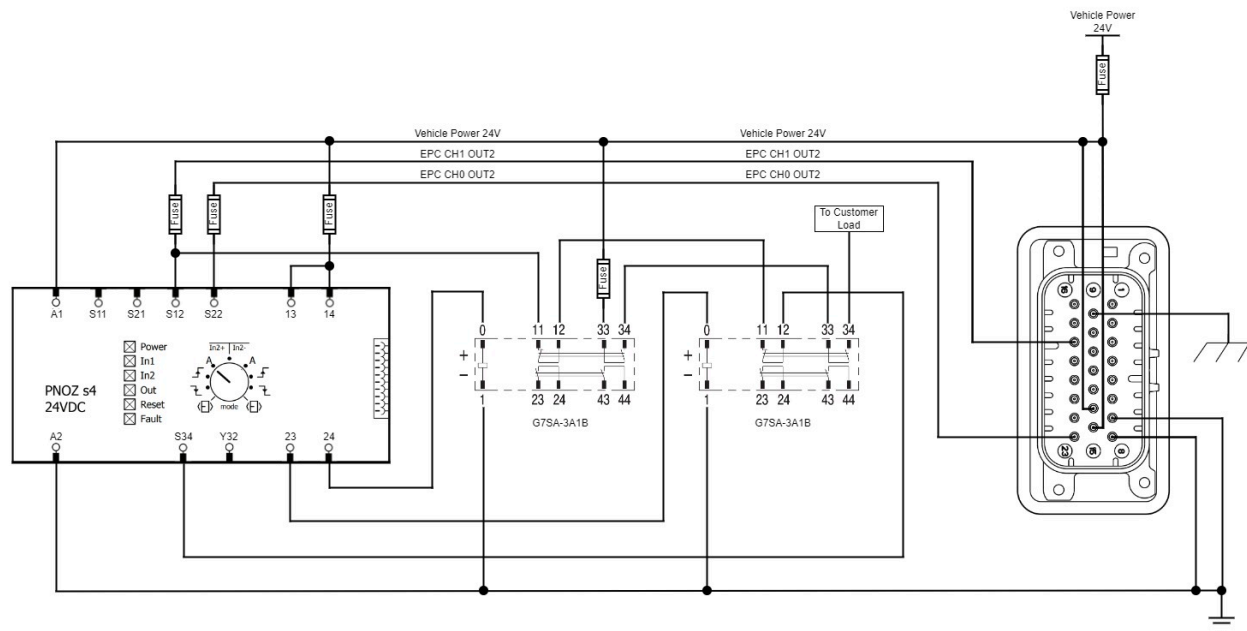
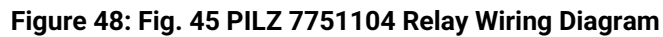
The EPC utilizes OSSD test pulses to detect shorts, so the downstream safety input must be able to filter out these pulses (all of the recommended relays meet this criteria). Be sure that any chosen relay is compatible with these pulses and meets any other safety or reliability requirements of the application.

See [OSSD Pulses](#) (on page 190) for detailed information on how Pro series receivers use OSSD pulses, including how to turn them off for NSC Pro devices.

Table 99: Table 88 EPC Recommended and Tested Relays

Manufacturer	Model	Supply Voltage	Link to Wiring
Allen-Bradley	MSR127TP	24V	Allen-Bradley MSR127TP (on page 182)
EATON	ESR5-NV3-30	24V	EATON ESR5-NV3-30 (on page 182)
PILZ	751104	24V	PILZ 751104 (on page 183)
IDEM	SCR-3-1P-i	24V	IDEM SCR-3-1P-I (on page 183)
OMRON	G7SA-3A1B	24V	OMRON G7SA-3A1B (on page 184)
PANASONIC	SFS3-L-DC12V-D	12V	PANASONIC SFS3-L-DC12V-D (on page 185)

Allen-Bradley MSR127TP**Figure 46: Fig. 43 Allen-Bradley MSR127TP Relay Wiring Diagram****EATON ESR5-NV3-30**



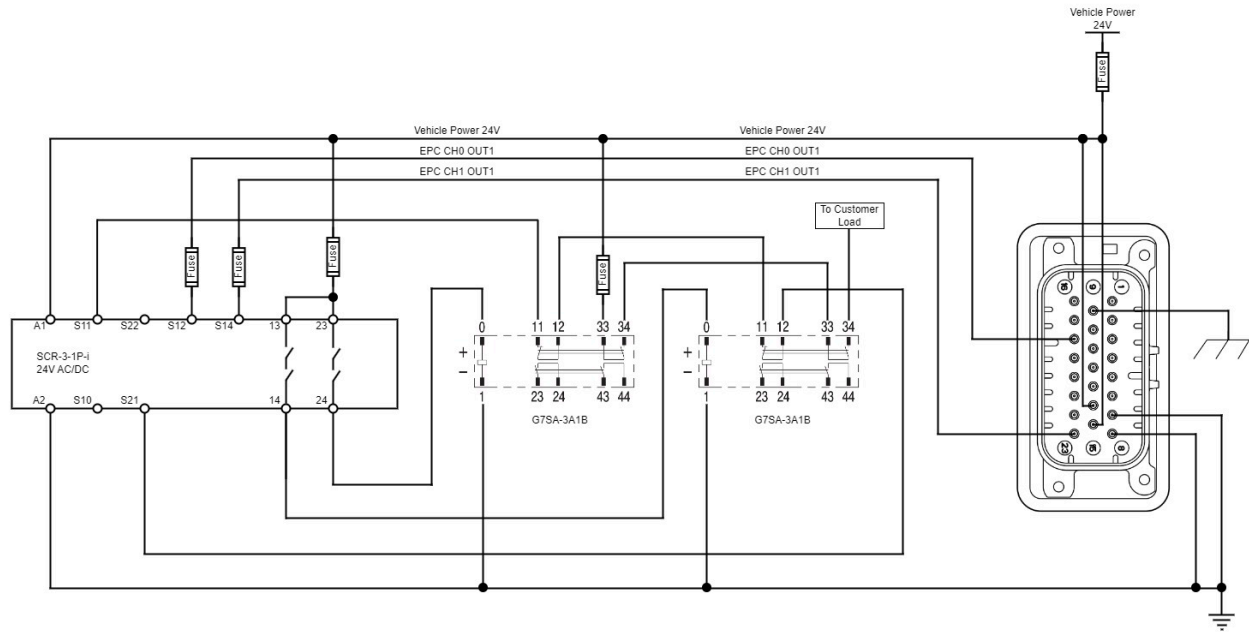


Figure 49: Fig. 46 IDEM SCR-3-1P-I Relay Wiring Diagram

OMRON G7SA-3A1B

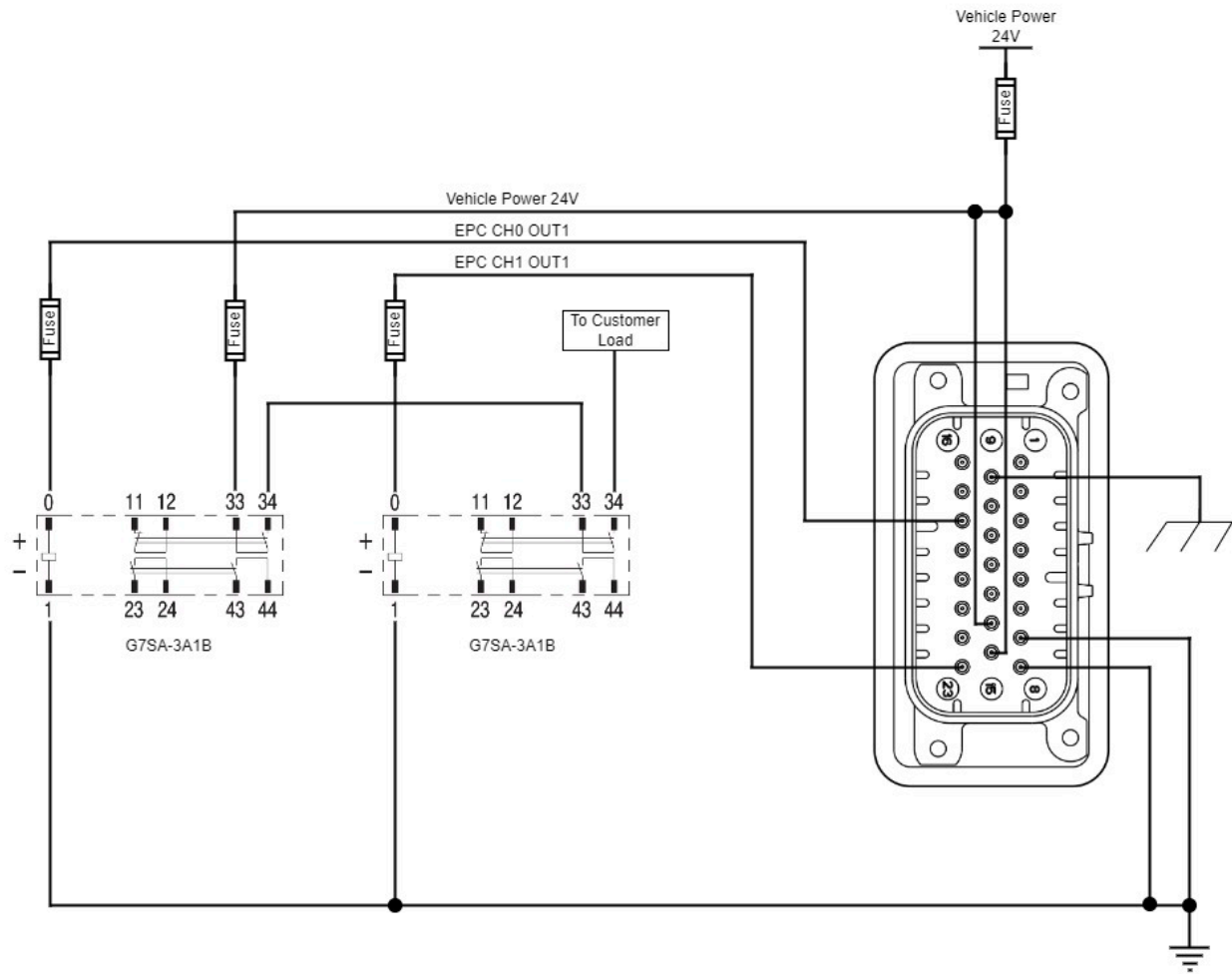


Figure 50: Fig. 47 OMRON G7SA-3A1B Relay Wiring Diagram

PANASONIC SFS3-L-DC12V-D

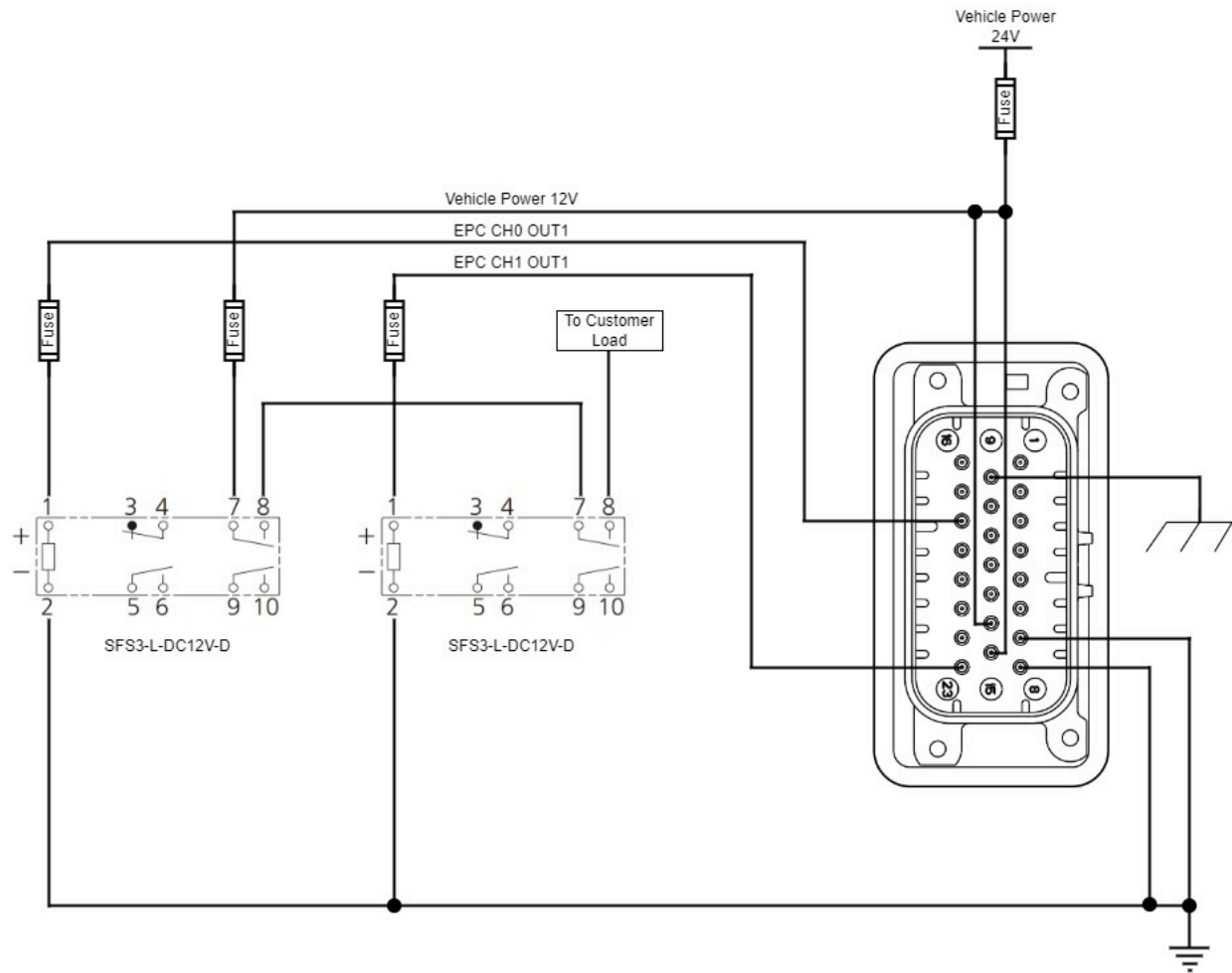


Figure 51: Fig. 48 PANASONIC SFS3-L-DC12V-D Relay Wiring Diagram

NSC Pro Recommended Relays

The sections that follow provide a wiring diagram for each relay that we have tested for use with an NSC Pro.

Note:

These wiring guides are intended as a *quick start* to assist you in wiring FORT devices to your equipment, but are in no way a definitive guide to any of the relays. Be certain to consult the manufacturer's documentation for whichever relays you are using.

To satisfy applicable wiring codes and conditions, you are responsible for protection of field devices and wiring through appropriate fusing of the circuitry. As a rule of thumb, calculate fuse size on PVin as:

$$(\text{pvin_current} + \text{output-driving-current(perchannel)} + \text{relay_current}) \times 1.5$$

The table in [Recommended Operating Conditions](#) (on page 152) shows the current and driving current as:

- **current:** 80 mA (serial comms) or 650 mA (ISM max power)
- **driving current per channel:** 230 mA.

When testing your system, and before putting it into production, be certain to measure your actual current.



CAUTION:

To ensure reliable operation, you must connect a Schottky diode in reverse bias across the relay coil terminals. The following table shows the diodes that we recommend.

Table 100: Table 89 NSC Pro Recommended Diodes

Manufacturer	Part #
Onsemi	NRVB130LSFT1G
Various	1N5822

Important:

The NSC Pro utilizes OSSD test pulses to detect shorts, so the downstream safety input must be able to filter out these pulses (all of the recommended relays meet this criteria). Be sure that any chosen relay is compatible with these pulses and meets any other safety or reliability requirements of the application.

See [OSSD Pulses](#) (on page 190) for detailed information on how Pro series receivers use OSSD pulses, including how to turn them off for NSC Pro devices.

Table 101: Table 90 NSC Recommended and Tested Relays

Manufacturer	Model	Supply Voltage
TE	V23047-A1005-A501	5
TE	V23047-A1012-A501	12
PANASONIC	SFS3-L-DC12V-D	12V
OMRON	G7SA-3A1B DC12	12

Important:

For each of the following relays, be certain to consult the manufacturer's documentation for proper installation instructions, including what size fuse to attach to the relay contactors.

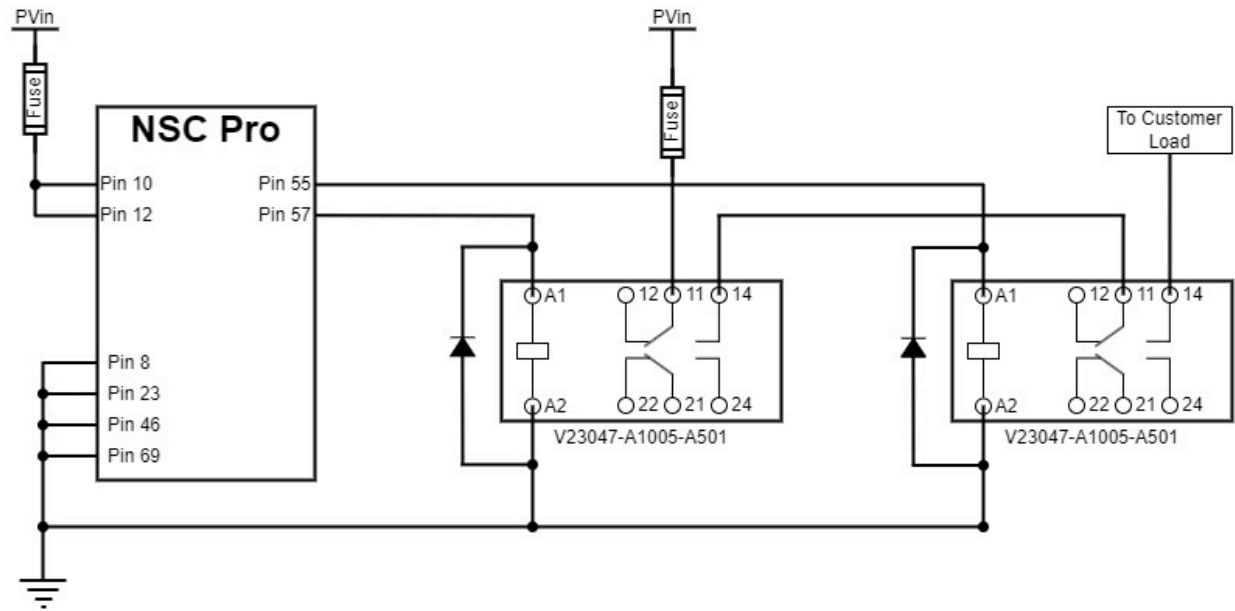


Figure 52: Fig. 49 TE V23047-A1005-A501 Relay Wiring Diagram

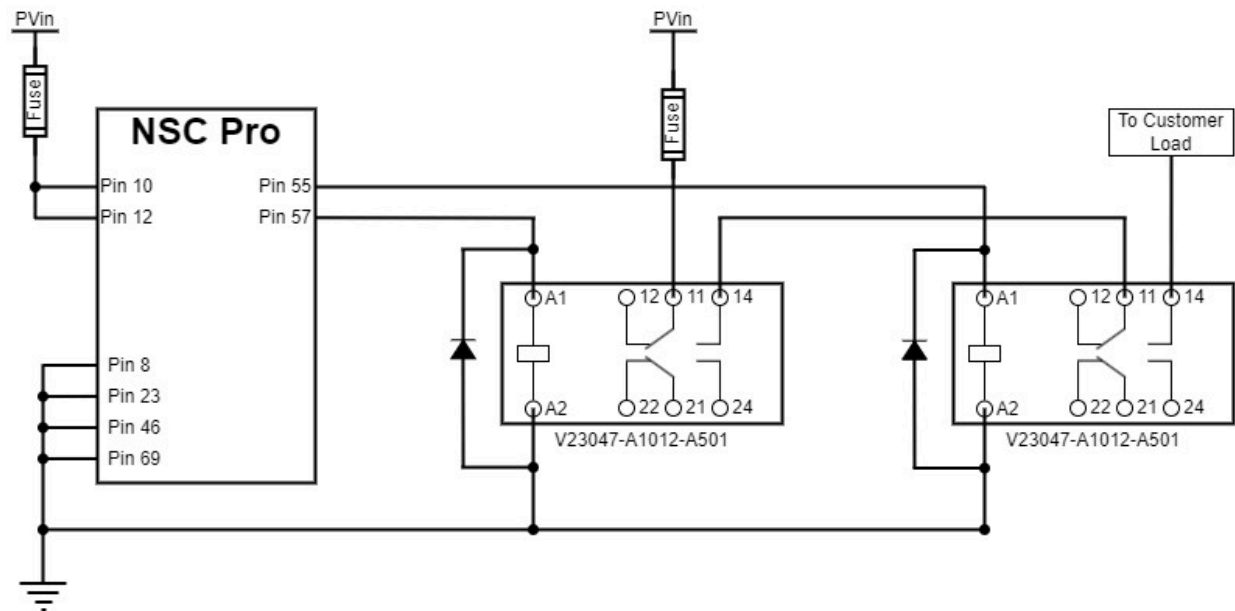
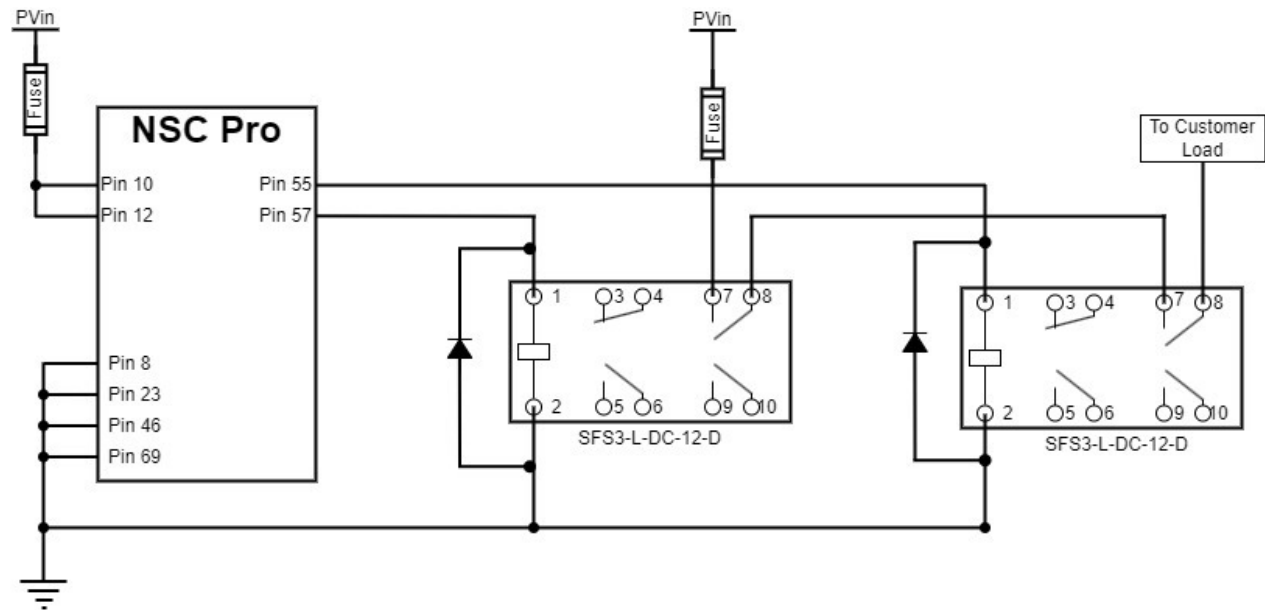


Figure 53: Fig. 50 TE V23047-A1012-A501 Relay Wiring Diagram



19

Figure 54: Fig. 51 PANASONIC SFS3-L-DC12V-D Relay Wiring Diagram

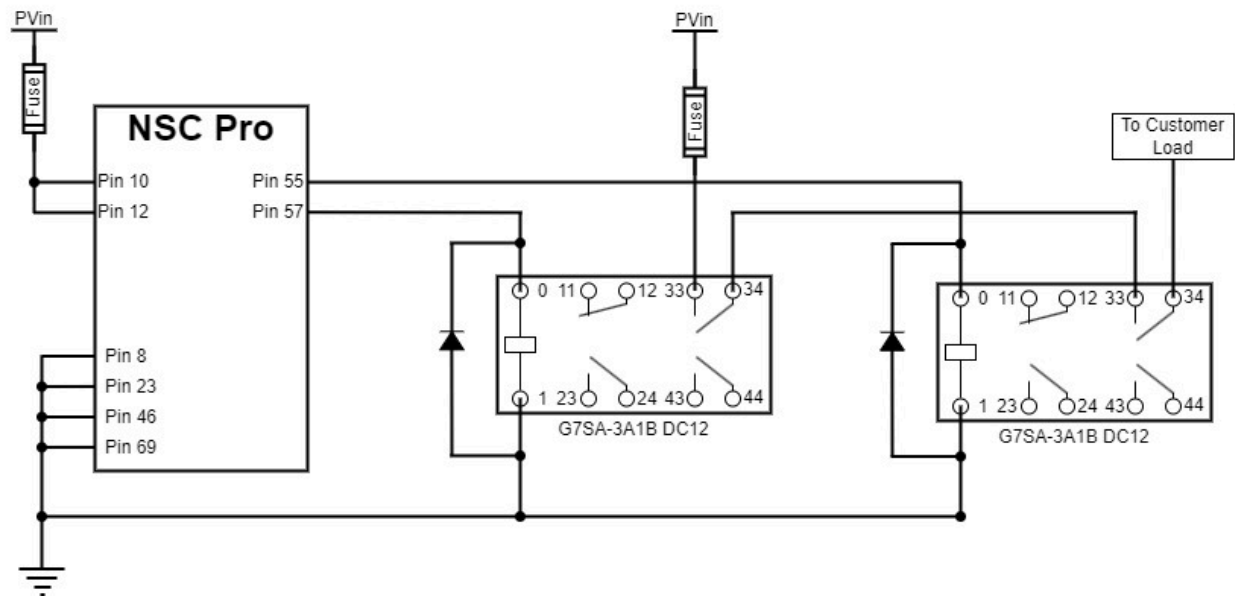


Figure 55: Fig. 52 OMRON G7SA-3A1B DC12 Relay Wiring Diagram

¹⁹ Although this relay has a built-in diode, you must attach a Schottky diode across the relay coil as well.

OSSD Pulses

This appendix explains how EPC receivers and NSC Pros use OSSD test pulses to detect shorted outputs, describes the side effects those pulses can have on the equipment wired to them, and shows how to turn them off.

An EPC receiver and NSC Pro generate OSSD (Output Signal Switching Device) test pulses that allow the device to detect a shorted output to battery (or a voltage source) and output wires that are shorted together. If a fault is detected, the safety system triggers a safe state.

OSSD pulses are only generated when an output is commanded ON (i.e. when safety is not being requested). They are not generated when the output is commanded off (i.e. when safety is being requested).

When an output is commanded ON, the safety system of the receiver device periodically turns off that output for a short period of time to detect the presence or lack of a voltage at the output pin. If a voltage is detected, it is treated as a fault, and both redundant outputs are turned off. The fault will persist and cannot be cleared until both of these conditions are met:

- The underlying cause of the fault has been resolved.
- The receiver has been power-cycled.

Important:

Besides applying OSSD, NSC Pros and EPC receivers perform an additional diagnostic test when an output has been commanded OFF; the receiver checks the voltage at the output pin and if it senses a voltage, it detects that a shorted output to battery (or some other voltage source) is present. The fault will persist and cannot be cleared until both of these conditions are met:

- The underlying cause of the fault has been resolved.
- The receiver has been power-cycled.

Characteristics of OSSD pulses:

- OSSD pulse width = $\sim 300 \mu\text{S}$
- OSSD pulse period = $\sim 200 \text{ mS}$

The following figure shows OSSD pulses; note the 200 ms spacing between each of the yellow channel 0 pulses and the 100ms spacing between each yellow channel 0 pulse and pink channel 1 pulse:

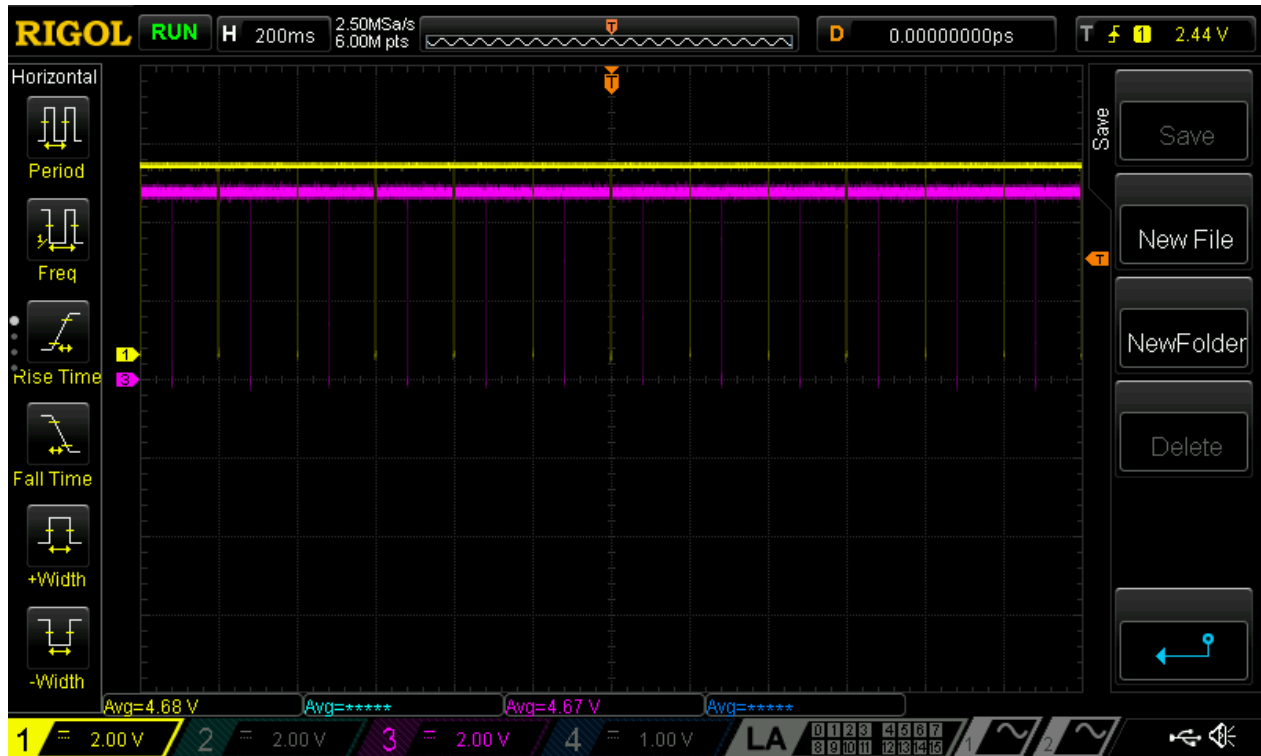


Figure 56: Fig. 53 Sample OSSD Pulse

Configurability of OSSD pulses

On EPC receivers, OSSD is not configurable and OSSD pulses are always generated when safety is not being requested (i.e. when an output is commanded ON).

On NSC Pros, OSSD is configurable and can be turned ON (default) or OFF in FORT Manager (see below for details).

Potential side effects of OSSD pulses

If you use the recommended relays that have been tested by FORT and listed in the user's manual for the receiver device that you are using, you will not see any side effects.

However, for both an EPC receiver and an NSC Pro, if you use relays other than those listed in the user's manual, OSSD pulses may cause chatter on the contactor side of the relays.

If you notice chatter on the contactor side of the relays while using an NSC Pro without the recommended relays, you can turn off OSSD in FORT Manager but be aware that NSC Pro will not be able to detect a shorted output to battery while the outputs are commanded ON (i.e. when safety is not being requested).

If you notice chatter on the contactor side of the relays while using an EPC without the recommended relays, you must either switch to using a recommended relay or come up with your own filter to negate the effect of the OSSD pulses.

In all cases, consult the documentation for your chosen relay and verify that it is compatible with OSSD pulses and meets any other safety or reliability requirements of the application.

To Turn OSSD Off

You can turn OSSD off in FORT Manger for an NSC Pro, as follows:

1. Open FORT Manager, click **Configurations > New Setup** and build a configuration (give it a name, add a sender(s), and NSC Pro receiver(s)).
2. Select **Settings > Devices** and select an NSC Pro.
3. Click **Off** to toggle the OSSD switch off (it's on by default).
4. Make sure other settings are correct and click **Save** to save the settings for this device.
5. **Repeat for any other NSC Pros for which to turn off OSSD pulses.** You can mix and match, turning OSSD off for some devices and leaving it on for others.
6. Click **Done** when you've configured all desired and necessary settings.

Antennas

This appendix lists the antennas that FORT recommends for each wireless communication method, identifies which devices need an antenna as a separate accessory, and gives the rules you must follow when using an approved antenna.

FORT offers a variety of antenna options to support the wireless communication method you will be using. The antennas for the NSC Pro and EPC are accessories that you need to select prior to purchase. The antennas for the Safe Remote Control Pro and WES Pro are built into the device, thus select the device version that contains the radio you intend to use.

Important:

This appendix provides a list of FORT recommended antennas, but you may use your own antenna if you so choose. Be certain that it meets the standards for antennas listed in [Notifications and Certifications](#) (on page 218).

Note:

In a configuration where every device communicates over LRBLE — for example a [Two-to-One over Long-Range Bluetooth](#) — each device needs an antenna suited to that radio. The SRC Pro's antenna is built in; the antennas for both the EPC sender and the EPC receiver are accessories you must select and attach. Range depends on both ends of a link, so an under-specified or poorly placed antenna on the EPC sender limits how far a supervisor can be from the machine and still stop it.

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

Table 102: Table 91 FORT Recommended Antennas

Antenna	275-0108	275-0096	275-0112	275-0120;	275-0112
Attribute					
FORT Device	EPC 1001, SRC Pro 1001	EPC 1000, EPC 1003	SRC Pro 1003	WES Pro 1003	NSC Pro 1003
Antenna Type	Whip, Tilt/Swivel	Dome	Whip, Tilt, Swivel	Whip, Straight	Whip, Tilt, Swivel
Monopole or Dipole	Dipole	Dipole	Dipole	Dipole	Dipole

Antenna	275-0108	275-0096	275-0112	275-0120;	275-0112
Attribute					
Termination/ Connector	RP-SMA Male Connector	N Type Female Panel	RP-SMA Connector	RP-SMA Male Connector	RP-SMA Connector
Usage	ISM 915 MHz LPWA	Wi-Fi, BLE, Long range BLE (EPC 1003 only)	Long range BLE (SRC Pro 1003 only)	Long Range BLE (WES Pro 1003 only)	Long Range BLE (NSC Pro 1003 only)
Frequency Range	902–930 MHz	2.4-2.5GHz 5.1 to 5.9GHz	2.3–2.6 GHz	2.4–2.5 GHz	2.3–2.6 GHz
Peak Gain	2.7 dBi	4.5dBi @ 5.1-5.9Ghz 7.2dBi @ 2.4-2.5Ghz	3.2 dBi	2 dBi	3.2 dBi

Use grommets when routing the antenna cable through enclosures.



CAUTION:

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

Ideally, you should place the antenna such that it has a clear line of sight (LOS), it's not too high or too low, no metal is between it and the sender, and it's pointed straight up (whip antenna), or pointed towards other devices (puck antenna). The following table shows rules for using approved antennas in the USA, Canada, and Europe:

Table 103: Table 92 Rules for using Approved Antennas

Device	FCC ID (US)	IC (Canada)	CE (Europe)
EPC & 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

Implement FORT SDK as a Service

This appendix explains how to run the FORT SDK as a service on a Linux machine so that IP communication between an NSC Pro and its sender starts automatically after every restart, with separate procedures for an EPC sender and an SRC Pro sender.

Implement FORT SDK as a Service

When you configure an NSC Pro to communicate with its EPC sender via Wi-Fi or Ethernet, the FORT SDK must be running at all times in order to enable IP communications between the sender and the NSC Pro (see [Install and Run the FORT SDK](#) (on page 33)). One way to ensure that the FORT SDK is running is to implement it as a service that launches automatically whenever the Linux machine restarts.

This appendix explains how to implement the FORT SDK as a service in a configuration with an EPC sender (next section) and in a configuration with an SRC Pro sender ([Implement SDK as a Service for SRC Pro Sender](#)).

Implement SDK as a Service for EPC Sender

For a configuration with an EPC sender and NSC Pro receivers, the FORT SDK must be running at all times to enable Ethernet traffic between the EPC and the NSC Pro. This section shows how to implement the FORT SDK as a service to run on an Ubuntu Linux machine.

To Implement FORT SDK as a Service

1. Create the directory `etc/fort-sdk`:

```
>mkdir/etc/fort-sdk/
```

2. Create an environmental file in the new directory (`/etc/fort-sdk/fort-agent-pro.conf`) with the following content:

```
/*--fort-agent-pro.conf--*/
1FORT_SAFETY_CHARDEV=/dev/serial/by-id/usb-FTDI_Dual_RS232-HS-if01-
port0
2FORT_CONFIG_CHARDEV=/dev/serial/by-id/usb-FORT_Robotics__Inc._NSC_Pro_
<SerialNumber>-if00
```

3. Use `chmod` to set the read-write permissions to the `/etc/fort-sdk` directory as shown by the following `ls` command:

```
>ls-la/etc/fort-sdk/

total20
drwxr-xr-x2rootroot4096Nov2212:55.
drwxr-xr-x151rootroot12288Nov2212:55..
-rw-r--r--1rootroot154Nov2212:55fort-agent-pro.conf
```

4. Define a service configuration file `/etc/systemd/system/fort-agent-pro.service`:

```
>sudotouch/etc/systemd/system/fort-agent-pro.service
```

5. In the file, specify the command-line options for launching `fort-agent-pro` as a service:

```
/*--fort-agent-pro.service--*/
1[Unit]
2Description=FORTAgentProservice
3After=network.target
4[Service]
5EnvironmentFile=/etc/fort-sdk/fort-agent-pro.conf
6ExecStart=/usr/local/bin/fort-agent-pro--
safety"${FORT_SAFETY_CHARDEV}"--config"${FORT_CONFIG_CHARDEV}"
7ExecReload=/usr/local/bin/fort-agent-pro--
safety"${FORT_SAFETY_CHARDEV}"--config"${FORT_CONFIG_CHARDEV}"
8Restart=always
9Type=simple
10[Install]
11WantedBy=default.target
12RequiredBy=network.target
```

6. Use `chmod` to set the read-write permissions to `/etc/systemd/system/fort-agent-pro.service` as shown by the following `ls` command:

```
>ls-la/etc/systemd/system/fort-agent-pro.service
-rw-r--r--1rootroot427Nov2212:57/etc/systemd/system/fort-agent-
pro.service
```

7. Run the following command to start the service:

```
>sudo systemctl start fort-agent-pro.service
```

8. To verify that FORT Agent Pro is running, run the following command and you should see similar output:

```
> sudo systemctl status fort-agent-pro.service
# fort-agent-pro.service - FORT Agent Pro service
   Loaded: loaded (/etc/systemd/system/fort-agent-pro.service;
   disabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-11-22 12:58:52 EST; 5min
   ago
     Main PID: 210832 (fort-agent-pro)
        Tasks: 5 (limit: 35659)
       Memory: 240.0K
          CGroup: /system.slice/fort-agent-pro.service
                  ##210832 /usr/local/bin/fort-agent-pro --safety /dev/
serial/by-id/usb-FTDI_Dual_RS232-HS-if01-port0 --config /dev/serial/by-
id/usb-FORT_Robotics__Inc._NSC_Pro_NOTSET-if00

Nov 22 13:04:18 FORT-PF2PKENV fort-agent-pro[210832]: [1700676258118]
[info] config->udp (2 packets, 22 bytes, 0 bytes/sec)
Nov 22 13:04:18 FORT-PF2PKENV fort-agent-pro[210832]: [1700676258118]
[info] udp->config (2 packets, 60 bytes, 0 bytes/sec)
Nov 22 13:04:18 FORT-PF2PKENV fort-agent-pro[210832]: [1700676258118]
[info] comms->udp (1 packets, 0 bytes, 0 bytes/sec)
Nov 22 13:04:18 FORT-PF2PKENV fort-agent-pro[210832]: [1700676258118]
[info] udp->comms (0 packets, 0 bytes, 0 bytes/sec)
Nov 22 13:04:18 FORT-PF2PKENV /usr/local/bin/fort-agent-pro[210832]:
[fort-agent_show_statistics:275] Uplink Statistics
```

```
Nov 22 13:04:18 FORT-PF2PKENV /usr/local/bin/fort-agent-pro[210832]: [fort-agent_show_statistics:276]
-----
Nov 22 13:04:18 FORT-PF2PKENV /usr/local/bin/fort-agent-pro[210832]: [fort-agent_show_statistics:277] config->udp (2 packets, 22 bytes, 0 bytes/sec)
Nov 22 13:04:18 FORT-PF2PKENV /usr/local/bin/fort-agent-pro[210832]: [fort-agent_show_statistics:281] udp->config (2 packets, 60 bytes, 0 bytes/sec)
Nov 22 13:04:18 FORT-PF2PKENV /usr/local/bin/fort-agent-pro[210832]: [fort-agent_show_statistics:285] comms->udp (1 packets, 0 bytes, 0 bytes/sec)
Nov 22 13:04:18 FORT-PF2PKENV /usr/local/bin/fort-agent-pro[210832]: [fort-agent_show_statistics:289] udp->comms (0 packets, 0 bytes, 0 bytes/sec)
```

You can run the following command to stop the service:

```
sudo systemctl stop fort-agent-pro.service
```

Implement SDK as a Service for SRC Pro Sender

While it is not strictly necessary to install and run the FORT Agent Pro in a configuration with an SRC Pro sender and NSC Pro receivers, installing and enabling FORT Agent Pro allows you to configure an NSC Pro over IP as long as the host Linux device connected to the NSC is TCP/IP network enabled.

The general procedure is the same as that detailed in the previous section: you create a `/etc/fort-sdk/fort-agent-pro.conf` file and a `/etc/systemd/system/fort-agent-pro.service` file. However, since the agent is to be run in config-only mode in this use case, the contents of the files should look like this:

Contents of `/etc/fort-sdk/fort-agent-pro.conf`:

```
/*--fort-agent-pro.confsrcproversion--*/
1FORT_CONFIG_CHARDEV=/dev/serial/by-id/usb-
FORT_Robotics__Inc._NSC_Pro_<SerialNumber>-if00
Contentsof/etc/systemd/system/fort-agent-pro.service:
/*--fort-agent-pro.servicesrcproversion--*/
1[Unit]
2Description=FORTAgentProservice
3After=network.target
4[Service]
5EnvironmentFile=/etc/fort-sdk/fort-agent-pro.conf
6ExecStart=/usr/local/bin/fort-agent-pro--config"${FORT_CONFIG_CHARDEV}"
7ExecReload=/usr/local/bin/fort-agent-pro--config"${FORT_CONFIG_CHARDEV}"
8Restart=always
9Type=simple
10[Install]
11WantedBy=default.target
12RequiredBy=network.target
```

To start, stop, and check status of the service, use the following commands:

- `sudo systemctl start fort-agent-pro.service`
- `sudo systemctl status fort-agent-pro.service`

- `sudo systemctl stop fort-agent-pro.service`

Updating Firmware on Your Devices

This appendix explains how to find out when new firmware is available for your Pro Series devices and how to install it, using the FORT Manager Desktop App or either of the FORT command-line tools.

For all devices, FORT releases periodic updates to the firmware for performance, safety, and security reasons.

When new firmware is released it appears in the firmware release table on the **Dashboard** page with a **New** badge. You can also navigate to the **Firmware** page to see the latest version that is available for each type of device, together with the downloads. If you are not sure whether your firmware is up to date, or if you are eligible for updates, email support@fortrobotics.com or submit a request from the **Dashboard** page of FORT Manager (**Submit Request**) to get help.

You can access the firmware interface of any Pro Series device in any of the following ways:

- By using the FORT Manager Desktop application (see [Updating Pro Series Device Firmware with Desktop App](#) (on page 200)).
- Directly through a USB connection using the `fort_cli_cfg` tool (see [Updating the Firmware with the CLI Tool](#) (on page 201)).

Note:

FORT does not publish further firmware for a model that has reached end of support. The device keeps the firmware it is running. For more information, see [SRC Pro Models and Support Status](#) (on page 171).

Important:

Firmware updates are one-way. A Pro Series device accepts a newer firmware version only; you cannot return one to an earlier version, with the FORT Manager Desktop App or with either command-line tool. Check the version on the **Firmware** page against the version on the device before you start.

The Firmware Page

The **Firmware** page lists the published firmware version for each device type and carries the **Downloads** card for the Desktop App, the CLI Configuration Tool, and the FORT SDK.

Each row carries a status badge: **Up to date** where nothing is needed, or the time remaining on the download, for example **77d left**. For more information, see [Download Expiry](#) (on page 199).

Firmware is published for each device type separately. FORT does not publish further firmware for a model that has reached end of support, and no device can be returned to an earlier version.

Download Expiry

Downloads offered on the **Firmware** page carry an expiry. The status badge on each row shows the time remaining — for example **77d left** — or **Up to date** where no action is needed. The expiry travels with the download, so it applies wherever that file ends up: stored inside the Desktop App, saved to your file system for `fort_cli_cfg`, or fetched with `fortcli device firmware download`.

Important:

Check the expiry badge before you rely on a file you downloaded earlier. This matters most when you are preparing to work without an internet connection: a file downloaded and stored for offline use can expire while it is sitting on your machine, and you cannot refresh it from a site with no connectivity. For more information, see [Before You Begin](#).

If a download has expired, return to the **Firmware** page while connected to the internet and download it again. Files already applied to a device are unaffected; expiry applies to the download, not to firmware or a configuration that is running.

Updating Pro Series Device Firmware with Desktop App

This section explains how to update the firmware for any type of Pro Series device with the FORT Manager Desktop App. Note that this is the *Desktop* app, not the *Web* app; if you don't already have it, you can download the Desktop app, Windows or Linux version, from the Web app or directly from [GitHub](#).

To Update Firmware using FORT Manager Desktop App**Required Items:**

- A newer firmware version is available.
- Windows or Linux computer running with Ethernet networking capability (required for using the FORT Manager Desktop app).
- FORT Manager Desktop app (find latest version in FORT Manager Web app or at [GitHub](#)).
- The Device is in a safe state.

To Update Firmware with the Desktop App

1. Launch the FORT Manager Desktop App on your computer.
2. Boot up or power on your device.
3. Connect your computer to the device:
 - For an EPC, connect over Ethernet to port J2 on the EPC using the M12-RJ45 cable.
 - For an NSC Pro, SRC Pro, or WES Pro, connect via USB. Note that the WES Pro requires the docking station.

The application displays a message that it has detected a device for tethering. If multiple devices are connected to the computer, the application displays a list of devices to choose from.

4. Select the device and click **Tether**.

The application displays information about the device including the name of the configuration to which the device belongs.

- a. If FORT Manager doesn't auto detect the device, click **Tether a Device** and select the type of device:
 - For an EPC, enter the IP address.

- For other devices, enter the COM port, generally **COM3**.
- b.** Click **Connect**.

5. Click **Update** next to **Firmware** to upload the firmware to the device.

The application shows that the configuration has been updated and automatically untethers the device. You can unplug the device from the computer unless you have a firmware update to apply as well.

Repeat this procedure for every device in the configuration.

To Download Firmware for Offline Loading

One of the advantages of the desktop app is that you can use it without an internet connection. If you plan to load configurations or make firmware updates when the internet is not available, you can download the firmware and configurations when connected to the internet and store them in the app for later retrieval.

- 1.** Launch the FORT Manager Desktop App on your computer.
- 2.** Click **Firmware**.
- 3.** Next to the type of device to update, click **Download**.

The Download Status changes to *Downloaded*.

Note:

Downloaded files are stored in the application, not in the computer's file system. To download a file for use with the `fort_cli_cfg` tool, click the version number next to a device and save it to your file system.

Repeat for any other firmware that you plan to upload when offline.

Updating the Firmware with the CLI Tool

This section explains how to update Pro Series device firmware with the CLI tool. The previous section shows how to do so with the desktop app.

Depending on your type of device, go to one of the following procedures:

- [Updating EPC Firmware with the CLI Tool](#) (on page 202)
- [Updating NSC Pro, SRC Pro, or WES Pro Firmware with the CLI Tool](#) (on page 203)

If you haven't done so already, download the firmware upgrade file for your type of device by completing the steps in the following procedure (click the procedure to open it):

To Download the Firmware Upgrade File

Note:

Requires FORT Manager DeviceManager or Admin role.

- 1.** Launch FORT Manager and enter your username and password when prompted.
- 2.** Click **Firmware** in the left navigation pane to open the Firmware page.
- 3.** Click the version number next to your type of device and save the file to a location on your computer.

Note that the file is in a compressed format but you *don't* need to uncompress it to install it.

The **Downloads** card on this page holds the Desktop App, the CLI Configuration Tool, and the FORT SDK. It does not hold device firmware; firmware comes from the version link in the device-type row.

If you're using the Desktop App, *don't* click the **Download** link next to the device type. It downloads the firmware update file to FORT Manager desktop to make it available for offline update. For updating with the CLI Tool, you need to download the file through the version link.

4. (Optional, this step is required only if you are running FORT Manager in a browser on a different computer than your Linux computer, for example, on a Windows machine. If you are running FORT Manager on a Linux machine, you can skip this step.)

Copy the file from a directory on your Windows machine to the home directory on your Linux computer by using the secure copy command (scp):

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

```
scpC:\\<myDir>\\<device_firmware_file><user>@<ipaddress>:/home/
<user>
```

Updating EPC Firmware with the CLI Tool

Required Items

- Linux computer running (Ubuntu 20.04) or a Windows machine.
- Firmware upgrade file for your device type.

You can download an archive package that contains the latest version from FORT Manager on the Firmware page by clicking on the version number next to the type of your device (see [Firmware Download Procedure](#) (on page 201)).

- Latest FORT CLI Configuration Tool (fort_cli_cfg).

If you don't already have this tool, you can download it from the Firmware page of FORT Manager.

To Install the EPC Firmware Update File

Note:

Requires Admin or Operator role.

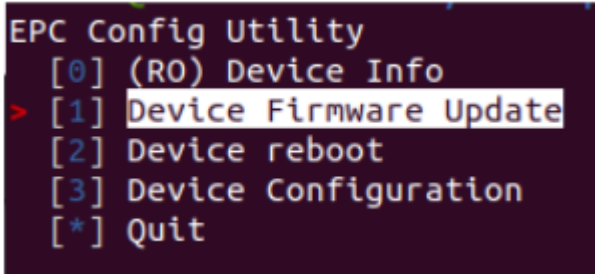
1. Power on the EPC.
2. Connect your Linux computer to the EPC J2 port using an M12-RJ45 cable.
3. Open a terminal and execute the FORT CLI Configuration Tool:

```
fort_cli_cfg-e192.168.3.10-m
```

Where:

- -e192.168.3.10
 - Specifies the EPC's IP address (default value, yours might be different).
- -m(--menu)
 - Specifies the interactive menu option for the configuration tool.

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



```
EPC Config Utility
[0] (RO) Device Info
> [1] Device Firmware Update
[2] Device reboot
[3] Device Configuration
[*] Quit
```

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

6. Type the path to the update file and press **Enter**, for example:

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

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

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

Note:

Power cycling the device with the power button is not equivalent to a firmware reboot via the Device reboot option of the CLI tool.

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

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

```
fort_cli_cfg-e192.168.3.10-m
```

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

3. Use the arrow keys to navigate to **Version Info** and press **Enter**.

Updating NSC Pro, SRC Pro, or WES Pro Firmware with the CLI Tool

This section shows how to use the CLI tool update the firmware on an NSC Pro, SRC Pro, or WES Pro in the field.

Required Items

- Linux computer running (Ubuntu 20.04) or a Windows machine.
- Firmware upgrade file for your device type.

- You can download an archive package that contains the latest version from FORT Manager on the Firmware page by clicking on the version number next to the type of your device (see [Firmware Download Procedure](#) (on page 201)).
- Latest FORT CLI Configuration Tool (`fort_cli_cfg`).
 - If you don't already have this tool, you can download it from the Firmware page of FORT Manager.

To Upgrade the NSC Pro, SRC Pro, WES Pro Firmware Through the CLI Tool:

Note:

Requires Admin or Operator role.

1. Connect the USB port on the device to a Linux computer.
2. Open a terminal and execute the FORT CLI Configuration Tool:

(Note that you need to execute permission to `/dev/ttyACM0`.)

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

Where:

`-n (npx) /dev/ttyACM0`

Specifies an NSC Pro, SRC Pro, or WES 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 **Device firmware file data** and press **Enter**.
5. Use the arrow keys to navigate to **Upload file** and press **Enter**.
6. Type the path to the update file and press **Enter**, for example:

```
./4.1.1-NSC-Production-ProdSigned.zip
```

Note:

The update process may take up to three minutes to complete.

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

Note:

Power cycling the device manually is *not* equivalent to a firmware reboot via the Device reboot option of the CLI tool.

Product Maintenance

This appendix explains how to care for your devices, retrieve and share logs, work through common device and configuration problems, recalibrate an SRC Pro's joysticks, and proof test a configuration before you return it to service.

This appendix explains the following items:

- How to care for your devices ([Care and Handling of Devices](#) (on page 205)).
- How to handle a device that is damaged or fails for any reason ([Troubleshooting Your Devices](#) (on page 206)).
- How to proof test your devices and configurations ([Proof Testing Pro Series Devices](#) (on page 214)).
- How to calibrate the SRC Pro if necessary ([Calibrating the Axis](#) (on page 210)).

Care and Handling of Devices

The **EPC**, **SRC Pro**, and **WES Pro**, because they are enclosed devices, share the following characteristics (the NSC Pro, which is an open board, is described separately):

- They are designed and built to operate in extreme environmental conditions and as such, have been subjected to rigorous mechanical and electrical tests.
- You can safely operate them in a humid or dusty environment without fear of damaging the device. However, do *not* charge the SRC Pro or WES pro in a humid or dusty environment. For the WES Pro, wipe off the docking station with a towel, if it is wet, before inserting the WES Pro.
- You can operate them in the rain. However, when you are locating the *EPC* outside or attaching it to equipment that is operating outside or can be exposed to any amount of water, you must mount the EPC vertically.

Mounting the EPC horizontally allows water to pool and block airflow through a membrane, potentially causing the EPC to malfunction.

- Avoid placing the EPC in an area or on a machine with extended exposure to direct sunlight.
- All three devices are able to withstand an occasional drop from a height of one meter or less onto a hard surface, however, be careful not to drop them repeatedly. Although they are durable, they are not unbreakable, so (especially with the SRC Pro and WES Pro) be careful not to set them down and accidentally run over them with heavy equipment.
- You can clean them with a mild detergent and cloth.



CAUTION:

Do not apply harsh chemicals to clean any of these devices. Do not immerse them in water, avoid spilling liquids on them (wipe them off immediately if this happens), and do not subject them to intense water jets.

The **NSC Pro** is an embedded board that is designed and built to operate in extreme temperature ranges (-40 °C - 85 °C). That said, when testing and installing the NSC Pro be certain to take all precautions that you would for any electronic device (making sure that you are grounded, minimizing exposure to dust, moisture, etc.)

See [Wiring an NSC Pro for ISM/Bluetooth \(SRC Pro, WES Pro, EPC\)](#) (on page 33) for instructions on wiring and mounting the NSC Pro, including precautions to take when handling it.

Troubleshooting Your Devices



CAUTION:

None of the FORT devices have user-serviceable parts. Do not attempt to make any changes or repairs to these devices. If you have maintenance or repair questions email 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, email 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. For more information, see [Configurations and Use Cases](#) (on page 50).

Note:

You cannot register a replacement for a model that has reached end of support, so you cannot swap one in through FORT Manager. Contact FORT support, who can advise on repair and on transitioning to a supported model. For more information, see [SRC Pro Models and Support Status](#) (on page 171).



CAUTION:

If the battery for an SRC Pro or WES Pro needs replacement, contact [customer support](#) and request service. Do **not** attempt to replace the battery yourself. These devices have no user-serviceable parts, including the battery.

For a WES Pro, periodically check the health of the battery by pressing the **Menu** button # and clicking **Device Attributes > Battery Health**, especially if you notice the battery is holding a charge for a shorter period of time. We recommend having the battery replaced when the battery health indicator is at 80% or lower.

Using Logs

To assist you with safety, security, power, and communication issues, FORT devices record events as they happen. There are two ways to read them, and they show different things:

- The **Logs** tab in the device's detail view in the FORT Manager web app shows the entries already held in the FORT Manager database for that device, most recent first, defaulting to the last 24 hours. It does not reach the device.
- The FORT Manager Desktop App fetches entries from the device itself over a tethered connection and adds them to the FORT Manager database. Use it whenever you need entries the database does not have yet, and to download a log file.

The procedure below covers the Desktop App. For the web app tab, see [The Logs Tab](#) (on page 209).

Log retrieval is supported on the Endpoint Controller, the NSC Pro, the WES Pro and the SRC Pro.

To Retrieve Log Files

1. Launch the FORT Manager Desktop App on your computer.
2. Boot up or power on your device.
3. Connect your computer to the device:
 - For an EPC, connect over Ethernet to port J2 on the EPC using the M12-RJ45 cable.
 - For an NSC Pro, SRC Pro, or WES Pro, connect via USB. The NSC Pro requires the docking station, the WES Pro requires its docking station, and the SRC Pro uses mini-USB on models 1001 and 1002 and USB-C on the 1003. For more information on cables, see [Loading a Configuration with the Desktop App](#) (on page 79).

The application displays a message that it has detected a device for tethering. If multiple devices are connected to the computer, the application displays a list of devices to choose from.

4. Select the device and click **Tether**.

The application displays information about the device including the name of the configuration to which the device belongs.

- a. If FORT Manager doesn't auto detect the device, click **Tether a Device** and select the type of device:

- For an EPC, enter the IP address.
- For other devices, enter the COM port, generally **COM3**.

- b. Click **Connect**.

5. Click **Logs > Fetch Logs**.

FORT Manager categorizes messages by severity, type, and sub-type, and shows which component of the device produced each entry.

- Log Levels:
 - DEBUG
 - INFO
 - WARNING
 - ERROR

- CRITICAL
- Log Types:
 - Safety
 - Security
 - Power
 - Communication

Note:

The types above are those available at the time of writing. FORT adds types and sub-types as devices and features change, so a log you fetch may contain a type this list does not name.

By default, FORT Manager shows all levels and all types (and sub-types). You can filter by severity, such that the app shows messages at that level and *greater*. For example, if you select ERROR, it shows all ERROR and CRITICAL messages but no INFO or WARNING messages. Note that DEBUG shows all levels.

In addition, you can filter by a specific type or a type and sub-type. For example, you could display only Safety messages, or only a specific safety message such as Low RSSI; or do both and combine a type/sub-type filter with a level filter, such as Critical Safety messages.

You can also filter logs by selecting a date and time window:

1. Click the calendar icon in **Start Date** and select a date and time (or click in the **Start Date** field and manually enter a date and time).
2. Click the calendar icon in **End Date** and select a date and time (or click in the **End Date** field and manually enter a date and time).

FORT Manager immediately shows messages in the specified range.

3. Click the calendar icon and click **Clear** if you want to remove the date/time range.

Click **Download** to download a txt-, json-, or csv-formatted list of all messages that are stored in the FORT Manager database.

Note:

A downloaded log file may contain personal data — for example, a device or configuration name that identifies an individual, or a timestamped record of an action that can be attributed to a known operator.

Once downloaded, the file is outside FORT Manager's access controls and your organization is responsible for it. Store it accordingly, and see [Information You Send to FORT Support](#) (on page 230) before you attach it to a support request.

As events happen, the device records them in its own log store. Fetching copies the entries it holds into the FORT Manager database, where they are added to everything you have fetched before. **Download** gives you the contents of the FORT Manager database, not of the device — so a download includes entries the device has since overwritten, and does not include anything the device has recorded since your last fetch.

Note:

The device's log store is limited. For more information, see [Log Storage on the Device](#) (on page 210).

The FORT Manager database is not limited in the same way, which is why fetching regularly builds a longer history than the device can hold on its own.

The Logs Tab

Open a device from the **Devices** page and select the **Logs** tab. The tab lists the entries held in the FORT Manager database for that device, each with a timestamp, most recent first.

Note:

The tab opens on the last 24 hours. The Desktop App, by contrast, shows all levels and all types by default. If the tab looks emptier than you expect, widen the time range before concluding that entries are missing.

The tab shows what has already been fetched. Entries the device has recorded since the last fetch are not in the database and therefore not in the tab; to collect them, tether the device with the Desktop App and use **Logs > Fetch Logs** as described above. To download a log file as txt, json, or csv, use the FORT Manager Desktop App.

Important:

Seeing entries in this tab is not the same as having fetched them. The device overwrites its oldest entries when its log store fills. For more information, see [Log Storage on the Device](#) (on page 210). If you are investigating a fault, fetch with the FORT Manager Desktop App rather than relying on what the tab already shows.

The Health and History Tabs

Two more tabs in a device's detail view help with troubleshooting before you tether anything.

- Health
 - Shows the device's configuration state, its firmware version, its signal strength and the time it last synchronised with FORT Manager, on one page. Signal strength is reported as RSSI – Received Signal Strength Indicator – the same measure a WES Pro shows under **Device Attributes** and the same measure behind the **Low RSSI** log sub-type.
- History
 - Lists events for the device – deployments, configuration changes, and firmware updates – colour-coded by type, with a filter to show one type at a time. History records what was done to the device through FORT Manager; the **Logs** tab records what the device itself reported.

Note:

A weak signal is a common cause of intermittent faults. If the **Health** tab reports a degraded signal, check antenna selection and placement before investigating anything else. For more information, see [Antennas](#) (on page 193).

Note:

The **Health** tab reports what FORT Manager last heard from the device. While you are working offline it will be out of date, and the device remains the source of truth. For more information, see [Confirming Configurations After You Reconnect](#).

Log Storage on the Device

Each device stores its log entries in a fixed amount of space.

Important:

When the space is full, the device deletes its oldest entries to make room for new ones. Entries the device has overwritten cannot be recovered. Fetch the logs soon after you see a problem, and before you contact support — if the device keeps running, the entries covering the fault will eventually be overwritten by newer ones.

Entries you have already fetched are safe: they are held in the FORT Manager database and are not affected by what the device later overwrites. Fetching regularly is what builds a history longer than the device itself can hold.

Sharing Logs

Exported logs are sized to be shared by email or attached to a support request. For more information before you send exported logs, see [Information You Send to FORT Support](#) (on page 230).

Calibrating the Axis

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

To Verify Calibration

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

Each axis should read 0 when the fingerstick or thumbstick is centered and the full range should be from -2048 to 2047.

5. Press **1** to exit the menu.

If the values you see are incorrect, follow the steps in the next procedure to recalibrate your device.

To Recalibrate the SRC Pro

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

The screen displays an indicator of the current position and the full range that it has reached so far. You can press 2 at any point to exit the menu without applying the new calibration settings.

5. Let go of all fingersticks and thumbsticks when complete and press **1** to select the Finish option and accept the new calibration settings.
6. Press **1** or **2** to close.
7. Press the down arrow to scroll to and select **Axis Values** to verify the new calibration settings.
8. Move each individual fingerstick and thumbstick around its full range of motion.

Each axis should read 0 when the fingerstick or thumbstick is centered and the full range should be from -2048 to 2047.

9. Press **1** to exit the menu.

Troubleshooting Configurations

Table 104: Configuration Issues

Symptom	Root Cause	Resolution
A device cannot be added to a configuration in FORT Manager.	The device does not carry the radio the configuration uses. LRBLE configurations require model 1003.	Check the device model on its nameplate or on the Devices page and compare it against Device Models and Communication Methods (on page 51).
Ethernet is not offered as an interface for the EPC sender at the device level.	Long Range Bluetooth is selected for that sender on the General tab.	Return to the General tab and change the interface there. For more information, see Settings in a 2:1 LRBLE Configuration (on page 72).

Symptom	Root Cause	Resolution
The EPC sender's E-Stop does not stop the machine, but the SRC Pro's does.	The E-Stop device is wired to the wrong channel on the EPC sender, or the EPC sender is out of LRBLE range of the receiver.	Confirm the E-Stop is wired to the channel FORT Manager assigned, then confirm the EPC sender is within range throughout the work area. For more information, see Two-to-One over Long-Range Bluetooth (on page 59).
The machine will not restart after an E-Stop is released.	The other sender is still requesting a stop. The output stays off while either sender requests one.	Check both senders. Release the E-Stop on the WES Pro and confirm the E-Stop device wired to the EPC sender's Input 1 is also released. For more information, see Two-to-One with a WES Pro and an EPC (on page 61).
The WES Pro stops the machine but the EPC sender does not.	The E-Stop device is wired to the wrong input on the EPC sender, or the EPC sender is out of LRBLE range of the receiver.	Confirm the E-Stop is wired to Input 1 — Inputs 2 and 3 do nothing in this configuration. Then confirm the EPC sender is in range throughout the work area. For more information, see Settings in a WES Pro and EPC Configuration (on page 73).
The EPC sender stops the machine but the WES Pro does not.	The WES Pro is not paired to the receiver, is out of range, or its battery is flat.	Check the WES Pro's connection status and battery. For more information, see Connecting the WES Pro to a Receiver (on page 99).
You cannot select CANopen for a configuration with an NSC Pro receiver.	Expected. The NSC Pro supports J1939 only.	Select J1939 or disable CAN. For more information, see Data Interfaces (NSC Pro) (on page 163).

Symptom	Root Cause	Resolution
You want each sender to stop a different part of the machine.	Not supported in this configuration. Both senders act on Output 1.	Contact FORT support to discuss your requirement. For more information, see Two-to-One with a WES Pro and an EPC (on page 61).
Neither sender stops the machine, though both show as connected.	The output wired on the receiver does not match the Output to Control selection.	Check the selection, then confirm the receiver's J1 wiring uses the matching pin pair – 18 and 23 for Output #1, 17 and 22 for Output #2. For more information, see Choosing Which Output the Senders Control (on page 62).
The WES Pro stops the machine but the EPC sender does not.	The E-Stop device is wired to the input that does not match the output selection.	Wire it to Input 1 for Output #1 or Input 2 for Output #2. The other input is grayed out in FORT Manager and does nothing.
The machine stops on only one channel, or a channel fault is reported.	Only one pin of the output pair is wired.	Each output is a dual channel pair. Wire both pins. For more information, see EPC I/O Connector Pinout and Cable (on page 143).
You cannot change Output to Control on an existing configuration.	Expected. The setting is fixed when the configuration is created.	Build a new configuration with the output you need and load it onto your devices.
The receiver EPC does not appear in the device list.	Expected when the configuration uses LRBLE and CAN is disabled – the receiver has no settings to configure.	No action. The receiver is still in the configuration and still needs the configuration loaded onto it.
A device you own does not appear in the device list when you build a configuration.	The model has reached end of support, or the device was never registered.	Check the model against SRC Pro Models and Support Status (on page 171). If the model is supported, register the device in FORT Manager and try again.

Symptom	Root Cause	Resolution
A firmware update for a device is refused, or no update is offered.	No firmware is published for the model, either because it is already current or because the model has reached end of support.	Check the model against SRC Pro Models and Support Status (on page 171). An end-of-support device keeps the firmware it is running and continues to operate.
A control this guide describes is not present in FORT Manager.	The control does not apply to the configuration type or device model you selected, your role does not permit it, or the feature is not enabled for your organization.	Check the configuration type and device model against Device Models and Communication Methods (on page 51). If none of those explains it, see What You See in FORT Manager (on page 7).
The logs contain nothing from the period you are investigating, or start later than you expect.	The device has overwritten its oldest entries. The device stores a fixed amount and deletes the oldest to make room.	Nothing recovers overwritten entries. Reproduce the problem if you can, then fetch the logs immediately. To keep a longer history, fetch regularly rather than only when something goes wrong. For more information, see Log Storage on the Device (on page 210).

Proof Testing Pro Series Devices

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

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



Warning:

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

We recommend separate tests for each type of configuration, EPC-to-EPC, EPC-to-NSC Pro, SRC Pro-to-EPC, WES Pro-to-NSC Pro, etc. and we provide some examples below, but there are multiple combinations that we do not show. You should test the devices in the configurations that you have built and implemented.

Important:

The tests we show are basic guidelines for the types of tests you should perform, however, they are not exhaustive by any means and you must develop specific tests for your specific use case.

To Proof Test an EPC-to-EPC or EPC-to-NSC Pro Configuration



Warning:

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

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

1. Make sure that the sender and receiver are up and running and communicating with each other.
2. While safety is not being requested by the sender EPC, measure the voltages at the input pins of the sending EPC.

The voltages should be high and close to the supply voltage of the EPC.

- If any of the measured voltages is low, or much lower than the supply voltage, then a failure is present and you must inspect the wiring and the connected components to identify the source of failure.
- If no error is present, verify that the contactors of the relays attached to the receiver EPC(s) are all closed.

If any of the contactors is open, investigate the source of the failure.

3. Request safety (by activating the safety sensor/element attached to the input(s) of the sending EPC); the contactors of the relays attached to the receiver (EPC or NSC Pro) should all be open.

- Verify that both of the voltages at the input pins of the sending EPC indicate a low voltage.

If one or both voltages is high, it indicates that a failure is present at the external input wiring (this includes switches or solid state devices that are connected to the inputs of the EPC). Inspect the wiring and connected input devices to find the source of failure.

- Verify that both contactors on the relays connected to the receiver (EPCs(s) or NSC Pro(s)) are open. If one or both contactors are not open it indicates a failure is present. Inspect the wiring and the relays to find the source of failure.

4. Remove the request for safety and verify that the devices are up and running.

To Proof Test an SRC Pro-to-EPC or SRC Pro-to-NSC Pro Configuration

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

1. While the SRC Pro is up and running, use Machine Select and mode select to connect it to a running EPC or NSC Pro in the configuration.
2. While safety is not being requested, verify that the contactors on the receiver (EPC or NSC Pro) are all closed.

If any of the contactors is open, investigate and identify the source of the failure.

3. Request safety by pressing the E-Stop button on the SRC Pro and verify that both contactors on the relay connected to the receiver (EPC or NSC Pro) are open. If one or both contactors are not open, which indicates a failure, inspect the wiring and the relays to find the source of the failure.
4. Remove the request for safety on the SRC Pro and verify that the devices are up and running.

Repeat this procedure for each EPC or NSC Pro in the configuration.

To Proof Test WES Pro-to-EPC or WES Pro-to-NSC Pro Configuration

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

1. While the WES Pro is up and running, be certain that one or more EPCs²⁰ or NSC Pros in the configuration are running.
 2. While safety is not being requested, verify that the contactors on the receiver EPC are all closed.
- If any of the contactors is open, investigate and identify the source of the failure.
3. Request safety by pressing the E-Stop button on the WES Pro and verify that both contactors on the relay connected to the receiver (EPC or NSC Pro) are open.

If one or both contactors are not open, which indicates a failure, inspect the wiring and the relays to find the source of the failure.

4. Remove the request for safety on the WES Pro and verify that the devices are up and running.

Repeat this procedure for each EPC or NSC Pro in the configuration.

Wireless Communication Loss

A wide range of events can cause loss of signal events; for example, moving the transmitter out of range of the receiver, introducing enough interference or obstructions, turning off the transmitter, or anything else that prevents communication between the devices.

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

²⁰ A WES Pro can pair with one receiver only. The receiver can be an EPC or an NSC Pro. Consult the [Release notes](#) for information specific to the version of the product that you are using.

timeout period is exceeded, the safety processor on the EPC opens the safety relays to initiate the E-Stop command.

In other words, the **timeout** value defines the maximum time the receiver holds its outputs ON without receiving a valid safety message from the transmitter.

This value sets the worst-case delay between an E-Stop activation on the transmitter and output deactivation on the receiver (outputs will turn OFF no later than the configured timeout after the last valid message is received).

FORT recommends a 500 ms timeout as a starting point. You must assess whether a timeout longer than 500 ms is safe for your application, based on factors such as required stopping time/distance and applicable safety standards.

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, 500 ms, 750 ms, 1 sec, 3 sec, or 5 sec,²¹ to address any issues you find. You set the timeout value in FORT Manager when building a configuration. See [Building a Configuration](#) (on page 50).

In good communication conditions the actual response is typically much faster than the timeout; the timeout value only bounds the *worst case* under lossy or lost communication.

For example: With a 3-second timeout, receiver outputs may remain ON for up to 3 seconds after the E-Stop is pressed before turning OFF.



Warning:

FORT Manager provides a timeout of 250 msec that you can use for testing. Once you put your system into production, we strongly recommend that you do *not* keep this value as it has been shown to lead to frequent unstable communication. Consult with your system safety manager before using this timeout value.

²¹ The timeout values could change in later versions of the product. Be certain to check the [Release notes](#) for current information.

Notifications and Certifications

This appendix provides the FCC and ISED notices, RF exposure requirements, approved radio transmitter and antenna lists, and safety certifications for each Pro Series device.

EPC Notifications

This section contains the notifications for the Endpoint Controller (EPC). The next section contains the notifications for the Safety Remote Control Pro (SRC Pro).

FCC Notifications (EPC)



CAUTION:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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
2. This device must accept any interference received, including interference that may cause undesired operation.

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RF Exposure Information (EPC)

To comply with FCC/IC RF exposure limits for general population/uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

ISED (EPC)

The radio transmitters in the following table have been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed in the next table, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Les émetteurs radio du tableau suivant ont été approuvés par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antennes répertoriés dans le tableau suivant,

avec le gain maximum autorisé indiqué. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Approved radio transmitters:

Table 105: Table 93 EPC Approved Radio Transmitters

Function	Part #	FCC	ISED	Products
900MHz ISM	100-0235	2A818-100235	29381-100235	EPC/SRCP/WES/ NSC
WiFi/BT	CMP9377-UA	W7Z-WB609102	8254A-WB609102	EPC
LR BLE	BT832X	X8WBT832XE	4100A-BT832XE	SRCP/EPC/WES

The following table shows antenna type(s) that can be used with the transmitter (note that antennas are under review and subject to change):

Table 106: Table 94 EPC Approved Antenna Types

Manufacturer	Antenna Type	Model	Gain (dBi)	Impedance (Ω)
Linx Technologies Inc	Dipole, 1/2 Wave, Whip, Straight Antenna	ANT-915-IPW1-RPS	2.7	50
Linx Technologies Inc	Dipole, 1/2 Wave, Whip, Straight Antenna	ANT-2.4-CW-HWR-RPS	3.2	50
Linx Technologies Inc	Dipole, 1/2 Wave, Dual Band, Dome	ANT-W63-SPNF1	4.5 @ 2.4GHz 7.2 @ 5.0GHz	50

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

RF Exposure Requirements (EPC)

This equipment complies with ISSED RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements ISSED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps. The transmitter module may not be co-located with any other transmitter or antenna. Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

The declaration of conformity is available upon request.

EPC Certification

The EPC has been certified as SIL 3 for functional safety (per IEC 61508) by exida® corporation.

SRC Pro Notifications

This section contains the notifications for Safety Remote Control Pro (SRC Pro). The next section contains the notifications for the Endpoint Controller (EPC).

FCC Notifications (SRC Pro)



CAUTION:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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.

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates,

uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RF Exposure Information (SRC Pro)

This portable device complies with FCC RF exposure limits for general population/uncontrolled exposure. To ensure compliance, only use an authorized antenna type listed in this manual with this product. Use of an antenna type other than those specified may result in RF exposure levels exceeding the FCC requirements for RF exposure.

ISED (SRC Pro)

The radio transmitters in the following table have been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed in the next table, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Les émetteurs radio du tableau suivant ont été approuvés par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antennes répertoriés dans le tableau suivant, avec le gain maximum autorisé indiqué. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Approved radio transmitters:

Table 107: Table 95 SRC Pro Approved Radio Transmitters

Function	Part #	FCC	ISED
900MHz ISM	100-0235	2A818-100235	29381-100235
BT	BMD-300-A-R	2AA9B04	12208A-04
LR BLE	100-0308	2A818-1000308-1	29381-1000308A

Antenna type(s) that can be used with the transmitter (note that antennas are under review and subject to change):

Table 108: Table 96 SRC Pro Approved Antenna Types

Manufacturer	Antenna Type	Model	Gain (dBi)	Impedance (Ω)
Linx Technologies Inc	Dipole, 1/2 Wave, Whip, Straight Antenna	ANT-915-IPW1-RPS	2.7	50
Linx Technologies Inc	Dipole, 1/2 Wave, Whip, Straight Antenna	ANT-2.4-CW-HWR-RPS	3.2	50
Linx Technologies Inc	Dipole, 1/2 Wave, Dual Band, Dome	ANT-W63-SPNF1	4.5 @ 2.4GHz 7.2 @ 5.0GHz	50

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

RF Exposure Requirements (SRC Pro)

This portable device complies with ISED RF exposure limits for general population/uncontrolled exposure. To ensure compliance, only use an authorized antenna type listed in this manual with this product. Use of an antenna type other than those specified may result in RF exposure levels exceeding the ISED requirements for RF exposure.

The declaration of conformity is available upon request.

SRC Pro Certification

The SRC Pro has been certified as SIL 3 for functional safety (per IEC 61508) by exida® corporation.

WES Pro Notifications

This section provides notifications and certifications regarding the WES Pro.

FCC Notifications WES Pro



CAUTION:

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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.



CAUTION:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RF Exposure Information WES Pro

This portable device complies with FCC RF exposure limits for general population/uncontrolled exposure. To ensure compliance, only use an authorized antenna type listed in this manual with this product. Use of an antenna type other than those specified may result in RF exposure levels exceeding the FCC requirements for RF exposure.

ISED (WES Pro)

This radio transmitter (IC: 29381-1000415A) has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio [IC: 29381-1000415A] a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur

Approved radio transmitter(s):

Table 109: Table 97 WES Pro Approved Radio Transmitters

Function	Part #	FCC	ISED	Products
HP BLE	BT832X	X8WBT832XE	4100A-BT832XE	SRCP/EPC/WES

Antenna type(s) that can be used with the transmitter:

Table 110: Table 98 WES Pro Built-in Antenna

Manufacturer	Antenna Type	Model	Gain (dBi)	Impedance (Ω)
Pasternack	Rubber duck, omnidirectional	PE51RD1021	2.0	50

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

RF Exposure Requirements WES Pro

This portable device complies with ISED RF exposure limits for general population/uncontrolled exposure. To ensure compliance, only use an authorized antenna type listed in this manual with this product. Use of an antenna type other than those specified may result in RF exposure levels exceeding the ISED requirements for RF exposure.

The declaration of conformity is available upon request.

WES Pro Certification

The WES Pro has been certified as SIL 3 for functional safety (per IEC 61508) by exida® corporation.

NSCP Notifications

This section contains the notifications for the Nano Safety Controller Pro (NSCP).

FCC Notifications (NSCP)

**CAUTION:**

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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
2. This device must accept any interference received, including interference that may cause undesired operation.

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RF Exposure Information (NSCP)

To comply with FCC/IC RF exposure limits for general population/uncontrolled exposure, the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

ISED (NSCP)

The radio transmitters in the following table have been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed in the next table, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Approved radio transmitters:

Table 111: Table 93 NSCP Approved Radio Transmitters

Function	Part #	FCC	ISED	Products
900MHz ISM	100-0235	2A818-100235	29381-100235	EPC/SRCP/WES/ NSC
LRBLE	BT832X	X8WBT832XE	4100A-BT832XE	EPC

The following table shows antenna type(s) that can be used with the transmitter (note that antennas are under review and subject to change):

Table 112: Table 94 NSCP Approved Antenna Types

Manufacturer	Antenna Type	Model	Gain (dBi)	Impedance (Ω)
Linx Technologies Inc	Dipole, 1/2 Wave, Whip, Straight Antenna	ANT-915-IPW1-RPS	2.7	50
Linx Technologies Inc	Dipole, 1/2 Wave, Whip, Straight Antenna	ANT-2.4-CW-HWR-RPS	3.2	50
Linx Technologies Inc	Dipole, 1/2 Wave, Dual Band, Dome	ANT-W63-SPNF1	4.5 @ 2.4GHz 7.2 @ 5.0GHz	50

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

RF Exposure Requirements (NSCP)

This equipment complies with ISSED RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

The declaration of conformity is available upon request.

NSCP Certification

The NSCP has been certified as SIL 3 for functional safety (per IEC 61508) by exida® corporation.

Agreements and Data Protection

This appendix points you to FORT's end-user, OEM, and data processing agreements, and summarizes what personal data FORT Manager and the devices themselves hold, where it is stored, and how to remove a user from your organization.

You can view the [End-User Agreement](#) on the FORT Robotics website.

You can view the [OEM Supply and License Agreement](#) on the FORT Robotics website.

You can view the [Data Processing Agreement](#) on the FORT Robotics website. The Data Processing Agreement sets out how FORT Robotics handles personal data on your behalf when you use FORT Manager.

The rest of this appendix summarizes what personal data the Pro Series and FORT Manager hold, and what you can do about it. It is a summary for integrators and administrators. The agreements above are the binding documents; where this appendix and an agreement differ, the agreement governs.

Personal Data in FORT Manager

FORT Manager holds account information for the people in your organization. When you add someone to your organization you supply their email address and choose a role, and FORT Manager records their membership of your organization.

Table 113: Personal Data Held by FORT Manager

Data	Where It Comes From
Email address	You supply it when you add the person to your organization.
User Role	You choose one of Admin, Config Manager, Device Manager, or Operator.
Organization membership	Recorded when the account is created.

The following list outlines the different user roles:

- **Admin:** Manage all aspects of FORT Manager, including users.
- **Config Manager:** Create, edit, and delete both configurations and devices; Apply firmware and configurations to devices.
- **Device Manager:** Enroll, edit, and delete devices; Apply firmware and configurations to devices.
- **Operator:** View and apply firmware and configurations to devices.

On the **Users** page, roles are colour-coded so you can scan access levels at a glance, and the role chips above the list filter to one role at a time.

Who is responsible for what

Your organization decides who gets a FORT Manager account and what role each person holds. Under data protection law that makes your organization the **controller** of your users' personal data. FORT Robotics operates the platform on your behalf, which makes FORT the **processor**. The Data Processing Agreement sets out the terms of that relationship, including how FORT assists you when one of your users exercises their rights.

Where the Data is Held

FORT Manager runs in the hosting region.

Note:

FORT Robotics uses other companies to help operate FORT Manager. Before adding or replacing one of them, FORT tells you. For more information, see [Sub-processor Change Notifications](#) (on page 229)

Personal Data on the Devices Themselves

Pro Series devices do not hold FORT Manager account information. Personal data reaches a device only where you put it there, in fields whose contents you choose:

- Configuration names and device names.
- **Custom Display Text Line 1** through **Line 4**, the text an application sends to an SRC Pro screen. For more information, see [SRC Pro User Display Text String Message](#) (on page 116).

Important:

Text you send to a device travels over the machine's CAN bus or serial link as part of a control message. Those links are internal to the machine and are not protected in the way that the safety radio link is. Do not put a person's name or other personal data in a device name, a configuration name, or custom display text.

API Key Expiry

On the **Organization** page, each API key shows its expiry state. A key with an expiry date set is shown in green; a key that never expires is shown in red.

Note:

A key that never expires is a standing credential. If it is disclosed it stays valid until someone notices and revokes it. Set an expiry on every key, and treat a never-expiring key that holds the Admin role as something to fix rather than something to note.

Use the search box and the role filter above the list to find keys in a large inventory.

Note:

An expired key stops working. If a script or a CLI login that worked yesterday is refused today, check the key's expiry state before anything else. For more information, see [Logging In](#).

API Key Roles

An API key carries a role that determines what it can do, set with `PUT /v1/organizations/{orgId}/apiKeys/{keyName}/role`. The role set for API keys is wider than the role set for users:

Table 114:

Role	Users	API Keys
Operator	Yes	Yes
Device Manager	Yes	Yes
Config Manager	Yes	Yes
Admin	Yes	Yes
Service	No	Yes
Key Manager	No	Yes

Note:

Because the two sets differ, the role filter on the **Users** page and the role filter on the API keys list do not offer the same choices.

Sub-Processor Change Notifications

FORT Robotics uses other companies — sub-processors — to help operate FORT Manager, for example to host it. Before FORT adds a new sub-processor or replaces an existing one, FORT notifies its customers, so that you have the opportunity to review the change and object to it before it takes effect.

To receive these notifications, subscribe to the sub-processor notification list on the FORT Robotics website.

FORT gives at least **X** days' notice of a change.

If you object to a change, follow the process in the Data Processing Agreement. Your rights on objection, including any right to terminate, are set out there.

Note:

Make sure the person who receives these notifications is someone who can act on them. The notification period only helps if it reaches your data protection contact rather than the engineer who set up the devices.

Removing a User

When someone leaves your organization, or asks you to erase their personal data, remove their FORT Manager account using the steps outlined below.

1. Log in to FORT Manager. If you're using the FORT Manager Desktop App, confirm you have online connectivity.
2. Navigate to the **Users** tab on the left navigation.
3. Select the FORT Manager account targeted for removal.

To find an account in a long list, filter with the role chips above the list.

Note:

An invitation that has not been accepted is not an account. Outstanding invitations are counted by the badge on the **Pending** tab and are withdrawn from there, not through this procedure.

4. In the **Actions** column, select **Delete**. Alternatively, you can select the FORT Manager account and navigate to that account's page containing the name, profile image, email address, and user role. Select **Delete** in the top, right corner to remove the account from FORT Manager.

To remove a FORT Manager account using the FORT Manager API interface, use `DeleteUser`. For more information, see [FORT Manager API: DeleteUser](#).

Note:

FORT retains all account information indefinitely when it is deleted via FORT Manager desktop app, web app, or FORT Manager API. For more information, contact FORT support at support@fortrobotics.com

Note:

Removing a user from FORT Manager has no effect on data you have already exported. Downloaded log files, configuration files, and support ticket attachments stay wherever you put them

Information You Send to FORT Support

When you file a request on the Customer Support Portal, or email support@fortrobotics.com, you typically send some or all of the following:

- Device serial numbers and model numbers.
- Configuration names and device names, which you chose.
- Log files retrieved through the FORT Manager Desktop App. For more information, see [Using Logs](#) (on page 206)
- Screenshots, which may show account names or email addresses.

FORT handles what you send under the Data Processing Agreement. Even so, review an attachment before you send it. Device logs are designed to be shared whole — they are sized to attach to an email or a support request — so send the complete log rather than an extract, and apply the smallest-amount principle to screenshots and other material instead.

Note:

If a support request needs data you would rather not attach to a ticket, say so in the request and ask support how to send it.