Safety System Products

# Safety Simplifier

## Installation and Safety Manual

### Generation 2



**Version 2.3**
**November 2026**

**SSPN**
**Safety System Products North AB**

# Installation and Safety Manual

Manual version 2.3.0 | 2026-11-12

SSPN Safety System Products North AB
Tullkammarvägen 14, S-439 31 Onsala, Sweden
www.sspn.se | info@sspnorth.se | Phone: +46 10 212 31 50 | Org: 559050-4105
Person authorized to compile the technical documentation and to sign the EU Declaration of Conformity: Jesper Ribbe

SSPN Safety System Products North AB (SSPN) reserves the right to revise this document at any time without prior notice. The latest revision is available at www.sspn.se/downloads/. Users are responsible for ensuring that they work from the latest revision.

SSPN does not warrant that this document is free from errors or omissions. Please report any error found to info@sspnorth.se.

Depending on the features of your device, descriptions of optional functions may be provided as additional sheets complementing this document.

**This document supersedes all previous versions.**

## Revision History

| Version | Date | For firmware | Changes to this manual |
|---|---|---|---|
| 2.3.0 | 2026-11-12 | 2.3.x | • New format: the manual's version follows the firmware's major.minor; the cover and the page footers show it, the full manual version is on this page; this revision history.<br>• New: the Modbus and CANlibre chapters; Modbus RTU on the USB port, and the LED-display connector for an SSPN Black Channel implementation or an RFID reader (Communication Interfaces, Principle Layout and Design).<br>• New in the technical manual: the General Black Channel chapter, with the UART line to an SSPN Black Channel implementation.<br>• Changed: Operating Voltage Specifications, the default voltage limits.<br>• Changed: Firmware Update (Bootloader), a logic compiled for another firmware version.<br>• Changed: Communication Interfaces and the Radio Equipment Directive, Ethernet only through a separate SSPN Black Channel implementation.<br>• Changed: Cybersecurity, Secure Installation: physical access including the memory card and the debug pins, the CAN bus, the LED-display connector, memory card handling, loss of the radio link.<br>• Changed: Cybersecurity, Protection of Safety Functions: no return to firmware without signed updates.<br>• Changed: every safety message follows the hazard, consequence and avoidance structure; Safety Messages replaces Symbols.<br>• Removed: the last page; its details are on this page. |
| 1.0 | 2026-10-13 | 2.2.x | Initial publication. |

## Table of Contents

1 Purpose of the Manual ..... 5
1.1 Provision of Instructions and Declaration of Conformity ..... 5
1.2 Abbreviations ..... 5
1.3 Authorized Personnel ..... 5
1.4 Safety Instruction for Authorized Personnel ..... 5
1.5 Safety Messages ..... 5
1.6 Device Application ..... 6
1.6.1 Classification and Conformity Assessment ..... 6
1.7 Contact ..... 6
1.8 Warranty ..... 6
2 Safety Information ..... 7
2.1 Design and Safety Assessment ..... 7
2.2 Communication Standards Compliance ..... 7
2.2.1 Radio Equipment Directive ..... 7
2.3 Reasonably Foreseeable Misuse ..... 7
2.4 Residual Risks ..... 7
2.4.1 Electrical Hazards ..... 8
2.4.2 Communication Loss Between Networked Units ..... 8
2.4.3 Configuration Error or Unauthorized Modification ..... 8
2.4.4 Environmental and Installation Risks ..... 8
2.4.5 Mechanical Vibration and Shock Damage ..... 8
2.4.6 Programming and Logic Risks ..... 9
2.4.7 Integration and System-Level Risks ..... 9
2.4.8 Residual Risk Management Summary ..... 9
2.4.9 Responsibility Statement ..... 9
3 Maintenance and Service ..... 10
3.1 Periodic Inspection ..... 10
3.2 Response to Malfunction ..... 10
3.3 Liability Disclaimer ..... 10
3.4 Transport, Handling and Storage ..... 11
3.5 Disposal Considerations ..... 11
4 Safety Simplifier Features ..... 12
4.1 Simplifier Manager and Software Version Control ..... 12
4.2 Hardware Components ..... 12
4.3 Supported Safety Devices ..... 12
4.4 Output Configurations ..... 13
4.5 Combined I/O Functions ..... 13
4.6 Redundant Relay Outputs ..... 13
4.7 I/O Non-Safety Data ..... 13
4.8 LED Display ..... 13
4.9 Model Variants ..... 13
4.10 Housing Material ..... 13
5 System Design and Safety Principles ..... 14
5.1 Operating Modes ..... 14
5.2 Safe State Definition and De-energization Principle ..... 14
5.3 Failure and Communication Loss Handling ..... 14
5.4 Subsystem Deployment Configurations ..... 14
5.5 Wireless Network Design ..... 15
5.5.1 Understanding Radio Quality ..... 15
5.5.2 Redundancy and Minimal Reaction Times ..... 15
5.5.2.1 Optimal Wireless Configuration ..... 15
5.5.3 Internal and External Antenna ..... 16
5.6 Programming and Requirements ..... 16
5.7 Safety and Non-Safety Functions ..... 17
5.8 Technical and Environmental Notes ..... 17
5.8.1 Non-Ionising Radiation and Radio Frequency Exposure ..... 17
6 I/O & Relay Hardware Architecture ..... 18
6.1 Safety Relay Outputs ..... 18
6.2 Solid-State Transistor Outputs ..... 18
6.2.1 OSSD ..... 18
6.2.2 Coded Pulse Trains (A, B, C, D) ..... 19
6.3 Input Structure and Configuration ..... 19
6.4 Handling External I/O Faults ..... 19
7 Safety Calculations and Compliance ..... 21
7.1 Mission Profile for Failure Rate Derivation ..... 21
7.2 Safety Standard Classifications ..... 21
7.3 Requirements for Achieving Safety Categories (EN ISO 13849-1:2023) ..... 22
7.3.1 Category 4 (Highest Integrity) ..... 22
7.3.2 Category 3 (High Integrity) ..... 22
7.3.3 General Compliance Note ..... 22
7.4 Calculating PFH D Values ..... 22
7.4.1 Component-Level PFH D Values ..... 22
7.4.2 System-Level PFH D Calculation Formulas ..... 23
7.4.3 Worked Example: Black Channel Communication Path ..... 23
7.5 Calculating System Reaction Time ..... 23
7.5.1 System Reaction Time Formulas ..... 23
7.5.2 Chained Communication Interfaces and Age Forwarding ..... 24
7.6 General Functional Test Requirements ..... 24
8 Principle Layout and Design ..... 26
8.1 Configuration Availability ..... 27
8.2 Dimensions ..... 27
8.2.1 Outer Dimensions ..... 27
8.2.2 Inner Dimensions ..... 27
9 Mounting Procedures ..... 28
9.1 Small Bracket Installation ..... 28
9.2 Large Bracket Installation ..... 28
9.3 Direct Surface Mounting (Without Brackets) ..... 28
9.4 Center Knockout Preparation ..... 28
9.5 Multiple Enclosure Stacking ..... 28
9.6 Mounting Accessories ..... 28
9.7 Scope of Supply ..... 29
9.8 Spare Parts and Accessories ..... 29
10 Electrical Installation ..... 30
10.1 Power Supply Requirements ..... 30
10.2 Operating Voltage Specifications ..... 30
10.3 Terminal Specifications and Wiring ..... 30
10.4 Installation Standards Compliance ..... 30
10.5 I/O Connections Procedure ..... 31
11 Bus Communication via Radio and/or RadioCAN ..... 32
11.1 SimpleCAN ..... 32
11.1.1 Network and Node Limits ..... 33
11.1.2 Master Node Requirement ..... 33
11.1.3 SimpleCAN Data Blocks ..... 33
11.1.4 Calculating $\mathrm{PFH}_D$ Value ..... 33
11.1.5 Calculating Maximum Reaction Time ..... 33
11.1.6 Cycle Time ..... 33
11.1.7 Timeout Configuration ..... 33
11.1.8 Installation and Commissioning ..... 34
11.1.9 Diagnostics and Maintenance ..... 34
11.1.9.1 No Communication ..... 34
11.1.9.2 Online Mode ..... 34
12 Modbus ..... 35
12.1 Connecting ..... 35
12.2 Function codes ..... 35
12.3 Register map ..... 35
12.4 Examples ..... 35
12.5 Aux input timeout ..... 35
12.6 Memory blocks ..... 36
12.7 Black channel status ..... 36
12.8 Exceptions ..... 36
13 CANlibre ..... 37
13.1 Settings ..... 37
13.2 Frames ..... 37
13.3 Received frames ..... 37
13.4 Sending TPDOs ..... 37
13.5 NMT states ..... 37
13.6 Aux input timeout ..... 37
14 Electrical Wiring with Safety Devices ..... 39
14.1 Two-Hand Control Devices ..... 39
14.2 Safety Devices with OSSD Outputs ..... 39
14.3 Safety Gate Limit Switches ..... 39
14.4 Relay Outputs for Contactors with Feedback Supervision ..... 40
14.5 Relay Outputs for Machines and Safety Devices ..... 40
14.6 OSSD Outputs for Machines, Contactors, and Safety Devices ..... 40
15 LED Display ..... 41
15.1 Navigation Procedure ..... 41
15.2 Menu Overview ..... 41

15.3 Maintenance States ... 41
15.3.1 Configuration Mode ... 41
15.3.2 Fatal Error Indication ... 41
15.3.3 Firmware Update (Bootloader) ... 41
16 Menu Structure ... 43
16.1 N Menu ... 43
16.2 I/O Menu ... 43
16.3 U Menu ... 43
16.4 M Menu ... 44
16.5 Radio Menu ... 44
16.6 CAN Menu ... 44
16.7 Fatal Error Mode ... 44
16.7.1 Fatal Error Condition ... 44
16.8 Error Codes ... 44
17 Cybersecurity ... 45
17.1 Security by Design ... 45
17.2 Software and Firmware Components ... 45
17.3 Communication Interfaces ... 45
17.4 Intended Operational Environment ... 45
17.5 Protection of Safety Functions (Machinery Regulation 2023/1230, Annex III, EHSR 1.1.9 and 1.2.1) ... 45
17.6 Secure Installation ... 46
17.7 Secure Configuration ... 46
17.8 Firmware Updates ... 47
17.9 Product Security Support Lifecycle ... 47
17.10 Security Updates and Advisories ... 47
17.11 Reporting a Vulnerability ... 47
17.12 Responding to a Suspected Security Incident ... 47
17.13 Decommissioning ... 47
17.14 Known Vulnerabilities ... 48
18 Performance Specifications ... 49
18.1 General Technical Data ... 49
18.2 I/O and Contact Specifications ... 49
18.3 Wire Specifications ... 50
18.4 Environmental and Durability ... 50
18.5 Radio Frequency (RF) Channels ... 50
18.6 CAN Communication Card ... 51
18.7 CAN 2.0 ... 52

# 1 Purpose of the Manual

**Original instructions.** This document constitutes the original instructions for the Safety Simplifier product series within the meaning of Directive 2006/42/EC and Regulation (EU) 2023/1230. It has been drawn up in English by SSPN. Any version issued in another language is a translation of these original instructions and is marked **"Translation of the original instructions."**

This manual contains all essential information required for the assembly, installation, safe operation, and disassembly of the Safety Simplifier product series by SSPN. It must **remain accessible and legible** throughout the entire operational life of the device. Before using the equipment, read this manual thoroughly. Ensure that future owners and users receive this manual, along with any supplementary documentation provided by the manufacturer.

**The manual is valid until new documentation is published. The latest version of these original instructions is available at www.sspn.se.**

## 1.1 Provision of Instructions and Declaration of Conformity

In accordance with Regulation (EU) 2023/1230, this manual and the EU Declaration of Conformity are provided in digital format and remain accessible online for at least 10 years after the product has been placed on the market, and for the expected lifetime of the product. Customers may request a printed paper copy of this documentation free of charge within one month of purchase.

**Accessing the instructions**

- The Safety Simplifier product label carries the website address and the postal address of SSPN. These instructions are published on that website, at www.sspn.se/downloads/.
- The instructions are published in a format that can be printed, downloaded, and saved on an electronic device, so that they remain available when the machinery is not operational.
- To request a paper copy free of charge, contact SSPN at info@sspnorth.se, stating the product designation and the date of purchase.

**EU Declaration of Conformity**
The EU Declaration of Conformity for the Safety Simplifier is issued by SSPN as document **SSPN-Q202.** It states the Union legislation applied to the product and the harmonised standards used.

EU Declaration of Conformity and product documentation:
www.sspn.se/downloads/
Select **"Certificates & Declarations"** to access the applicable declaration.

**Language**
These instructions are supplied in a language accepted by the Member State in which the Safety Simplifier is placed on the market or put into service. Contact SSPN if the instructions are required in a further official language of the Union.

## 1.2 Abbreviations

| | |
|---|---|
| CAN | Controller Area Network |
| DC | Diagnostic coverage |
| ESPE | Electro-sensitive Protective Equipment |
| EUC | Equipment Under Control |
| MRT | Mean Repair Time |
| OSSD | Output Signal Switching Device |
| PCB | Printed Circuit Board |
| PFH | Average frequency of a failure per hour |
| $PFH_D$ | Average frequency of a dangerous failure per hour |
| PL | Performance Level |
| PLC | Programmable Logic Controller |
| SFF | Safe Failure Fraction |
| SIF | Safety Instrumented Function |
| SIL | Safety Integrity Level |
| SSPN | Safety System Products North AB |
| USB | Universal Serial Bus |

## 1.3 Authorized Personnel

The Safety Simplifier may only be assembled, installed, programmed, commissioned, maintained, and decommissioned by personnel who possess sufficient competence. **Competent personnel are defined as individuals who meet the following criteria:**

- Have experience with industrial machinery and safety-related control systems
- Are knowledgeable in relevant safety standards, including the Machinery Directive and other applicable regulations
- Possess a foundational understanding of electronics
- Are proficient in programming Safety PLC systems
- Have received formal training in the use of both the Safety Simplifier and Simplifier Manager
- Have thoroughly read and understood the contents of this manual

It is recommended to have Simplifier Manager installed on a nearby computer, along with its user manual and one or more Safety Simplifier units available for testing. This setup enables users to follow the examples provided and gain practical insight into how the functions operate.

## 1.4 Safety Instruction for Authorized Personnel

All tasks outlined in this manual must be performed exclusively by **qualified personnel who have been authorized by the plant owner.** Before operating the device, it is essential to read and fully understand the contents of this manual. Personnel must be familiar with all relevant industrial safety standards and accident prevention regulations. Compliance with applicable national and international laws is mandatory for assembly, installation, and routine technical inspections.

## 1.5 Safety Messages

Safety messages in this manual are marked by a signal word that gives the level of the hazard. The general warning sign (ISO 7010 W001) marks a hazard to persons.

**⚠ DANGER**

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

**⚠ WARNING**

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

**⚠ CAUTION**

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

**NOTICE**

Indicates information not related to personal injury. If not observed, the product or other property could be damaged.

**Note:** Additional information that is not a safety message.

## 1.6 Device Application

The Safety Simplifier is intended for use in machinery covered by the Machinery Directive 2006/42/EC (or Machinery Regulation (EU) 2023/1230 for products placed on the market from 20 January 2027) and for safety circuits according to EN ISO 13849-1 and IEC 61508 up to PL e, Cat. 4 and SIL 3.

See technical data and CE declaration for Safety Simplifier for more information on intended use. It is the responsibility of the machine or plant manufacturer to ensure the system operates correctly and reliably as a whole.

### 1.6.1 Classification and Conformity Assessment

The Safety Simplifier is a **safety component** as defined in Regulation (EU) 2023/1230 — a logic unit that ensures safety functions. It is placed on the market as an independent safety component and does not, by itself, constitute a complete safety solution for a machine.

Products of this category — "Logic units to ensure safety functions" — are listed in **Annex I, Part B, item 17** of Regulation (EU) 2023/1230, and were listed in **Annex IV, item 21** of Directive 2006/42/EC under the preceding legislation. They are not listed in Annex I Part A, which covers specified high-risk mechanical machinery and safety systems embedding self-evolving behaviour based on machine learning.

**Permissible conformity assessment routes**

For products listed in Annex I Part B, Article 25(3) of the Regulation permits either of the following routes:

- **Internal production control (Module A)** — permitted only where harmonised standards covering all applicable essential health and safety requirements have been applied in full.
- **EU-type examination (Module B) followed by conformity to type (Module C)** — carried out with an accredited notified body.

The route applied to the Safety Simplifier is EU-type examination with a notified body, followed by conformity to type. The certificate is identified below.

**EC Type-Examination**

The Safety Simplifier has been type-examined by a notified body in accordance with **Annex IX of Directive 2006/42/EC.**

| Item | Detail |
|---|---|
| Certificate | EC Type-Examination Certificate **C901009,** issue 2 |
| Notified body | RISE Research Institutes of Sweden AB, **Notified Body No. 0402** |
| Procedure | Annex IX of Directive 2006/42/EC, for products listed in Annex IV, item 21 |
| Scope | Safety Simplifier SXXLDRBCAYY — see the Model Variants section |
| Basis of certification | Type test according to **EN 61508:2010,** SIL 3 |
| Corresponding performance level | According to Table 3 of **EN ISO 13849-1:2023,** a subsystem developed to SIL 3 in EN 61508 corresponds to an SRP/CS of **PL e** in EN ISO 13849-1:2023. The product also fulfils **Category 4** according to EN ISO 13849-1:2023. |
| First issued | 2023-11-28 |
| Current issue | Issue 2, dated 2025-08-29 |
| Technical file | Manufacturer's technical file dated 2025-07-02 |
| Valid until | 2028-11-28, provided that the certified specifications are not significantly modified |

The current validity of the certificate can be verified on the RISE website. The installation and safety information supplied by SSPN has been inspected by the notified body and found to fulfil the relevant requirements of the Directive.

The Union legislation and the harmonised standards applied to the Safety Simplifier are listed in the EU Declaration of Conformity.

**Validity under the Machinery Regulation**

Regulation (EU) 2023/1230 applies to products placed on the market from **20 January 2027.** EC type-examination certificates issued under Directive 2006/42/EC remain formally valid until their stated expiry date — **2028-11-28** for certificate C901009 — provided that no major modification is made to the product design or to the relevant harmonised standards.

## 1.7 Contact

In the event of a hazardous malfunction involving a Safety Simplifier unit, please contact SSPN using the contact details on page 2 of this document. Additional contact information is available at www.sspn.se.

SSPN may also be reached through their authorized distribution network. Distributors are responsible for forwarding critical information that supports the correct use of the Safety Simplifier and helps prevent hazardous situations.

## 1.8 Warranty

SSPN products are covered by a warranty against defects in materials, construction, and manufacturing. During the warranty period, SSPN may replace the product or any faulty components. All warranty-related work **must be performed** either by SSPN or by an authorized service center designated by SSPN.

**The warranty does not cover the following:**

- Normal wear and tear resulting from regular use
- Failure of consumable components
- Damage caused by unauthorized modifications
- Faults due to incorrect installation
- Faults resulting from improper use
- Water or moisture damage caused by exposure to environments exceeding the applicable IP rating

# 2 Safety Information

Always observe the safety instructions outlined in this operating manual, which are marked as safety messages with a signal word (see Section 1.5). Adhere to all applicable national regulations concerning installation, safety, and accident prevention.

**The information provided is subject to change without liability.** Technical modifications may be made to improve performance. Provided that all safety instructions and guidelines for assembly, installation, operation, and maintenance are followed, the risks arising from the Safety Simplifier itself are reduced as far as is reasonably practicable by design. Residual risks nevertheless remain; these are described in the Residual Risks section of this chapter and must be assessed and managed at machine level by the integrator and the end user.

**Before beginning installation, disconnect both the plant and the device from the power supply.** Safety functions must never be bypassed, disabled, or otherwise rendered ineffective (see Reasonably Foreseeable Misuse).

## 2.1 Design and Safety Assessment

Before designing a safety system, a **comprehensive safety assessment** must be conducted in accordance with the **Machinery Directive 2006/42/EC** or **Machinery Regulation (EU) 2023/1230** and other relevant standards.

The **functional safety** of the Safety Simplifier is guaranteed when used as a component within a properly designed system. However, the **design and programming** of the safety system—using Safety Simplifier and Simplifier Manager software—is the **sole responsibility of the installer or user.**

The complete system must be thoroughly **tested with all connected components** to ensure it meets the required safety standards. Any **modification** to the safety system necessitates **retesting and updated documentation.**

The Safety Simplifier system is designed to achieve up to:

- **SIL 3** (IEC 61508); as a subsystem, **maximum SIL 3** under EN IEC 62061:2021
- **PL e / Category 4** (ISO 13849-1)

Note: The actual **SIL and PL levels** of an application depend on the parameters of all safety-related components, including safety devices, machine control systems, and other relevant equipment. All applicable standards for the specific application must be followed.

Refer to the **CE Declaration of Conformity** for details on the standards for which the Safety Simplifier is approved and intended.

## 2.2 Communication Standards Compliance

The CAN and radio safety communication channels used in the Safety Simplifier comply with IEC 61784-3:2016. These channels are utilized solely as physical layers within the system.

### 2.2.1 Radio Equipment Directive

Safety Simplifier variants fitted with the 2.4 GHz radio card are **radio equipment** within the meaning of Directive 2014/53/EU (Radio Equipment Directive) and are subject to that Directive in addition to the machinery legislation. The radio interface is assessed against the applicable harmonised standards for efficient use of the radio spectrum, electromagnetic compatibility, and the protection of health and safety, including the exposure of persons to electromagnetic fields.

The cybersecurity essential requirements in Article 3(3)(d), (e) and (f) of Directive 2014/53/EU, activated by Commission Delegated Regulation (EU) 2022/30, apply to internet-connected radio equipment, to wearable, childcare and toy radio equipment, and to radio equipment capable of transferring monetary value. The Safety Simplifier is none of these — it has no Ethernet interface and no internet connectivity of its own, and its radio carries only safety communication between units — so those requirements do not apply to it. Ethernet is available only through an SSPN Black Channel implementation fitted to the LED-display connector, a separate product with its own conformity assessment. The cybersecurity measures built into the product are described in the Cybersecurity chapter of this manual.

Refer to the EU Declaration of Conformity for the complete list of Union legislation and harmonised standards applied to the Safety Simplifier.

## 2.3 Reasonably Foreseeable Misuse

The following uses are reasonably foreseeable but are **not permitted.** They are listed so that the machine integrator can address them in the machine risk assessment, in the operator instructions, and in training.

**The Safety Simplifier must not be:**

- Used as the sole safety measure for a machine without a completed machine-level risk assessment
- Programmed so that a stop or off function is generated by a logic “1”, an energized signal, or a closed circuit, contrary to the de-energization principle
- Used with non-safety I/O, memories, or logic signals to implement a safety function
- Configured or reprogrammed by personnel who do not meet the competence requirements stated in the Authorized Personnel section
- Operated with the configuration password shared beyond the authorized group, left at a default value, or left unchanged after personnel changes
- Returned to service after a configuration change, a firmware update, or a repair without complete functional verification of all affected safety functions
- Operated outside the environmental limits stated in the technical data, or with a damaged enclosure, ventilation membrane, cable gland, or terminal
- Installed so that a loss of radio or CAN-bus communication, or the transition of any unit to the Safe State, creates a hazardous condition
- Modified, opened for repair, or fitted with spare parts or accessories not approved by SSPN
- Relied upon to disconnect an external voltage source; the Safety Simplifier cannot switch off voltage originating outside its own supply
- Operated beyond the mission time determined for the safety system in which it is used

**⚠ DANGER**

**Defeated safety function**
While a safety function implemented with the Safety Simplifier is bypassed, disabled or otherwise defeated — including the temporary bridging of inputs during commissioning or fault finding — the machine does not stop when a person enters the hazard zone. This will result in death or serious injury.

- Never bypass, disable or defeat a safety function.
- Where such an intervention is unavoidable, cover it by a documented and supervised procedure at machine level, and fully verify the safety function before the machine is returned to service.

## 2.4 Residual Risks

Despite the implementation of protective measures in the design and construction of the Safety Simplifier, certain residual risks remain that cannot be entirely eliminated through technical means. The following residual risks must be managed through proper installation, operation, maintenance, and user awareness.

> **Note:** The machine integrator and end user are responsible for conducting a complete risk assessment of the entire machine system. The residual risks listed below pertain specifically to the Safety Simplifier component and must be integrated into the overall machine risk assessment.

### 2.4.1 Electrical Hazards

**⚠ WARNING**

**Electric shock from a wrong supply**
Connecting the unit to a voltage above the rated range **(>33 VDC)** or to an AC source can cause an electric shock, which could result in death or serious injury.
- Connect only a SELV or PELV supply within the rated range, and apply the measures below.

**Mitigation Measures:**

- Verify all wiring against circuit diagrams before energizing
- Use only a SELV or PELV power supply with protective separation from the mains — see Power Supply Requirements for the accepted sources
- Ensure all connected cables and devices are rated for isolation at 240V AC
- Install an external 2.5 A fast-acting fuse in the supply line (mandatory — see Power Supply Requirements)
- Connect 0V terminal to protective bonding circuit per EN 60204-1

**User Responsibility:**

- Only qualified electrical personnel shall perform installation
- Use a multimeter to verify voltage levels before connection
- Never operate the device with damaged cables or terminals

### 2.4.2 Communication Loss Between Networked Units

**⚠ WARNING**

**Unexpected machine behaviour on loss of communication**
Loss of radio or RadioCAN (CAN-bus) communication between Safety Simplifier units sets the safety signals to logic "0" (safe state). If the logic is not programmed for this transition, the machine can behave unexpectedly, which could result in death or serious injury.
- Program and test every function that depends on networked signals for loss and return of communication, as listed below.

**Mitigation Measures:**

- System is designed to fail to safe state (de-energized) on communication loss
- Use communication timeout settings (T(C)) appropriate to application response requirements
- Program logic to require restart after communication restoration for critical functions
- You can use both radio AND RadioCAN (CAN-bus) for redundant communication paths where available

**User Responsibility:**

- Configure startup settings for all inputs dependent on networked signals
- Test communication loss scenarios during commissioning
- Ensure machine risk assessment accounts for communication loss behavior
- Maintain clear line-of-sight for optimal radio communication (avoid metal obstructions)
- Follow CAN-bus cable length and termination requirements (see Bus Communication chapter)

### 2.4.3 Configuration Error or Unauthorized Modification

**⚠ WARNING**

**Faulty or unauthorized change to the safety logic**
Incorrect programming, configuration errors, or unauthorized changes to the safety logic can leave a safety function that does not stop the machine, which could result in death or serious injury.
- Restrict the configuration password, and verify every change completely before operation, as listed below.

**Mitigation Measures:**

- Download of configurations must be password-protected
- Each configuration has unique verification code
- Simplifier Manager software includes validation checks

**User Responsibility:**

- Restrict configuration password to authorized personnel only
- Maintain documented change control procedures
- Perform complete functional verification after any configuration change
- Use independent verification personnel (not the original programmer)
- Keep backup copies of validated configurations
- Document all configuration changes in machine technical file

### 2.4.4 Environmental and Installation Risks

**NOTICE**

**Moisture ingress**
While the enclosure is rated IP65 (freestanding) or IP66 (wall-mounted), improper installation of cable glands, M12 connectors, or damage to the GORE-TEX ventilation membrane can allow moisture ingress, which can damage the unit.
- Install, seal and inspect the unit as listed below.

**Mitigation Measures:**

- Enclosure constructed from PC+ABS UL 94 rated
- GORE-TEX membrane provides pressure equalization while excluding moisture
- Proper installation of cable glands and connectors maintains IP rating

**User Responsibility:**

- Install all cable glands and M12/M16 connectors per manufacturer specifications
- Ensure unused ports are sealed with appropriate plugs
- Protect GORE-TEX membrane from mechanical damage
- Do not use solvents for cleaning
- Do not use high-pressure, unless the unit is correctly wall-mounted and fitted with IP66 rated accessories
- Operate only within specified humidity range (10-90% RH, non-condensing)
- Inspect seals and connectors during periodic maintenance

### 2.4.5 Mechanical Vibration and Shock Damage

**NOTICE**

**Vibration and shock**
While the unit is tested to EN 60068-2-6 (5-150 Hz, 1g) and EN 60068-2-27 (15g shock), excessive vibration or impact may cause spring terminal loosening or internal component damage.
- Mount, relieve and inspect the unit as listed below.

**Mitigation Measures:**

- Spring-type terminals designed for high-vibration environments
- Robust PC+ABS housing provides mechanical protection

**User Responsibility:**

- Mount unit securely to stable surface per installation guidelines
- Verify all terminal connections are tight during periodic inspection
- Use strain relief on cables to prevent terminal stress
- Avoid installation on surfaces subject to impact or excessive vibration
- Inspect mounting after any significant mechanical shock event

### 2.4.6 Programming and Logic Risks

**⚠ WARNING**

**Unsafe logic or logic specification**
The Safety Simplifier executes programmed logic faithfully; it cannot detect if the logic, or the specification it implements, is unsafe, even when certified function blocks are used. A safety function can then fail to stop the machine, which could result in death or serious injury.
- Assess the risks before programming, and have the logic reviewed and fully tested, as listed below.

**Mitigation Measures:**

- Pre-certified function blocks provided for common safety functions (two-hand, dual-channel monitoring, etc.)
- Simplifier Manager includes validation checks for common errors
- $\mathrm{PFH}_D$ calculations automatically generated
- System reaction time automatically calculated

**User Responsibility:**

- **CRITICAL:** Conduct thorough machine risk assessment before programming
- Use pre-certified function blocks wherever possible
- Have programming reviewed by independent qualified personnel
- Perform complete functional testing of all safety scenarios
- Test both normal operation AND fault conditions
- Document all safety logic with clear functional descriptions
- Never use logic “1” to generate stop/off functions (violates de-energization principle)
- Maintain configuration version control and change logs

### 2.4.7 Integration and System-Level Risks

**⚠ WARNING**

**Inadequate design of the overall safety system**
The Safety Simplifier is a component within an overall machine safety system. An inadequately designed overall system can leave hazards unprotected, which could result in death or serious injury.
- Assess the machine and verify the complete safety chain, as listed below.

**Mitigation Measures:**

- Clear specification that Safety Simplifier is a component, not a complete safety solution
- Guidance provided for achieving Category 3 and 4 (see Requirements for Achieving Safety Categories section)
- $\mathrm{PFH}_D$ calculation methodology provided (see Calculating PFHd Values section)

**User Responsibility:**

- **MANDATORY:** Conduct complete machine risk assessment per Machinery Directive 2006/42/EC or Machinery Regulation (EU) 2023/1230 as applicable
- Integrate Safety Simplifier $\mathrm{PFH}_D$ values into overall system calculations
- Ensure external safety devices (e-stops, light curtains, etc.) are properly rated
- Verify complete safety chain from sensor to actuator
- Account for all reaction times in safety distance calculations
- Consider environmental factors (noise, vibration, temperature)
- Maintain complete technical documentation file

**Substantial Modification**

Regulation (EU) 2023/1230 defines a **substantial modification** in Article 3(16) as a modification of machinery, **physical or digital,** that introduces a new hazard or increases an existing risk, and which is not mitigated by the measures of the original risk assessment. Under Article 18, any natural or legal person who carries out such a modification is legally considered the manufacturer of the modified machinery. When reconfiguring distributed Safety Simplifier networks or adding new safety devices, the integrator must evaluate whether the overall system modification requires a new CE conformity assessment.

In practice, the following changes to a Safety Simplifier installation should trigger that evaluation:

- Adding, removing, or re-routing a safety function across networked units
- Adding a Safety Simplifier node to, or removing one from, an existing network
- Changing the safety logic so that a previously assessed hazard is addressed by different means
- Introducing a new safety device, actuator, or hazard zone into the safety chain
- Changing the intended use or the operating modes of the machine

Where the evaluation concludes that the modification is substantial, the person carrying it out assumes the obligations of a manufacturer under the Regulation for the modified machine, including risk assessment, technical documentation, conformity assessment, CE marking, and the EU Declaration of Conformity.

### 2.4.8 Residual Risk Management Summary

The machine integrator and end user must:

- Conduct Risk Assessment: Integrate these residual risks into overall machine risk assessment
- Implement Administrative Controls: Training, procedures, warning signs
- Establish Maintenance Program: Functional testing, inspections, documentation
- Provide Operator Training: Proper use, emergency procedures, limitations
- Maintain Documentation: Test results, maintenance logs, configuration changes
- Monitor Performance: Track errors, failures, response times
- Plan Lifecycle Management: Determine the mission time for the safety system and plan accordingly

### 2.4.9 Responsibility Statement

> **Note:** SSPN has designed the Safety Simplifier to minimize risks through inherent safety design principles. However, the residual risks described in this section cannot be entirely eliminated through product design alone.

The machine integrator and end user are responsible for:

- Conducting complete machine-level risk assessment
- Implementing appropriate risk reduction measures
- Providing adequate training to personnel
- Maintaining proper documentation
- Ensuring compliance with all applicable standards and regulations

SSPN is not liable for:

- Injuries or damages resulting from foreseeable misuse
- Inadequate overall safety system design
- Failure to perform required functional testing
- Operation outside specified environmental conditions
- Use beyond the mission time determined for the safety system
- Improper installation or maintenance

# 3 Maintenance and Service

**⚠ WARNING**

**Unauthorized repairs**
Incorrect maintenance or repairs may cause unintended malfunction of the safety functions, which could result in death or serious injury.
- Have repairs carried out only by SSPN or qualified personnel authorized by SSPN.

Component wear, particularly relay contacts, increases failure probability over time. Operating beyond the mission time determined for the safety system increases the dangerous failure rate. Please follow the guidelines below.

- Track operational lifetime from installation date
- Perform a functional test of the complete safety function at intervals not exceeding those given in the **General Functional Test Requirements** section — 30 days for PL e / SIL 3, 12 months for PL d / SIL 2 — unless normal operation demands the function at least that often
- Track relay switching cycles in high-frequency applications
- Check the mission time of the Safety Simplifier within your safety system, and plan replacement before it is reached
- Increase testing frequency for units approaching the end of their mission time
- Document all test results and maintenance activities

## 3.1 Periodic Inspection

**⚠ WARNING**

**Damaged or defective device**
A damaged or defective device may compromise the integrity of the safety system, so that a safety function fails, which could result in death or serious injury.
- Never commission or operate a device that is damaged or exhibits defects.

This section covers the general inspection of the **installation** — the physical condition of the unit, its mounting and its wiring. It is separate from the functional test of the safety function, which has its own intervals; see **General Functional Test Requirements.**

The machine owner or operator is **responsible for ensuring** inspections are conducted at appropriate intervals. Inspection frequency must be determined based on:

- Formal risk assessment results
- Manufacturer recommendations
- Operating environment conditions
- Activation frequency
- Regulatory requirements
- Insurance requirements

**Recommended Inspection Intervals:**

- Normal indoor use - Annually
- Moderate use - Every 6 months
- Heavy use/harsh environment - Monthly
- After any incident involving emergency stop - Immediately

**Minimum Requirement:** Regardless of usage, inspect at least annually.

**Inspection scope includes:**

- Mechanical and electrical verification of the unit and its connected devices
- Mounting integrity: Confirm secure and stable attachment
- Visual assessment: Check for signs of tampering or physical damage
- Electrical connections: Ensure all wire terminals are tight and undamaged
- Configuration integrity: Read the application program verification code and the firmware version through Simplifier Manager and compare them with the values recorded in the machine technical file — see **Protection of Safety Functions** in the Cybersecurity chapter

## 3.2 Response to Malfunction

This section describes the operating method to be followed in the event of an accident or a breakdown involving a Safety Simplifier.

**Immediate actions**

1. Bring the machine to a safe state and prevent restart. The machine must be secured against unexpected start-up in accordance with the machine emergency procedures.
2. Secure the area and, where an injury has occurred, follow the accident procedures of the plant before any equipment is disturbed.

**⚠ DANGER**

**Defeated safety function to restore production**
Restarting a machine with a bypassed, bridged or reprogrammed safety function leaves persons in the hazard zone unprotected. This will result in death or serious injury.
- Do not bypass, bridge, or reprogram a safety function in order to restore production.

**Diagnosis**

1. Establish the condition of the unit. A unit in **Fatal Error Mode** has detected an internal fault, has already de-energized all of its outputs, and reports an error code on the LED display (units with the LD option) and via USB in Simplifier Manager. A unit that shows **no LED activity at all** — for example after fire, water ingress, or mechanical destruction — is not in Fatal Error Mode; it is unpowered or destroyed, its outputs are de-energized for that reason, and it must be replaced.
2. Read the error code from the LED display or, on a unit without a display, via USB in Simplifier Manager, and record it together with the unit node number and the state of the I/O at the time of the fault. Error codes are listed in the Error Codes section.
3. Distinguish an **internal** fault from an **external** fault. Internal faults place the unit in Fatal Error Mode and are reported only on the LED panel and via USB on the affected unit. External faults, such as a short circuit on an OSSD output, switch the affected terminal off — it shows red in the I/O menu like any OFF terminal — and are identified in Online Mode in Simplifier Manager and as a signal in the application logic.
4. Where the fault is external, trace it in the installation before replacing the unit. The Safety Simplifier cannot disconnect a voltage source outside its own supply.

**Rectification and return to service**

1. Identify and rectify the fault condition. Repairs to the unit itself must only be carried out by SSPN or by personnel authorized by SSPN.
2. Perform a full mechanical and electrical function test of every safety function affected by the fault and by its rectification.
3. Verify that the application program verification code and the firmware version still match the values recorded in the machine technical file.
4. Record the fault, the diagnosis, the action taken, and the test results in the maintenance documentation before the machine is returned to service.

Report any hazardous malfunction to SSPN using the contact details on page 2 of this document.

## 3.3 Liability Disclaimer

The manufacturer assumes no responsibility for damages or operational failures resulting from **improper** installation or **non-compliance** with the instructions provided in this manual. Liability is also excluded for any harm caused by the use of **spare parts or accessories not expressly approved by the manufacturer**. For safety reasons, unauthorized repairs, alterations, or modifications are strictly **prohibited and will void** any manufacturer liability for resulting damages.

## 3.4 Transport, Handling and Storage

The Safety Simplifier is a compact electronic device and is normally transported as a packaged unit. No lifting equipment is required.

- **Mass:** refer to the technical data for the mass of the specific variant.
- **Transport and storage temperature:** refer to the technical data. The permitted operating temperature range is narrower than the storage range.
- **Humidity:** store in dry conditions. Condensation on or inside the enclosure must be avoided; allow the unit to reach ambient temperature before opening or energizing it after transport from a cold environment.
- **Packaging:** transport and store the unit in its original packaging wherever possible. The packaging protects the enclosure, the GORE-TEX ventilation membrane, and the connectors from mechanical damage.
- **Handling:** do not subject the unit to impact or to mechanical shock beyond the values stated in the technical data. Protect the ventilation membrane, the terminal block, and the M12 or M16 ports from damage.
- **Electrostatic discharge:** the enclosure protects the electronics in normal handling. When the enclosure is open, observe ESD precautions before touching the printed circuit boards or the plug-in communication cards.
- **After transport damage:** a unit whose packaging or enclosure shows evidence of impact, moisture ingress, or other damage must not be commissioned. Inspect it in accordance with the Periodic Inspection section and return it to SSPN if any defect is found.

## 3.5 Disposal Considerations

It is **recommended** to send the out-of-commissioned device back to SSPN at:

SSPN Safety System Products North AB
Tullkammarvägen 14
S-439 31 Onsala
Sweden

Otherwise when disposing of the Safety Simplifier, please follow these guidelines:

- Verify the mission time of the Safety Simplifier within your safety system to determine if disposal is necessary.
- Comply with local regulations regarding the disposal of electronic equipment and other components of the Safety Simplifier.

Proper disposal helps ensure environmental safety and compliance with applicable laws.

# 4 Safety Simplifier Features

The Safety Simplifier system is designed to function as a Safety PLC within an Equipment Under Control (EUC). It is responsible for executing safety-related logic for one or more safety functions in the system.

When integrated into an EUC, the Safety Simplifier contributes to achieving high safety performance levels, including:

- **SIL 3** according to **IEC 61508**
- **PL e**, **Category 4** according to **ISO 13849-1**

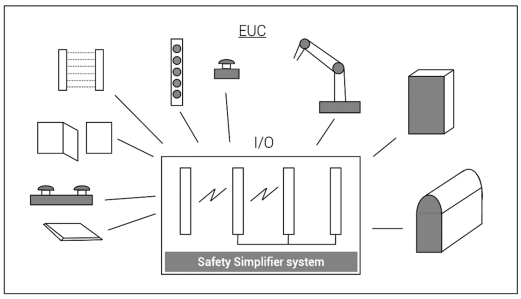



Figure 1: Safety Simplifier system as part of an EUC.

Safety connections to external safety devices and machinery are intended to be made via the I/O interfaces of the Safety Simplifier. For distributed safety logic, multiple Safety Simplifier units can communicate with each other using radio and/or CAN-bus cable connections (RadioCAN); separate systems can be linked over SimpleCAN or a general black channel.

These communication channels are used exclusively as physical layers and comply with IEC 61784-3:2016, ensuring reliable and standardized safety communication.

Simplifier Manager is the configuration software used for managing Safety Simplifier systems. It provides the following key functions:

- Programming and compiling safety logic to be executed on Safety Simplifier devices
- Configuring Safety Simplifier units as part of a complete safety system
- Monitoring and debugging system performance and behavior
- Generating documentation for system configuration and safety validation

Safety Simplifier devices can be configured using either of the following methods:

- Via USB: Using the micro USB or USB-C connector located inside the Safety Simplifier
- Wirelessly: Through the Simplifier Monitor device

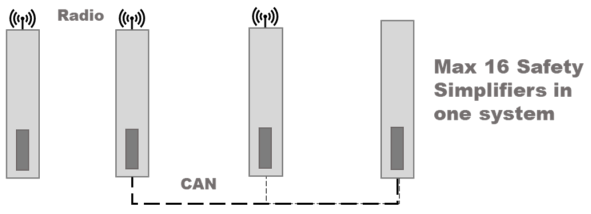



Figure 2: Example configuration of four Safety Simplifier units communicating via CAN and Radio

## 4.1 Simplifier Manager and Software Version Control

Simplifier Manager generates and compiles the safety logic executed by the Safety Simplifier. Under Regulation (EU) 2023/1230, software that performs a safety function is itself a safety component, and the configuration produced by Simplifier Manager is safety-related software within the meaning of the Regulation. The following version information must therefore be recorded and kept under change control as part of the machine technical file:

| Item | Why it must be recorded |
|---|---|
| Simplifier Manager version | Determines the certified function block library and the validation checks applied when the configuration was compiled. |
| Safety Simplifier firmware version | Executes the configuration. All units in a network must carry the same firmware. |
| Application program verification code | Uniquely identifies the compiled configuration. Any change to the configuration alters the code. |
| Unit serial numbers | Identify the physical units on which the configuration was validated. Every unit in a system is configured with the serial numbers of all other units. |

Simplifier Manager is updated independently of the Safety Simplifier hardware. After any update to Simplifier Manager, verify that the installed version remains compatible with the firmware of every unit in the system, and regenerate the configuration report so that the recorded version information stays consistent with what is installed.

A change of Simplifier Manager version does not by itself alter a configuration already downloaded to a unit. A configuration that is **recompiled** under a new Simplifier Manager version must, however, be treated as a configuration change: it must be verified in full and the new verification code recorded before the machine is returned to service.

## 4.2 Hardware Components

- Supports up to 14 configurable transistor I/O channels, usable as inputs, outputs, or mixed-mode.
- Provides two optional potential-free safety relay outputs. Each output is built from two relays in a doubled arrangement, providing the redundancy needed for Category 4 / SIL 3; both contacts of an output must be used in the safety function.
- Includes an optional LED display for real-time fault codes and system status indicators.
- Equipped with 2.4 GHz wireless and/or CAN-bus interfaces for safety communication across up to 16 interconnected units.
- Utilizes spring-loaded terminals for streamlined I/O wiring and reliable connections.
- Features a durable enclosure rated IP66 when wall-mounted or bracketed; IP65 when freestanding.
- Cabinet type Safety Simplifier units are rated IP20
- Each short side includes two ports for M12 connectors or M16 cable glands, allowing flexible cabling options.
- Offers an optional cutout for pushbuttons, selector switches, emergency stops, and other control elements.
- Supports configuration and diagnostics via USB interface and/or wireless link through Simplifier Manager software.

## 4.3 Supported Safety Devices

The Safety Simplifier system is compatible with a wide range of safety input and monitoring devices, including:

- Emergency stop switches
- Two-hand control stations compliant with EN ISO 13851:2019 (formerly EN 574) up to Type IIIC
- Safety gate limit switches
- Reset actuators
- Light beam sensors
- Light curtains
- Safety scanners
- Enabling switches
- Hold-to-run devices
- Operating mode selectors
- Safety mats and pressure-sensitive strips
- RFID-based safety sensors

- NC contacts for monitoring relays actuated via outputs
- Eight coded signal channels from the same unit (four regular, four inverted)
- Two coded signal channels from other units (one regular, one inverted)
- Voltage window comparators and inverted voltage window detection
- Dedicated voltage comparators for specific threshold monitoring

The electrical limits that apply to every connected device — input voltage range, output current, and relay switching capacity — are specified in the Technical Data chapter and must not be exceeded.

## 4.4 Output Configurations

The Safety Simplifier supports a range of output configurations for machine control and safety signaling:

- 7–33 VDC standard outputs for direct machine actuation.
- 7–33 VDC OSSD (Output Signal Switching Device) outputs, with integrated short-circuit detection across up to 14 channels.
- 7–33 VDC outputs for 8 safety-coded signals transmitted within a single Safety Simplifier unit.
- 7–33 VDC outputs for 2 safety-coded signals exchanged between separate Safety Simplifier units.

## 4.5 Combined I/O Functions

Combined I/O channels offer dual functionality by serving simultaneously as safe inputs and non-safe outputs, enabling compact and efficient control configurations.

Typical applications include:

- Reset pushbuttons with integrated lamp indicators
- Start/Stop pushbuttons featuring lamp indication
- Other control devices or pushbuttons equipped with lamp feedback

## 4.6 Redundant Relay Outputs

The system supports two optional potential-free redundant relay outputs, designed to meet stringent safety requirements.

These outputs are typically used for:

- Safety input interfacing on industrial robots (IRBs) and other machinery
- Actuation of safety mechanisms, such as door interlocks and locking devices

## 4.7 I/O Non-Safety Data

Transistor I/O channels can be repurposed for non-safety functions, including:

- Serial transmission of up to 32 internal logic signals, enabling data exchange between:
  - Separate Safety Simplifier systems
  - Safety Simplifier units and external PLCs. This communication does not require a shared application program, simplifying integration.
- Status and indication outputs for visual or system-level feedback

Relay outputs may also be used for non-safety purposes, such as:

- Indication and status signaling

## 4.8 LED Display

The LED display on a Safety Simplifier provides real-time system diagnostics and status indicators. For operational details, refer to the **LED Display** and **Menu Structure** chapters.

Displayed information includes:

- Node identification: Current node number and total nodes in the system
- I/O status: Active I/O states of the unit
- Supply voltage levels: Voltage monitoring
- Radio communication: Channel assignment
- Network connectivity: Link status to every other node, over radio or RadioCAN
- Error codes: Fatal error indication and error code

## 4.9 Model Variants

The Safety Simplifier is available in multiple configurations, with standard models including:

- S14: 14 I/O channels
- S16: 14 I/O channels + 2 redundant relay outputs

Custom models follow the format **SXXLDRBCAYY**, where each segment defines specific hardware features. The designations listed below are those covered by EC Type-Examination Certificate C901009:

| Segment | Description |
|---|---|
| XX = 00–14 | 0 to 14 I/O channels |
| XX = 16 | 14 I/O channels + 2 × double relay outputs |
| XX = 20–33 | 2 relay outputs + 0–13 I/O channels |
| XX = 40–43 | 2 × double relay outputs + 0–13 I/O channels |
| LD or blank | **LD** indicates LED display is mounted |
| RB or blank | **RB** indicates radio communication card is mounted |
| CA or blank | **CA** indicates CAN communication card (plug-in, optional) |
| YY = 00 | No terminals |
| YY = 02 | Connectors, no spring terminals |
| YY = 20 | 2 spring terminals |
| YY = 21 | One connector and one spring terminal |

## 4.10 Housing Material

PC + ABS (Polycarbonate and Acrylonitrile Butadiene Styrene). UL 94 rated.

Ventilation enclosure: GORE-TEX membrane (ensures pressure equalization)

# 5 System Design and Safety Principles

**Note:** Read this information carefully as it is essential information on how to design and use the Safety Simplifier System in a safe way.

## 5.1 Operating Modes

The Safety Simplifier operates in three distinct modes:

- **Normal Mode**
  - The device executes logic and controls outputs based on configured inputs and safety logic. This is the standard operational state.
  - The Safety Simplifier contains internal automatic online monitoring logic that runs continuously and **cannot be affected or overridden by the user or application program.**
- **Fatal Error Mode**
  - All outputs are **de-energized: transistor outputs go to 0 V**, and relay outputs de-energized (contacts open). This state is triggered by an internal fault, or by an external fault that the application logic has been programmed to escalate. Loss of communication does **not** by itself cause Fatal Error Mode; it sets the affected signals to logic "0" as described in the Failure and Communication Loss Handling section.
- **Configuration Mode**
  - The device is offline. All outputs are forced into the Safe State. This is the **only mode** where a new configuration can be downloaded from a PC via USB or radio.

## 5.2 Safe State Definition and De-energization Principle

The Safe State is defined as the condition where:

- Outputs are **turned off** ($0V$ or "low").
- Output relays are **de-energized** (all contacts open).
- Logic state is "0" (Logic "1" must **not be used** to generate a stop/off function).

The system is fundamentally designed around the de-energization principle:

- A Safe State (stop/off) must be generated by a **low signal, open circuit, logic "0", loss of radio signal**, or **loss of bus communication**.
- All stop functions must operate by **de-energizing.**
- A fault in the system is designed to set affected inputs, outputs, or memories to a **logic "0" (Safe State)**.

**⚠ WARNING**

**Stop function that depends on a signal being present**
The de-energization principle applies equally to the wiring and to the logic designed in Simplifier Manager. A stop or off function that depends on a signal being **present** — an energized input, a logic "1", a closed circuit, or an active communication link — will fail to stop the machine when that signal is lost, which could result in death or serious injury.
- Generate every stop and off function by the **absence** of a signal.

## 5.3 Failure and Communication Loss Handling

In a multi-Simplifier system (nodes):

- If a node **loses communication** with another, it immediately treats all safety information from that absent node as 0 (off, open, de-energized).
- The system **must** be designed so that any loss of communication results in the relevant outputs turning off ($0V$).
- It is **essential** that the loss of both **radio** and **CAN-bus** communication leads to the Safe State.

**⚠ WARNING**

**Safety function that relies on a networked signal**
Loss of radio or CAN-bus communication can occur at any time, like loss of power. A safety function that relies on a networked signal remaining present then fails, which could result in death or serious injury.
- Design the system so that loss of communication leads to the Safe State without creating a hazard.

If the Safety Simplifier detects an internal dangerous failure:

- The affected unit immediately transitions to the Safe State.
- **Safety communication** (radio and CAN-bus) is shut off.
- Other nodes will lose connection, setting all safety information from the failed unit to 0.
- **Error Information** on the cause is available only on the LED-panel and via USB on the unit itself. It is **not** available via wireless or CAN.

If the Safety Simplifier detects an **external dangerous failure** (e.g., short circuit on an OSSD output or an invalid coded input signal):

- The affected inputs and/or outputs are immediately turned **off.**
- **Error Information** is available in Online Mode in Simplifier Manager — over radio, CAN or USB — and as an internal signal within the logic. The LED panel shows the affected terminal as OFF only and does not distinguish an external fault; see the I/O Menu section.
- The **system integrator** must program the logic to decide if further actions are required (e.g., setting the device to Safe State or turning off other functions).

## 5.4 Subsystem Deployment Configurations

The Safety Simplifier may be deployed in four distinct configurations, each with specific integration requirements for maintaining the achieved safety integrity:

**A) Standalone SRP/CS**

A single Safety Simplifier unit, together with external sensors and output devices, forms a complete SRP/CS implementing a safety function according to ISO 13849-1 (Category 4 potential). The resulting safety integrity must be evaluated for each specific application, taking into account the reliability data of the external components and the diagnostic techniques applied.

**B) Safety Simplifier as a Subsystem with External Subsystems**

The Safety Simplifier implements a safety function as a subsystem in combination with at least one external subsystem (either on the input side or the output side). The external subsystem must be interconnected with the Safety Simplifier by compatible means to maintain the overall SIL, either by:
- Comparing the external subsystem's safety manual with the Safety Simplifier safety manual, or
- Conducting a separate and detailed analysis of the external subsystem and its interconnections.

**C) Multiple Safety Simplifier Units via Radio/RadioCAN**

A Safety Simplifier unit is interconnected to one or more other Safety Simplifier units using the provided data communication interfaces (RadioCAN or radio).

**D) Relay Outputs as Power Control Elements**

The relay outputs (Output 15 and Output 16) of the Safety Simplifier are used as power control elements — for example, controlling the power supply of an external subsystem. The external subsystem switched by the relay outputs must be assessed in accordance with IEC 61508 or ISO 13849-1. Both relay contacts and their respective monitoring are fully integrated.

## 5.5 Wireless Network Design

The physical placement of Simplifier units significantly impacts radio communication performance. To ensure reliable radio communication throughout the system, follow these guidelines:

1. Maximize direct line-of-sight paths between units
2. Ensure line-of-sight paths remain unobstructed by personnel, vehicles, or equipment
3. Place every unit so that it has direct line of sight and good signal strength to at least three other units (meeting criteria 1 and 2)
4. Arrange units in order of node number (N01 close to N02, N02 close to N03, and so on), so that units with adjacent node numbers have good radio contact with each other
5. Arrange the last unit in the system and N01 close together
6. Ensure that no other radio equipment transmits on the same frequency band. In particular, lock nearby WiFi access points to fixed WiFi channels that do not overlap the Safety Simplifier radio channel in use — see the Radio Frequency (RF) Channels table in the technical data for the overlap between the two channel plans.

Note: For systems containing 2, 3, or 4 units, establish reliable radio contact between all units.

### 5.5.1 Understanding Radio Quality

The system shown in Figure 3 demonstrates optimal radio quality. All units operate within range of each other with direct communication paths, eliminating reliance on repeated transmissions. This configuration provides redundancy—if unit 3 fails to receive a transmission from unit 1 due to interference, it can still receive the repeated signal from unit 2. This redundancy enhances system reliability against random interference, though it does not guarantee immunity from all disturbances.

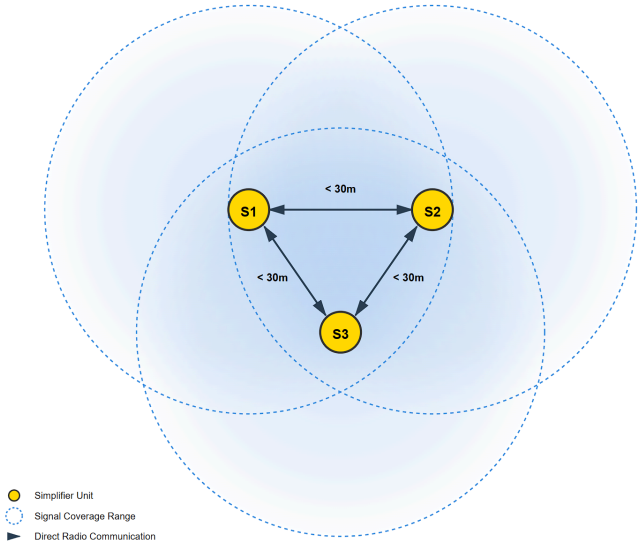



Figure 3: Recommended spacing between Simplifier units varies based on location properties and obstructions on site.

### 5.5.2 Redundancy and Minimal Reaction Times

In the network shown in Figure 4, units 1, 2, and 3 have direct radio contact with one another. While Unit 3 acts as a repeater for all traffic to and from units 4 and 5. While this setup functions, it violates fundamental system design principles, resulting in a less reliable system with slower reaction times.

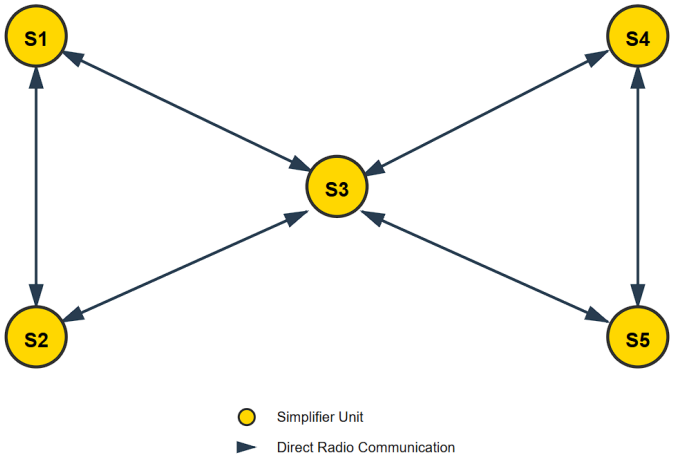



Figure 4: Simplifier unit 3 as the only connection bridge for the rest of the units.

**Design Violations**

- Unit Hierarchy:
  - Unit 1 (the system's lead unit) should have direct radio contact with the last unit in the system, so that the communication chain closes and all safety information propagates correctly.
- Redundancy:
  - Units 1, 2, 4, and 5 have only one communication path to the rest of the network (via Unit 3).

**Reliability Impact**

If Unit 3 loses power, stops transmitting, or encounters an error, Units 4 and 5 will immediately lose connection to the network. This single point of failure makes the network entirely reliant on Unit 3 for operational integrity.

**Reaction Time Impact**

Information flowing between units 4/5 and 1/2 is delayed by the repeating function of Unit 3, as it must repeat the signal "backwards" to complete the path. This increases the average reaction times in the system, though it does not affect the maximum specified reaction time.

#### 5.5.2.1 Optimal Wireless Configuration

To resolve the reliability and reaction time issues, the system must be modified to adhere to the principle of full redundancy and correct unit hierarchy (as detailed in the start of this chapter).

The solution involves adding a new unit (Unit 6) and placing it after Unit 3 in the communication hierarchy, as illustrated in Figure 5.

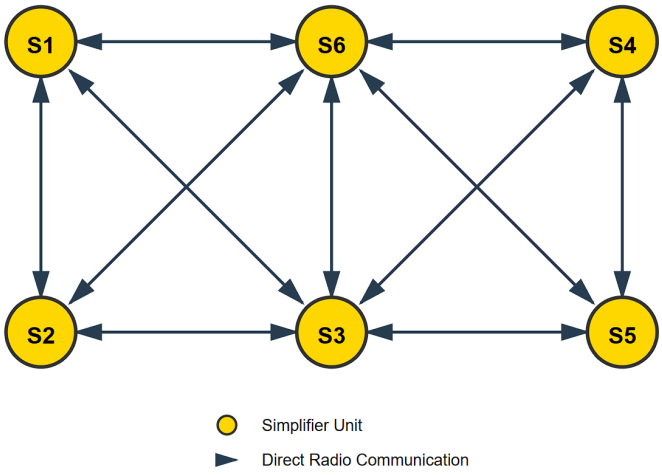



Figure 5: Simplifier units 3 and 6 acts as the bridging units

In the new configuration:

- Unit Hierarchy:
  - Unit 1 now hears the last unit in the system (Unit 6), and every unit in the system hears at least three other units (one of which is always the previously connected unit).
- Redundancy:
  - The system still utilizes the repeating function but now has full redundancy. If Unit 3 fails, units 4 and 5 will still be able to hear Unit 1 and 2 via Unit 6, preventing a total communication loss and network shutdown. This ensures compliance with the redundancy and reaction time requirements.

### 5.5.3 Internal and External Antenna

We recommend using the internal antenna in the Safety Simplifier unit for environments where there is a clear line of sight between units. This eliminates signal attenuation and simplifies installation, provided that signal integrity is not compromised by structural or environmental factors.

**When to use external antenna**

1. Shielded and Sealed Compartments
   - Equipment housed in EMC-shielded enclosures, IP-rated cabinets, or pressurized compartments to protect against electromagnetic interference.
   - Wireless signals cannot penetrate these barriers reliably, making cable-based signal routing essential.
2. Metallic Structures and Signal Obstruction
   - Environment with metal hulls, frames, or bulkheads that severely attenuate or reflect wireless signals.
   - Antenna cables allow signals to be routed externally, bypassing these obstructions and enabling reliable communication.
3. Safety and Regulatory Compliance
   - Wireless transmission may be restricted or require certification.
4. Fixed Infrastructure
   - When signals need to be routed through and/or around walls.

When selecting and installing antenna cables, the following factors must be considered:

- Cable Type and Attenuation: Choose cables with low $\mathrm{dB/m}$ ratings appropriate for the operating frequency.
- Cable Length: Minimize length to reduce cumulative signal loss.
- Connector Quality: Use high-quality connectors to avoid additional insertion loss.
- Environmental Protection: Ensure cables are rated for the installation environment (e.g., UV-resistant, waterproof).

> **Note:** SSPN provides optional coaxial antenna cables. RG-58 has an attenuation of approximately $1.1–1.2\ \mathrm{dB/m}$ at $2.4\ \mathrm{GHz}$; refer to the datasheet of the supplied cable for the exact figure when planning the link budget.

> **Note:** A weaker power signal has significant negative consequences that fall primarily into two main categories: reduced coverage/range and slower, less reliable data transfer.

## 5.6 Programming and Requirements

When a multi-Simplifier system loses and then **re-establishes communication:**

- Only functions dependent on the lost signals will react during the loss. Other functions continue operating.
- The **risk analysis** for the system **must** determine the action upon return of communication. The programmer can choose to:
  - Require all functions to **stop.**
  - Require a **restart** after communication is restored.

For control devices that start a function when actuated, you **must** use the **Startup** setting in the function block for:

- Inputs connected to these devices.
- Global and CAN memories used between Safety Simplifiers.

The Startup setting **requires** a control device to be released and re-activated following a loss of power, communication, or one or more input signals.

**⚠ WARNING**

**Restart when communication returns**
A function that restarts by itself when radio or CAN-bus communication returns can start the machine unexpectedly, which could result in death or serious injury.
- Make every function that depends on a networked signal go to the Safe State when the signal is lost, like on loss of power.
- Use the Startup setting so that a deliberate operator action is required to restart.

Programming and Verification:

- The system must be designed so that a unit or output transitioning to the Safe State **does not cause any hazardous conditions.**
- The use of the pre-checked and certified **Function Blocks** (e.g., two-hand, dual channel monitoring) offered in the software is **strongly recommended.**
- All programming, logic, and connections must adhere to the **Safety Simplifier Manuals** and relevant **safety requirements/legislation** for the Equipment Under Control (EUC).
- The Safety Simplifier unit(s) **must be restarted at least once per year** to fulfill safety requirements, or more often if the application requires it. The restart runs the power-on self-tests and is performed in connection with the periodic functional test — see the General Functional Test Requirements section.

Security and Verification:

- Download of application programs must be **password protected.** The password should be kept confidential by the responsible person.
- Before the application is taken into use, **thorough verification is mandatory:**
  1. Test **all safety functions** to verify correct behavior against the specification and risk analysis.
  2. Review **drawings and PLC program** to find design faults difficult to detect in practical tests.
- It is recommended that testing and verification are performed by **personnel other than the designer** to prevent design and systematic failures.

## 5.7 Safety and Non-Safety Functions

The Safety Simplifier includes I/O and logic signals for both safety and non-safety use.

| Function Type | Monitored by Dual Processors | Programming Software Indicator |
|---|---|---|
| Safety | Yes | Solid **Yellow** line/function block color |
| Non-Safety | No | **White** line / **Grey** function block color |

**Non-safety functions** are optimized for flexibility and **must not be used for safety**, as they are not controlled and monitored by the dual processors. Examples include:

- Information communication between Safety Simplifiers.
- Information via the Simplifier Monitor to a computer.
- Information displayed on the LED-display.

The Safety Simplifier offers a range of certified **safety functions**, including:

- Up to 2 x 2 double relay outputs.
- Up to 14 I/O selectable as input, output, or a combination.
- Up to 14 **OSSD outputs** with short circuit detection.
- Detection of voltage levels ($0–33$ VDC), pulsed signals, and short circuits on inputs and outputs.
- 16 Global memories for radio and RadioCAN (CAN-bus) communication.

## 5.8 Technical and Environmental Notes

It is **vital** that personnel involved in design, programming, and maintenance possess sufficient knowledge about:

- The Safety Simplifier system.
- The field of machinery safety for the actual machinery.

System Identification:

- Each Safety Simplifier has a unique **serial number,** printed on the unit label.
- In a system of 2 to 16 Simplifiers, every unit is configured with the **serial numbers of all other units** in that system. Only units whose serial numbers are part of the configuration exchange safety information with each other. All serial numbers must be entered in Simplifier Manager before a configuration can be downloaded.
- All units in a network **must have the same firmware** to communicate.
- Every application program has a unique code to verify integrity; **any change alters the code.**

Environment and Use:

- The device must **only** be used within the environmental conditions stated in the technical data.
- This equipment is intended for use in locations where **children are not likely to be present.**

### 5.8.1 Non-Ionising Radiation and Radio Frequency Exposure

Safety Simplifier variants fitted with the 2.4 GHz radio card emit non-ionising radio frequency radiation during normal operation. The transmitted power is low, and the unit is not intended for hand-held or body-worn use.

**Separation distance**
A separation distance of $20$ cm **or more** must be maintained between the antenna and persons during continuous operation. This distance satisfies the RF exposure requirements of the FCC.

Compliance of the radio interface with the basic restrictions on human exposure to electromagnetic fields is assessed according to **EN 62479:2010** and **EN 50663:2017,** the harmonised standards for low-power electronic and electrical equipment in the range $10$ MHz to $300$ GHz. The standards applied to the Safety Simplifier are listed in the EU Declaration of Conformity.

**⚠ WARNING**

**Radio frequency fields and implanted medical devices**
Radio frequency fields may interfere with active implantable medical devices such as cardiac pacemakers, implantable cardioverter defibrillators, cochlear implants, and neurostimulators, and may affect non-active implants.

- Persons with an implanted medical device must maintain the stated separation distance from the antenna, and must consult their physician and the instructions of the implant manufacturer before working close to an energized unit.
- Do not work inside an opened enclosure while the unit is energized.
- The machine integrator shall include the exposure of persons with implants in the machine risk assessment, and shall mark installation areas in which the separation distance cannot be maintained.

The machine integrator is responsible for assessing cumulative radio frequency exposure where several Safety Simplifier units, or other radio equipment, are installed in the same area.

# 6 I/O & Relay Hardware Architecture

## 6.1 Safety Relay Outputs

The Safety Simplifier provides **two optional, potential-free, doubled safety relay outputs** for controlling safety functions up to **SIL 3 / PL e / Category 4.**

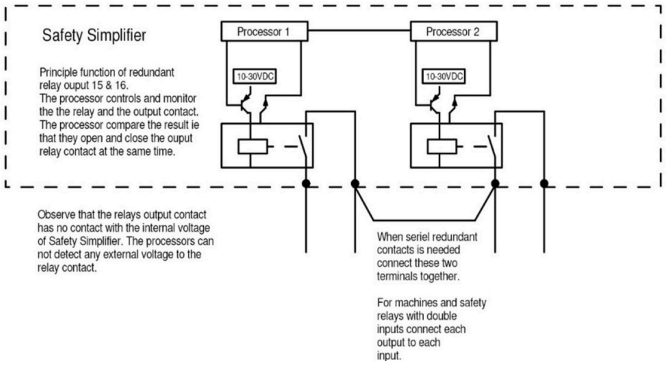



Figure 6: Relay outputs

Output Structure and Redundancy:

- Each safety relay output (Output **15** and Output **16**) consists of **two separate relays.**
- Each of the two separate relays has one **Normally Open (NO)** contact connected to terminals.
  - Output 15 uses terminals **23-24** and **33-34.**
  - Output 16 uses terminals **43-44** and **53-54** and has the identical safety functionality.

To ensure high safety integrity, each relay's operation is independently monitored:

- Each of the two relays is controlled and supervised by its own **dedicated processor.**
- The two processors **continuously compare their results** with each other.
- The processors check that the contact in each **relay is successfully opened** every time a relay is de-energized.

> ⚠ **WARNING**
>
> **Single relay contact as a redundant output**
> A single contact of a relay output is not a redundant output. A safety function wired through one contact does not reach Category 3 or 4 and can be lost by a single fault, which could result in death or serious injury.
> - Use **both contacts of the same relay output** — terminals **23-24 and 33-34** for Output 15, or terminals **43-44 and 53-54** for Output 16.
> - Perform any necessary short circuit detection across a contact or within the connecting cable in the external device; relay outputs do not check for it.

The relay's $\mathrm{PFH}_D$ (Probability of Dangerous Failure per Hour) value is affected by the number of switching operations and the breaking capacity (switched current).

- Low Number of Operations (e.g., E-stop): The relays can safely switch a higher current throughout their lifetime.
- High Number of Operations: The switched current must be lower to maintain the required lifetime and $\mathrm{PFH}_D$.
- For detailed technical data and instructions on calculating $\mathrm{PFH}_D$ values, refer to the Calculating PFHd Values section.

## 6.2 Solid-State Transistor Outputs

The Safety Simplifier's 14 configurable I/O points can be set to different output types in Simplifier Manager software.

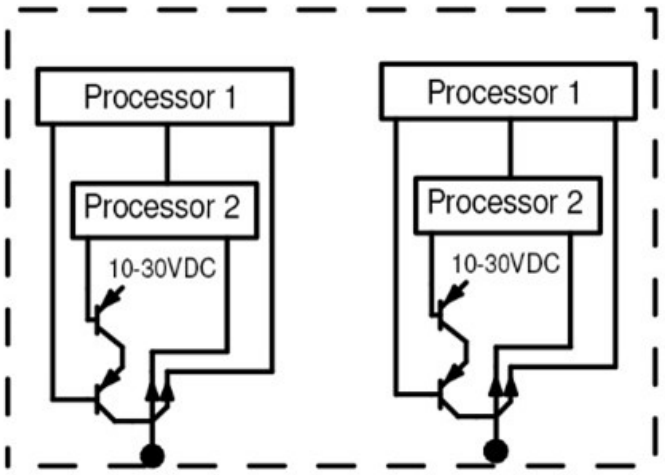



Figure 7: Two I/O, each with 2 transistors in series.

Each output features two transistors connected in series, with each transistor controlled by one of the unit's dual processors. This design provides a degree of inherent redundancy (refer to the $\mathrm{PFH}_D$ values and notes in the technical data for specifics).

Both processors also read back the signal from the output, allowing them to verify the actual voltage level and coded signals being transmitted.

A single output that detects an external short circuit can turn itself off, but it cannot physically clear the external short circuit. A single transistor output is rated Category 3 / PL d, with a maximum SIL of 2 — see the Safety Standard Classifications table. For applications requiring SIL 3, PL e, or Category 4, two outputs **must** be used.

The I/O can be configured to output one of two voltage levels in the ON and OFF states:

- **VDC / +V:** Output voltage is $\leq 0.5V$ less than the supply voltage.
- **0 VDC:** Output voltage is $0V$.

### 6.2.1 OSSD

**OSSD (Output Signal Switching Device)** outputs are commonly used in the industry for safety devices and machine stop signals. Up to **14** I/O points can be configured as OSSD outputs.

- In the ON state, the output voltage is $\leq 0.5V$ less than the supply voltage.
- OSSD outputs feature **built-in short circuit detection** to:
  - Other OSSD outputs on the same unit.
  - Internal and external fixed voltages.

If an external short circuit is detected, the Safety Simplifier initiates a response:

- The affected output(s) will be **shut off** or set to the **OFF-state** (i.e., $0V$).
- Depending on the fault type and application program logic, this may escalate to a **fatal error.**
- The affected terminal is switched off and shows red in the I/O menu; the fault itself is identified in Online Mode in Simplifier Manager and as a signal in the application logic.
- The system checks the output by briefly dropping the voltage level to $0V$ during a very short test interval, which is **less than** $150$ microseconds.
- A standard contactor or relay connected to the OSSD output will **normally not drop out** during this brief test pulse. Consult the technical data for the exact test interval specification.

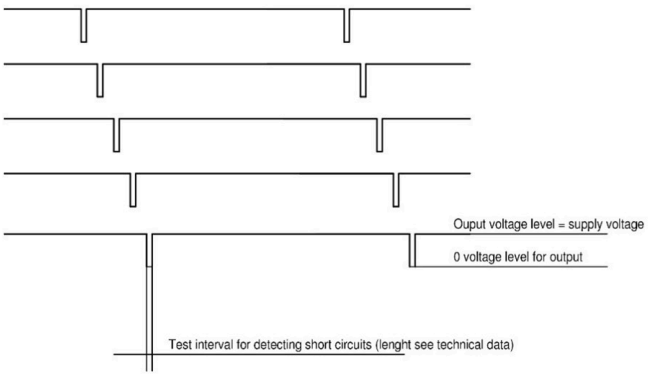



Figure 8: 5 OSSD outputs with short circuit detection.

### 6.2.2 Coded Pulse Trains (A, B, C, D)

The Safety Simplifier can generate up to **eight uniquely distinguishable pulse trains:**

- The four primary signals are the **A, B, C,** and **D** pulses.
- Each of these can also be generated as an inverted signal (**Inv A, Inv B,** etc.).

These pulse signals are primarily used to implement cable and device integrity checks:

- They allow the system to send a unique pulse signal out of an output, through an external safety device, and back into a Safety Simplifier input (often on the same unit).
- By checking that the expected unique (or inverted) pulse returns, the system can verify the **correct functioning** of the external device and confirm that there are **no short circuits** between the cables or to fixed voltage.

If a short circuit is detected between any of these different pulse signals or to a fixed voltage, the relevant outputs can be shut off, set to the OFF-state, or transition to a fatal error, as programmed by the application logic. Refer to the **Simplifier Manager Manual** for detailed programming information.

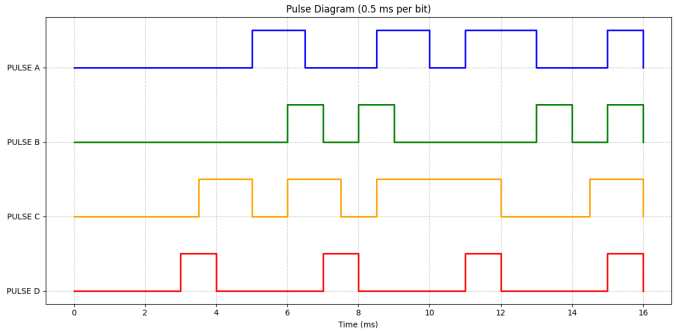



Figure 9: All pulse trains (non inverted)

## 6.3 Input Structure and Configuration

Each input on the Safety Simplifier is a **voltage input** that is simultaneously read by both internal processors. The processors determine the logical state from a low and a high threshold relative to the power supply voltage ($V_{\text{Supply}}$). The thresholds are programmable in Simplifier Manager; the default values are:

- **Logical "1" (HIGH)**: Voltage $> 75\%$ of $V_{\text{Supply}}$ (default).
- **Logical "0" (LOW)**: Voltage $< 25\%$ of $V_{\text{Supply}}$ (default).

Some inputs can also be configured to respond to a specific, user-defined voltage level (specified in Volts).

#### Hysteresis behavior of VDC

When the analog input voltage lies between the low and high thresholds (by default 25 % and 75 % of the supply voltage), the system applies hysteresis logic:

- If the previous state was ON, it remains ON.
- If the previous state was OFF, it remains OFF.

Only when the signal drops below the low threshold or rises above the high threshold does the input state change.

When configuring an input in Simplifier Manager, a specific signal type must be defined for both the **ON-state** and the **OFF-state.** The allowed signal types are:

| Signal Type | Description |
|---|---|
| 0V | Voltage below the low threshold (default $< 25\%$ of $V_{\text{Supply}}$) |
| VDC | Voltage above the high threshold (default $> 75\%$ of $V_{\text{Supply}}$) |
| Pulse Trains | Any of the A, B, C, or D pulse trains or their inverted counterparts |
| Voltage Window | A specific range of voltages (defined by the programmer) |

VDC is used interchangeably with the supply voltage for logic purposes.

> ⚠ **WARNING**
>
> **0V as the only ON-state signal**
> Using a **single input with $0V$ as the ON-state signal** (typical of a Normally Closed, or NC, device) as a safety input **violates the de-energization principle.** If the cable is disconnected or broken, the input will float to an **ON-state** (Logic "1"), which could result in death or serious injury.
> - **ALWAYS** combine this type of input with a Normally Open (NO) input or use a dual-channel configuration, so that a disconnected cable leads to the Safe State.

For maximum safety and integrity, the use of active signals (coded pulsed signals) is recommended for both the ON-state and the OFF-state.

- Active signaling provides the capability to **detect short circuits to external voltage sources,** which is a critical diagnostic function.
- Refer to the Simplifier Manager manual for the recommended combinations of active signals for the ON-state and OFF-state.

## 6.4 Handling External I/O Faults

If an I/O line experiences a **short circuit to an external voltage** (a voltage source other than the Safety Simplifier's supply):

- The Safety Simplifier **cannot disconnect the external voltage source** itself.
- The system can only respond by either:
  - **Disconnecting** other outputs associated with the same programmed function as the faulty I/O.
  - Transitioning the entire unit to a **Fatal Error** state.

An output is considered to be in the **ERROR-state** if it is neither in the **ON-state** nor the **OFF-state.** This is the standard response when an external fault is detected, with a key exception:

| Detected Fault | Default Action | Resulting Output State |
|---|---|---|
| Short circuit to external voltage | Go to ERROR-state | Outputs with failure set to 0V; others in the group set to OFF-state |
| Short circuit to 0V | Go to Fatal Error | Requires system restart |
| Short circuit to 0V | External fuse actuation | Leads to power loss |

Fault Indication and Restart:

1. **Indication:** Outputs in the ERROR-state are switched off and therefore show red in the I/O menu of the LED display; the fault itself is reported in Online Mode in Simplifier Manager and is available as a signal in the application logic.
2. **Restart Requirement:** Even after the physical error on the outputs has been cleared, the affected outputs remain in the ERROR-state until a restart of the affected outputs is performed.
3. **Programmer Actions:** The system programmer can define additional actions in Simplifier Manager for external faults, such as forcing the system into a Fatal Error or executing other programmed safety functions.

# 7 Safety Calculations and Compliance

**Safety Parameters** for the Safety Simplifier components, calculated according to the **IEC 61508** standard for systems operating in a high demand or continuous mode. The hardware has been evaluated according to **route 1S and route 1H** as defined in IEC 61508-2.

## 7.1 Mission Profile for Failure Rate Derivation

The $\mathrm{PFH}_D$ values in this section are valid for the following certified mission profiles, as specified by the client and used as the basis for failure rate derivation per IEC TR 62380:

| Application Area | On/Off | | Permanent | | Storage | |
|---|---|---|---|---|---|---|
| | Operation/24h | Avg Temp (°C) | Operation/24h | Avg Temp (°C) | Operation/24h | Avg Temp (°C) |
| Industrial area 1<br>Robot controls, indoor, 365 days/yr, 24 h/day | N/A | 20 | 24 h | 20 | N/A | 20 |
| Industrial area 2<br>Robot controls, indoor, 5 days/wk, 8 h/day | 8 h | 20 | N/A | N/A | 16 h | 20 |

If the operating environment of the installation differs significantly from these profiles, the applicable $\mathrm{PFH}_D$ values must be re-evaluated.

> **Note:** Simplifier Manager software presents a $\mathrm{PFH}_D$ (Probability of Dangerous Failure per Hour) value for the configured safety functions, but this is only an aid. Every user is responsible for calculating the $\mathrm{PFH}_D$ of their own safety functions from the parameters in this section.

| Parameter | Input | Double CPU Logic | Output (Transistor, Single Channel) | Output (Transistor, Dual Channel) | Double Relay Output | Unit |
|---|---|---|---|---|---|---|
| $\mathrm{PFH}_D$ | $4.61 \times 10^{-9}$ | $2.11 \times 10^{-9}$ | $1.34 \times 10^{-9}$ | $7.76 \times 10^{-10}$ | $3.87 \times 10^{-9}$ | $1/\mathrm{h}$ |
| $\lambda_{\mathrm{DD}}$ (Rate of Detected Dangerous Failures) | $5.98 \times 10^{2}$ | $4.03 \times 10^{2}$ | $1.89 \times 10^{2}$ | $2.39 \times 10^{2}$ | $5.03 \times 10^{2}$ | $10^{-9}/\mathrm{h}$ |
| DC High (Diagnostic Coverage) | 99% | 99% | 99% | 99% | 99% | |
| Diagnostic Test Interval | Continuous<br>(ratio of diagnostic test rate to demand rate ≥ 100) | | | | | |
| Operational Lifetime | 10 | | | | | years |
| Proof Test Interval | 10<br>(proof test equal to lifetime — no interim proof test and no periodic maintenance requirement) | | | | | years |
| MRT (Mean Repair Time) | 8 | | | | | hours |
| Type | $B$ | $B$ | $B$ | $B$ | $B$ | |
| SFF (Safe Failure Fraction) | 99.5% | 99.5% | 99.5% | 99.5% | 99.5% | |
| HFT (Hardware Fault Tolerance) | 1 | 1 | 1 | 1 | 1 | faults |

## 7.2 Safety Standard Classifications

This table shows the classifications achieved by each component on the basis of its architectural design. The Category and Performance Level are those certified under **EN ISO 13849-1:2023.** The maximum SIL — the term EN IEC 62061:2021 uses in place of the former SIL Claim Limit (SIL CL) — is given for integrators applying **EN IEC 62061:2021;** it is derived from the certified safe failure fraction and hardware fault tolerance, and is not a separate certification.

> **Note:** $\mathrm{TM}$ (Mission Time): The lifetime used for calculations according to EN ISO 13849-1:2023.

| Component | EN ISO 13849-1 Category | EN ISO 13849-1 Performance Level (PL) | EN IEC 62061:2021 Maximum SIL (formerly SIL Claim Limit, SIL CL) | TM (Years) |
|---|---|---|---|---|
| Input | 4 | e | 3 | 20 |
| Double CPU Logic | 4 | e | 3 | 20 |
| Output (Transistor, Single Channel) | 3 | d | 2 | 20 |
| Output (Transistor, Dual Channel) | 4 | e | 3 | 20 |
| Double Relay Output | 4 | e | 3 | 20 |

## 7.3 Requirements for Achieving Safety Categories (EN ISO 13849-1:2023)

The Safety Simplifier is designed to support different safety categories based on the wiring configuration and the type of external device used. The following sections detail the requirements for achieving Category 4 and Category 3.

### 7.3.1 Category 4 (Highest Integrity)

Category 4 requires that a single fault does not lead to the loss of the safety function, and that the single fault is detected at or before the next demand upon the safety function. Where such detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function. This is achieved through redundancy and continuous diagnostic testing.

**Single Input Configuration (Category 4)**

While the Safety Simplifier's **Input component inherently fulfills Category 4** due to its double transistor architecture and dual-CPU cross-checking, the **installation** must meet specific requirements to maintain this rating:

- **Dynamically Coded Sensors:** Use **dynamically coded safety sensors** (Type A, B, C, or D) that send a **coded pulsed signal.** The sensor must be wired to a single input and an output on the same Safety Simplifier, with the sensor inverting the signal before sending it back.
- **Double Safety Relay Output:** Category 4 may be achieved when connecting a **double safety relay output** (two relay contacts in series) to a single input, provided that **short circuits can be reliably excluded** in the installation.

**Two Input Configuration (Category 4)**

This is the standard and most straightforward method for achieving Category 4:

- **Dual-Channel Wiring:** Always use **two separate inputs** on the Safety Simplifier for sensors equipped with **two OSSD outputs** or **two mechanical contacts.**
- **OSSD Short Circuit Note:** Supervision of short circuits between the two OSSD signals is **only performed by the sensor itself,** not the Safety Simplifier. OSSD pulses are typically shorter than the Safety Simplifier's cycle time.

**Two Output Configuration (Category 4)**

Achieving Category 4 for an output safety function requires redundant actuation:

- **Dual-Channel Output:** Use **two outputs** simultaneously. The Safety Simplifier supports this using either its **two relay outputs** or **two transistor outputs.** Refer to the examples in this manual for specific wiring guidance.

### 7.3.2 Category 3 (High Integrity)

Category 3 requires that a single fault does not lead to the loss of the safety function, and that, whenever reasonably practicable, a single fault is detected at or before the next demand upon the safety function. Unlike Category 4, an accumulation of undetected faults may lead to the loss of the safety function.

**One Output Configuration (Category 3)**

Category 3 can be achieved using a **single output** under specific limitations:

- **External Voltage Protection:** Risks of short circuits to external voltage must be limited in the installation, as the Safety Simplifier cannot shut off external voltage.
- **Output-to-Output Short Circuit Detection:** If multiple OSSD outputs from the same Safety Simplifier are used, the device includes **short circuit detection between those OSSD outputs.** A short circuit between two or more OSSD outputs will result in **all involved outputs being turned off** (safe state).

### 7.3.3 General Compliance Note

Always check the applicable standards for safety devices and machinery relevant to your specific installation. Special means or additional requirements may be mandated by these standards to achieve the necessary safety level for the machine's overall function.

## 7.4 Calculating PFH D Values

The Probability of Dangerous Failure per Hour ($\mathrm{PFH}_D$) for each safety channel (input to output path) is automatically calculated and generated in the report from Simplifier Manager software. The guidelines below are provided to verify the values in that report.

> **Note:** The $\mathrm{PFH}_D$ for a safety function is highly dependent on the system's programming structure and complexity.
>
> Always refer to the recommended architectural and software design patterns provided in this manual.

### 7.4.1 Component-Level PFH D Values

The base $\mathrm{PFH}_D$ values for the Safety Simplifier are as follows. They are taken from the RISE hardware evaluation report (P124473), which identifies five safety-related hardware elements: input, logic, single transistor output, double transistor output, and relay output. The element names used in this manual map to the report as noted in the table.

| Component Type | $\mathrm{PFH}_D$ Value $(1/\mathrm{h})$ | Notes |
|---|---|---|
| Input (Single or Dual Channel) | $4.61 \times 10^{-9}$ | Single-channel and dual-channel inputs share the same value. |
| Logic | $2.11 \times 10^{-9}$ | |
| Output (Transistor, Single Channel) | $1.34 \times 10^{-9}$ | Named "Single transistor output element" in the hardware evaluation report. |
| Output (Transistor, Dual Channel) | $7.76 \times 10^{-10}$ | Named "Double transistor output element" in the hardware evaluation report. |
| Black Channel (Generic Communication Link) | $0.5 \times 10^{-9}$ | Covers only the communication medium/protocol itself. The Logic value of **each** physical unit that packs or unpacks the safety packet must be added separately — see the worked example below. |
| SimpleCAN | $1 \times 10^{-9}$ | Applies to a SimpleCAN communication link, as specified in the SimpleCAN Manual. See the SimpleCAN section. |

> **Note:** The Black Channel $\mathrm{PFH}_D$ value of $0.5 \times 10^{-9}/\mathrm{h}$ (0.5 FIT) applies to a generic point-to-point safety communication link carried over an unsafe physical medium.
>
> This value is **distinct** from the SimpleCAN-specific $\mathrm{PFH}_D$ value given in the SimpleCAN section — do not combine the two for the same communication path.

The $\mathrm{PFH}_D$ value for the double relay output is dependent on the switching frequency and switched current of the application.

| Max Switched Current | Max Operations / Year | Double Relay Output $\mathrm{PFH}_D$ Value $(1/\mathrm{h})$ |
|---|---|---|
| $2.0A$ | 1260 | $3.87 \times 10^{-9}$ |
| $0.5A$ | 3780 | $3.87 \times 10^{-9}$ |
| $0.2A$ | 100800 | $1.09 \times 10^{-9}$ |

### 7.4.2 System-Level PFH D Calculation Formulas

The total $\mathrm{PFH}_D$ for a complete safety channel is the sum of the $\mathrm{PFH}_D$ values of all elements in the signal path.

| System Architecture | $\mathrm{PFH}_D$ Calculation Formula |
|---|---|
| Single Safety Simplifier | $\mathrm{PFH}_D = \mathrm{Input} + \mathrm{Logic} + \mathrm{Output}$ |
| Multiple Units (Radio Comm. with Repeating Info) | $\mathrm{PFH}_D = \mathrm{Input} + (n \times \mathrm{Logic}) + \mathrm{Output}$ |
| Multiple Units (Radio Comm. without Repeating Info) | $\mathrm{PFH}_D = \mathrm{Input} + (2 \times \mathrm{Logic}) + \mathrm{Output}$ |
| Multiple Units (RadioCAN Safety Communication) | $\mathrm{PFH}_D = \mathrm{Input} + (2 \times \mathrm{Logic}) + \mathrm{Output}$ |
| Multiple Units (Generic Black Channel Communication) | $\mathrm{PFH}_D = \mathrm{Input} + (2 \times \mathrm{Logic}) + \mathrm{Black\ Channel} + \mathrm{Output}$ |
| Multiple Units (Hardwired I/O Interconnection) | $\mathrm{PFH}_D = (\mathrm{Input} + \mathrm{Logic} + \mathrm{Output}) \times m$ |

$n$ = number of Safety Simplifiers in the system
$m$ = number of units from input to output

The following operational lifetimes were used when calculating the $\mathrm{PFH}_D$ values:

- Lifetime used for EN 61508 calculations: 10 years
- Mission Time (TM) for EN ISO 13849-1: 20 years

### 7.4.3 Worked Example: Black Channel Communication Path

Consider a safety function where an E-Stop input on one Safety Simplifier node controls a relay output on a second Safety Simplifier node, linked via a generic Black Channel communication path:

**E-Stop (Input) → Logic (Node 1 — packs packet) → Black Channel → Logic (Node 2 — unpacks packet) → Relay Output**

Both the **transmitting** unit (Node 1, packing the safety packet) and the **receiving** unit (Node 2, unpacking the safety packet) process the data through their own logic. The Logic value must therefore be counted **twice** — once for each physical unit that touches the packet — in addition to the Black Channel's own $\mathrm{PFH}_D$ contribution:

$$\mathrm{PFH}_D = \mathrm{Input} + (2 \times \mathrm{Logic}) + \mathrm{Black\ Channel} + \mathrm{Output}$$

| Element | $\mathrm{PFH}_D$ Value |
|---|---|
| Input (Dual Channel, E-Stop) | $4.61 \times 10^{-9}$ |
| Logic × 2 (Node 1 + Node 2) | $2 \times 2.11 \times 10^{-9} = 4.22 \times 10^{-9}$ |
| Black Channel | $0.5 \times 10^{-9}$ |
| Output (Double Relay, $2.0A$, 1260 ops/yr) | $3.87 \times 10^{-9}$ |
| **Total**: $4.61 + 4.22 + 0.5 + 3.87 = 13.20 \times 10^{-9}/\mathrm{h}$ | |

## 7.5 Calculating System Reaction Time

The Reaction Time (Response Time) is the total time it takes for a safety signal to travel from an input device, through the logic, and to an output device. The guidelines below define the underlying values and formulas.

> **Note:** Simplifier Manager presents a Reaction Time in its report, but this is only an aid. Every user is responsible for calculating the Reaction Time of their own safety functions using the values and formulas in this section. Use the value shown in Simplifier Manager to verify your own calculation.

The logic scan time is $1$ ms. The safety calculation does not add a scan time per unit; instead a fixed **logic margin** $T(L)$ of $2$ ms is added **once per safety function**, covering the logic execution in every unit the signal passes through.

#### Component Delay Times

The total delay is the sum of delays from the input, logic, and output components ($T(I), T(L), T(O)$) plus any configured delay-off times.

| Component Type | $T$ (Component Delay) | Value |
|---|---|---|
| Input (VDC / OSSD / Voltage Window) | $T(I)$ | $2$ ms |
| Input (Pulse train A, B, C or D, or inverted) | $T(I)$ | $9$ ms |
| Logic Margin (once per safety function) | $T(L)$ | $2$ ms |
| Output (Transistor) | $T(O)$ | $1$ ms |
| Output (Relay) | $T(O)$ | $11$ ms |

#### User-Defined Delay-Off Times:

- T(DI): Selected Delay-off for input.
- T(DL): Selected Delay-off in logic.
- T(DO): Selected Delay-off for output.

### 7.5.1 System Reaction Time Formulas

1. Single Safety Simplifier

   The reaction time for a signal processed within a single unit is the sum of all component and programmed delay times.
   $\mathrm{Response\ (ms)} = T(I) + T(\mathrm{DI}) + T(L) + T(\mathrm{DL}) + T(O) + T(\mathrm{DO})$

2. Multiple Safety Simplifiers (Networked)

   When a safety function uses Global Memory (GM) transmitted via Radio or RadioCAN between $2$ to $16$ Safety Simplifiers, the communication timeout ($T(C)$) must be included. $T(C)$ is selected in Simplifier Manager (system-defined timeout value or user-defined).

   The formula breaks the total time into the transmitting unit, the communication link, and the receiving unit.

   **Conceptual formula**
   $\mathrm{Response\ Time} = \mathrm{Node\ 1\ Path} + T(C) + \mathrm{Node\ 2} \rightarrow 16\ \mathrm{Path} + T(L)$

| Conceptual Component | Detailed Expansion |
|---|---|
| Node 1 Path | $T(I) + T(\mathrm{DI}) + T(\mathrm{DL})$ |

| | |
|---|---|
| | This represents the time taken for the signal to process through the input device ($T(I)$), the input's Delay-Off ($T(\mathrm{DI})$), and the logic's Delay-Off ($T(\mathrm{DL})$) in the originating Safety Simplifier (Node 1). |
| T(C) | $T(C)$<br><br>The communication timeout applied to the crossing: the project communication timeout, or the timeout configured for that Global Memory where one overrides it. It bounds the time for the signal to transmit between nodes (Radio/ RadioCAN). |
| Node 2-16 Path | $T(\mathrm{DL}) + T(O) + T(\mathrm{DO})$<br><br>This represents the time taken for the signal to process through the logic's Delay-Off ($T(\mathrm{DL})$), the output device ($T(O)$), and the output's Delay-Off ($T(\mathrm{DO})$) in the receiving Safety Simplifier (Node 2-16). |
| T(L) | $T(L) = 2\ \mathrm{ms}$<br><br>The logic margin, added once per safety function regardless of how many Safety Simplifiers the signal passes through. |

**Fully expanded formula**

$$\text{Response Time (ms)} = [T(I) + T(\mathrm{DI}) + T(\mathrm{DL})] + T(C) + [T(\mathrm{DL}) + T(O) + T(\mathrm{DO})] + T(L)$$

> **Note:** The overall system Response Time is minimized by streamlining the use of Global Memory (GM) across Safety Simplifier units (Node 1 to Node 2-16).
>
> Always use a GM in the originating unit (Node 1) directly to control the output logic in all receiving units (Node 2-16). This uses the shortest Response Time formula, adding only one communication delay ($T(C)$) to the total path.
>
> Do not chain Global Memories (e.g., Node 1 GM → Node 2 GM → Node 3 Output). Each cascaded node introduces any logic delay-off time ($T(\mathrm{DL})$) configured in that node. Neither the logic margin $T(L)$ nor the communication timeout $T(C)$ is added again for a chain of Radio or RadioCAN links — $T(L)$ is counted once per safety function, and these interfaces forward the age of the data, so the chain costs only its longest timeout; see the Chained Communication Interfaces and Age Forwarding section.
>
> $$\text{Cascading Penalty Per Node Added} = T(\mathrm{DL})$$

### 7.5.2 Chained Communication Interfaces and Age Forwarding

When a safety signal passes through more than one communication interface before reaching the output, the way the communication timeouts accumulate depends on whether each interface **forwards the age** of the data.

An interface with age forwarding transmits the already accumulated age of the safety data together with the data itself. The receiving interface then evaluates that total age against its own timeout, instead of starting a new timeout window from zero.

| Interface | Age Forwarding | Effect on Reaction Time |
|---|---|---|
| Radio | Yes | Consecutive interfaces of these types share one age window. The chain contributes only the **longest** timeout of the interfaces in that chain, not the sum of them. |
| RadioCAN (CAN-bus between nodes) | Yes | |
| General Black Channel | Yes | |
| SimpleCAN | No | The age of the data is lost across the link. Everything accumulated before the SimpleCAN link must be added in full, and a new age chain starts at the SimpleCAN link itself. |

**Rule**
Split the communication path immediately **before** every SimpleCAN link. Within each resulting segment, count only the longest timeout. Then add the segments together with the input, logic and output delay times.

**Example 1 — Age forwarded through the whole chain**

**Input → Radio → General Black Channel → Output**

Radio and General Black Channel both forward the age, so they form a single segment and only the longer of the two timeouts counts:

$$\text{Response Time} = T(I) + T(\mathrm{DI}) + \max(T(C_{\text{Radio}}), T(C_{\text{GBC}})) + T(O) + T(\mathrm{DO})$$

**Example 2 — Age chain broken by SimpleCAN**

**Input → Radio → SimpleCAN → General Black Channel → Output**

SimpleCAN does not forward the age, so the Radio timeout can no longer be absorbed by the interfaces that follow it and must be added in full. SimpleCAN and the General Black Channel that follows it form the next segment:

$$\text{Response Time} = T(I) + T(\mathrm{DI}) + T(C_{\text{Radio}}) + \max(T(C_{\text{SimpleCAN}}), T(C_{\text{GBC}})) + T(O) + T(\mathrm{DO})$$

**Note:** The logic delay-off times ($T(\mathrm{DL})$) configured in each unit still apply for **every** Safety Simplifier the signal passes through, and the logic margin $T(L)$ is added once; both are added in addition to the communication timeouts above.

## 7.6 General Functional Test Requirements

The certified hardware data for the Safety Simplifier specifies a **proof test equal to its lifetime:** the unit itself requires no interim proof test and no periodic maintenance within its 10-year operational lifetime, because its internal diagnostics run continuously at a diagnostic coverage of 99 % — see **Safety Parameters.**

The intervals below apply to the **complete safety function,** from the input device through the Safety Simplifier to the output device. External sensors, contactors and other devices in the chain are not covered by the Safety Simplifier's certified data and carry their own diagnostic and test requirements. A functional test of the complete chain, performed either automatically or manually, detects dangerous undetected ($\lambda_{\mathrm{DU}}$) failures in those external parts and confirms that the installation and the application program still perform the safety function as specified.

A functional test of each safety function shall be performed at intervals not exceeding those below, **unless the safety function is demanded at least that often in normal operation.** Where normal operation demands the function more frequently than the stated interval, those demands constitute the functional test and no additional test is required. The integrator shall determine the applicable interval from the machine risk assessment; the values below are maximum intervals specified by SSPN, and are not themselves requirements of EN ISO 13849-1:2023 or EN IEC 62061:2021.

| Maximum Test Interval | Safety Level (EN ISO 13849-1:2023) | Safety Level (EN IEC 62061:2021) |
|---|---|---|
| 30 days (1 month) | PL e with Category 3 or Category 4 | SIL 3 with HFT=1 |
| 12 months (1 year) | PL d with Category 3 | SIL 2 with HFT = 1 |

**Interpretation Notes**

- **HFT (Hardware Fault Tolerance) = 1:** This value indicates that the system architecture is designed to tolerate one single fault and still be able to perform its safety function.
- **Interval Selection:** The specific test interval must be chosen based on the **lowest achieved safety rating** of the safety function chain (input to output). Higher integrity levels (PL e / SIL 3) require more frequent verification.

## 8 Principle Layout and Design

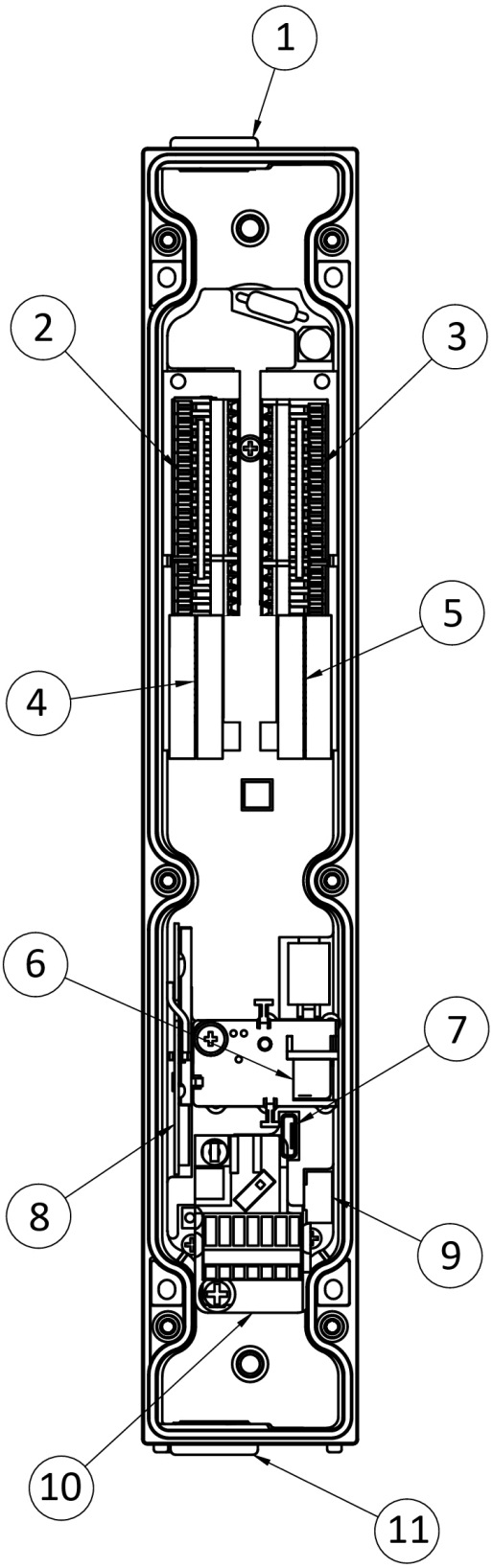



Figure 10: Components inside housing enclosure

**1.** M16/M12 Connector
- Dependent on unit configuration

**2** & **3.** I/O Terminal
- **2** is on the left and **3** is on the right

| | | I/O | I/O | | |
|---|---|---|---|---|---|
| S16 | S14 | 0V | +V | S14 | S16 |
| | | 0V | +V | | |
| | | 0V | +V | | |
| | | +V | +V | | |
| | | 0V | 0V | | |
| | | 1 | 2 | | |
| | | 3 | 4 | | |
| | | 5 | 6 | | |
| | | 7 | 8 | | |
| | | 9 | 10 | | |
| | | 11 | 12 | | |
| | | 13 | 14 | | |
| | 15* | 23 | 43 | 16** | |
| | | 24 | 44 | | |
| | | 33 | 53 | | |
| | | 34 | 54 | | |

**4.** $2x$ Relays ($2x$ Normally Open)
- *Relay output 15 in software

**5.** $2x$ Relays ($2x$ Normally Open)
- **Relay output 16 in software

**6.** Memory Card
- Optional for expanding units memory capacity

**7.** USB
- Micro-USB or USB-C dependant on model

**8.** Radio Module
- External antenna optional

**9.** LED-Display Connector
- Also used for an SSPN Black Channel implementation or an RFID reader

**10.** CAN-Bus Module
- Opto-isolated

**11.** M16/M12 Connector
- Dependent on unit configuration

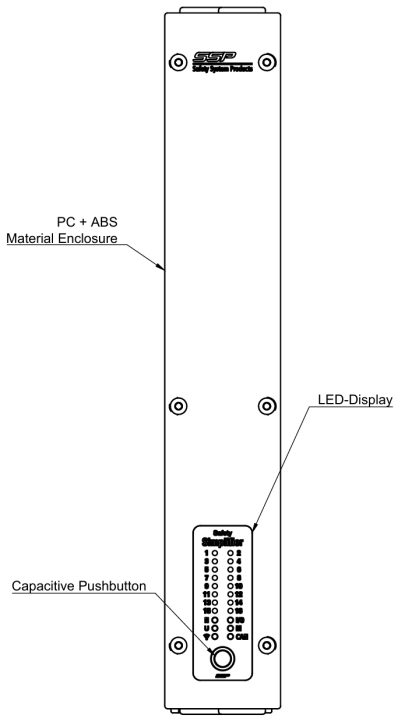
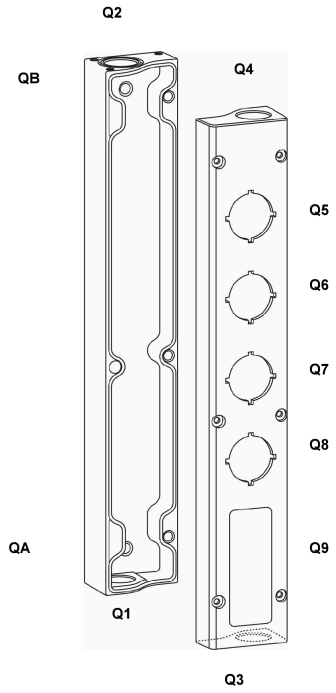



Figure 11: Housing enclosure design

## 8.1 Configuration Availability




| Position | Available Configuration |
|---|---|
| Q1 → Q4 | M16 Cable Gland, M12 Connector & Plug |
| Q5 → Q8 | E-stop, Pushbutton, Selector, Key Selector, Blindplug |
| Q9 | LED Display |
| QA → QB | Screw mounting hole, Ø16 mm |

## 8.2 Dimensions

> **Note:** Dimensions may vary depending on configured unit. Specific dimensions for each customization will be available along the delivered unit.

### 8.2.1 Outer Dimensions

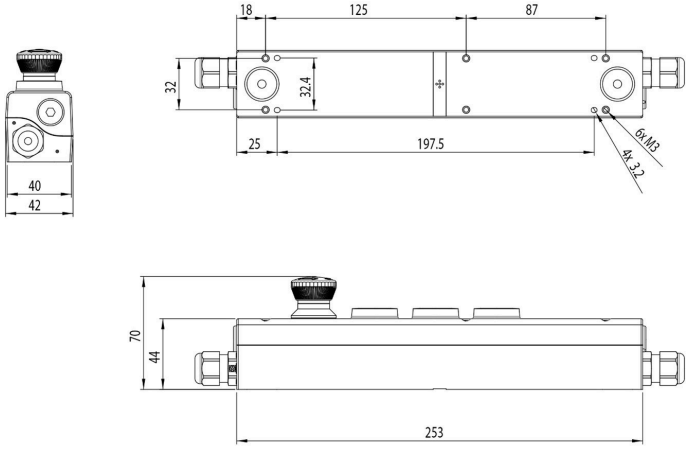
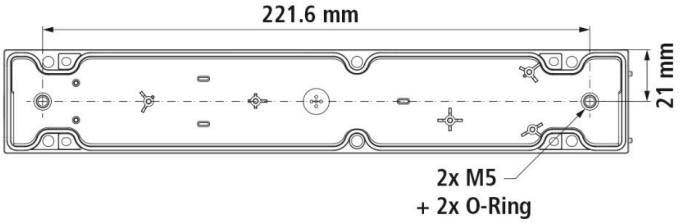


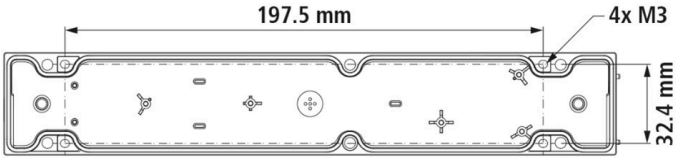

Figure 13: General dimensions of an unit with e-button.

### 8.2.2 Inner Dimensions

**Below shows two mounting holes with sealings for M5 screws.**




**Below shows four mounting holes for M3 screws.**



# 9 Mounting Procedures

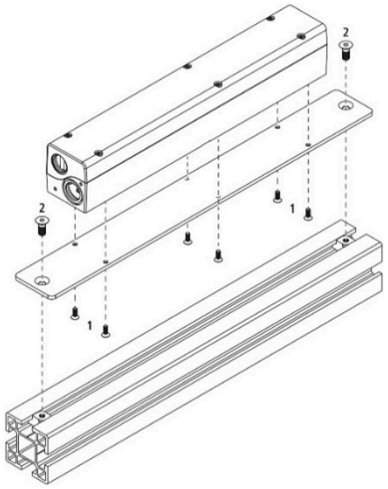
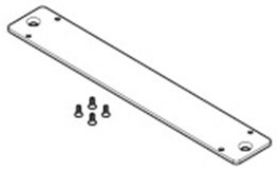


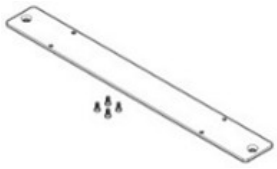
Figure 16: Mounting a Safety Simplifier unit on a large bracket, onto a aluminum 44x44 profile.

## 9.1 Small Bracket Installation

| Aluminum - 253 x 40 x 3 mm | Article No. SP-N-88-850-01 |
|---|---|
|  | |

1. Secure the small bracket to the mounting surface using two screws. The bracket length matches the Safety Simplifier unit dimensions.
2. Attach the Safety Simplifier to the mounted bracket using the four supplied M3 screws.

## 9.2 Large Bracket Installation

| Aluminum - 338 x 40 x 3 mm | Article No. SP-N-88-850-02 |
|---|---|
|  | |

1. Attach the large bracket directly to the bottom surface of the Safety Simplifier using the six supplied M3 screws.
2. Mount the bracket assembly to the installation surface using two M5 screws through the 5 mm mounting holes.

## 9.3 Direct Surface Mounting (Without Brackets)

The Safety Simplifier base features four mounting holes designed for M3 screws, enabling direct surface installation without bracket hardware.

## 9.4 Center Knockout Preparation

Two pre-formed knockout holes are located in the center of the Safety Simplifier enclosure. These knockouts can be removed by applying pressure with a flathead screwdriver.

**NOTICE**

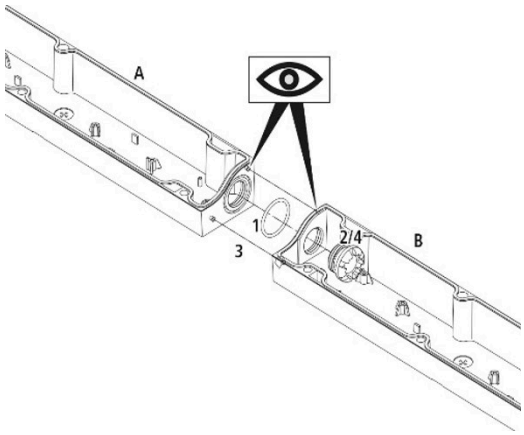
**Loss of the IP rating at center knockouts**
Other screws break the enclosure's IP rating, so water can enter and damage the unit.
- When utilizing center knockouts, use only the specified M5 screws with integrated sealing washers.

## 9.5 Multiple Enclosure Stacking

Two or more Safety Simplifier enclosures can be mechanically joined using the connection screw assembly.

**Installation Procedure:**

1. Position the bottom surface of the upper unit (A) against the top surface of the lower unit (B).
2. Verify alignment pins (Item 3) on the lower unit engage with corresponding receptacles in the upper unit.
3. Insert the O-ring seal (Item 1) onto the connection screw (Item 2/4).
4. Thread the connection screw through the lower unit into the upper unit until secure.




**NOTICE**

**Loss of the IP rating when stacking**
Without the O-ring seal, the enclosure loses its IP rating, so water can enter and damage the unit.
- Install the O-ring seal.
- Ensure alignment pins are properly seated before tightening connection screws.

## 9.6 Mounting Accessories

| M5 screw with O-ring | Article No. SP-N-88-001-89 |
|---|---|
|  | |
| O-ring plug for mounting from outside.<br><br>O-ring plug for inside mounting when joining two units | Article No. SP-N-88-001-73<br><br>Article No. SP-N-88-001-60 |
|  | |
| Connection M16 screw and O-ring | Article No. SP-N-88-001-90 |



## 9.7 Scope of Supply

- Safety Simplifier unit in the configuration ordered, as identified by the model designation on the product label
- Cable gland or connector plugs fitted to unused ports, according to the ordered configuration
- Optional accessories as ordered: mounting brackets, M12 connectors, M16 cable glands, external antenna and antenna cable, CAN communication card, Simplifier Monitor

Check the delivery against the order and against the model designation on the product label before installation. Report any discrepancy or transport damage to SSPN before commissioning.

## 9.8 Spare Parts and Accessories

The Safety Simplifier contains no user-replaceable internal parts. Repairs to the unit are carried out only by SSPN or by a service centre authorized by SSPN.

The following items affect the health and safety of operators and must therefore be obtained from SSPN, or must meet the specification given in this manual:

| Item | Requirement |
|---|---|
| Cable glands and port plugs | Must maintain the declared IP rating of the enclosure. Unused ports must be sealed. |
| M12 connectors | Must be rated for the installation environment and correctly torqued to maintain the IP rating. |
| Mounting brackets | Use only the small or large bracket specified in the Mounting Accessories section. Wall or bracket mounting is a condition of the IP66 rating. |
| GORE-TEX ventilation membrane | Not user-replaceable. A unit with a damaged membrane must be returned to SSPN. |
| External antenna and antenna cable | Must meet the attenuation and environmental requirements given in the Internal and External Antenna section. |
| CAN communication card | Plug-in card supplied and fitted by SSPN or by authorized personnel. |

The use of spare parts or accessories not approved by SSPN voids manufacturer liability, as stated in the Liability Disclaimer section.

# 10 Electrical Installation

**⚠ WARNING**

**Unexpected activation during installation**
Installing while the supply is connected can activate hazardous equipment unexpectedly, which could result in death or serious injury, or equipment damage.
- Disconnect or de-energize the supply voltage before installing the Safety Simplifier and all external devices.

## 10.1 Power Supply Requirements

The Safety Simplifier shall be supplied from a power supply meeting the requirements for **SELV** (safety extra-low voltage) or **PELV** (protective extra-low voltage) in accordance with **IEC 61140.** The supply shall provide protective separation between the mains and the extra-low voltage output. SELV and PELV here describe the power supply that may be selected; the installed circuit is always a PELV circuit, because the 0V terminal is bonded to the protective bonding circuit — see **Earthing and protective bonding** below.

Where the Safety Simplifier forms part of the electrical equipment of a machine, **EN 60204-1,** clause 6.4 additionally governs the use of PELV and places requirements on the supply source. The following applies to the power supply unit whether it feeds the Safety Simplifier directly or through an intermediate control circuit.

**Source**
Protective separation between the mains and the output, and between the output and all other circuits, shall be achieved by double insulation, reinforced insulation, or an earthed protective screen. The supply shall be one of the following:

- A **safety isolating transformer** complying with **IEC/EN 61558-2-6**
- A **switch-mode power supply** complying with **IEC/EN 61558-2-16**
- A power supply whose output is classified **ES1** in accordance with **EN IEC 62368-1,** so that the energy available at the output is not hazardous under normal, abnormal, and single-fault conditions

In every case the source shall be constructed so that its output voltage cannot exceed the extra-low voltage limit even in the event of an internal fault.

Protective separation is a property of the output of the supply, not of the protection class of the supply unit. A **class I** (earthed) power supply unit is acceptable provided its output meets SELV or PELV. **Protection class II is not required.**

**Voltage**
- Nominal output within the operating range of the Safety Simplifier: 7–33 VDC, normally 10–30 VDC. 24 VDC is the customary choice.
- The output shall be **ripple-free DC not exceeding 60 V** — the PELV limit where the equipment is in a dry location and large-area contact with the human body is not expected (EN 60204-1, clause 6.4). Where either condition is not met, the limit is **15 V.** Ripple-free means an r.m.s. ripple content of not more than 10 % of the DC component.

**Earthing and protective bonding**
The Safety Simplifier has no internal electrical connection between its 0V terminal and protective earth or the enclosure, so either a SELV or a PELV supply may be used as the source. The 0V terminal of the Safety Simplifier shall nevertheless be connected to the protective bonding circuit in accordance with EN 60204-1, clause 9.4.3.1 (method a) — see Installation Standards Compliance. This connection makes the installed circuit a PELV circuit and is what allows earth faults in single-channel circuits to be detected. It shall not be omitted. A SELV supply therefore does not remain a SELV circuit once installed: the choice between a SELV and a PELV supply is a choice of equipment, not a choice of installation method.

**Current and protection**
- Rate the supply for the total load: up to 210 mA for the Safety Simplifier itself, plus up to 2 000 mA for the transistor outputs (600 mA per output) — a design load of approximately 2.2 A. The supply shall deliver at least the external fuse rating continuously at the chosen nominal voltage.
- An external **2.5 A fast-acting fuse** shall be installed in the supply line — see the Performance Specifications chapter. The internal overcurrent protection of the Safety Simplifier does not replace it.

## 10.2 Operating Voltage Specifications

**⚠ WARNING**

**Electric shock from voltages above 33 VDC or AC**
The Safety Simplifier is designed exclusively for low-voltage DC systems: the absolute operating range is 7–33 VDC and the normal operating range is 10–30 VDC. Outside the configured voltage limits the unit enters the Safe State; connection to voltages above 33 VDC or to AC may damage the unit and cause an electric shock, which could result in death or serious injury.
- Use only cables and connected devices (including sensors, pushbuttons, and selector switches) rated for isolation at 240V AC.
- Connect only to a supply within the operating range.

The Safety Simplifier is compatible with both 12V and 24V DC systems, with an operational voltage range of 7–33 VDC. The acceptable voltage range may be restricted through software configuration to accommodate external sensors and equipment with more stringent voltage requirements. If the supply voltage exceeds or falls below the configured limits, the unit will transition to a safe state and display a voltage fault indication via the LED interface. From firmware 2.3 the default limits are a low-voltage warning at 8 V and a minimum of 7 V, so that a 9 V supply can be used; a unit keeps its stored limits until its settings are reset.

Due to radio or optically isolated CAN-bus communication between Safety Simplifier units, each device may be configured to operate at different voltage levels as required by the application.

## 10.3 Terminal Specifications and Wiring

The Safety Simplifier utilizes spring-type terminals designed to withstand high-vibration environments. Multiple terminals are provided for both supply input and output distribution.

## 10.4 Installation Standards Compliance

**⚠ WARNING**

**Operation before the installation is validated**
An installation that is not verified and validated can leave a safety function that does not work as specified, which could result in death or serious injury.
- Do not operate the Safety Simplifier until the complete installation has been verified and validated in accordance with the functional specifications derived from the system risk analysis.

The Safety Simplifier is designed for applications conforming to IEC-EN 60204-1:

- Control circuits shall be supplied through a safety isolating transformer (IEC/EN 61558-2-6) or an equivalent PELV source — see Power Supply Requirements
- For electrical safety, and to enable detection of safety-critical earth faults in single-channel circuits, the 0V terminal must be connected to the protective bonding circuit (EN 60204-1, clause 9.4.3.1, method a)

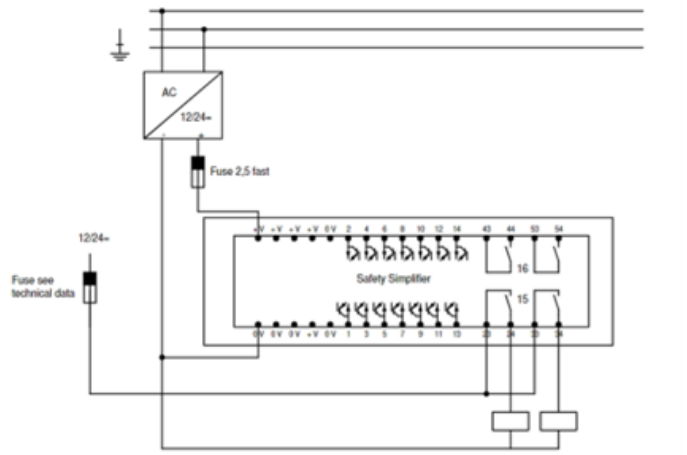



Figure 18: Fusing and power supply to Safety Simplifier and external relays/contactors

## 10.5 I/O Connections Procedure

The I/O spring-clamp terminals on the Safety Simplifier can be actuated using a small flat-blade screwdriver (typically 2.5–3.0 mm width). Insert the screwdriver into the terminal actuator slot and slide towards the insertion point to release the clamp mechanism for wire insertion or removal.

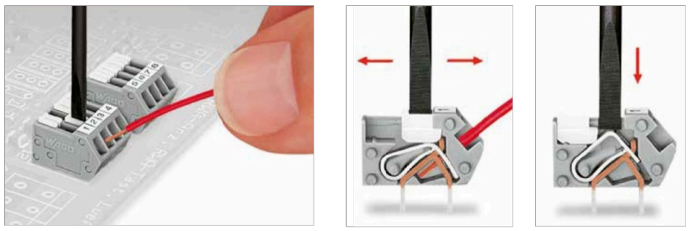


Figure 19: I/O spring-clamp terminal wiring — insert a flat-blade screwdriver to release the clamp for wire insertion or removal.

> **Note:** The I/O terminals accept both **solid** and **fine-stranded** conductors of $0.08–0.5\text{mm}^2$ (28–20 AWG). Fine-stranded conductors may be fitted with an insulated or uninsulated ferrule of $0.25\text{mm}^2$. Strip the conductor to $5–6\ \text{mm}$ and insert it at approximately $40°$ to the board.
>
> $0.75\text{mm}^2$ (18 AWG) conductors can be terminated, but their insulation diameter then allows only every other clamping unit on the terminal strip to be used.

# 11 Bus Communication via Radio and/or RadioCAN

### Communication Interface Overview

Both the S14 and S16 standard models support optional radio and CAN-bus communication modules. A networked system may include up to 16 Safety Simplifier units, each capable of accessing 16 Global Memory (GM) variables from any other Safety Simplifier within the network — up to **256 bits of safety information** in total, freely distributed between the nodes. These GM variables may be utilized for safety-critical functions as well as diagnostic and status information purposes.

**RadioCAN** is the name for GM communication between Safety Simplifier nodes carried over the CAN-bus module — the wired counterpart to the Radio interface, and a plug-and-play replacement for it: the same GM variables and the same configuration, with no change to the application logic. SimpleCAN uses the same physical CAN-bus module but is a separate protocol for communication between different systems; see Section 11.1.

### Dual-Interface Operation

When a Safety Simplifier is equipped with both radio and CAN communication modules, both interfaces (Radio and RadioCAN) will transmit GM status data by default. The receiving Safety Simplifier always uses the freshest GM data available from either interface, which gives the lowest response time.

### Communication Topology

**Radio Communication:** The wireless network operates with mesh topology, where GM data is repeated and relayed between all radio-equipped units within range.

**RadioCAN Communication:** The RadioCAN interface transmits GM data only to devices physically connected to the **same network system of Safety Simplifiers.** To communicate with **external network system,** please refer to Section 11.1. Both communication systems use the same CAN-bus module.

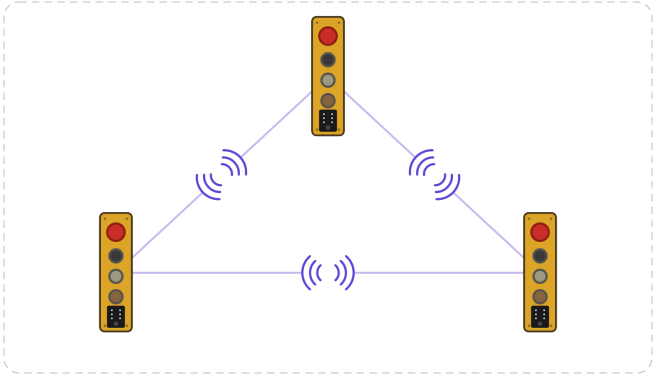


Figure 20: Radio is a broadcast mesh inside one system installation

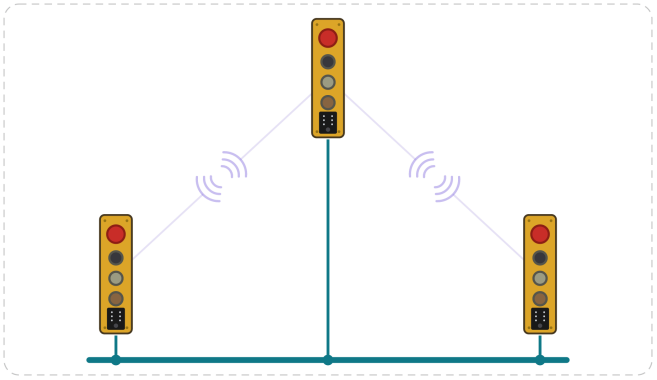


Figure 21: RadioCAN is the wired alternative to radio, not a second network

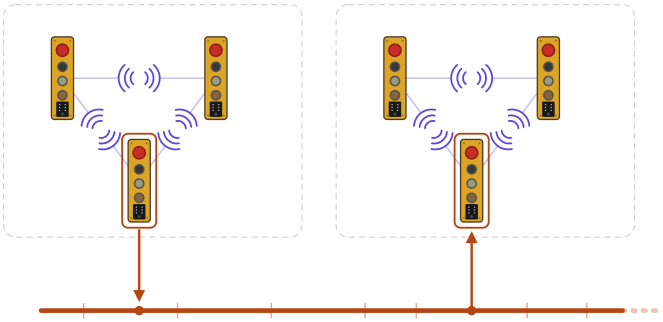


Figure 22: SimpleCAN crosses the boundary between system installations

### Module Installation Requirements

**Radio Module:** Must be specified and installed at the time of initial order. The radio card cannot be retrofitted in the field.

**CAN Module:** May be installed at any time during the product lifecycle. The CAN card installation procedure consists of inserting the module into the designated slot until fully seated, then securing it with the provided retention screw.

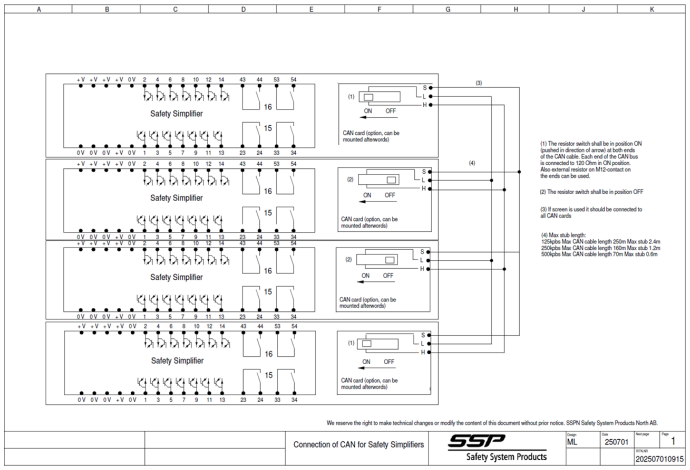



Figure 23: Wiring diagram for CAN-Bus connections between four Safety Simplifiers

## 11.1 SimpleCAN

SimpleCAN is a safety-rated communication protocol designed for transmitting safety-critical information between separate Safety Simplifier networks, and between Safety Simplifier networks and Simplifier Gateway (enabling communication with systems such as

Siemens/PROFIsafe). A SimpleCAN network supports up to 64 unique SimpleCAN identifiers (SC01–SC64). Each identifier transmits:

- 16 bits of safety-rated data
- 16 bits of non-safety data (for diagnostic and status information)

This architecture provides a maximum capacity of **1,024 safety bits per SimpleCAN network.** The physical CAN layer must maintain **continuous** topology, repeater devices shall not be used to extend network segments.

For programming and configuration procedures, refer to the separate **SimpleCAN Manual.**

### 11.1.1 Network and Node Limits

| Parameter | Maximum |
|---|---|
| Unique SimpleCAN identifiers per network (SC01–SC64) | 64 |
| Transmit (TX) blocks per network | 64 |
| TX + RX blocks per Safety Simplifier node (combined total) | 64 |
| Safety data per Safety Simplifier node | 1,024 bits |
| Non-safety data per Safety Simplifier node | 1,024 bits |
| SimpleCAN networks per Simplifier Gateway | 2 (one on CAN 1, one on CAN 2) |

A SimpleCAN identifier may be used only **once** within a network — two nodes shall not transmit the same SimpleCAN ID. The 64 blocks per node may be divided freely between transmit and receive (for example 64 TX and 0 RX, or 0 TX and 64 RX). Additional SimpleCAN networks can be created by adding further Simplifier Gateways.

### 11.1.2 Master Node Requirement

Every SimpleCAN network requires at least one node to act as **master** on the bus. Any Safety Simplifier node configured with at least one SimpleCAN TX block is a potential master. A Simplifier Gateway cannot act as master, and neither can a node configured with receive blocks only.

### 11.1.3 SimpleCAN Data Blocks

Data is exchanged using SimpleCAN **TX blocks** (transmit) and **RX blocks** (receive), configured in Simplifier Manager. Each block carries 16 safe bits (CM01–CM16) and 16 non-safe bits (CM17–CM32); the non-safe bits may be used for status and indication tasks that do not require redundant safety.

A data point is identified by its block ID (SC01–SC64) together with its data number (CM01–CM32).

> **Note:** The SimpleCAN network settings — baud rate, cycle time and timeout — must be **identical** in every project that shares the network. A SimpleCAN network typically spans several separate Safety Simplifier projects, and mismatched settings prevent communication from being established.

### 11.1.4 Calculating $\mathrm{PFH}_D$ Value

Use $1 \times 10^{-9}$ as the $\mathrm{PFH}_D$ value for SimpleCAN when calculating the total system $\mathrm{PFH}_D$.

### 11.1.5 Calculating Maximum Reaction Time

The maximum reaction time for SimpleCAN is determined by the **user-configured SimpleCAN network timeout value.** Since the timeout is dependent on the cycle time, both parameters are defined below.

### 11.1.6 Cycle Time

The minimum permissible cycle time is determined by the configured baud rate and by how the nodes in the network are configured. Simplifier Manager validates the cycle time against the configuration parameters and displays an error if the specified cycle time is insufficient.

General Guideline: The cycle time should be **at least** equal to the number of SimpleCAN identifiers on the bus plus 2 milliseconds:

$$T_{\text{cycle}} = N_{\text{IDs}} + 2$$

Example: 4 SimpleCAN IDs → minimum 6 ms cycle time

This requirement applies to baud rate configurations of 125 kbit/s and may also be applied to higher baud rates for consistent operation.

### 11.1.7 Timeout Configuration

The **recommended** timeout value is calculated as $2 \times \text{cycle time} + 5$ ms:

$$T_{\text{timeout}} = T_{\text{cycle}} \times 2 + 5$$

Example: 20 ms cycle time → 45 ms timeout

This configuration ensures that two consecutive dropped or invalid packets do not trigger a timeout condition.

An **alternate**, stricter timeout may be configured where a shorter reaction time is required; however, this reduced timeout allows only **one dropped packet** before a timeout occurs:

$$T_{\text{timeout}} = T_{\text{cycle}} \times 1 + 5$$

**Table: Cycle Time and Timeout Calculations for 125 kbit/s Baud Rate**

| | | Recommended | Alternate |
|---|---|---|---|
| SimpleCAN IDs | Cycle Time (ms) | Timeout (ms) | Timeout (ms) |
| 2 | 4 | 13 | 9 |
| 3 | 5 | 15 | 10 |
| 4 | 6 | 17 | 11 |
| 5 | 7 | 19 | 12 |
| 6 | 8 | 21 | 13 |
| 7 | 9 | 23 | 14 |
| 8 | 10 | 25 | 15 |
| 9 | 11 | 27 | 16 |
| 10 | 12 | 29 | 17 |
| .. | .. | .. | .. |
| 54 | 56 | 117 | 61 |
| 55 | 57 | 119 | 62 |
| 56 | 58 | 121 | 63 |
| 57 | 59 | 123 | 64 |
| 58 | 60 | 125 | 65 |
| 59 | 61 | 127 | 66 |
| 60 | 62 | 129 | 67 |
| 61 | 63 | 131 | 68 |
| 62 | 64 | 133 | 69 |
| 63 | 65 | 135 | 70 |
| 64 | 66 | 137 | 71 |

**Note:** Values for SimpleCAN IDs 11–53 follow the same progression and are omitted for brevity.

> **Note: SimpleCAN requirements.** SimpleCAN shall only be implemented using the data link layer specified in ISO 11898-1 (Controller Area Network). SimpleCAN is a protocol layer operating on CAN 2.0; all requirements and limitations defined in CAN 2.0 apply to SimpleCAN implementations.
>
> Application-specific standards must be observed based on the operational environment; for machinery and process control applications, the principles defined in EN 61918 (common section) shall be applied.
>
> Only SimpleCAN-compatible devices (Safety Simplifier and Simplifier Gateway) are authorized as transmitters in a SimpleCAN network. Silent listeners are permitted to monitor the network in silent mode (per CAN 2.0 specifications).

### 11.1.8 Installation and Commissioning

A Safety Simplifier system using SimpleCAN is connected in exactly the same way as a system using RadioCAN — refer to the CAN-bus wiring described in the Bus Communication chapter. Downloading the configuration is also performed in the same way.

Cable requirements, termination and maximum cable lengths for the CAN bus are specified in the CAN 2.0 section of the Performance Specifications chapter.

### 11.1.9 Diagnostics and Maintenance

#### 11.1.9.1 No Communication

The CAN status LED on the Safety Simplifier, located to the right of the CAN card, is the primary indication of the bus state:

- **Red:** Bus disconnected — no communication.
- **Orange:** Bus error.
- **Blinking green:** Communication established and synchronized.

The RX and TX LEDs on the CAN card itself indicate raw bus activity: when either or both are dimly lit or blinking fast, traffic is present on the bus.

If communication cannot be established, verify the following:

- The termination resistors are correctly fitted at both ends of the bus.
- The CAN-H and CAN-L conductors are connected to the H and L terminals respectively in **all** nodes on the CAN bus.
- All nodes in the network use the correct network settings (baud rate, cycle time and timeout). This is particularly important for SimpleCAN networks, which span several separate Safety Simplifier networks and therefore several separate projects.

#### 11.1.9.2 Online Mode

SimpleCAN can be diagnosed using Online Mode in Simplifier Manager, where the state of each bit can be observed live in the logic diagram. Online mode can be entered either wirelessly via the Simplifier Monitor, or via USB connected directly to the Safety Simplifier.

# 12 Modbus

(from firmware 2.3.0)

The Safety Simplifier is a Modbus server. A PC, a PLC or an HMI can read and write the node's aux signals and read its measurements, memories and black channel status.

> ⚠ **WARNING**
>
> **Modbus signals used for safety**
> Modbus data is not safe: the aux signals exist on one processor only, and are white (unsafe) in the logic. A safety function built on them, in the Simplifier or in the Modbus client, can fail without the fault being detected, which could result in death or serious injury.
> - Use Modbus for status, control requests and diagnostics only.
> - Send safety data between nodes over SimpleCAN.

## 12.1 Connecting

Modbus RTU runs on the USB port. Open the node's USB serial port at **19200 baud, 8 data bits, even parity, 1 stop bit**. At any other setting the port speaks the Simplifier Manager protocol, so Simplifier Manager and a Modbus client use the same cable, one at a time.

- The node answers Modbus only in normal operation, not in the bootloader or during a firmware update.
- Every server (slave) address except 0 is answered, with the request's address. Broadcast (address 0) is ignored.
- A frame ends after 3 ms without bytes.
- A frame with a bad CRC gets no answer.

**Modbus TCP.** An Ethernet-enabled Simplifier, one with an SSPN Black Channel implementation on Ethernet, also answers Modbus TCP, with the same function codes, registers and behaviour as over USB:

- TCP port 502; every unit id is answered. One client at a time.
- The IP address, netmask and gateway are set on the Ethernet board's own web page (Ethernet Communicator manual, MAN003).
- At most 20 requests per second, with bursts of 2 in a row; a request over that is not executed and gets exception 0x06.
- A request that the Simplifier does not answer, for example while its logic is not running, gets exception 0x0B, about 170 ms after the request.
- A request for more than 9 registers is carried in parts; only each part is read consistently.
- Once the Ethernet board has the time from its NTP server, it sets the node's clock, registers 60..61, every minute.

## 12.2 Function codes

| Code | Function | Registers per request |
|---|---|---|
| 0x03 | Read Holding Registers | 1..125 |
| 0x04 | Read Input Registers | 1..125 |
| 0x06 | Write Single Register | 1 |
| 0x10 | Write Multiple Registers | 1..123 |

0x03 and 0x04 read the same registers. There are no coils or discrete inputs: the aux bits are packed in registers.

## 12.3 Register map

Addresses are 0-based, as sent on the wire: register 1 in a 1-based client is address 0. Registers are 16 bit. A 32-bit value is two registers, low word first.

| Address | Content | Writable, default |
|---|---|---|
| 0..15 | aux inputs 0..255, 16 per register | yes, 0 |
| 16..31 | aux outputs 0..255, 16 per register; one consistent copy per read | |
| 32 | ms since an aux input was last written; stops at 65535 | |
| 33 | aux input timeout flags: bit n is set when register n timed out, until it is written again | |
| 50 | aux input timeout, ms; 0 is none (Section 12.5) | yes, 2000 |
| 60..61 | clock: seconds since 1970-01-01 00:00 UTC, 32 bit; 0 is not set. Write both registers in one request (0x10); the node counts on from the value written. The clock is lost at a restart. | yes, 0 |
| 100 | supply voltage, mV | |
| 101 | board temperature, 0.01 °C, signed | |
| 110..123 | SIO1..14 voltage measured by CPU1, mV. Not correct while the SIO is an output driving high. | |
| 130..143 | SIO1..14 voltage measured by CPU2, mV; up to a few tens of ms old; above 65.535 V reads 65535. Correct in every configuration. | |
| 1000..1064 | radio memories, safe (Section 12.6) | |
| 1200..1248 | radio memories, non-safe | |
| 2000..2259 | SimpleCAN memories, safe | |
| 2400..2595 | SimpleCAN memories, non-safe | |
| 3000..3112 | black channel memories, safe | |
| 3200..3264 | black channel memories, non-safe | |
| 4000..4905 | black channel status (Section 12.7) | |

Addresses not listed are not mapped or are for internal use. A request that reaches an unmapped address, or writes a register that is not writable, is answered with exception 0x02.

**Aux bit order:** aux input n is bit n mod 16 of register n ÷ 16, rounded down; bit 0 is the least significant bit. Aux input 0 is register 0 bit 0; aux input 17 is register 1 bit 1. The aux outputs follow the same order from register 16. In the logic they are the **Aux Input** and **Aux Output** blocks.

## 12.4 Examples

Bytes in hex, server address 1; the last two bytes of each frame are the CRC, low byte first.

**Read the supply voltage** (input register 100, Section 12.3):

| | |
|---|---|
| Send | `01 04 00 64 00 01 70 15`: address 1, function 0x04, first register 0x0064, 1 register |
| Receive | `01 04 02 5D C0 81 F0`: 2 data bytes, 0x5DC0 = 24000 mV, so 24.000 V |

**Set aux inputs 0 and 2, all others of register 0 to 0** (write register 0 = 0x0005):

| | |
|---|---|
| Send | `01 06 00 00 00 05 49 C9`: address 1, function 0x06, register 0x0000, value 0x0005 |
| Receive | `01 06 00 00 00 05 49 C9`: the request repeated, written |

## 12.5 Aux input timeout

The aux inputs work as a heartbeat: a client that fails cannot keep outputs active for ever.

- After a restart the timeout is 2000 ms. Writing register 50 changes it until the next restart; 0 switches the timeout off.
- Each aux input register (0..15) has its own countdown, started again by every write to it, also when the value does not change. A client therefore writes its registers well within the timeout.
- When a register is not written within the timeout, its 16 aux inputs are reset to 0, and its bit in register 33 is set until the register is written again.
- The timeout and the countdowns are shared by every way of writing the aux inputs: Modbus, Simplifier Manager and CANlibre. A write by any of them starts the register's countdown again.

## 12.6 Memory blocks

**NOTICE**

This section describes internal information. Its layout may change in future firmware releases.

Each block is the node's memory group data, word by word: group n is word n of each field.

| Block | Fields |
|---|---|
| radio, safe | `raw` 1000..1015, `mem` 1016..1031, `age` 1032..1047, `invalid` 1048..1063, `link_ok` 1064 |
| radio, non-safe | `raw` 1200..1215, `mem` 1216..1231, `age` 1232..1247, `link_ok` 1248 |
| SimpleCAN, safe | `raw` 2000..2063, `mem` 2064..2127, `age` 2128..2191, `invalid` 2192..2255, `link_ok` 2256..2259 |
| SimpleCAN, non-safe | `raw` 2400..2463, `mem` 2464..2527, `age` 2528..2591, `link_ok` 2592..2595 |
| black channel, safe | `raw_rx` 3000..3015, `rx` 3016..3031, `rx_invalid` 3032..3047, `rx_age` 3048..3063, `rx_link_ok` 3064, `tx` 3065..3080, `tx_invalid` 3081..3096, `tx_age` 3097..3112 |
| black channel, non-safe | `raw_rx` 3200..3215, `rx` 3216..3231, `tx` 3232..3247, `rx_age` 3248..3263, `rx_link_ok` 3264 |

| Field | Meaning |
|---|---|
| `raw`, `raw_rx` | the last value received for the group; never cleared |
| `mem`, `rx` | the value the logic uses; 0 after the group's timeout |
| `tx` | the value the node sends |
| `age`, `rx_age`, `tx_age` | the age of the group's value |
| `invalid`, `rx_invalid`, `tx_invalid` | invalid flags, one per bit; safe memories only |
| `link_ok`, `rx_link_ok` | bit n is set while group n is within its timeout; SimpleCAN has 64 groups, so two 32-bit values, low word first |

## 12.7 Black channel status

**NOTICE**

This section describes internal information. Its layout may change in future firmware releases.

| Address | Content |
|---|---|
| 4000 | UART packets received with a bad checksum |
| 4001 | good UART packets received; wraps after 65535 |
| 4004 | low byte: channels still setting up |
| 4006 + 56·n | channel n = 0..15: low byte setup state, high byte channel type |
| 4008 + 56·n, 4009 + 56·n | channel n status flags, 32 bit: channel up, peer to peer, broadcast send and receive, packet received |
| 4012 + 56·n, 4013 + 56·n | channel n packets with a bad checksum, 32 bit |
| 4902, 4903 | UART packets rejected for framing or length, 32 bit |

The other words in 4000..4905 are internal.

## 12.8 Exceptions

| Code | When |
|---|---|
| 0x01 Illegal Function | a function code other than those in Section 12.2 |
| 0x02 Illegal Data Address | an address in the request is not mapped, a write reaches a register that is not writable, or a write covers only one of the clock registers 60..61 |
| 0x03 Illegal Data Value | wrong quantity, byte count or frame length |
| 0x04 Server Device Failure | the request reaches addresses 0..33 or 1000..3264 while the logic is not running |
| 0x06 Server Device Busy | Modbus TCP only: over the request rate limit (Section 12.1) |
| 0x0B Gateway Target Device Failed to Respond | Modbus TCP only: the Simplifier did not answer the Ethernet board |

# 13 CANlibre

(from firmware 2.2.0)

CANlibre is a non-safe, CANopen-style exchange of the node's aux signals over a CAN port. A PC, a PLC or any CANopen device writes up to 256 aux inputs into the node and reads up to 256 aux outputs from it with plain PDO frames. The other side needs no CANopen stack, only standard 11-bit CAN frames. CANlibre follows CANopen NMT and heartbeat (CiA 301) and can start the other nodes as NMT master (CiA 302-2).

**⚠ WARNING**

**CANlibre signals used for safety**
CANlibre data is not safe: the aux signals exist on one processor only, and are white (unsafe) in the logic. A safety function built on them, in the Simplifier or in the device at the other end, can fail without the fault being detected, which could result in death or serious injury.

- Use CANlibre for status, control requests and diagnostics only.
- Send safety data between nodes over SimpleCAN.

## 13.1 Settings

CANlibre is set per node in Simplifier Manager.

| Setting | Meaning |
|---|---|
| Mode, per CAN port | off, or the start-up behaviour (Section 13.5): NMT slave, self-starting, or NMT master that starts all nodes |
| Node ID | CANopen node ID 1..127, the same on both ports; it decides every CAN ID (Section 13.2) |
| Heartbeat | heartbeat period, ms; 0 sends the boot-up message only |
| Max burst | TPDOs sent back to back before the burst limit applies (Section 13.4) |
| Burst refill | time, ms, to regain one TPDO of burst allowance |
| TPDO on change | send a TPDO when its data changed |
| TPDO periodic, period | also send every TPDO every period, ms, changed or not |

A port with CANlibre runs at the bit rate of its CAN network and may share the bus with SimpleCAN.

## 13.2 Frames

All frames use standard 11-bit identifiers; ID is the node ID.

| CAN ID | Direction | DLC | Content |
|---|---|---|---|
| 0x000 | to the node, or from it as NMT master | 2 | NMT: byte 0 command, byte 1 node ID (0 = all nodes) |
| 0x200 + ID | to the node | 8 | RPDO1: aux inputs 0..63 |
| 0x300 + ID | to the node | 8 | RPDO2: aux inputs 64..127 |
| 0x400 + ID | to the node | 8 | RPDO3: aux inputs 128..191 |
| 0x500 + ID | to the node | 8 | RPDO4: aux inputs 192..255 |
| 0x180 + ID | from the node | 8 | TPDO1: aux outputs 0..63 |
| 0x280 + ID | from the node | 8 | TPDO2: aux outputs 64..127 |
| 0x380 + ID | from the node | 8 | TPDO3: aux outputs 128..191 |
| 0x480 + ID | from the node | 8 | TPDO4: aux outputs 192..255 |
| 0x700 + ID | from the node | 1 | boot-up (0) and heartbeat: the NMT state (Section 13.5) |

With node ID 1, RPDO1 is 0x201 and TPDO1 is 0x181.

**Bit order:** the 8 bytes of a PDO are one little-endian 64-bit word. Byte 0 bit 0 is the first signal of the frame, byte 7 bit 7 the last: in TPDO1, byte 0 bit 0 is aux output 0 and byte 7 bit 7 is aux output 63; in TPDO2, byte 0 bit 0 is aux output 64. The RPDOs and the aux inputs follow the same order. In the logic the signals are the **Aux Input** and **Aux Output** blocks. A TPDO is one consistent copy of its 64 signals.

When 64 signals each way are enough, send RPDO1, read TPDO1 and ignore the others.

## 13.3 Received frames

- An NMT command is obeyed when byte 1 is 0 or the node ID. A frame with another length is ignored.
- An RPDO is accepted in OPERATIONAL only. An RPDO with fewer than 8 bytes is ignored.
- SYNC, TIME, SDO and EMCY are not supported and are ignored. There are no synchronous PDOs.
- Node ID collision: when another node sends a heartbeat with our node ID after our boot-up, or, in OPERATIONAL, a TPDO with our node ID, the node goes to STOPPED and stays there until an NMT start.

## 13.4 Sending TPDOs

In OPERATIONAL the node serves its 4 TPDOs in turn. A TPDO is sent when **TPDO on change** is set and its data differs from the last sent, or when **TPDO periodic** is set and the period has passed since it was last sent. On entering OPERATIONAL each periodic timer starts at a random point in its period, so the nodes do not send at the same time.

Burst limit: at most **Max burst** TPDOs back to back, then one more per **Burst refill** time. Heartbeat and NMT frames are not counted. The burst limit keeps CANlibre from flooding a bus it shares with SimpleCAN.

## 13.5 NMT states

| State | Heartbeat | PDOs |
|---|---|---|
| PRE-OPERATIONAL | 127 | none |
| OPERATIONAL | 5 | RPDOs accepted, TPDOs sent |
| STOPPED | 4 | none |

- After start-up the node sends its boot-up message (0x700 + ID, data 0) and enters PRE-OPERATIONAL.
- Then, by mode: an NMT slave waits for NMT *start remote node*; a self-starting node enters OPERATIONAL; an NMT master sends one *start remote node* to all nodes (0x000, data 01 00) and enters OPERATIONAL. This happens once per boot-up; later NMT commands are obeyed as they come.
- NMT commands: 0x01 start (from PRE-OPERATIONAL or STOPPED), 0x02 stop, 0x80 enter PRE-OPERATIONAL. 0x81 *reset node* and 0x82 *reset communication* both reset communication: the node sends a new boot-up and starts again by its mode. The safety logic is never reset from CAN, which deviates from CiA 301.
- The heartbeat is sent every heartbeat period in every state after boot-up, STOPPED included.
- As NMT master, while OPERATIONAL, the node sends *start remote node* to any other node whose boot-up or heartbeat shows state 0 or 127.
- Keep at most one NMT master per network.

## 13.6 Aux input timeout

(from firmware 2.3.0)

An RPDO is a write of its 4 aux input words, 16 aux inputs each. Each word has its own countdown, and every RPDO starts the countdown of its 4 words again. One timeout applies to all words: 2000 ms after start-

up, changeable over USB, 0 is no timeout. When a word's countdown runs out, its 16 aux inputs go to 0 until the word is written again. Writes over USB follow the same rule.

A device that writes the aux inputs therefore sends its RPDOs cyclically, well within the timeout, also when the values have not changed. Watch the node's heartbeat: when it is missing for a few periods, treat every aux output as stale.

# 14 Electrical Wiring with Safety Devices

Pushbutton, selector switch, and key-selector functions are fully programmable to meet application-specific requirements. Available functions include, but are not limited to, Start, Reset, Stop, and Mode Selection operations.

The Safety Simplifier software allows customization of input device behavior, including:

- Momentary or latching operation
- Normally open (NO) or normally closed (NC) contact configuration
- LED illumination control (where applicable)
- Multi-position selector configuration
- Key-selector position assignment
- Assignment to safety or non-safety functions

Refer to Simplifier Manager manual for detailed programming procedures.

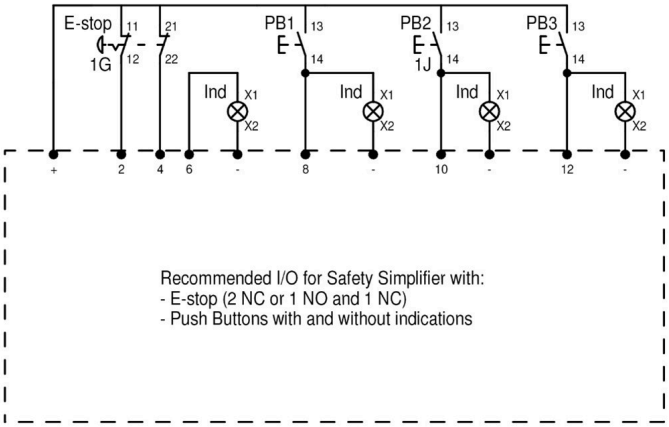



Figure 24: Safety Simplifier with e-stop and three pushbuttons

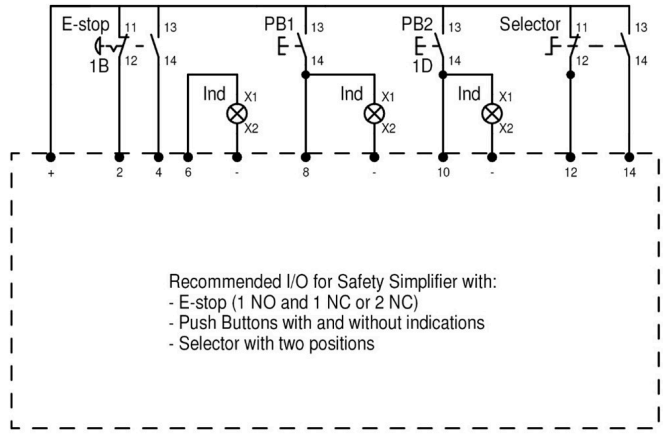



Figure 25: Safety Simplifier with e-stop, two pushbuttons and a selector

## 14.1 Two-Hand Control Devices

**Compliance Standard**

The Safety Simplifier supports two-hand control stations compliant with **EN ISO 13851:2019** (formerly EN 574) **up to Type IIIC.**

EN ISO 13851:2019, "Safety of machinery — Two-hand control devices — Principles for design and selection," supersedes the withdrawn EN 574+A1:2008. The certified two-hand function blocks were type tested against EN 574 and satisfy the corresponding requirements of EN ISO 13851:2019; see the EC Type-Examination Certificate referenced in the Classification and Conformity Assessment section for the certified scope.

**Configuration Requirements** Two-hand control circuits can be programmed to meet the following EN ISO 13851:2019 (formerly EN 574) operational requirements:

- Type II or Type III operation, up to Type IIIC (synchronous actuation with or without time monitoring)
- Adjustable synchronization timing parameters
- Anti-defeat protection through software logic
- Configurable reset requirements

Refer to Simplifier Manager manual for two-hand control setup procedures and timing parameter configuration.

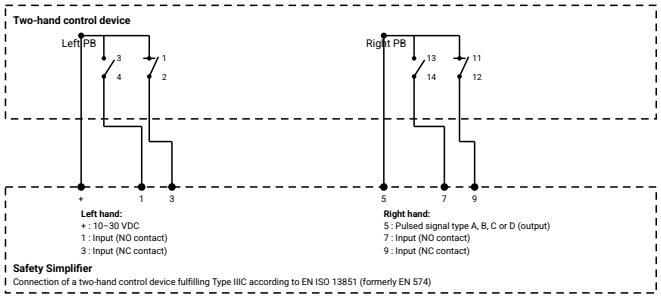



Figure 26: Safety Simplifier with a two-hand control device fulfilling Type IIIC according to EN ISO 13851:2019 (formerly EN 574)

## 14.2 Safety Devices with OSSD Outputs

The Safety Simplifier accepts input connections from safety devices equipped with Output Signal Switching Device (OSSD) interfaces, including but not limited to:

- Safety light curtains
- Safety laser scanners
- Safety mats and pressure-sensitive edges
- Two-hand control devices with OSSD outputs

The Safety Simplifier inputs accept the OSSD (Output Signal Switching Device) signals used by safety sensors, including the test pulses such devices superimpose on their outputs, and monitor the two channels for signal integrity and discrepancy.

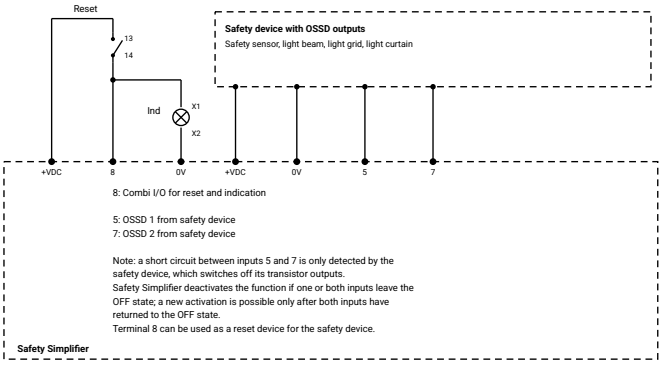



Figure 27: Safety Simplifier with OSSD capable device

## 14.3 Safety Gate Limit Switches

Safety gate monitoring can be implemented using:

- Coded magnetic safety switches
- Trapped-key interlocks
- Safety position switches with guard locking

The Safety Simplifier supports both single-channel and dual-channel safety gate monitoring configurations, with programmable guard locking and time delays. Standard mechanical limit switches without a safety rating are not safety devices and may be used for non-safety signalling only.

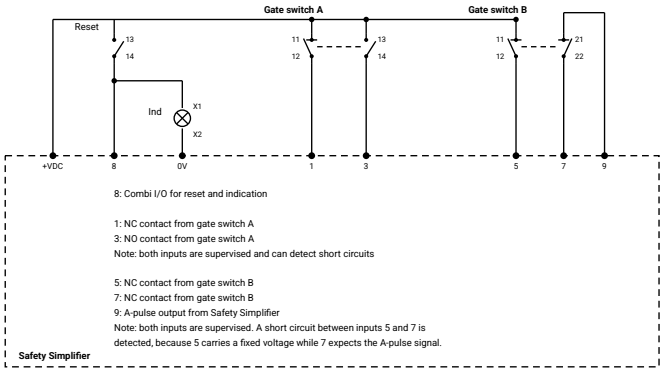



Figure 28: Safety Simplifier with gate switches

## 14.4 Relay Outputs for Contactors with Feedback Supervision

The Safety Simplifier provides relay outputs specifically designed for contactor control with mandatory feedback monitoring. This configuration enables:

- Contactor auxiliary contact supervision
- Welded contact detection
- Delayed dropout monitoring
- Configurable fault response behavior

Feedback monitoring ensures detection of contactor malfunctions, including contact welding or mechanical failure, before hazardous machine motion can occur.

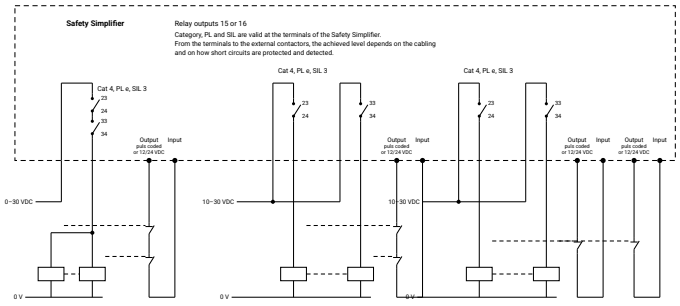



Figure 29: Safety Simplifier with relay wiring

## 14.5 Relay Outputs for Machines and Safety Devices

General-purpose safety-rated relay outputs are available for controlling:

- Machine actuators and drives
- Brake systems
- Pneumatic and hydraulic valve solenoids
- External safety modules and relays

These outputs may be configured for safety-critical or non-safety control functions based on application requirements.

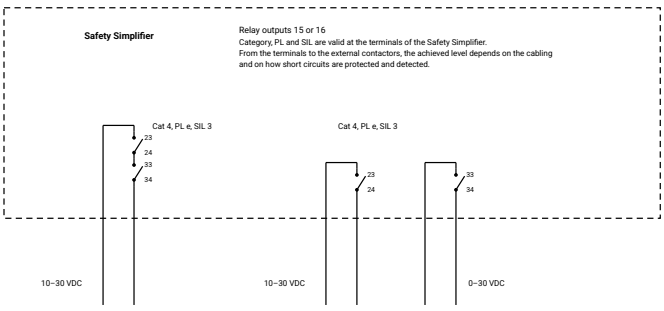



Figure 30: Safety Simplifier with relay wiring

## 14.6 OSSD Outputs for Machines, Contactors, and Safety Devices

The Safety Simplifier provides OSSD output interfaces for direct connection to:

- Machine control systems with OSSD inputs
- Safety contactors equipped with OSSD monitoring
- Safety PLCs and distributed I/O systems

OSSD outputs provide semiconductor-switched, short-circuit monitored signalling of the kind used by safety sensors, and can be connected to equipment with OSSD-compatible inputs. Their safety performance is that certified in the Safety Standard Classifications table: a single OSSD output supports Category 3; two OSSD outputs are required for Category 4.

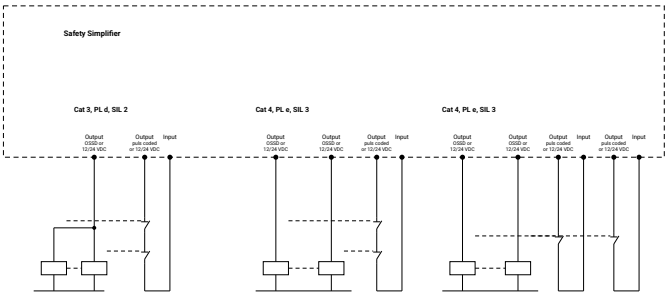



Figure 31: Safety Simplifier with multiple OSSD outputs

# 15 LED Display

**Display Interface Overview**

Safety Simplifier units with the LD option feature an integrated LED display with capacitive touch navigation for diagnostics. Units without a display provide the same information via USB in Simplifier Manager.

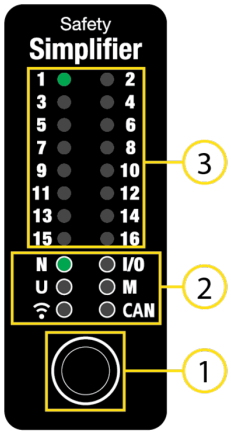



Figure 32: LED Display Interface

1. **Capacitive Pushbutton** – Navigation control for scrolling through display menus
2. **Menu Indicator** – Displays the currently active menu selection
3. **Information Display Area** – Shows menu-specific data and status information

Press the **capacitive pushbutton (1)** to cycle through available menus. The active menu identifier appears in the **menu indicator field (2),** with corresponding data displayed in the **information area (3).**

Available menus and their functions are described in the following sections.

## 15.1 Navigation Procedure

To navigate between display menus, use the capacitive pushbutton located on the front panel. A firm, short press (duration less than 1 second) advances the display to the next menu in the sequence.

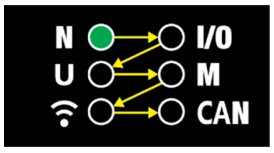



Figure 33: Menu navigation sequence

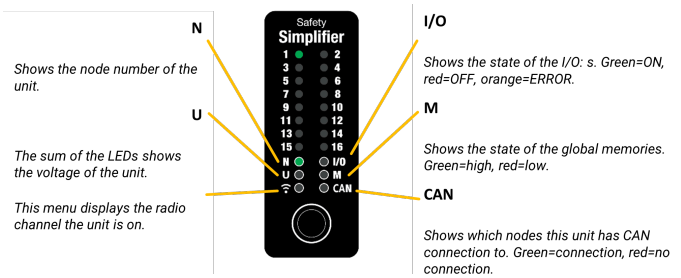
**Cycling Behavior**

Each press of the capacitive pushbutton advances the display by one menu position. When the CAN menu is active, pressing the button returns the display to the N menu, completing the cycle.

Note: To navigate backward through the menu sequence (e.g., from I/O menu to N menu), the button must be pressed repeatedly to cycle through all subsequent menus. In this example, 5 button presses are required to return from I/O to N.

## 15.2 Menu Overview

The menu indicators (see Figure 32, number **2**) illuminate green for the active menu. Navigate between menus by applying a brief, firm press to the capacitive button. After 5 minutes without a button press the display automatically returns to the I/O menu, since the I/O status is the information most often wanted at a glance.




## 15.3 Maintenance States

The unit leaves Normal Mode in two situations: while a configuration is being downloaded (Configuration Mode), and when it has detected an error (Fatal Error Mode). In both states all outputs are in the Safe State. The LED display distinguishes the two as shown below.

### 15.3.1 Configuration Mode

The unit is offline and all outputs are forced to the Safe State. This is the only state in which a new configuration can be downloaded from a PC via USB or radio (Figure 35).

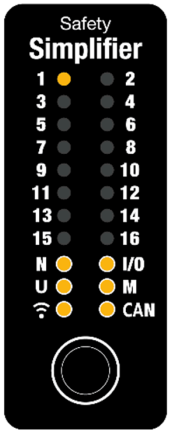



Figure 35: Unit in Configuration Mode

### 15.3.2 Fatal Error Indication

When the unit detects an internal or external error, it may enter Fatal Error Mode (Figure 36). For detailed information, see Section 16.7.

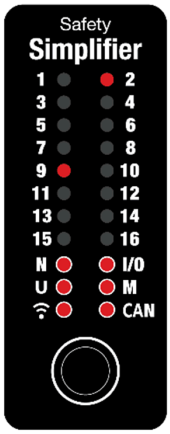



Figure 36: Unit in Fatal Error Mode

### 15.3.3 Firmware Update (Bootloader)

While a firmware update is in progress, all six menu LEDs are lit **orange.** Once the radio has started, the Radio menu LED changes to green and the numbered LED for the active radio channel is lit. Do not disconnect power while the unit is in this state.

A unit also stays in this state when its logic was compiled for

another firmware version: firmware 2.3 refuses a logic compiled for 2.2. Recompile the logic with the compiler of the installed firmware (C3 v2.3.0 for firmware 2.3.0) and download it again; the recompiled logic is a configuration change (Simplifier Manager and Software Version Control).

# 16 Menu Structure

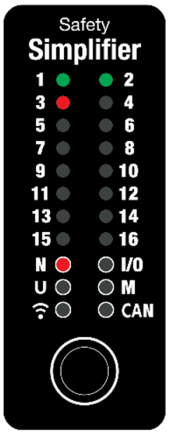
The following sections describe the information displayed in each menu and submenu, including visual representations of different menu states.

The display illustrations presented in the following sections are representative examples. Actual display content will vary based on system configuration, installation parameters, and operational state.

## 16.1 N Menu

Displays the node number assigned to the current Safety Simplifier unit, and the network connectivity status for all other nodes in the system.

- **Solid green LED:** This unit's own node number
- **Slowly blinking green LED:** Active radio or RadioCAN (CAN-bus) connection established with the displayed node
- **Slowly blinking red LED:** No radio or RadioCAN (CAN-bus) connection to the displayed node
- **No LED (off):** Node number not part of the configured system




In Figure 37, the unit has established connection with Node 1 (itself) and Node 2 (via either radio or CAN-bus). No connection exists with Node 3. An active connection ensures that Global Memory (GM) variables are exchanged between connected nodes.

**Information**
This menu indicates the presence of either radio or RadioCAN (CAN-bus) connectivity, but does not differentiate between the two. To determine which interface carries the link to a given node, use Online Mode in Simplifier Manager.

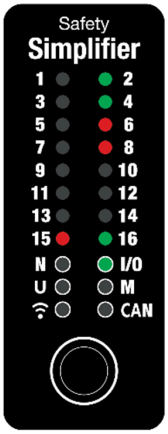
## 16.2 I/O Menu

This menu displays the real-time status of all I/O terminals on the unit. The display automatically returns to this menu after 5 minutes without a button press. Terminal status is indicated by LED color as follows:

**Normal Operation Status:**

- **Green LED:** I/O terminal in ON state (active)
- **Red LED:** I/O terminal in OFF state (inactive)
- **No LED (off):** Terminal not programmed or not configured

For transistor I/O (terminals 1–14) the LED reflects the measured voltage on the terminal; for the relay outputs (15 and 16) it reflects the relay drive state.




In Figure 38, I/O terminals 2 and 4 are in the ON state, I/O terminals 6 and 8 are in the OFF state, relay output 15 is in the OFF state, and relay output 16 is in the ON state.

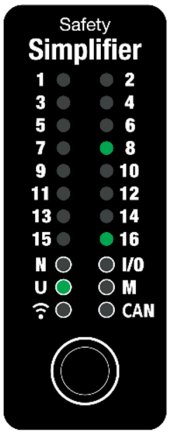
**External I/O Faults**

External faults on input and output terminals (short circuit, external voltage, invalid coded signal) are not indicated separately in this menu: the affected terminal is switched off and therefore shows red. The fault itself is reported in Online Mode in Simplifier Manager and is available to the application logic — see the Handling External I/O Faults section.

## 16.3 U Menu

Displays the supply voltage of the unit, rounded to the nearest volt. The voltage value is calculated as the sum of the illuminated LED numbers.

**Voltage Calculation Example:**




In Figure 39, LEDs 8 and 16 are illuminated, indicating a supply voltage of $8 + 16 = 24V$.

**Display Behavior:**

- For voltages ≤16 V, only a single LED is illuminated
- For voltages 17–31 V, LED 16 plus one further LED are illuminated and summed
- For voltages 32–45 V, LEDs 16 and 15 plus one further LED are illuminated and summed

**Voltage Warning Indication:**

When the supply voltage is outside the configured warning limits, the voltage LEDs change from green to **orange.** By default the warning limits are 8 V and 32 V, and the unit enters Fatal Error below 7 V or above 33 V — the operating range stated in the technical data. All four limits are configurable in Simplifier Manager.

**Waiting for Power**

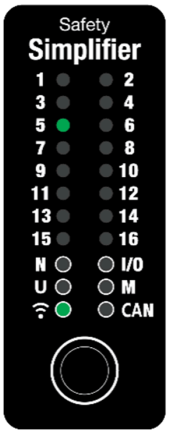
After power-on the unit waits until the supply voltage reaches the **low warning limit** (8 V by default) before starting its logic. While waiting, the U menu LED is orange and the measured voltage is shown in **red.**

## 16.4 M Menu

Reserved.

## 16.5 Radio Menu

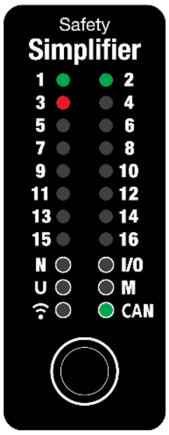
This menu displays the radio channel assigned to the unit. Figure 40 shows a unit operating on channel 5. If the unit is configured with more than one radio channel, every channel in use is shown.




## 16.6 CAN Menu

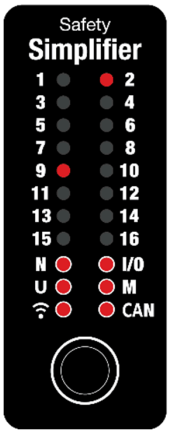
The CAN menu is indicated by the CAN menu LED lit green together with the M menu LED blinking green. In the current firmware this menu is reserved for SimpleCAN status and displays no information in the numbered LED area.

RadioCAN (CAN-bus) link status to the other nodes is shown in the N menu, combined with the radio link status. SimpleCAN status is available in Online Mode in Simplifier Manager.




## 16.7 Fatal Error Mode

When the unit detects an internal or external error, it may transition to Fatal Error Mode. Upon entering this state, all I/O channels are deactivated, safety communication over radio and RadioCAN (CAN-bus) ceases, and an error code is displayed on the LED interface.




### 16.7.1 Fatal Error Condition

Fatal error conditions are indicated on the LED display when the N, I/O, U, M and CAN menu LEDs illuminate in red, accompanied by one or more numbered LEDs also illuminated in red. The Radio menu LED remains **green**, indicating only that the radio module is still powered; safety communication has ceased, and the error code is available solely on the LED display and via USB.

The numbered LEDs show the 16-bit error code as a binary pattern: LED $n$ is lit when bit $n-1$ of the code is set, so LED 1 is the least significant bit and LED 16 the most significant. The error code is the sum of $2^{n-1}$ over all lit LEDs.

**Example:** error code 1025 (**Power supply too low**) is $2^0 + 2^{10}$, so LEDs **1** and **11** are lit. The figure above is an illustration of the display pattern, not a specific code.

The online decoder at https://www.sspn.se/error-code/ converts a lit-LED pattern to the error name and back. **Restarting from Fatal Error**

The unit leaves Fatal Error Mode only by a restart: switch the supply off and on again. The capacitive pushbutton does not restart the unit. Before restarting, read and record the error code — it is held only until the next restart. If the cause of the error is still present, the unit returns to Fatal Error Mode after the restart.

## 16.8 Error Codes

Visit https://www.sspn.se/error-code/ to view a list of error codes.

# 17 Cybersecurity

Cybersecurity is an integral part of the product development and quality management processes. SSPN continuously works to identify, assess, and manage cybersecurity risks throughout the product lifecycle.

## 17.1 Security by Design

Safety Simplifier has been developed with both functional safety and product cybersecurity in mind. Current product security characteristics include:

- **SIL 3 / PL e certified architecture** — fail-safe design with continuous hardware diagnostics
- **Password-protected programming and configuration** — only authorized personnel with the correct password can download or modify a configuration
- **Signed and encrypted firmware updates** — every firmware update is digitally signed and verified by the device before installation; unsigned or tampered firmware is rejected
- **Version-controlled firmware releases** — controlled release process for all firmware updates
- **Established quality management processes** — cybersecurity activities are integrated into the company's Quality Management System

## 17.2 Software and Firmware Components

Safety Simplifier firmware is developed by SSPN and incorporates a combination of proprietary software and open-source components. A Software Bill of Materials (SBOM) for the current firmware version will be published on the Product Security webpage: https://www.sspn.se/security/

**Simplifier Manager**

Simplifier Manager is configuration software that compiles the safety logic executed by the Safety Simplifier, and is therefore safety-related software. It is versioned and released independently of the Safety Simplifier firmware. The version of Simplifier Manager used to compile a configuration, together with the resulting application program verification code, must be recorded in the machine technical file — see the Simplifier Manager and Software Version Control section. Obtain Simplifier Manager only from SSPN or an authorized distributor.

## 17.3 Communication Interfaces

The Safety Simplifier provides the following communication interfaces:

| Interface | Purpose |
|---|---|
| USB (Micro-USB or USB-C, model dependent) | Configuration and diagnostics via Simplifier Manager. From firmware 2.3, also Modbus RTU on the USB virtual COM port, without a password: reading measurements, memories and black channel status, and writing the aux inputs, which are unsafe signals and never part of a safety function (Modbus chapter). Requires physical access to the unit. |
| LED-display connector | The LED display, or instead one of: an SSPN Black Channel implementation, carrying the general black channel at 500 kbit/s (an implementation made for firmware 2.2, at 115200 baud, does not work with 2.3); an RFID reader (Pepperl+Fuchs IQT4, multidrop), from firmware 2.3. Requires physical access to the unit. |
| 2.4 GHz radio (a special protocol based on IEEE 802.15.4) | Safety communication between Safety Simplifier units. Also used for wireless configuration via Simplifier Monitor connected to a PC running Simplifier Manager. |
| CAN bus | Safety communication between Safety Simplifier units (RadioCAN), and between separate systems (SimpleCAN). |

The Safety Simplifier itself has no Ethernet interface and no internet connectivity. Ethernet, including Modbus TCP (Modbus chapter), is available only through an SSPN Black Channel implementation fitted to the LED-display connector, a separate product with its own conformity assessment and its own manual, the Ethernet Communicator manual (MAN003).

## 17.4 Intended Operational Environment

Safety Simplifier is intended for use in industrial environments where physical access to the installation area is controlled and restricted to authorized personnel. The product's security properties are designed on the assumption that:

- The unit and its communication interfaces (USB port, CAN bus, radio) are not physically accessible to untrusted parties during normal operation
- The configuration password is held by a defined group of authorized personnel
- The installation is within a controlled facility subject to access management appropriate for the safety application

The product is not designed for deployment in environments where the wireless interface or CAN bus is exposed to untrusted parties without additional network security measures in place.

## 17.5 Protection of Safety Functions (Machinery Regulation 2023/1230, Annex III, EHSR 1.1.9 and 1.2.1)

The Machinery Regulation (EU) 2023/1230, Annex III, Essential Health and Safety Requirement 1.1.9, requires that safety-relevant software, data, and the hardware components that transmit them be identified as such and protected against corruption, whether accidental or deliberate. The Regulation further requires that interventions in safety software be traceable. The following architectural properties address these requirements.

**Configuration integrity**

Downloading a configuration to the Safety Simplifier requires Simplifier Manager with either a direct USB connection or a Simplifier Monitor, and the correct password. The unit verifies the authenticity and integrity of the configuration before applying it. An incomplete, corrupted, or unauthorized configuration will not be accepted.

**Firmware authenticity**

Firmware updates are digitally signed. The device verifies the signature against a public key stored in immutable, write-locked memory before an update is installed — unsigned or tampered firmware is rejected. The device additionally enforces rollback protection: a validly signed but older firmware version is refused, so a security fix cannot be silently reverted. Once a unit has run firmware with signed updates, it cannot be returned to earlier firmware without signed updates, by anyone, the manufacturer included.

**Continuous hardware diagnostics**

The Safety Simplifier contains internal automatic online monitoring logic that runs continuously and cannot be affected or overridden by the user or application program. If an internal fault is detected — including inconsistency between redundant channels — all outputs transition to the safe (de-energized) state regardless of the programmed logic.

**Safety communication integrity**

CAN bus and radio communication between Safety Simplifier units

uses a safety protocol compliant with IEC 61784-3. The safety layer includes sequence numbers, CRC integrity checks, and watchdog timeout monitoring. Safety integrity does not depend on the security of the physical bus or radio link. Manipulation or corruption of communication link causes the safety protocol to detect an error and transition to safe state.

**Limited network attack surface**
Safety Simplifier itself has no Ethernet or internet interface; an SSPN Black Channel implementation on Ethernet is a separate product with its own assessment. Configuration is performed using Simplifier Manager via a direct USB connection or a Simplifier Monitor. There is no persistent remote access interface. The configuration password is the primary access control in both cases.

**Evidence of intervention**
The Regulation requires that evidence be collected of a legitimate or illegitimate intervention in software or configuration that is critical for compliance. Every application program carried by a Safety Simplifier has a unique verification code derived from the contents of the program. Any change to the configuration, however small, produces a different code.

The verification code, the installed firmware version, and the unit serial number are read out through Simplifier Manager, over USB or through a Simplifier Monitor, and are reproduced in the configuration report that Simplifier Manager generates for the safety documentation. Comparing the code recorded in the machine technical file against the code read from the unit establishes whether the safety configuration has been altered since it was validated.

This comparison shall form part of every periodic inspection — see the Periodic Inspection section — and the result shall be recorded. An unexplained change of the verification code shall be treated as a suspected security incident and handled according to the Responding to a Suspected Security Incident section.

**Five-year retention of tracing data**
In compliance with Regulation (EU) 2023/1230, Annex III, EHSR 1.2.1, a tracing log of all safety software modifications, configuration uploads, and firmware updates must be maintained and retrievable for a period of **five (5) years** after such upload. Simplifier Manager generates a timestamped configuration report containing the unique verification code, firmware version, and unit serial numbers. The machine integrator and plant owner must archive these reports in the machine technical file for the mandatory five-year period to demonstrate conformity upon request from competent authorities.

Each record shall capture:

- **Type of intervention** — whether the event was a configuration download, a modification of the safety logic, or a firmware update
- **Timestamp or counter** — the date and time of the intervention, or another means of correlating it with other records
- **Application program verification code** — the unique code generated by Simplifier Manager for the compiled configuration
- **Software and firmware versions** — the Safety Simplifier firmware version, and the Simplifier Manager version used to compile the program
- **Target hardware identity** — the serial number of every Safety Simplifier node the upload was applied to

The tracing log shall be protected against tampering, and the deletion of any record shall itself be evidenced in the log.

This tracing data is maintained exclusively to demonstrate conformity to a national market surveillance authority upon a reasoned request.

**Division of responsibility**
SSPN ensures that Simplifier Manager and the Safety Simplifier generate the traceability data listed above in the exported configuration report and project archive. The machine integrator and the plant owner are responsible for archiving those reports and retaining them for the full five-year period as part of the machine technical file.

**Identification of installed software**
The Safety Simplifier identifies the software installed on it and makes that information available at any time, without special tools, through Simplifier Manager:

- **Firmware version** — the version executing on the unit
- **Application program verification code** — the identity of the compiled safety configuration
- **Unit serial number** — the identity of the physical unit the configuration is installed on

Record these items in the machine technical file at commissioning, after every configuration change, and after every firmware update, together with the Simplifier Manager version used.

**Residual responsibility**
The architectural properties above provide inherent protection of the safety functions within the Safety Simplifier itself. However, they do not substitute for the physical access controls and installation measures described in the Secure Installation section. Unauthorized physical access to the unit or its communication interfaces remains the primary residual risk and must be managed at the installation level.

## 17.6 Secure Installation

To reduce the risk of unauthorized access to the Safety Simplifier:

- **Physical access:** Install the Safety Simplifier where only trusted, authorized persons have physical access to it — its enclosure, USB port, memory card, debug pins and terminal blocks — for example inside a locked enclosure. Connecting a PC, a CAN adapter or any other device to the unit is physical access.
- **USB port:** The USB port is used for configuration and diagnostics via Simplifier Manager. Ensure the USB port is not accessible to unauthorized persons in the final installation.
- **Simplifier Monitor:** A Simplifier Monitor allows Simplifier Manager to configure Safety Simplifier units wirelessly without a direct USB connection to the unit. When a Simplifier Monitor is in use, the configuration password is the primary barrier against unauthorized access. Do not leave a Simplifier Monitor unattended in a PC that is within radio range of operational units.
- **CAN bus:** Its data are not authenticated. Keep the CAN cabling, and every node or device connected to it, inside the area of restricted physical access, and connect no CAN node to a network outside that area except through a connection you protect.
- **LED-display connector:** Connect it only to an SSPN Black Channel implementation located close to the unit, inside the area of restricted physical access; the line between them is not authenticated, and the security beyond the implementation is that product's.
- **Memory card:** A memory card holds the unit's logic, settings and firmware, and anyone holding it can read it. Keep memory cards, fitted or spare, under the same physical access control, and sanitize or destroy a card before it leaves your control.
- **Wireless communication:** Select an RF channel appropriate for the environment. Ensure the wireless network is used only within the intended safety application scope. A loss of the radio link, including deliberate jamming or flooding, cannot be prevented: plan it as a loss of availability of every function that depends on radio signals, and do not rely on radio where availability under attack is required.

## 17.7 Secure Configuration

- Restrict the configuration password to authorized personnel. The password shall be kept confidential and not shared beyond those responsible for programming and maintenance of the safety system.
- Choose a strong, unique password. Do not reuse the same password across independent machines or facilities.
- Change the configuration password whenever personnel with access to it change — for example, when a programmer leaves the organization or changes role. A former employee must not retain the ability to modify the safety configuration.
- Any modification to the safety configuration requires retesting and updated documentation as described in the Safety Information chapter.

- Monitor for unauthorized configuration changes as part of periodic inspections.

## 17.8 Firmware Updates

SSPN provides firmware updates through Simplifier Manager. Firmware updates are protected by the following security measures:

- **Digital signature:** Each firmware update is signed using ECDSA P-256 with SHA-256. The Safety Simplifier verifies the signature against a public key stored in immutable, write-locked memory before the update is installed. Unsigned or tampered firmware is rejected.
- **Encrypted distribution:** Firmware images are distributed in encrypted form.
- **Rollback protection:** The device refuses a validly signed firmware image that is older than the currently installed firmware version. A security update, once installed, cannot be reverted through the update channel.

To apply a firmware update:

1. Open Simplifier Manager and check for available firmware updates. Updates are distributed through Simplifier Manager and do not require a separate download.
2. Review the release notes for the update before proceeding.
3. Apply the update using Simplifier Manager and verify the firmware version after the update completes.
4. Perform a complete functional test of the safety system before returning the machine to service.
5. Record the update in the machine technical file and retain the record for five years — see the **Five-year retention of tracing data** subsection.

**⚠ WARNING**

**Unverified firmware update**
A wrong firmware version or an untested system can leave a safety function that does not work, which could result in death or serious injury.
- Verify the firmware version after an update.
- Perform a complete functional test of the safety system before returning the machine to operation.

## 17.9 Product Security Support Lifecycle

SSPN provides security support for the Safety Simplifier firmware for **10 years** from the date the product is placed on the market. During this period, security updates and advisories for the safety-related software are published as described in the following sections.

The support end date for the product is therefore 10 years after its placing on the market.

## 17.10 Security Updates and Advisories

Security-related information is published on the Product Security webpage when relevant. This may include security advisories, firmware updates, mitigation recommendations, and other product security information.

The Product Security webpage is the authoritative source for the current advisory status of the Safety Simplifier. Check it before commissioning a system, and as part of periodic inspections.

Product Security webpage: https://www.sspn.se/security/

## 17.11 Reporting a Vulnerability

If you believe you have identified a cybersecurity vulnerability or security-related issue affecting a Safety Simplifier product, contact SSPN:

**Security Contact:** security@sspnorth.se

Please include the following information where possible:

- Product name and product ID number
- Description of the issue
- Steps to reproduce or evidence of the vulnerability
- Your contact information

SSPN aims to acknowledge received reports within **five (5) business days.** Each report is assessed and handled according to the company's Product Security Management Procedure.

SSPN follows a coordinated vulnerability disclosure approach. Where applicable, a remediation period is agreed with the reporter before any public disclosure of the vulnerability.

## 17.12 Responding to a Suspected Security Incident

If a Safety Simplifier unit is suspected of having been accessed or modified without authorization — for example, an unexpected configuration change is discovered during a periodic inspection — the following steps shall be taken:

1. **Remove from service:** Take the affected unit out of operation immediately. Do not re-enable until the investigation is complete.
2. **Preserve evidence:** Do not clear or overwrite the configuration. Connect via Simplifier Manager, record the current configuration, firmware version, and any available diagnostic information.
3. **Verify the configuration:** Compare the configuration on the unit against the last known-good version in the application documentation. If changes cannot be accounted for, treat the configuration as untrusted.
4. **Restore from a verified source:** If the configuration has been altered without authorization, restore from a verified backup downloaded from an authorized programming device.
5. **Report to SSPN:** Contact security@sspnorth.se with a description of the incident, including the unit ID number, firmware version, and a description of what was found.
6. **Retest before returning to service:** Perform a full functional test of the safety system before returning the unit to operation.

## 17.13 Decommissioning

When a Safety Simplifier unit is taken permanently out of service, the following steps shall be carried out before disposal or reuse of the hardware:

1. **Remove from the safety system:** Disconnect the unit from all I/O, power, CAN bus, and radio network. Update the safety system documentation to reflect the change. If other units in the network referenced this node, update their configurations accordingly and retest the remaining system.
2. **Clear the configuration:** Use Simplifier Manager to erase the application program and configuration from the unit. This prevents the safety logic from being read out or reused without authorization.
3. **Reset the password:** Reset the unit password so that the configuration cannot be restored or accessed on a repurposed device.
4. **Document the decommissioning:** Record the unit serial number, firmware version at time of decommissioning, and the date in the machine safety documentation.
5. **Dispose of the hardware:** The Safety Simplifier contains electronic components and must be disposed of in accordance with the WEEE Directive (2012/19/EU) and applicable national regulations. Do not dispose of as general waste.

**⚠ WARNING**

**Unit transferred with its old configuration**
A unit moved to another machine with its old configuration runs safety functions meant for the old machine, which could result in death or serious injury.
- Clear the configuration and reset the password before transfer.
- The receiving party must perform a full safety assessment and commissioning test for the new application.

## 17.14 Known Vulnerabilities

Known vulnerabilities affecting the Safety Simplifier, together with any available mitigations and corrective firmware, are published on the Product Security webpage. That page, not this manual, states the current position: https://www.sspn.se/security/

This manual is not revised each time the vulnerability status changes. Consult the Product Security webpage when commissioning a system, before applying a firmware update, and at each periodic inspection.

# 18 Performance Specifications

> **Important Notice**
>
> All electrical connections must be carried out by authorized and qualified personnel in accordance with applicable safety standards and installation guidelines.

## 18.1 General Technical Data

| | Specification | Notes |
|---|---|---|
| Power Supply | $7 - 33$ VDC | Normal Operating Range: $[10 - 30$ VDC$]$ |
| External Fuse (required) | Fast Acting Fuse, $2.5A$ | Mandatory — see Power Supply Requirements |
| Current Consumption (no load) | Inactive Mode: $90$ mA | LED and relays not activated. Typical value; current draw depends on supply voltage |
| | Active Mode (LED on): $110$ mA | Relays not activated. Typical value; current draw depends on supply voltage |
| Current Consumption (max, device only) | Active Mode (Max Load): $210$ mA | LED, I/O, and 4 relays activated. Excludes output load |
| Supply Current (max, with full output load) | Up to $2.2A$ | Device consumption plus the maximum total transistor output current of $2000$ mA. Size the supply and fuse for this value |
| Enclosure Material | PC + ABS | UL 94 rated |
| Degree of Protection (IEC 60529) | IP66 | Wall-mounted or bracketed: dust-tight, protected against powerful water jets |
| | IP65 | Freestanding: dust-tight, protected against low-pressure water jets |
| | IP20 | Cabinet type units: protected against solid objects of 12.5 mm and larger, no protection against water |
| Ventilation Enclosure | GORE-TEX membrane | Ensures pressure equalization |
| Airborne Noise Emission | $\leq 70$ dB(A) | A-weighted emission sound pressure level at workstations |
| USB Connector | Micro-USB/USB-C, model dependant | For configuration and diagnosis |
| Dimensions (Mounting Surface) | 253 mm x 40 mm x 44 mm | Length x Width x Height |
| Dimensions (Maximum Housing) | 253 mm x 42 mm x 44 mm | Length x Width x Height |
| Weight (Approximate) | S14RBLD: $235g$ | Without holes/plugs |
| | S16RBLD: $265g$ | Without holes/plugs |
| Lifetime Calculations | $\mathrm{PFH}_D$ (IEC 61508): Up to 10 years | |
| | $\mathrm{PFH}_D$ (EN ISO 13849-1): Up to 20 years | |

## 18.2 I/O and Contact Specifications

| | Specification | Notes |
|---|---|---|
| I/O Functionality | Input, Output, or combined I/O | Customizable |
| I/O as Input (PNP Sensors) | $0$ VDC $- 33$ VDC | Permissible input voltage range. For connection of PNP sensors |
| I/O as Output Transistor | $7$ VDC $- 33$ VDC | |
| OSSD Output Self-Test Duration | $< 150\mu s$ | For safe output monitoring |
| Combined I/O for Reset | $7$ VDC $- 33$ VDC | |
| Max Output Current (per transistor) | $600$ mA | Short-circuit protected |
| Voltage Drop ($I_{\text{out}} = 600$ mA) | $0.5V$ below supply $V$ | |
| Maximum Total Output Current | $2000$ mA | Sum of all transistor outputs |
| Terminals (Spring) | 32 positions | Max wire size: $0.5\text{mm}^2$ or $20$ AWG |
| Relay Contacts (S16 Only) | Gold plated $\mathrm{AgSnO_2}$ | For DC13 load type |

| | | |
|---|---|---|
| Relay Current Rating (DC13) | $2A$ | Max $I_e$ |
| Relay Life (Resistive/Inductive) | Max $2.0A$ @$49$ VDC | Estimated $1260$ operations per year for 10 years |
| | Max $0.5A$ @$49$ VDC | Estimated $3780$ operations per year for 10 years |
| | Max $0.2A$ @$49$ VDC | Estimated $100800$ operations per year for 10 years |

### 18.3 Wire Specifications

| Specification Category | Wire Type | Cross Section Area ($mm^2$) |
|---|---|---|
| Conductor Cross Section | Single Core | 0.08 to 0.5 |
| | Fine Stranded | 0.08 to 0.5 |
| | Fine Stranded (w/ insulated ferrule) | 0.25 |
| | Fine Stranded (w/ uninsulated ferrule) | 0.25 |
| Preparation | Stripping Length | 5 to 6 mm |

### 18.4 Environmental and Durability

| | Specification | Notes |
|---|---|---|
| Operating Temperature | $-20°C$ to $+65°C$ | Ambient. The internally measured board temperature is higher than ambient |
| Storage Temperature | $-30°C$ to $+70°C$ | |
| Relative Operating Humidity | $10-90\%$ | Non-condensing |
| Operating Altitude | Up to $2000m$ | |
| Vibration Resistance | $5-150$ Hz, Acceleration 1 g | EN 60068-2-6 |
| Shock Stress | Acceleration 15 g, Duration 11ms | EN 60068-2-27 |

### 18.5 Radio Frequency (RF) Channels

| Channel Number | Frequency |
|---|---|
| 1 | 2405 MHz |
| 2 | 2410 MHz |
| 3 | 2415 MHz |
| 4 | 2420 MHz |
| 5 | 2425 MHz |
| 6 | 2430 MHz |
| 7 | 2435 MHz |
| 8 | 2440 MHz |
| 9 | 2445 MHz |
| 10 | 2450 MHz |
| 11 | 2455 MHz |
| 12 | 2460 MHz |
| 13 | 2465 MHz |
| 14 | 2470 MHz |
| 15 | 2475 MHz |
| 16 | 2480 MHz |

**Coexistence with WiFi**

A 2.4 GHz WiFi access point occupies a band approximately $22$ MHz wide, centred on $2407 + 5 \times n$ MHz for WiFi channel $n$. The commonly used non-overlapping WiFi channels 1, 6 and 11 therefore occupy roughly $2401–2423$, $2426–2448$ and $2451–2473$ MHz. Safety Simplifier channels **5, 10, 15 and 16** fall outside these three bands; every other channel is overlapped by at least one of them. Where WiFi and Safety Simplifier radio share a site, lock the access points to fixed WiFi channels and select a Safety Simplifier channel that lies outside the bands in use.

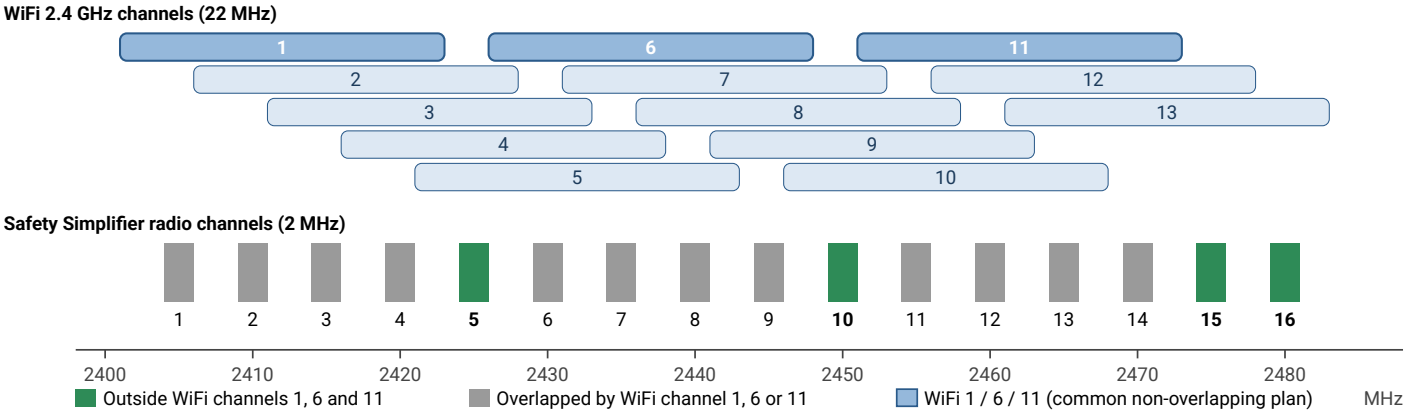



Figure 43: Overlap between 2.4 GHz WiFi channels 1–13 (22 MHz each) and Safety Simplifier radio channels 1–16. Channels 5, 10, 15 and 16 lie outside WiFi channels 1, 6 and 11.

## 18.6 CAN Communication Card

| | Specification | Notes |
|---|---|---|
| Power Supply | $3.3$ VDC | Supplied internally by the Safety Simplifier unit |
| Current Consumption | $0.02A$ @$24$ VDC | Additional draw on the Safety Simplifier supply |
| Terminals (Spring) | Card dependent | Max wire size: $0.5\text{mm}^2$ |
| Termination Resistor Selector | Position ON: $120$ Ohm between H& L | Used for bus end points |
| | Position OFF: No resistor | Used for intermediate nodes |

### 18.7 CAN 2.0

| | Parameter | Specification | Notes |
|---|---|---|---|
| Cable Type | Twisted Pair | Standard | For CAN_H and CAN_L signal pairs to minimize EMI |
| | Shielded Twisted Pair (STP) | Recommended | High-EMI environments (e.g., industrial applications) |
| | Unshielded Twisted Pair (UTP) | Acceptable | Low-EMI environments (e.g., laboratory settings) |
| Electrical Characteristics | Characteristic Impedance | 120 Ω ±10% | |
| | Capacitance | < 30 pF/ft (≈ 98 pF/m) | |
| | Conductor Size | 22–24 AWG (≈ 0.34–0.25 mm²) | |
| Termination Requirements | Termination Resistors | 120 Ω | Two resistors required (one at each bus end) |
| | Purpose | | Prevents signal reflections; establishes bus idle voltage |
| Maximum Cable Length | 500 kbit/s | ≈ 100 m | General value per ISO 11898-2; the achievable length varies with cable quality and environment |
| | 250 kbit/s | ≈ 250 m | General value per ISO 11898-2; the achievable length varies with cable quality and environment |
| | 125 kbit/s | ≈ 500 m | General value per ISO 11898-2; the achievable length varies with cable quality and environment |
| Maximum Single Stub Length | 500 kbit/s | 0.6 m | |
| | 250 kbit/s | 1.2 m | |
| | 125 kbit/s | 2.4 m | |

**Note:** Units connected on a stub must not have termination resistors fitted. The two $120\Omega$ terminators belong at the ends of the trunk only.