Emergency Stop Switch Instruction Sheet

According to EN ISO 13849-1 and IEC 62061

About the Document

This document describes the GP4000H Series emergency stop switch and 3-position enable switch with special regard to how it meets the Safety requirements of the ISO 13849-1 and IEC 62061. It provides detailed information on how to design and maintain the system correctly in order to protect human beings as well as to prevent damage to environment, equipment, and production.

The emergency stop switch is intended to be integrated in the emergency stop function of machines up to Performance Level / Safety Integrity Level PLe/ SIL3.

According to EN ISO 12100, an emergency stop is a function which is intended:

- to avert arising or to reduce existing hazards to persons, damage to machinery or to work in progress
- to be initiated by a single human action

This documentation is intended for qualified personnel familiar with Functional Safety and GP4000H Series (the display unit). Commissioning and operating the display unit in a safety related part of a control system may only be performed by persons who are authorized to commission and operate systems in accordance with established functional safety standards.

NOTE: The original document is in English, the documents in the other languages are translations from the English.

Validity Note

The data and illustrations found in this documentation are not binding. Schneider Electric or any of its affiliates or subsidiaries (hereinafter, referred to as Schneider Electric) reserves the right to modify our products in line with our policy of continuous product development. The information in this documentation is subject to change without notice and should not be construed as a commitment by Schneider Electric.

NHA94216 02 Printed in

Pro-face
by Schneider Electric

Related Documents

You can download the technical publications and other technical information from our support site at *http://www.pro-face.com/trans/en/manual/1001.html*.

NOTE: All restrictions regarding electrical safety and external cabling and wiring must follow the documents in this table and the contents of this manual.

Reference	Designation
NHA87487	GP4000H Series Installation Guide
GP4000H-MM01-EN-PDF	GP4000H Series Hardware Manual
NVE42149	GP3000H Conversion Adapter Installation Guide
15RT-4RD00065	EC declaration for GP4000H
CNB/M/11.050 Revision 05	CO-ORDINATION OF NOTIFIED BODIES Machinery Directive 2006/42/EC + Amendment RECOMMENDATION FOR USE

Conformity to European Directives

Schneider Electric declares that the emergency stop switch is in conformity with the provisions of the following EC Machinery directive(s) 2006/42/EC and following standards and/or technical specifications referenced below have been applied and validated by INERIS.

Standards used

Reference	Designation
EN ISO 13850: 2015	Safety of machinery - Emergency stop - Principles for design
EN ISO 13849-1: 2015	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
EN ISO 13849-2: 2012	Safety of machinery - Safety-related parts of control systems - Part 2: Validation
EN IEC 62061: 2005	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

PLEASE NOTE

Electrical equipment should be installed, operated, serviced and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

PRODUCT RELATED INFORMATION

Please contact us if you have any suggestions for improvements or amendments, or if you have found any errors in this publication.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When controllers are used for applications with technical safety requirements, please follow the relevant instructions.

Refer to:
- ISO 13849-1, “Safety of machinery - Safety-related parts of control systems - Part1: General principles for design”.
- IEC 62061, “Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control system”.

The PL and SIL requirements are based on the standards current at the time of certification.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Completely understand the applications and environment defined for:
  - emergency stop function: Performance Level (PL)e within ISO 13849-1 and by Safety Integrity Level (SIL) 3 within IEC 62061.
- Do not exceed SIL3 ratings in the application of this product.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

TERMS USED IN THIS DOCUMENT

Safety requirements	ISO 13849-1
Safety Integrity level	IEC 62061
Functional safety	IEC 62061
Safety function	ISO 13849-1
Safety standard	ISO 13849-1
Safety of machinery	ISO 13849-1
Safety related part of control system	ISO 13849-1
Well tried safety principles	ISO 13849-2
Safety monitoring relay (Preventa)	XPSAF5130
Fault	IEC 60204-1
Failure	IEC 60204-1
Dangerous failure	ISO 13849-1
Risk	IEC 60204-1
Emergency, emergency stop and emergency stop function	ISO 13850
Enabling control	IEC 60204-1
Enabling device	ISO 12100

EMERGENCY STOP FUNCTION

Safety requirements

The emergency stop switch is dedicated to be integrated in the emergency stop function of machines when the safe state of the emergency stop function is de-energize to trip.

The emergency stop system is used as part of a comprehensive risk reduction strategy. Make sure the device, its installation, and associated configuration satisfy your risk assessment and associated risk reduction strategy.

When designing, installing or operating any emergency stop device, such as the emergency stop, you must ensure that the national and international standards and regulations that apply to your application are fulfilled. The national and international safety of machinery regulations specific to the application must be observed, for example:

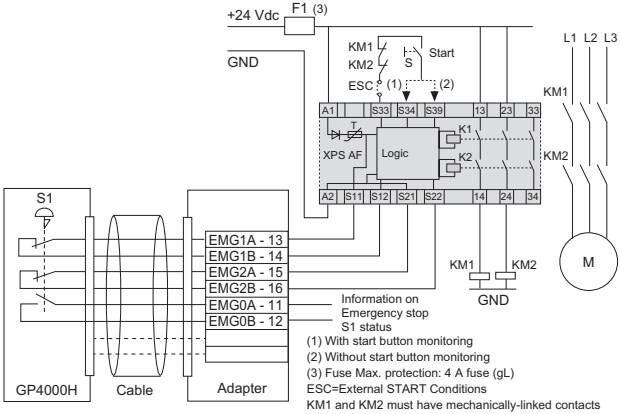
- EN 12100, Safety of machinery, Basic concepts, general principles for design
- EN 60204-1, Safety of machinery, Electrical equipment of machines
- EN ISO 13850 Safety of machinery, Emergency stop. Principles for design
- EN ISO 13849-1, Safety of machinery, Safety related parts of control systems, General principles for design

Hardware architecture design

The following diagram is an example of an emergency stop diagram of a single display unit. The activation of the emergency stop switch or disconnection of the display unit sends a signal to the rest of the system to initiate stopping moving parts of the machine.

In the following example, the Monitoring device is a safety monitoring relay for monitoring emergency stop circuits: reference XPSAF5130 (Schneider Electric, Preventa range of products) or equivalent.

The XPSAF5130 module or equivalent provides three safety related outputs of stop category 0 (EN ISO 13850, EN 60204-1).



The architecture above is based on two channels with cross monitoring.

The safety monitoring relay continuously checks the signals from contacts EMG1A/EMG1B (Channel 1) and EMG2A/EMG2B (Channel 2) of the emergency stop switch. As long as both circuits are closed, the safety monitoring relay closes the motor contactors when the start button is pressed.

As soon as the emergency stop switch is pressed or in case of any detected failures on channel 1 or channel 2, the safety monitoring relay will open both motor contactors of the machine or system.

Restart will then be allowed only if the fault conditions are cleared before the start button is pressed.

The safety monitoring relay also checks the position of the motor contactors through the mirror contact. In case a contactor remains closed on emergency stop actuation, the other contactor will perform the emergency stop function and restart, then will be allowed only if the fault conditions are cleared.

NOTE: When the display unit is unplugged:

1. The safety circuit becomes open and the system stops immediately.
2. It is recommended to keep it away from the operating equipment because, in case of an emergency, the operator may try to stop the system with the emergency stop integrated in the display unit that is no longer part of the system.
3. It is recommended to provision of proper storage for detached operator control station (the display unit).

Probabilistic properties

The emergency stop system has been designed and validated for use in safety functions up to:

- EN ISO 13849-1: Performance level (PL) PLe
  The safety-related properties of the emergency stop sub-system (a display unit, a direct-connect cable and a conversion adapter) according to EN ISO 13849-1, if used according to architecture principles shown in "Emergency Stop function PLe, SIL 3" on page 6:
  - Architecture category 4
  - Mean time to dangerous failure of each channel (MTTFd): High (MTTFd = 113 years with a worst case assumption of 1 operating cycle per hour and 8760 operating hours per year)
  - Diagnostic coverage (DC): High, all diagnostics are performed by the safety monitoring relay (DC = 99%)
  - Measure against common cause failure (CCF) are applied.

  Therefore the emergency stop system (including a direct-connect cable and a conversion adapter) is suitable for use in emergency stop safety functions up to PLe.

NOTE: The MTTFd of the Emergency Stop sub-system strongly depends on the emergency stop switch. As an electromechanical component, the $MTTF_d$ of the emergency stop switch is based upon the lifetime of the components and the frequency of operating cycle (worst case assumption: 1 operating cycle per hour and 8760 operating hours per year).
A detailed calculation of the $MTTF_d$ per channel is given below:

$$MTTF_{d\ \text{Channel 1 (GP4000H)}} = MTTF_{d\ \text{Channel 2 (GP4000H)}} = \frac{1}{\frac{0,1 \times n_{op}}{B_{10d}} + \frac{1}{MTTF_{d(\text{GP4000H/Cable/Adapter})}}}$$

With:

$MTTF_{d\ (\text{GP4000H/Cable/Adapter})} > 8\ 000$ years

$B_{10d} = 100\ 000$ operations

n_{op} = mean number of annual operations

- IEC 62061: Safety integrity level SIL CL 3
  The safety related properties of the emergency stop sub-system (including a display unit, a direct-connect cable and a conversion adapter) according to EN/IEC 62061, if used according to the architecture principle in "Emergency Stop function PLe, SIL 3" on page 6:
  - Safe Failure Fraction (SFF): SFF > 99% for each channel (SFF = 99.8%)
  - Subsystem architecture type D

- Diagnostic coverage DC = 99%, all diagnostics are performed by the safety monitoring relay
- Equivalent Failure rate per channel $\lambda_{de1} = \lambda_{de2} = 1.01 \times 10^{-6}$/h (with a worst case assumption of 1 operating cycle per hour and 8760 operating hours per year)
- Susceptibility of common cause factor: $\beta = 2\%$
  According to EN/IEC 62061, and an assumption of proof test interval of 1 year, the probability of dangerous failure (PFH) of the emergency stop sub-system is $PFH_{DssD} = 2.88 \times 10^{-8}$.

NOTE: The λ_d of the emergency stop sub-system strongly depends on the emergency stop switch. As an electromechanical component, the λ_d of the emergency stop switch is based upon the lifetime of the components and the frequency of operating cycle (worst case assumption: 1 operating cycle per hour and 8760 operating hours per year).
A detailed calculation of the λ_d per channel is given below:

$$\lambda_{d\ \text{channel 1 (GP4000H)}} = \lambda_{d\ \text{channel 2 (GP4000H)}} = \frac{0,1 \times n_{op}}{B_{10d}} + \frac{1}{MTTF_{d(\text{GP4000H/Cable/Adapter})}}$$

With:

$MTTF_{d\ (\text{GP4000H/Cable/Adapter})} > 8\ 000$ years

$B_{10d} = 100\ 000$ operations

n_{op} = mean number of annual operations

3-Position Enable Switch

Safety Requirements

The enabling device is to be integrated in the enabling device function of machines when the safe state of the function is de-energize to trip.

The enabling device system is used as part of a comprehensive risk reduction strategy.

Make sure the device, its installation and associated configuration satisfy your risk assessment and associated risk reduction strategy.

When designing, installing or operating any enabling device, such as the enabling device, you must ensure that the national and international standards and regulations that apply to your application are fulfilled.

The national and international safety of machinery regulations specific to the application must be observed, for example:
- EN 12100, safety of machinery: basic concepts, general principles for design
- EN 60204-1, safety of machinery: electrical equipment of machines
- EN/ISO 13849-1, safety of machinery: safety related parts of control systems and general principles for design

Hardware Architecture Design

The following diagram is an enabling function of a single display unit. The enabling control is a manually activated control function interlock.

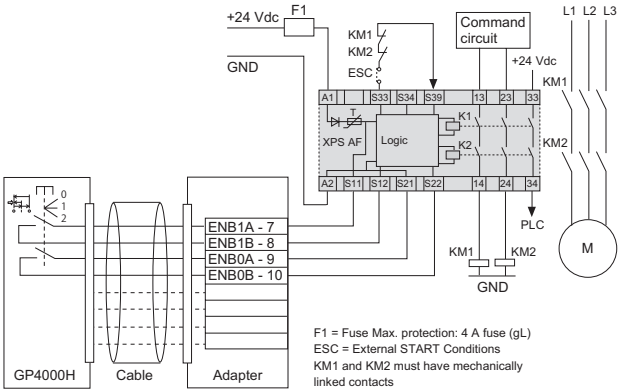
When:
- activated: a machine operation can be initiated by a separate start control
- de-activated: a stop function is initiated that prevents initiation of a machine operation

The activation of the 3-position enable switch, by pressing it to the intermediate position, sends a signal to the rest of the system to allow the command of moving parts of the machine.

The signal is removed when:
- 3-position enable switch is not pressed (released)
- 3-position enable switch is pressed to the innermost position (fully pressed)
- the display unit is unplugged
- there is a loss of the safety circuit power supply
- there is an internal fault detected

In the following example the Monitoring device is a safety monitoring relay: Schneider Electric reference XPSAF5130 (Preventa range of products) or equivalent.

The XPSAF5130 module or equivalent provides three safety related outputs of stop category 0 (EN/ISO 13850 and EN 60204-1) in the figure below.



The architecture above is based on two channels with cross monitoring. The safety monitoring relay continuously checks the signals from contacts ENB0A/ENB0B (Channel 1) and ENB1A/ENB1B (Channel 2) of the enabling switch. As long as both circuits are closed, the safety monitoring relay allows the command circuit to command the motor contactors.

As soon as the enabling switch is released, fully pressed or detects an error on channel 1 or channel 2, the safety monitoring relay opens both motor contactors of the machine or system.

The safety monitoring relay also checks the position of the motor contactors through the mirror contact. If a contactor remains closed on stop actuation, restart is then allowed only if the error conditions are cleared.

To minimize the possibility of defeating the enabling switch, the PLC output (33/34) of the safety relay can be use to check the de-activation of the enabling control function before machine operation is re-initiated.

NOTE: When the display unit is unplugged:

1. The safety circuit becomes open and the system stops immediately.
2. It is recommended to keep it away from the operating equipment because, in case of an emergency, the operator may try to stop the system with the emergency stop integrated in the display unit that is no longer part of the system.

Probabilistic Properties

The enabling control function has been designed and validated for use in safety functions up to:

- EN/ISO 13849-1: Performance level (PL) PLd

The safety-related properties of the enabling switch sub-system (a display unit, a direct-connect cable and a conversion adapter) according to EN ISO 13849-1, if used according to architecture principles shown in "Enabling control function category 3, PLd, SIL 2" on page 10 above (Enabling control function category 3, PLd, SIL 2):

- Architecture category 3
- Mean time to dangerous failure of each channel ($MTTF_d$): High ($MTTF_d$ = 175 years with an assumption of 1 operating cycle per hour and 8760 operating hours per year)
- Diagnostic coverage (DC): Low, with diagnostics are performed by the safety monitoring relay (DC = 75 %)
- Measure against common cause failure (CCF) are applied
- IEC 62061: Safety integrity level SIL CL 2

Therefore, the enabling device (including cable and conversion adapter) is suitable for use in enabling device safety functions up to PLd.

NOTE: The $MTTF_d$ of the enabling device depends on the enabling switch. As an electromechanical component, the $MTTF_d$ of the enabling switch is based upon the lifetime of the components and the frequency of operating cycle (worst case assumption: 1 operating cycle per hour and 8760 operating hours per year).
A detailed calculation of the $MTTF_d$ per channel is given below:

$$MTTF_{d\ \text{Channel 1 (GP4000H)}} = MTTF_{d\ \text{Channel 2 (GP4000H)}} = \frac{1}{\frac{0,1 \times n_{op}}{B_{10d}} + \frac{1}{MTTF_{d(\text{GP4000H/Cable/Adapter})}}}$$

With:

$MTTF_{d\ (GP4000H/Cable/Adapter)} > 8\ 000$ years

$B_{10d} = 100\ 000$ operations

n_{op} = mean number of annual operations

If the enabling device sub-system (that includes the display unit, cable and conversion adapter) is according to the architecture in "Enabling control function category 3, PLd, SIL 2" on page 10, the safety related properties according to EN IEC 62061 are:

- Safe Failure Fraction (SFF):SFF >80%
- Subsystem architecture type B
- Hardware fault tolerance is 1

- Architectural constraints on subsystem are meet up to a maximum of SIL2
- Equivalent Failure rate per channel $\lambda_{de1} = \lambda_{de2} = 1.01 \times 10^{-6}$/h (with a worst case assumption of one operating cycle per hour and 8760 operating hours per year)
- Susceptibility of common cause factor: $\beta = 2\%$

According to EN IEC 62061 and with an assumption of lifetime of 10 years, the probability of dangerous failure (PFH) of the enabling device sub-system is $PFH_{DssD} < 10^{-7}$.

NOTE: The λ_d of the enabling control sub-system strongly depends on the 3-position enable switch. As an electromechanical component, the λ_d of the 3-position enable switch is based upon the lifetime of the components and the frequency of operating cycle (worst case assumption: 1 operating cycle per hour and 8760 operating hours per year).
A detailed calculation of the λ_d (per year) per channel is given below:

$$\lambda_{d\ channel\ 1\ (GP4000H)} = \lambda_{d\ channel\ 2\ (GP4000H)} = \frac{0,1 x n_{op}}{B_{10d}} + \frac{1}{MTTF_{d\ (GP4000H/Cable/Adapter)}}$$

With:

$MTTF_{d\ (GP4000H/Cable/Adapter)} > 8\ 000$ years

$B_{10d} = 100\ 000$ operations

n_{op} = mean number of annual operations

OPERATION AND MAINTENANCE

Installation

The installation instructions for the monitoring device being used must be followed.

Operation

If the direct-connect cable is not permanently installed, make sure that it is kept out of the way to prevent any accidents which may cause the hand-held terminal to fall to the ground.

The direct-connect cable must not be pinched or come into contact with sharp corners, that would result in damage to the cable or its sheathing.

The emergency stop that is not connected might be confused with an active control device. Keep it away from dangerous areas.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Keep a disconnected the display unit away from dangerous areas.
- Do not operate the display unit with a damaged connection or switching cabinet cable.
- Enabling device function: Performance Level (PL)d within ISO 13849-1 and by Safety Integrity Level (SIL) 2 within IEC 62061.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Maintenance

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Check the emergency stop and the enabling control function the first time the display unit is connected.
- Perform a periodic maintenance test, at least once a year, to verify the emergency stop and the enabling control function.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

MAIN FUNCTIONAL AND ENVIRONMENTAL SPECIFICATIONS

GP4000H Series

Physical environment	Surrounding air temperature	0...40 °C (32...104 °F)
	Storage temperature	-20...60 °C (-4...140 °F)
	Surrounding air and storage humidity	10...90% RH (non-condensing, wet bulb temperature: 39 °C [102.2 °F] or less)
	Dust	0.1 mg/m^3 (10^{-7} oz/ft^3) or less (non-conductive levels)
	Pollution degree	For use in Pollution Degree 2 environment
	Corrosive gases	Free of corrosive gases
	Atmospheric pressure (operating altitude)	800...1,114 hPa (2,000 m [6,561 ft] or lower)

Conversion Adapter

Physical environment	Surrounding air temperature	0...50 °C*1 (32...122 °F)
	Storage temperature	-20...60 °C (-4...140 °F)
	Surrounding air and storage humidity	10...90% RH (non-condensing, wet bulb temperature: 39 °C [102.2 °F] or less)
	Dust	0.1 mg/m^3 (10^{-7} oz/ft^3) or less (non-conductive levels)
	Pollution degree	For use in Pollution Degree 2 environment
	Corrosive gases	Free of corrosive gases
	Atmospheric pressure (operating altitude)	800...1,114 hPa (2,000 m [6,561 ft] or lower)

*1 The ambient operating temperature of the display unit is 0 to 40 °C (32 to 104 °F).

Direct-Connect Cable (with connector)

Standards	UL1571
Surrounding air temperature	-10...60 °C (-14...140 °F)
Conductor material	Copper wire, tin plating
Size of conductor (emergency stop signals)	AWG 22
Outside diameter of conductor	0.76 mm (0.03 in)
Outside diameter of insulator	1.2 mm (0.05 in)
Resistance of conductor (20 °C)	59.4 Ω / km (95.6 Ω / mile) or less
Length	3 m (9.84 ft) 5 m (16.4 ft) 10 m (32.8 ft)

TECHNICAL DATA OF COMPONENTS

Emergency Stop Switch

Standards	EN60947-5-1, EN60947-5-5, UL508
Contact material	Gold plated silver
Contact resistance	50 mΩ or less (initial value)
Mechanical life	250 000 operations*1
Electrical life	100 000 operations*1
Degree of protection	IP65
Rated operating current according to IEC 60947-5-1	Main contacts (NC): (DC13) Ue = 30 V / Ie = 1 A Monitoring contact (NO): (DC13) Ue = 30 V / Ie = 1 A
B_{10d}	100 000 operations*1

*1 The actual number of operations varies based upon environment, duty cycle and load.

3-Position Enable Switch

Standards	EN 60947-5-1, EN 60947-5-8, UL508
Contact resistance	50 mΩ or less (initial value)
Mechanical life	Position 1 → 2: 100 000 000 operations or more*1 Positions 1 → 2 → 3 → 1: 100 000 operations or more*1
Electrical life	100 000 operations or more at rated load*1
Degree of protection	IP65
Rated operating current according to IEC 60947-5-1	Main contacts (NC): (DC13) Ue = 30 V / Ie = 1 A Monitoring contact (NO): (DC13) Ue = 30 V / Ie = 1 A
B_{10d}	100 000 operations*1

*1 The actual number of operations varies based upon environment, duty cycle and load.