ISO9001:2015 certified
Design, development, manufacturing, installation and servicing for customer safety products

SC3 AUTOMATION SAFETY PRODUCT PLATFORM

NVIDIA Preferred Partner

Sensor Fusion and Artificial Intelligence Safety Controller Datasheet

SC3 Automation SENFAI Safety Controller for the JAXi SOM

The **SENFAI** is a modular safety-related controller board combining a safety MCU, a communication co-processor, and designed to host the safety-capable NVIDIA Jetson AGX Xavier Industrial SOM (JAXi) (SENFAI support Jetson ORIN industrial).

The safety MCU processor is used to implement safety functions. This processor is SIL 3 capable according to [S29] IEC 61508 and ASIL-D capable according to [S36] ISO 26262. The processor provides safety-related external communications, data processing, and data storage. The SENFAI is designed to be used in various markets. It is compliant to Railway, Automotive and Industrial markets

Figure 1: SENFAI Safety Controller

The communication co-processor provides high-speed non-safe external communication and supports various industrial protocols such as EtherCAT®, EtherNet/IP™, PROFINET®, and others. The co-processor includes an SSD drive for data storage.

The JAXi provides high performance processing for safety-related functions such as sensor fusion and artificial intelligence applications. The JAXi is also capable of implementing safety functions.

The SENFAI is designed for the harsh environments of Rail, Automotive, and Industrial markets.

The SENFAI is available for use stand alone or combined with one of the available safety IO boards.

Refer to these documents for details related to the JAXi capabilities:

- [R5] DATA SHEET NVIDIA Jetson AGX Xavier Series System-on-Module
- [R6] JETSON AGX XAVIER INDUSTRIAL IN SAFETY-RELATED SYSTEMS application note
- [R7] Jetson AGX Xavier Series Interface Comparison and Migration (for most recent versions)

Table of Contents

Table References

Table of Figures

The **SENFAI** controller is available in various hardware configurations with or without IO boards. The available types of IO boards are the SC3 Automation Universal Digital IO, Universal Digital IO Double-cut, Universal Analog IO and the specialized transportation/rotating machinery Relay IO (with Quadrature encoders/pulse counters).

The **SENFAI** controller supports CAN, RS-232, RS-422, and RS-485 half-duplex and full-duplex communication. Industrial communication ports enable the use of the Ethernet protocols such as EtherCAT®, and Ethernet/IP™, ProfiNet™.

The **SENFAI** controller includes temperature monitoring that detects an under temperature and triggers a heater circuit, an over temperature that initiates a system safe state.

The **SENFAI** has one SIL 3 Master Disconnect Output to signal the safe state when there are no IO boards.

From a laptop, access the **SENFAI** embedded web server to configure the required parameters and set the real-time clock. Also, monitor and access application data, update the application, and access the system log.

Safety-related Functions

When combined with a safety IO board or remote sensors and actuators, the **SENFAI** safety contoller can perform safety functions. The safety performance level of the safety functions combining the use of the JAXi depends on the application and the features used.

Network of Safety Controllers

Set two **SENFAI** safety controllers in a network such that the two safety MCUs meet SIL 4 according to [S9] EN 50129.

The **SENFAI** can also be placed in a network with SC3 Automations SC3Node (SIL 3/ASIL-D) and/or SC4Node (SIL 4 according to [S9] EN 50129) controllers.

Safety System

The **SENFAI** controller is designed to support safety functions with SIL 3 according to [S29] IEC 61508:2010, Ple cat. 4 according to [S35] ISO 13849, and ASIL-D according to [S36] ISO 26262.

Integration of the JAXi on the SENFAI Board

The Jetson AGX Xavier Industrial (JAXi) system on module coupled with the Jetson Safety Extension Package (JSEP) provides the foundation for fault avoidance, detection, and control in safety-related systems. The hardware infrastructure for fault detection and control is implemented in the Xavier SOC on the JAXi module. NVIDIA JSEP software running on top of the NVIDIA JetPAck SDK exposes that infrastructure for use in customer-defined systems.

The **SENFAI** implements the safety MCU Interfaces as described in the JAXi documentation.

JAXi uses some of the existing signals to interface with a safety MCU if, implemented in a design. This includes:

- SPI2
- EQOS and RGMII (Ethernet)
- GPIO31 (SAFESTATE)
- GPIO12 (BOOT_CHAIN_SELECT strap)

In addition, several other interface pins that were not supported on JAX or JAX 64GB are available to interface with the safety MCU including:

- VM_I2C (Voltage Monitor I2C)
- VM_INT_N (Voltage Monitor Interrupt)
- NC_O3 (TEMP_THERM_OUT)

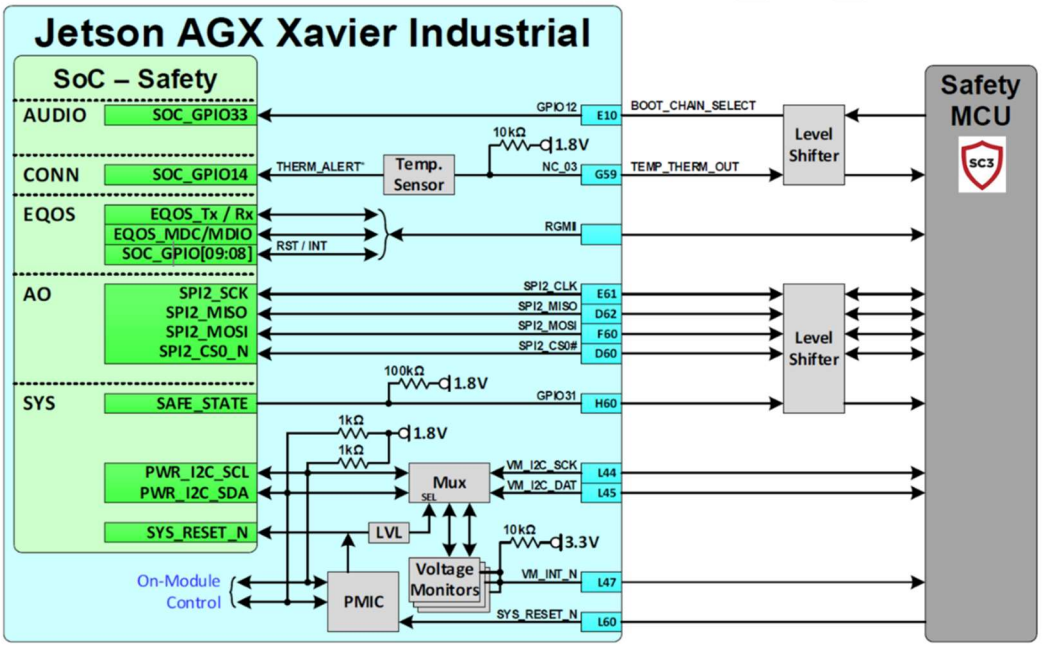


Figure 2: JAXi safety MCU interfaces

NVIDIA Jetson AGX Xavier Industrial module includes the Xavier SOC which is TÜV SUD assessed for meeting all applicable requirements for [S36] ISO 26262. The module also includes various built-in safety extensions:

- Safety Cluster Engine (SCE), a dedicated ARM Cortex R5F lock-step subsystem for integrated fault detection
- In-System-Test (IST), LBIST (Logic Built In Self Test), and MBIST (Memory Built In Self Test) for detecting permanent and latent failures
- Hardware Safety Manager (HSM) and Error Collator (EC) for monitoring and reporting error signals
- Support for adding external safety MCU
- DRAM and GPU ECC (Error-Correcting Code)*
- SEC (Single Error Correction), DED(Double Error Detection), and Parity protection for each IP*
- ARM CCPLEX RAS (Reliability, Availability and Serviceability)*
- Temperature, clock, and voltage monitoring*

*Feature is enabled by Jetson Linux and does not require JSEP.

The safety performance level achievable for an application implemented on the JAXi depends on a number of factors including the selected architecture, the operating system, and the components used. Each application requirement needs to be reviewed. SC3 Automation can assist customers to determine the appropriate safety strategy for a given application.

JSEP and Support of 3LSS Monitoring and Error Reporting

The **SENFAI** supports the JSEP including the 3LSS mechanism to perform monitor and error reporting from JAXi.

The Jetson Safety Extension Package provides error diagnostic and error reporting framework for implementing safety functions and concepts to achieve functional safety standard compliance.

Features:

- Enables safety extensions built-in the Jetson AGX Xavier Industrial module
- Diagnostic monitoring including Safe state and FuSa state monitoring and heartbeat mechanism at various layers
- Safe communication using L3SS component
- Error reporting of hardware and software errors

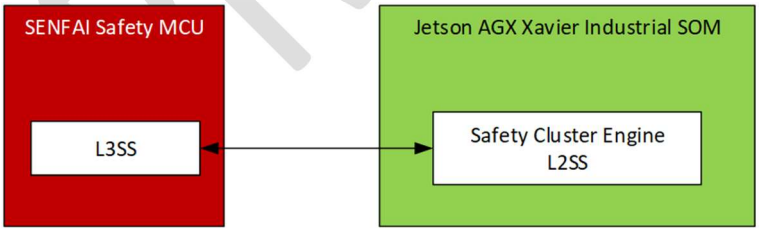


Figure 3: 3LSS Monitoring of the JAXi

Reference Design and Customization

The **SENFAI** offers a rich set of features and is ready to use. SC3 Automation's mission is to provide customers with safety controllers that meet their exact requirements. Customization of the **SENFAI** including the number of peripherals, the type of connectors, the type of enclosure is performed to fit the exact needs of the application.

Complementary Documentation

These documents have pertinent information relating to the use of the **SENFAI** controller:

- [R1] SENFAI Release Notes
- [R2] SENFAI Controller Manual
- [R3] SENFAI Safety Manual
- [R4] SENFAI Programming Guide

Ordering Information

The **SENFAI** controller can be ordered using the following part numbers. When ordering the controller with an IO board, make sure to order both at the same time since these will be assembled and tested prior to shipping.

Product	P/N
SENFAI	700-0026
UDIO	700-0016-05-03: 24VDC 700-0016-05-04: 48VDC 700-0016-05-05: 72VDC 700-0016-05-06: 110VDC
RIO	700-0017-04-05: 24VDC 700-0017-04-06: 48VDC 700-0017-04-07: 72VDC 700-0017-04-08: 110VDC
UDIODC	700-0023-03-03: 24VDC 700-0023-03-04: 48VDC 700-0023-03-05: 72VDC 700-0023-03-06: 110VDC

For pricing information, contact our team at safety@sc3automation.com

Expected delivery is three months following an order.

SENFAI Boards Detailed Descriptions

Dimensions

The physical dimensions of the fully loaded **SENFAI** are 155mm x 132mm x 170 mm (see Figure 4).

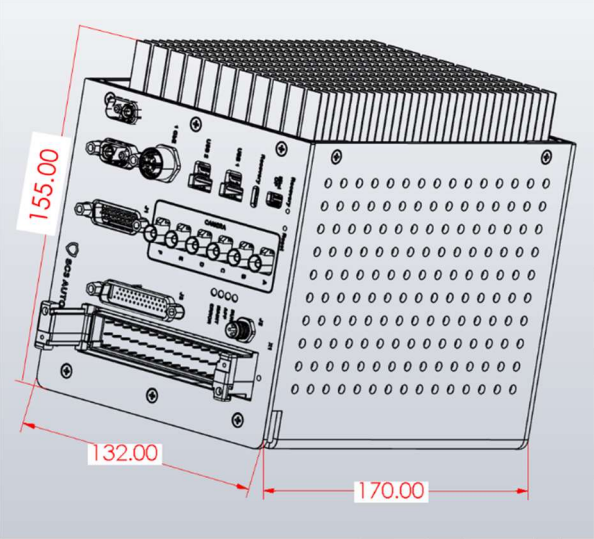


Figure 4: SENFAI dimensions

SENFAI controller components

The **SENFAI** controller consists of a main controller board and an optional IO board. Three types of IO boards are available for different applications.

Board	Description
SENFAI	Sensor Fusion and Artificial Intelligence controller board with a safety MCU and a communications co-processor and the JAXi.
RIO	The Relay IO board is a specialized board for wheel speed measurement or rotating machinery control. The Relay IO board has three SIL 3 universal relay output channels, four quadrature encoder inputs, and two non-safe analog outputs (0-20mA). Relay output channels are configurable as double cut or high side cut architecture. The outputs can be configured as a PWM. Individual channels are independent and galvanically isolated.
UDIO	Universal digital IO board each with up to eight SIL 3 independent universal digital input/output channels. Each channels is configurable as a digital input or a digital output. Individual channels are independent and galvanically isolated. Digital inputs (DI) are configurable for 24V or 115V AC/DC. Type 1 and Type 3 for 24V AC/DC. Type 1 for 115V AC/DC ([S19] EN 61373:2010). Digital outputs (DO) are configurable to 2A for 24V or 115V AC/DC. Individual channels are configurable with PWM.
UDIODC	Universal digital IO double-cut board each with up to eight SIL 3 independent universal digital input/output channels. Each channels is configurable as a digital input or a digital output Individual output channels are configurable as double cut or high side cut architecture. They are independent and galvanically isolated. Digital inputs (DI) are configurable for 24V or 115V AC/DC. Type 1 and Type 3 for 24V AC/DC. Type 1 for 115V AC/DC ([S19] EN 61373:2010). Digital outputs (DO) are configurable to 2A for 24V or 115V AC/DC.

Table 1: SENFAI controller and IO boards

SENFAI block diagram

Figure 5 provides a block diagram overview of the various components found on the **SENFAI**. The capabilities of these components are described in the following sections.

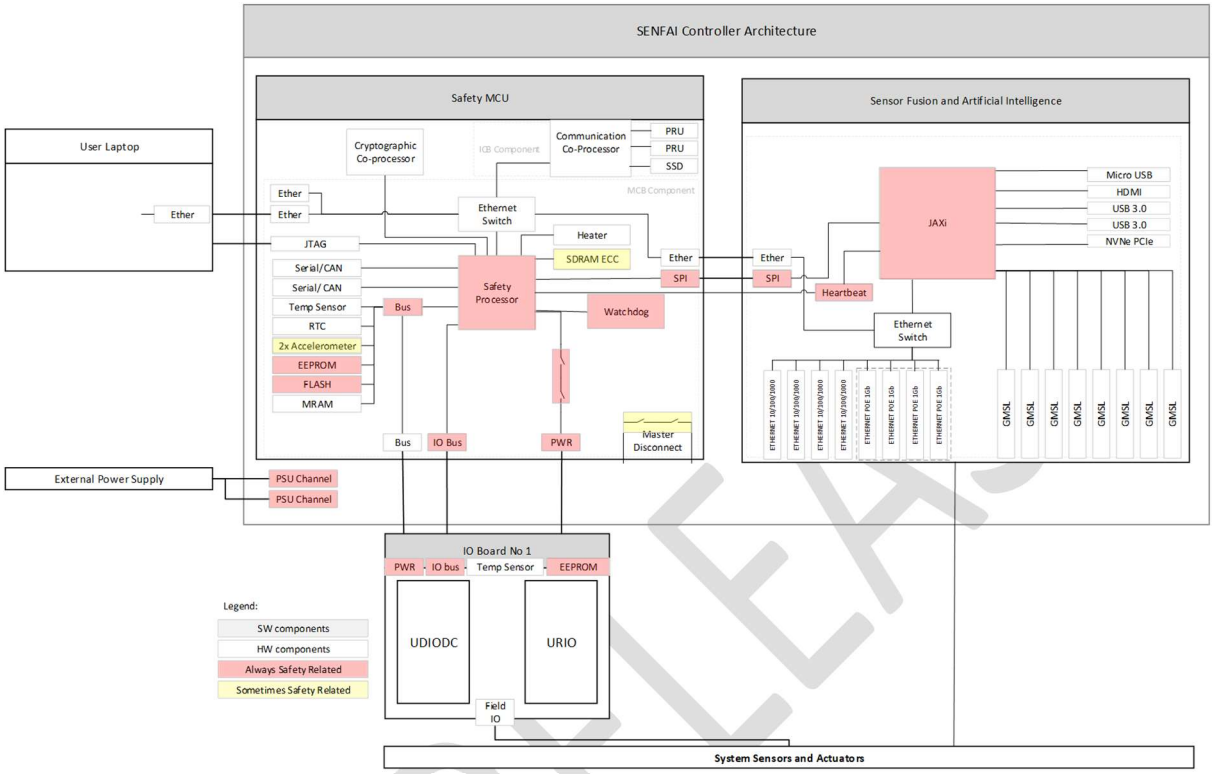


Figure 5: SENFAI block diagram overview

SENFAI safe controller board

Features	
Safety MCU ➢ High-speed 300MHz safety processor ➢ 512KB ECC internal RAM ➢ 64MB ECC external RAM ➢ 4MB ECC program flash ➢ 64Mbytes serial flash ➢ 2kbits EEPROM ➢ 512kbytes SPI MRAM ➢ Real-time clock (RTC) with either Lithium battery (-40° to +125°C) or Supercapacitor (- 40° to +85°C) ➢ Two diverse three-axis accelerometers ➢ Supports one IO board ➢ SIL 3 master disconnect **JAXi Interfaces** ➢ JAXi connector ➢ Access to all ethernet ports	**Communication Co-processor** ➢ 1.0GHz processor ➢ 64Gb (8M x 8) eMMC ➢ 4 Gbits (256M x 16) DDR3L SDRAM ➢ 8MB Flash NOR 133MHz Quad SPI ➢ 2Kb I2C EEPROM ➢ Two 10/100 Mpbs ports; reinforced insulation; M12 D-coded connector compatible with EtherCAT, PROFINET, etc. **Communication Ports** ➢ Two Universal Serial ports: RS-232, RS-422, RS-485 (galvanically-isolated) ➢ Two CAN ports (galvanically-isolated) ➢ Two Ethernet ports 10/100Mbps ➢ Four 10/100/1000 Mbps ports; reinforced insulation; M12 X-coded connector

➢ Two USB 3.0 ports with ruggedized IP67 connector, 950mA /port reinforced insulation power supply (reinforced insulation signalling available as option) ➢ HDMI port with ruggedized IP67 connector ➢ Eight GMSL ports with Power over Coax (PoC) **Cryptographic Companion Security IC** Hardware Security Module (HSM) support: ➢ Secure boot ➢ CAN message authentication ➢ Electric Vehicle (EV) battery authentication ➢ Transport Layer Security (TLS) ➢ Wireless Power Consortium (WPC) 1.3 Qi® authentication ➢ High-bandwidth Digital Content Protection (HDCP) ➢ And more	➢ Highly flexible Ethernet card as option that allows various customer specific requirements such as a mix of these: ▪ Up to four additional 10/100/1000 Mbps ports; reinforced insulation; M12 X-coded connector with Power Over Ethernet (802.3af) ▪ Up to four additional fiber optic ports (SFP) (1G / 2.5G/ 5G /10G possible on two ports) ▪ Up to four additional 100 Mbps or 1000 BaseT1 ports (two-wire Ethernet) **Environmental (Compliant to [S10] EN 50155)** ➢ Temperature (in-case): -40°C to +85°C ➢ PCB heater for startup at temperatures below -40°C ➢ Conformally coated ➢ Power consumption: 50W; 8 to 36V DC (24 V nominal) ➢ Redundant power supplies

RIO universal relay IO board

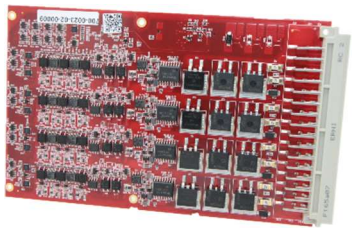
<table>
<tr><th colspan="2">Features</th></tr>
<tr><td>Relay Inputs/Outputs
➢ Up to three relay output channels, four quadrature encoder inputs, and two non-safe analog outputs (0-20mA)
➢ Relay output channels are configurable as double-cut or high side architecture
➢ Relay output 2A@24/115 V DC
➢ Encoder inputs configurable as counter inputs
➢ Channels configurable as pulse-width modulation (PWM)
➢ 1500 V channel-to-channel Galvanic isolation</td><td>Environmental (Compliant to [S10] EN 50155[S10] EN 50155:2017)
➢ Temperature rating (in-case): -40°C to +85°C
➢ Conformally coated
Form Factor
➢ Eurocard format (100mm x 160mm x 6.5mm)</td></tr>
<tr><th colspan="2">Description</th></tr>
<tr><td>The Universal Relay IO (URIORIO) board is designed for use with the SENFAI safety controller, the SIL 3-capable MCB11 safety controller, and the SIL 4-capable controller board assembly. This board provides a sample of the possible specialized IO boards that can be designed with the Safety Product Platform (SPP). The URIORIO board has three SIL 4 capable 24-110V DC double cut digital outputs with positively guided relays, four quadrature encoder inputs for locomotive tachometers, and two 0-20mA outputs for speed indicators. The URIORIO has channel-to-channel galvanic isolation.</td><td>  </td></tr>
<tr><td colspan="2">Relay IO board is designed to work with our SENFAI safety controller, our SIL 3 capable MCB11 Safety controller and our SIL4 capable Controller board assembly. This board provides a sample of the specialized IO boards we can design with the Safety Product Platform. The RIO board has three SIL4 capable 24-110V DC double cut digital outputs with positively guided relays, four quadrature encoder inputs locomotive tachometers, and two 0-20mA outputs for speed indicators. The RIO has channel to channel galvanic isolation.</td></tr>
</table>

UDIO universal digital IO board

Features	
Digital Inputs/Outputs ➢ Eight SIL 3/ASIL-D Universal Digital IOs ➢ 1500 V channel-to-channel Galvanic isolation ➢ Software configurable to [S30] IEC 61131-2:2017 compliant for these types: ▪ High speed counter (DC/AC) (20 kHz) ▪ DI 24 V DC/AC Type1 and Type3 ▪ DI 115 V DC/AC Type1 ▪ DO 2A@24/115 V DC/AC ➢ Pulse-width modulation (PWM)	**Environmental (Compliant to [S10] EN 50155)** ➢ Temperature rating (in-case): -40°C to +85°C ➢ Conformally coated **Form Factor** ➢ Eurocard format (100mm x 160mm x 6.5mm)
Description	
The Universal Digital IO (UDIO) board is designed for use with the **SENFAI** safety controller, the SIL 3-capable MCB11 safety controller, and the SIL 4 capable controller board assembly. This board has eight channels with channel-to-channel Galvanic isolation. Each channel can function as an input or an output. The UDIO board supports 24 to 110V AC or DC. The board can also be used as a Pulse Width Modulation (PWM) or pulse counter.	

UDIODC universal digital IO double-cut board

Features	
Digital Inputs/Outputs ➢ Eight SIL 3/ ASIL-D universal digital IOs ➢ Universal digital IO v output channels configurable as double-cut or high side cut architecture ➢ 1500 V channel-to-channel Galvanic isolation ➢ Software configurable to [S30] IEC 61131-2:2017 compliant for these types: ▪ High speed counter (DC) (20 kHz) ▪ DI 24 V DC Type1 and Type3 ▪ DI 115 V DC Type1 ▪ DO 2A@24/115 V DC ➢ Pulse-width modulation (PWM)	**Environmental (Compliant to [S10] EN 50155)** ➢ Temperature rating (in-case): -40°C to +85°C ➢ Conformally coated **Form Factor** ➢ Eurocard format (100mm x 160mm x 6.5mm)
Description	

The Universal Digital Double Cut IO (UDIODC) board is designed for use with the **SENFAI** safety controller, the SIL 3-capable MCB11 safety controller, and the SIL 4-capable controller board assembly. This board has eight channels with channel-to-channel Galvanic isolation. Each channel can function as an input or as a double cut output that switches the high side and the low side of a load. The UDIODC board supports 24 to 110V AC or DC. This board can also be used as a Pulse Width Modulation (PWM) or pulse counter.	

Specifications

General	Safety integrity level	SIL 3 capble according to [S29] IEC 61508, and ASIL-D capable according to [S36] ISO 26262)
	Performance level	PLe Category 4 according to [S35] ISO 13849
	Mounting position	Vertical or horizontal mounting. Ensure sufficient space to install and replace controller and connect cables.
	Overall dimensions	Dimensions vary with selected enclosures, connectors, and cables
	Overall weight	Weight varies with selected boards, enclosures, connectors, and cables
	Configuration interface	Web interface via Ethernet. Requires Cat5 RJ45 Ethernet cable.
Environmental	Ambient operating temperature	-40°C to +85°C in-case
	Ambient operating humidity	0 to 95% with no condensing ([S10] EN 50155, [S5] EN 50125-1, and [S6] EN 50125-3)
	Rapid temperature variations	H1 class ([S10] EN 50155)
	Operating altitude	4000 m
	Storage temperature and conditions	Store in a clean and dust-free environment at a temperature between - 40°C and +85°C with a relative humidity between 0 and 95%
	Pollution degree	Pollution degree 2 ([S4] EN 50124-1, [S10] EN 50155, [S28] IEC 61010-2-201
	Shock and vibration resistance	Category 1, Class B [S19] EN 61373, [S10] EN 50155
	Radiated and conducted immunity	The system is compatible with these EMI/EMC standards: [S10] EN 50155 [S3] EN 50121-3-2 [S13] EN 55011 [S14] EN 61000-4-2 [S15] EN 61000-4-3 [S16] EN 61000-4-4 [S17] EN 61000-4-5 [S18] EN 61000-4-6
	Conformal coating	**SENFAI** printed board assemblies are conformally coated [S27] IEC 60664-3 with a PC2 protective coating [S10] EN 50155. Glue is applied to the vibration-sensitive components.
	RoHS compliance	[S37] RoHS 3 (EU 2015/863). This controller contains no hazardous materials or substances identified in the directive.
	REACH compliance	N/A

Environmental (continued)	Manufacturing	The printed board assemblies have been manufactured in compliance with [S34] IPC A-610H; Class 3, [S38] UL 94 V-0 and the lead-free RoHs-compliant process.
	Fire Protection	This device is compliant to the standards [S1] EN 45545-1 and [S2] EN 45545-2
Electrical	Voltage supply	24 V DC; 8-36V DC continuous
	Power consumption	50 W with JAXi
	Voltage supply interruption	Class S2 (up to 10 ms) [S10] EN 50155
	IPC class	**SENFAI** printed board assemblies are IPC class 3 [S34] IPC A-610H
Network configuration	Processor 1 (SENFAI)	Default IPv4 configuration (Manually configurable or DHCP assignment)

Table 2: Product specifications

SENFAI Controller States

The **SENFAI** controller has these possible system states.

- **Safe Run** state where the **SENFAI** controller executes the application safety functions. The **SENFAI** controller loads the application into the system memory and cyclically executes without human intervention. The execution cycle is the following: perform diagnostics, read the inputs, execute the application logic, vote, and write the outputs.
- **Maintenance** state where maintenance personnel perform these operations: update the application, force IOs, perform static tests, download the event log, and debug the application. The **SENFAI** controller continues to cyclically execute without human intervention but with increased timeout values for communications.
- **Idle** state where maintenance personnel perform these operations: update the application, update the bootloader, update the firmware, and download the event log. The **SENFAI** controller does not contain or execute an application. The controller switches from the Maintenance state to the Idle state after deleting the application.
- **Safe** state where the **SENFAI** controller enters upon detection of a fault and continues in, even with the detection of subsequent faults, until resetting the controller following the identification and acknowledgement of the faults.

Refer to the *[R2] SENFAI Controller Manual* for further details on **SENFAI** maintenance.

The controller LED status display panel indicates the health and the state of both processors. Table 3 describes the meaning of the individual LEDs. The controller is in the Idle state when all LEDs are off.

P1	Description	ON	OFF	Blinking
	Run	N/A	Not Safe Run state	Safe Run state
	Health	Good health	Fault	N/A
	Maintenance	Maintenance state	Not Maintenance state	Safe Run state with minor fault
	Error	Safe state	No fault	N/A
All LEDs off	Idle	N/A	Idle state	N/A

Table 3: LED status display descriptions

Programming

Customize the **SENFAI** logic engine using either ANSI 'C' code from an IDE or code from modeling tools. Refer to the JAXi documentation for the detailed capabilities and programming options for JAXi.

Web Configuration and Maintenance

The **SENFAI** web interface enables to perform many tasks such as updating firmware, defining system parameters and system options, performing static tests and first-line maintenance diagnostics, and accessing logs. The interface is accessible from a laptop with Windows® 10 through the Ethernet port using the correct authentication parameters. The laptop connects to the **SENFAI** system port with a standard Cat5 RJ45 cable.

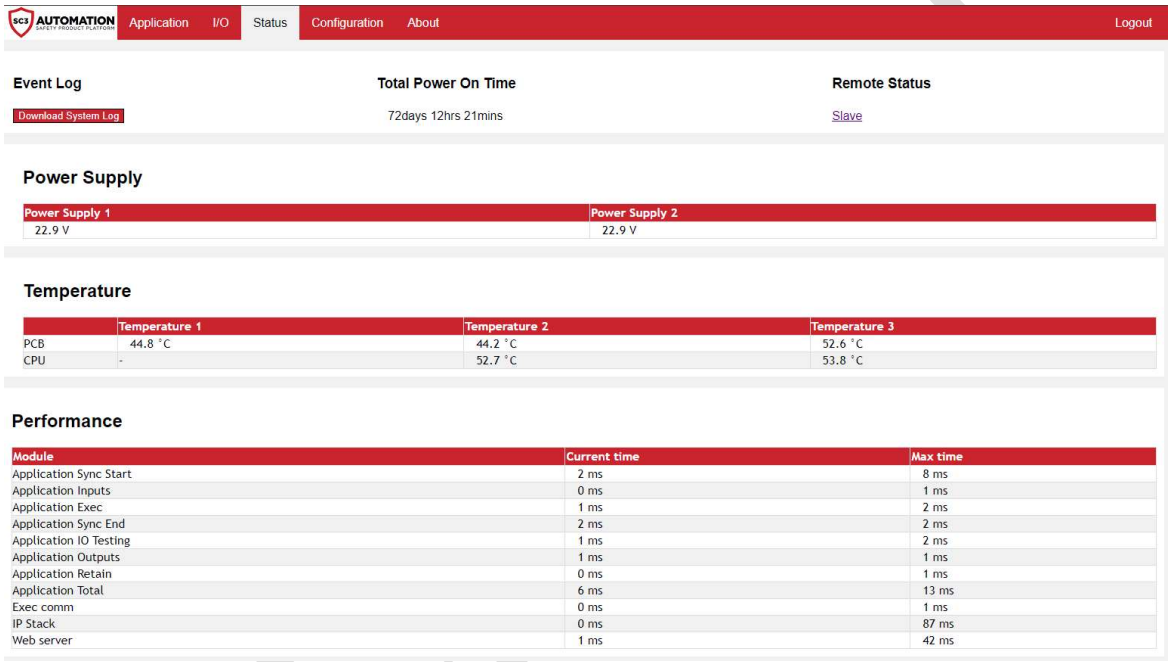


Figure 6: SC3 Automation web interface status information

Independent Safety Assessment

SC3 Automation provides support to customers that have an independent safety assessor (ISA) review their solutions.

Glossary

application software program that performs specific functions initiated by a user command or a process event and that can be executed without access to system control, monitoring, or administrative privileges
[Source: [S33] IEC 62443-1-1, 3.2.4]

architecture specific configuration of hardware and software elements in a system
[Source: [S32] IEC 61508-4, 3.3.4]

authentication security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information
[Source: [S33] IEC 62443-1-1, 3.2.13]

channel element or group of elements that independently implement an element safety function.
Example: a two-channel (or dual-channel) configuration is one with two channels that independently perform the same function.
[Source: [S32] IEC 61508-4, 3.3.6]

communication transfer of information between applications
[Source: [S11] EN 50159, 3.1.7]

compliance state where a characteristic or property of a product, system or process satisfies the specified requirements
[Source: [S7] EN 50126, 3.11]

component constituent part of software which has well-defined interfaces and behaviour with respect to the software architecture and design and fulfils the following criteria:
– it is designed according to “Components” (see Table A.20);
– it covers a specific subset of software requirements;
– it is clearly identified and has an independent version inside the configuration management system or is a part of a collection of components (e.g. subsystems) which have an independent version
[Source: [S12] EN 50657, 3.1.4]

configuration structuring and interconnection of the hardware and software of a system for its intended application
[Source: [S24] IEC 60050-821, 821-12-12]
[Source: [S9] EN 50129, 3.1.5]

data information represented in a manner suitable for communication, interpretation, or processing by computers
[Source: [S32] IEC 61508-4, 3.2.9]

design activity applied in order to analyse and transform specified requirements into acceptable solutions
[Source: [S24] IEC 60050-821, 821-12-16, modified – The end of the definition “design solutions which have the required safety integrity level” has been replaced by “solutions”.]
[Source: [S7] EN 50126, 3.1.8]

device material element or assembly of such elements intended to perform a required function
Note 1 to entry: A device may form a part of a larger device.
[Source: [S20] IEC 60050-151, 151-11-20]
[Source: [S10] EN 50155, 3.1.28]

double cut a double cut output is a system where the high side and the low side signals of a load are opened.
[Source: SC3 Automation]

environment all relevant parameters that can affect the achievement of functional safety in the specific application under consideration and in any safety lifecycle phase.
Note: This would include, for example, physical environment, operating environment, legal environment and maintenance environment.
[Source: [S32] IEC 61508-4, 3.2.2]

error discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: An error can be caused by a faulty item, e.g. a computing error made by faulty computer equipment.
Note 2 to entry: A human error can be seen as a human action or inaction that can produce an unintended result.
[Source: [S21] IEC 60050-192, 192-03-02]
[Source: [S9] EN 50129, 3.1.13]

event something that occurs in a certain place during a particular interval of time
[Source: [S10] EN 50155, 3.1.30]

failure, <of an item> loss of ability to perform as required
Note 1 to entry: Qualifiers, such as catastrophic, critical, major, minor, marginal and insignificant, may be used to categorize failures according to the severity of consequences, the choice and definitions of severity criteria depending upon the field of application.
Note 2 to entry: Qualifiers, such as misuse, mishandling and weakness, may be used to categorize failures according to the cause of failure.
Note 3 to entry: "Failure" is an event, as distinguished from "fault", which is a state.
[Source: [S24] IEC 60050-821, 821-11-19, modified – The note 3 to entry has been added]
[Source: [S9] EN 50129, 3.1.15]

fault, <in a system> abnormal condition that could lead to an error in a system
Note 1 to entry: A fault can be random or systematic.
[Source: [S24] IEC 60050-821, 821-11-20]
[Source: [S9] EN 50129, 3.1.17]

firmware software stored in read-only memory or in semi-permanent storage such as flash memory, in a way that is functionally independent of applicative software
[Source: [S12] EN 50657, 3.1.12]

function, <of an item> specified action or activity which can be performed by technical means and/or human beings and has a defined output in response to a defined input
Note 1 to entry: A function can be specified or described without reference to the physical means of achieving it.
[Source: [S24] IEC 60050-821, 821-12-25, modified – The specified use “of a product” and the definition have been made more general, the note 1 to entry has been added]
[Source: [S9] EN 50129, 3.1.19]

functional safety part of the overall safety that depends on functional and physical units operating correctly in response to their inputs
[Source: [S22] IEC 60050-351, 351-57-06]
[Source: [S9] EN 50129, 3.1.20]

high side cut a high side cut output is a system where the high side signal of a load is opened.
[Source: SC3 Automation]

safety supervisory layer 3 (L3SS) a software component developed by SC3 Automation in compliance with NVIDIA specifications to run on the safety MCU. This software is responsible for off-chip (Xavier SoC) and high integrity monitoring at the system level (L0/L1/L2SS are provided by NVIDIA as a black box with the JSEP).
[Source:[R6] JETSON AGX XAVIER INDUSTRIAL IN SAFETY-RELATED SYSTEMS application note]

operating temperature temperature range in which the electronic equipment will operate (e.g., cubicle temperature, rack temperature, roof box temperature) in full conformity with performance criteria, and outside which there can be temporary or permanent degradation of the equipment performances
[Source: [S10] EN 50155, 3.1.3]

safe state condition which continues to preserve safety
[Source: [S24] IEC 60050-821, 821-12-49]
[Source: [S9] EN 50129, 3.1.39]

safety freedom from unacceptable risk
[Source: [S25] IEC 60050-903, 903-01-19]
[Source: [S9] EN 50129, 3.1.40]

safety function function whose sole purpose is to ensure safety
Note 1 to entry: A safety-related function is a function whose failure affects safety (for details refer to definition of "safety-related"). Therefore, all safety functions are safety-related functions, but not vice versa.
Note 2 to entry: A safety function may contribute to one or more safety barriers. However, a safety barrier is not necessarily implemented by a safety function.
[Source: [S7] EN 50126, 3.68]

safety integrity level one of a number of defined discrete levels for specifying the safety integrity requirements for safety related functions to be allocated to the safety-related systems
[Source: [S7] EN 50126, 3.70, modified – The notes to entry have been removed]
[Source: [S9] EN 50129, 3.1.46]

[Source: [S32] IEC 61508-4]

safety-related carries responsibility for safety
[Source: [S24] IEC 60050-821, 821-01-73]
[S9] EN 50129, 3.1.50]

system set of interrelated elements considered in a defined context as a whole and separated from their environment
[Source: [S22] IEC 60050-351, 351-42-08, modified – The notes to entry have been omitted.]
[Source: [S9] EN 50129, 3.1.54]

Definitions, Acronyms, and Abbreviations

These definitions, acronyms, and abbreviations are used throughout this document.

Term/ Abbreviation/ Acronym	Definition
3LSS	The mechanism specified by NVIDIA for monitor and error reporting from JAXi to the safety MCU. NVIDIA 3LSS consists of four components (L0SS, L1SS, L2SS, and L3SS).
A	Ampere or amp unit measure of electrical current
CAN	Controlled Area Network
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DI	Digital input
DO	Digital output
Hz	Hertz
I/O	Input/output
ISA	Independent Safety Assessor
JAXi	Jetson AGX Xavier industrial
JSEP	Jetson Safety Extension Package
L3SS	Safety Supervisory Layer 3
LED	Light Emitting Diode
MCB1*x*	SC3 Automation Main Controller Board Possible options are MCB10, MCB11 , and MCB11
N/A	Not Applicable
PWM	Pulse-width modulation
RTC	Real-time Clock
SENFAI	Sensor Fusion and Artificial Intelligence Safety Controller
SIL	Safety Integrity Level
SOM	System on Module
UDIO	SC3 Automation Universal Digital Input Output board
UDIODC	SC3 Automation Universal Digital Input Output Double-cut board
RIO	SC3 Automation Universal Relay Input Output board
W	Watt

Table 4: Definitions, acronyms, and abbreviations

References

These documents provide additional information for this product. Please note that most documents from NVIDIA are only available under an NDA.

[#] Title	Rev	Description/Organization/ hyperlink
[R1] SENFAI Release Notes	-	SC3HW-1647119755-675
[R2] SENFAI Controller Manual	-	SC3HW-1647119755-676
[R3] SENFAI Safety Manual	-	SC3HW-1647119755-677
[R4] SENFAI Programming Guide	-	SC3HW-1647119755-678
[R5] DATA SHEET NVIDIA Jetson AGX Xavier Series System-on-Module	1.5	DS-09654-002_v1.5
[R6] JETSON AGX XAVIER INDUSTRIAL IN SAFETY-RELATED SYSTEMS application note	7	DA-10743-001_v01
[R7] Jetson AGX Xavier Series Interface Comparison and Migration	1.2	DA-10566-001_v1.2
[R8] XAVIER SAFETY EXTENSION MANUAL	01	DA-10743-001_v01

Table 5: Document references

Standards and Regulations

These standards and regulations are referenced throughout this document.

Standard/ Regulation	Rev	Description/Organization/ hyperlink
[S1] EN 45545-1	2013	Railway applications – Fire protection on railway vehicles – Part 2: General
[S2] EN 45545-2	2013+A1: 2015	Railway applications – Fire protection on railway vehicles – Part 2: Requirements for fire behaviour of materials and components
[S3] EN 50121-3-2	2007	Railway applications - Electromagnetic compatibility -- Part 3-2: Rolling stock - Apparatus
[S4] EN 50124-1	2017	Railway applications – Insulation coordination - Part 1: Basic requirements — Clearances and creepage distances for all electrical and electronic equipment
[S5] EN 50125-1	2014	Railway applications – Environmental conditions for equipment –Part 1: Rolling stock and on-board equipment
[S6] EN 50125-3	2003	Railway applications – Environmental conditions for equipment – Part 3: Equipment for signalling and telecommunications
[S7] EN 50126	2017	Railway Applications: The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)
[S8] EN 50128	2011	Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems
[S9] EN 50129	2018	Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling
[S10] EN 50155	2017	Railway Applications – Rolling stock – Electronic equipment
[S11] EN 50159	2020	Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems
[S12] EN 50657	2016	Railway Applications- Rolling Stock Applications- Software on board of rolling stock excluding control and protection applications
[S13] EN 55011	2009+A1: 2010	Industrial, scientific and medical equipment. Radio-frequency disturbance characteristics. Limits and methods of measurement
[S14] EN 61000-4-2	2009	Electromagnetic compatibility (EMC) — Part 4-2 : Testing and measurement techniques — Electrostatic discharge immunity test
[S15] EN 61000-4-3	2020	Electromagnetic compatibility (EMC) — Part 4-3: Testing and measurement techniques — Radiated, radio-frequency, electromagnetic field immunity test
[S16] EN 61000-4-4	2012	Electromagnetic compatibility (EMC) — Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test
[S17] EN 61000-4-5	2017	Electromagnetic compatibility (EMC) — Part 4-5: Testing and measurement techniques – Surge immunity test

Standard/ Regulation	Rev	Description/Organization/ hyperlink
[S18] EN 61000-4-6	2014	Electromagnetic compatibility (EMC) — Part 4-6: Testing and measurement techniques — Immunity to conducted disturbances, induced by radio-frequency fields
[S19] EN 61373	2010	Railway Applications – Rolling stock equipment – Shock and vibration tests
[S20] IEC 60050-151	2001	International Electrotechnical Vocabulary (IEV) - Part 151: Electrical and magnetic devices
[S21] IEC 60050-192	2015	International Electrotechnical Vocabulary (IEV) - Part 192: Dependability
[S22] IEC 60050-351	2013	International Electrotechnical Vocabulary (IEV) - Part 351: Control technology
[S23] IEC 60050-581	2008	International Electrotechnical Vocabulary (IEV) - Part 581: Electromechanical components for electronic equipment
[S24] IEC 60050-821	2017	International Electrotechnical Vocabulary (IEV) - Part 821: Signalling and security apparatus for railways
[S25] IEC 60050-903	2013	International Electrotechnical Vocabulary (IEV) - Part 903: Risk assessment
[S26] IEC 60529	2013	Degrees of protection provided by enclosures (IP code)
[S27] IEC 60664-3	2016	Insulation coordination for equipment within low-voltage systems - Part 3: Use of coating, potting or moulding for protection against pollution
[S28] IEC 61010-2-201	2017	Safety requirements for electrical equipment for measurement, control, and laboratory use- Part2:201 Particular requirements for control equipment
[S29] IEC 61508	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems
[S30] IEC 61131-2	2017	Industrial-process measurement and control - Programmable controllers - Part 2: Equipment requirements and tests
[S31] IEC 61131-3	2013	Programming controller – Programming Languages
[S32] IEC 61508-4	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations
[S33] IEC 62443-1-1	2017	Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models
[S34] IPC A-610H	2020	Acceptability of Electronic Assemblies
[S35] ISO 13849	2015	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
[S36] ISO 26262	2018	Road vehicles — Functional safety
[S37] RoHS 3 (EU 2015/863)	2015	Restriction of Hazardous Substances
[S38] UL 94 V-0	2013	UL 94, the Standard for Safety of Flammability of Plastic Materials for Parts in Devices and Appliances testing: burning stops within 10 seconds on a vertical specimen; drips of particles allowed as long as they are not inflamed.

Table 6: Referenced standards

Revision History

Version Number	Description	Date Modified	Author
0.1	Initial draft	2022-06-12	C. Deguire
0.6	Review and adjust content	2022-07-17	J. Chouinard
0.7	Technical revision and minor changes	2022-07-17	F. B-Desy
0.8	Layout and grammatical revision	2022-07-18	C. Deguire
0.10	Pre-Release	2022-07-18	J Chouinard
0.11	Pre-Release for circulation	2022-07-19	J Chouinard
0.13	Pre-Release for circulation, updated format	2022-07-26	J Chouinard
0.14	Update with new board layouts	2022-07-31	J Chouinard
1.0	Release for distribution	2022-07-31	J Chouinard
2.0	Update to NVIDIA logo	2023-08-14	F. B-Desy