SEW EURODRIVE

Safety Manual

Decentralized Safety Controller

MOVISAFE® HM31

(Version PFF-HM31A)

Edition 05/2014

21230595 / EN

Contents

21230595 / EN – 05/2014

21230595 / EN – 05/2014

21230595 / EN – 05/2014

1 General information

This manual contains information on the designated use of the safety controller.

The following conditions are required for safe installation, startup and safety during operation and maintenance:

- Knowledge of regulations
- Proper technical implementation of the safety instructions in this manual through qualified personnel.

Under the following circumstances, disruption or impairment of safety functions can cause severe injury to persons, damage to property or damage to the environment, for which SEW-EURODRIVE cannot assume liability:

- Unskilled access to the units
- De-activating or bypassing safety functions
- Non-observance of instructions in this manual

SEW-EURODRIVE develops, manufactures and tests safety controllers in compliance with the pertinent safety standards. The units may only be used if the following requirements have been met:

- They are only used for the intended applications
- They are only operated under the specified environmental conditions
- They are only operated in conjunction with approved non-SEW units

1.1 About the documentation and its structure

This safety manual contains the following topics:

- Designated use
- Safety concept
- Central functions
- Inputs
- Outputs
- Software
- Safety-related aspects of the user program
- Configuring the communication

The manual describes the following variant:

Programming tool	Processor operating system	Communication operating system
SILworX®	CPU-BS V.8 and later	COM-BS V.13 and later

1.2 Target group

This document was written for planners, project planners, and programmers of automation systems as well as for persons authorized to start up, operate, and service the units and systems. Specific knowledge of safety-related automation systems is required.

21230595 / EN – 05/2014

1.3 Text conventions

The following notation is used in this document to enhance readability and comprehensibility:

Notation	Meaning
Bold	To highlight important text. Designations of buttons, menu functions and tabs you can click in the programming tool.
Italics	Parameters and system variables.
`Courier`	Actual user entries.
RUN	Names of operating states in capital letters.
Chapter 1.2.3	Cross reference to other chapters.

1.4 Structure of the safety notes

1.4.1 Meaning of signal words

The following table shows the grading and meaning of the signal words for safety notes.

Signal word	Meaning	Consequences if disregarded
⚠ **DANGER**	Imminent hazard	Severe or fatal injuries
⚠ **WARNING**	Possible dangerous situation	Severe or fatal injuries
⚠ **CAUTION**	Possible dangerous situation	Minor injuries
NOTICE	Possible damage to property	Damage to the drive system or its environment
INFORMATION	Useful information or tip: Simplifies handling of the drive system.	

1.4.2 Structure of section-related safety notes

Section-related safety notes do not apply to a specific action but to several actions pertaining to one subject. The hazard symbols used either indicate a general hazard or a specific hazard.

This is the formal structure of a safety note for a specific section:

SIGNAL WORD

Type and source of hazard.

Possible consequence(s) if disregarded.

- Measure(s) to prevent hazard.

21230595 / EN – 05/2014

1.4.3 Structure of embedded safety notes

Embedded safety notes are directly integrated into the instructions just before the description of the dangerous action.

This is the formal structure of an embedded safety note:

- ⚠ **SIGNAL WORD** Type and source of hazard.

  Possible consequence(s) if disregarded.

  – Measure(s) to prevent hazard.

21230595 / EN – 05/2014

2 Notes on use

Strictly observe the safety information, notes and instructions in this manual. Use the product only in accordance with all the guidelines and safety instructions.

2.1 Designated use

2.1.1 Field of application

The safety-related controller can be used up to safety integrity level SIL 3 according to IEC 61508, and PL e according to EN ISO 13849-1.

The MOVISAFE® HM31 safety controller is certified for protective systems and machine controllers.

When using the safety-related communication between various units it is important that the overall response time of the system does not exceed the fault tolerance time. Calculations must be performed in accordance with the rules mentioned in chapter "Configuring the communication".

Connect only devices to communication interfaces that ensure safe electrical disconnection.

Normally energized principle / normally de-energized principle

The automation units were designed according to the normally energized principle. A system operating according to the normally energized principle will take on a de-energized condition in the event of a fault (de-energize to trip) to execute its safety function. In the event of a fault, input and output signals adopt a de-energized, safe state.

Safety controllers can also be used in applications operating according to the normally de-energized principle. A system operating according to the normally de-energized principle will, for example, activate an actuator to perform its safety function (energize to trip).

The requirements of the application standards have to be taken into account when designing the controller. Line diagnostics of the inputs and outputs might be necessary, for example, or feedback of the tripped safety function.

2.1.2 Non-designated use

The transfer of safety-relevant data over public networks (e.g. the Internet) is permitted provided additional measures are taken to increase security (such as VPN tunnel, firewall, etc.).

2.2 Operating conditions

The safety controller may only be used under the following environmental conditions.

21230595 / EN – 05/2014

The safety controller was developed to meet the following requirements of EMC, climatic and environmental standards:

Standard	Content
EN 61800-5-1:2007	Adjustable speed electrical power drive systems – part 5-1: Safety requirements – Electrical, thermal and energy.
EN 61800-3:2004	Variable-speed electric drives – part 3: EMC requirements including special test methods.
EN 62061:2005	Safety of machinery – Functional safety of safety-related electric, electronic and programmable electronic control systems.

The following general requirements must be met to operate the safety-related MOVISAFE® HM31:

Requirement	Content
Installation altitude (industry standard	< 2000 m Bit errors can occur in SRAM based cells caused by SEU (single event upset) effects. These effects increase with the installation altitude.
Degree of protection	IP54 (according to EN 60529)

2.2.1 Climatic requirements

The following table lists the most important tests and limit values for climatic requirements:

EN 61800-5-1	Climatic tests
	Operating temperature: -5 °C to +50 °C
	Storage temperature: −25 °C to +70 °C
	Dry heat (constantly), resistance and immunity tests according to IEC 60068-2-2:2007 (test Bd)
	Humid heat (constantly), resistance and immunity tests according to IEC 60068-2-78:2001 (test Cab)

2.2.2 Mechanical requirements

The following table lists the most important tests and limit values for mechanical requirements:

EN 61800-5-1	Mechanical tests
	Vibration immunity test according to IEC 60068-2-6:2007 (test Fc)

2.2.3 EMC requirements

Higher interference levels are required for the MOVISAFE® HM31 safety controller. The MOVISAFE® HM31 safety controller meets the requirements for emitted interference according to EN 61800-3:2004 (limit class C2) and the requirements for interference immunity according to EN 62061:2005 and EN 61800-3:2004 (second environment).

21230595 / EN – 05/2014

2.2.4 Voltage supply

The following table lists the most important tests and limit values for the voltage supply of the safety controller:

IEC/EN 61131-2	Review of the DC power supply characteristics
	The voltage supply must meet the following standards: IEC/EN 61131-2: SELV (Safety Extra Low Voltage) or PELV (Protective Extra Low Voltage)
	The safety controller must be fuse-protected as specified in this manual.
	Voltage range test: DC 24 V, −20% to +25% (19.2 V to 30.0 V)
	Momentary external current interruption immunity test: DC, PS 2: 10 ms
	Polarity reversal of the supply voltage: Note in the relevant chapter of the system manual or data sheet of the power supply.

2.2.5 ESD protection measures

Only personnel with knowledge of ESD protection measures may modify or extend the system, or replace a module.

NOTICE

Electrostatic discharge can damage the electronic components in the safety controller.

- **When performing work on the unit, make sure the workplace has anti-static protection and wear an ESD wrist strap.**
- **Store unused modules in such a way that they are protected from electrostatic discharge, for example by keeping them in their packaging.**

2.3 Requirements for machine and system manufacturers as well as operators

Machine and system manufacturers as well as operators are responsible for ensuring that the safety controller is safely operated in automation systems.

Machine and system manufacturers must validate that the safety controller is programmed properly.

2.4 Additional system documentation

- "Decentralized Safety Controller MOVISAFE® HM31" operating instructions
- "Decentralized Safety Controller MOVISAFE® HM31" system manual

21230595 / EN – 05/2014

The latest documentation versions are available for download from the SEW website (www.sew-eurodrive.com) under "Documentation".

2.5 Checklist for project planning, programming and startup

This checklist is a recommendation for the user

- for the project planning, programming and startup of safety-related inputs and outputs,
- for creating a user program with the SILworX® programming tool.

Filling in the checklist can ensure that requirements have been fully accounted for in an orderly format. The checklist also serves to document the connection between external wiring and user program.

The *PFF_HM31A_Checkliste_DE.pdf* checklist can be downloaded as a PDF document from the SEW-EURODRIVE homepage (www.sew-eurodrive.com). You find the checklist in the “safetyDRIVE” area of the “Documentation” category.

21230595 / EN – 05/2014

3 Safety concept for using MOVISAFE® HM31

This chapter contains important general aspects concerning the functional safety of MOVISAFE® HM31 safety controllers:

- Safety and availability
- Time parameters important for safety
- Repeat test
- Safety conditions
- Certification

3.1 Safety and availability

The safety controller is certified for protective systems and machine controllers.

Using the safety controller does not pose an immediate hazard.

⚠ WARNING

Risk of improperly connected or improperly programmed safety-related automation systems.

Severe or fatal injuries.

3.1.1 Self-test and error diagnostics

The operating system of the controllers performs comprehensive self-tests during booting and operation. The following components are tested:

- Processors
- Memory areas (RAM, non-volatile memory)
- Watchdog
- I/O channels

If faults are detected during the tests, the operating system switches off the defective safety controller or the defective I/O channel.

In non-redundant systems, this means that sub-functions or the entire PES can shut down.

All safety controllers are equipped with LEDs to indicate detected faults. Once a fault occurs, the LEDs allow the user to quickly diagnose the fault in a unit or the external wiring.

Additionally, the user program can evaluate various system variables that indicate the condition of the safety controller.

A comprehensive diagnostic record of the system behavior is logged and detected faults are stored in the diagnostic memory of the controllers. The error log can also be read after a system malfunction using the PADT.

The safety controller does not generate any diagnostic information in the event of a few minor module failures that do not influence safety.

21230595 / EN – 05/2014

3.1.2 PADT

The PADT (Programming and Debugging Tool) lets users create the program and configure the controller. The safety concept of the PADT supports users in implementing the control task properly. The PADT performs numerous measures for checking the entered information.

The PADT is a personal computer installed with the planning tool.

3.2 Time parameters important for safety

These are:

- Fault tolerance time
- Watchdog time
- Safety time
- Response time

3.2.1 Fault tolerance time (FTT)

The fault tolerance time is a property of the process and describes the period of time in which the process allows faulty signals to occur before the system assumes a dangerous condition.

3.2.2 Safety time of the PES

The safety time is the period of time in which the PES in RUN condition must respond to an internal error.

From perspective of the process, the safety time is the maximum period of time in which the safety system must respond to a change of input signals at the outputs (response time).

Operating system version	Safety time range
CPU-BS V.8 and later	20 – 22500 ms

3.2.3 Safety time of the user program

The safety time of the user program cannot be set directly. The MOVISAFE® HM31 safety controller calculates the safety time of a user program using the parameters *safety time of the resource* and *maximum number of cycles*. For more details, refer to chapter "Multitasking".

3.2.4 Multiple fault occurrence time (MOT)

The occurrence time for multiple faults is the period of time in which the probability for the occurrence of multiple faults, which in combination are critical for safety, is sufficiently low.

The multiple fault occurrence time is set to 24 hours in the operating system.

21230595 / EN – 05/2014

3.2.5 Response time

The maximum response time of cyclically operating safety controllers is twice the cycle time of these systems unless the configuration or logic of the user program causes a delay.

The cycle time of the controller consists of the following main elements:

- Reading inputs
- Processing the user program
- Writing outputs
- Process data communication
- Performing test routines

The switching times of the inputs and outputs have to be taken into account when determining the worst case for the overall system.

3.2.6 Watchdog time of the processor system

The watchdog time is specified in the menu for setting the PES properties. This time is the maximum permitted duration of a RUN cycle (cycle time). If the cycle time exceeds the specified watchdog time, the system shuts down. The system will restart if auto boot was configured. If auto boot was not set, the system will assume STOP/VALID CONFIGURATION state.

The watchdog time of the processor system may be set to:

Max. 0.5 × PES safety time

Operating system version	Watchdog time range of values	Default values for the controllers
CPU-BS V.8 and later	4 – 5000 ms	200 ms

3.2.7 Watchdog time of the user program

Each user program has its own watchdog and watchdog time.

The watchdog time of the user program cannot be set directly. The MOVISAFE® HM31 safety controller calculates the watchdog time of a user program using the parameters *max. watchdog time* of the resource and *maximum number of cycles*.

It is important that the calculated watchdog time is not greater than the resulting response time required for the portion of the process processed by the user program.

3.3 Repeat test

A repeat test is a test performed to detect hidden faults in a safety-relevant system so that the system can be restored, if necessary, to a state where it can perform its designated function.

Repeat tests must be carried out for SEW safety systems at certain intervals. This interval can be often extended by calculating and analyzing the implemented safety circuits.

21230595 / EN – 05/2014

3.3.1 Performing the repeat test

The repeat test depends on how the system (EUC = Equipment Under Control) is configured, its risk potential, and the standards that have to be met to operate the system and that are required for approval by the responsible test authority.

According to the standards IEC 61508 1-7, IEC 61511 1-3, IEC 62061 and VDI/VDE 2180 sheets 1 to 4, the operator of safety-relevant systems is responsible for performing the repeat tests.

3.3.2 Frequency of repeat tests

The MOVISAFE® HM31 safety controller can be subjected to a repeat test by testing the entire safety circuit.

In practice, shorter repeat test intervals are required for input and output field devices (for instance every 6 or 12 months) than for the safety controller. Testing the entire safety circuit for the field device automatically includes the test of the safety controller. In this case, no additional repeat tests need to be carried out for the safety controller.

If the repeat test of the field devices does not include the safety controller, then the safety controller must be replaced at least once every 20 years to comply with SIL 3. You find information on replacing the safety controller in the "Decentralized Safety Controller MOVISAFE® HM31 operating instructions, in chapter "Safety characteristics of MOVISAFE® HM31".

3.4 Safety conditions

The following safety conditions apply to the safety-related PES of the MOVISAFE® HM31 system.

3.4.1 Hardware configuration

Personnel configuring the hardware of the MOVISAFE® HM31 safety controller must observe the following safety conditions.

Product-independent conditions

- Use only hardware and software approved for safety-related operation. Approved hardware and software is listed in the version list of the MOVISAFE® HM31 safety controller, certificate number 968/EZ 529.00/11.
- Adhere to the operating conditions (see chapter "Operating conditions") specified for EMC, mechanical, chemical, and climatic influences.
- Hardware and software that is not fail-safe but non-reactive may be used for processing non-safety relevant signals but must not be used for handling safety-related tasks.
- The normally energized principle must be applied to all safety circuits that are connected to the system externally.

Product-dependent conditions

- Connect only devices to the system that ensure safe electrical disconnection.
- Safe electrical disconnection from the power supply must be ensured in the 24 V supply of the system. Use only power supply units of the type PELV or SELV.

21230595 / EN – 05/2014

Application-dependent conditions

Design measures of the application setup or organizational measures must ensure response to any reduced safety level. The following requirements have to be met to keep the probability of faults with a common cause as low as possible. Further approved measures to increase safety must be taken depending on the application.

- Route signal cables separately for all channels and at all points.
- Route signal cables and supply cables separately from one another.
- Protect inputs and outputs against possible overvoltage and overcurrent.
- Dimension all mechanical components in such a way that the requirements for functional safety are met. This can be achieved, for example, by overdimensioning with factor 2 or higher.
- Thoroughly analyze any failure in the field and inform the manufacturers immediately so they can take the necessary improvement measures as part of the QM processes. It is important that the procedure is documented.
- A written work instruction must be created that ensures that all component failures (or impairments) are detected, their cause determined, and similar objects will be checked for possible similar failure causes.
- Following maintenance and repair work on safety-relevant components (such as encoders, brakes, etc.), the system must be calibrated again and checked for proper function (which means all the diagnostic tests must have been passed successfully). This work has to be carried out for the independent channels with a time offset.
- The maintenance instructions must prescribe that no parts of the redundant systems (such as cables, etc.), which have to be independent of one another, are changed.
- Maintenance of all components (such as printed circuit boards) must be carried out at qualified repair centers. Any repaired unit must be subjected to a complete test prior to installation.
- Service engineers must be trained appropriately (with documentation of their training) so they know the reasons and consequences of failures resulting from a common cause.
- Access for personnel must be limited (for instance by closed areas, inaccessible positions/locations).
- The system must be used only within the temperature, humidity, corrosion, dust and vibration range for which it was tested.
- The system components must have been tested for resistance against all important ambient conditions (such as EMC, temperature, vibration, shock, humidity) according to an adequate level specified in approved standards.

3.4.2 Programming

Personnel creating user programs must adhere to the following safety conditions.

Product-independent conditions

- It is important that safety-relevant system parameters are set properly in safety-related applications.
- This applies in particular to defining the system configuration, maximum cycle time, and safety time.

21230595 / EN – 05/2014

Product-dependent conditions

Conditions for using the programming tool.

- Use the SILworX® tool for programming.
- After having created the application, manually compile the program twice. Then compare the two CRCs to ensure that the program was compiled properly.
- Validate and verify the proper implementation of the application's specification. A complete test of the logic must be performed by trial.
- Repeat this procedure every time the application is changed.
- The system response to faults in the fail-safe input modules, output modules and remote I/Os must be defined in the user program in accordance with the system-specific safety-related conditions.

3.4.3 Communication

- When using safety-related communication between various units, it is important that the overall response time of the system does not exceed the fault tolerance time. Calculations must be performed in accordance with the rules mentioned in chapter 8.2.
- Transmitting safety-relevant data across public networks (e.g. Internet) is not permitted unless additional safety measures are taken, such as VPN tunnel.
- If data is transmitted across company or plant internal networks, administrative or technical measures must be taken to ensure sufficient protection against manipulation (for instance by using a firewall to separate the safety-relevant parts of the network from other networks).
- Do not use standard protocols for transmitting safety-relevant data.
- Connect only devices to communication interfaces that ensure safe electrical disconnection.

3.4.4 Maintenance work

- Maintenance work must be carried out in accordance with the latest version of the document "Maintenance Override" published by TÜV Rheinland and TÜV Product Service (www.tuvasi.com).
- Whenever necessary, the operator must consult the test authority responsible for the final inspection of the system and define administrative measures for regulating access to the system.

3.5 Certification

The MOVISAFE® HM31 safety controller (Programmable Electronic System PES) has been tested and certified by TÜV for functional safety in accordance with CE and the standards listed below.

The TÜV certificate is available for download from the SEW homepage (www.sew-eurodrive.com) under "Documentation" in the "safetyDrive" section.

21230595 / EN – 05/2014

4 Inputs of the MOVISAFE® HM31 safety controller

The MOVISAFE® HM31 safety controller comes equipped with 26 safety-related digital inputs.

- 16 digital inputs, type I (EN 61131-2)
- 8 digital inputs, type II (EN 61132-2)
- 2 digital inputs are reserved for internal diagnostics

4.1 General information

Safety-related inputs can be used both for safety-related and non-safety related signals.

The controller provides status and error information by means of

- the diagnostic LED of the controller,
- system variables that can be evaluated by the user program,
- entries in the diagnostic memory, which can be read by the PADT.

Safety-related input modules automatically perform a high-quality, cyclic self-test during operation. These test routines have been tested by TÜV (German Technical Inspection Association) and monitor the safe functioning of the respective module.

In the event of a fault, the controller sends a low level to the user program (or the initial value for CPU-BS V.8 and later) and, if possible, generates an error information. The user program can evaluate this error information by reading the error code.

No safety information is provided for a few component failures that do not affect safety.

4.2 Safety of sensors, encoders, and transmitters

In safety-related applications, both the controller and the sensors, encoders, and transmitters connected to it must meet the requirements safety requirements and the specified SIL and PL.

4.3 Safety-related digital inputs

4.3.1 General information

Digital inputs are read once every cycle and are saved internally; they are tested cyclically to ensure safe function. Input signals that are present for a time shorter than the time between two samplings (i.e. shorter than a cycle time), might not be detected.

4.3.2 Test routines

Online test routines check whether the input channels are able to pass through both signal levels (LOW and HIGH), regardless of signals present on the input. This functional test is performed each time input signals are read.

21230595 / EN – 05/2014

4.3.3 Response in the event of an error

If test routines for digital inputs detect a fault, the user program processes a low level for the faulty channel in accordance with the normally energized principle.

The user program must consider the corresponding error code in addition to the signal value of the channel.

The MOVISAFE® HM31 safety controller activates the ERROR LED.

The error code provides users with additional options to monitor the external wiring and program additional error responses in the user program.

Access to the error code	Name of the error code
From the *...Channels* tab in the detailed view of the module or unit.	*-> Error code [bytes]* in the line indicating the channel number.

4.3.4 Surges on digital inputs

Due to the short cycle time of the safety controller, digital inputs can read a surge pulse as described in EN 61000-4-5 as a brief high level. The following measures ensure proper operation in environments where surges can occur:

1. Install shielded input wires
2. Activate noise blanking in the user program. A signal must be present for at least two cycles before it is evaluated.

INFORMATION

- Activating noise blanking increases the response time of the safety controller.
- The above mentioned measures are not necessary if the plant is designed in such a way that surges do not occur in the system. The design includes in particular protective measures with respect to overvoltage, lightning, grounding, and plant wiring.
- For detailed information on EMC, refer to the publication "Drive Engineering - Practical Implementation, Electromagnetic Compatibility (EMC) in Drive Engineering". The latest version of this publication is available for download from the SEW homepage (www.sew-eurodrive.com) under "Documentation".

4.4 Safety-related counters

4.4.1 General information

A counter channel can be parameterized for operation as a fast forward/backward counter with a resolution of 24 bits, or as a decoder in gray code.

When using the counter channel as fast forward/backward counter, the pulse input and the counting direction input in the application are required as signals. A reset is only performed in the user program.

The 4-bit or 8-bit encoder resolution applies to the CIO 2/4 01 encoder of F60; for F35, the encoder has a resolution of 3 or 6 bits. A reset is possible. Two independent 4-bit inputs are combined to an 8-bit input (example for F60) using solely the user program. A switching option is not provided for this purpose.

21230595 / EN – 05/2014

The encoder function monitors the changing of bit patterns at the input channels. The bit patterns at the inputs are passed directly to the user program. They are displayed in the PADT as decimal numbers that correspond to the bit patterns *(numerator[0x].value)*.

This number corresponds to the gray code bit pattern. Depending on the application, you can convert this number, for example, into the corresponding decimal value.

4.4.2 Response in the event of a fault

If the test routines detect a fault in the counter of the device or in the assembly, then they set a status bit for evaluation in the user program. The user program can additionally take account of the corresponding error code.

The MOVISAFE® HM31 safety controller activates the ERROR LED. The error code provides users with additional options to monitor the external wiring and program additional error responses in the user program.

Access to the error code	Name of the error code
From the *...Channels* tab in the detailed view of the module or unit.	*-> Error code [bytes]* in the line indicating the channel number.

4.5 Checklist for safety-related inputs

This checklist is a recommendation for the project planning, programming, and startup of safety-related inputs. It can be used as the basis for planning but also serves as the proof of having performed a careful and detailed planning.

A separate checklist must be filled in as part of project planning or startup for each safety-related input channel used in a system with the purpose of making sure that the necessary requirements are met. This is the prerequisite for ensuring that requirements have been fully accounted for in an orderly format. The checklist is also a documentation of the connection between external wiring and the user program.

The checklist *PFF_HM31_Checkliste.doc* is available as a Microsoft® Word document. You can download the checklist from the SEW website (www.sew-eurodrive.com).

21230595 / EN – 05/2014

5 Outputs of the MOVISAFE® HM31 safety controller

The MOVISAFE® HM31 safety controller comes equipped with 8 safety-related 2-pole outputs.

5.1 General information

The controller writes to the safety-related outputs once every cycle, reads back the output signals, and compares them with the specified output data. The safe state of the outputs is the value 0.

The safety-related output channels are equipped with two testable switches connected in series. This means a second independent shutdown function, which is a safety requirement, is integrated into the output channel. In the event of a fault, this integrated safety shutdown function safely de-energizes all channels of the defective output module (de-energized state).

The watchdog signal of the CPU is the second way to perform a safety shutdown: When the watchdog signal is removed, the safe state is adopted immediately.

This function is only effective for all digital outputs of the controller. The respective error code provides users with additional options for configuring error responses in the user program.

5.2 Safety of actuators

In safety-related applications, both the controller and the actuators connected to it must meet the safety requirements and the specified SIL.

5.3 Safety-related 2-pole digital outputs

5.3.1 Test routines for 2-pole digital outputs

The units are tested automatically during operation. Main test functions:

- Reading back the output signal of the switching amplifier. The diodes used prevent signals from being fed back.
- Checking the integrated (redundant) safety shutdown.
- A shutdown test of the outputs is carried out within Central European Time for a maximum of 200 µs. The minimum time between two tests is ≥ 20 seconds.

The system monitors its operating voltage and de-energizes all outputs at a low voltage of less than < 13 V.

21230595 / EN – 05/2014

5.3.2 Response in the event of an error

If a faulty signal is detected, the safety controller sets the affected output to a safe, de-energized state using the safety switches. A module fault of the safety controller causes all the outputs to be disabled. The MOVISAFE® HM31 safety controller additionally indicates both error types via the ERROR LED.

DO x.x_P outputs

If a faulty signal is detected, the safety controller sets the affected output to a safe, de-energized state using the safety switches. A safety controller fault causes all the outputs to be disabled. The MOVISAFE® HM31 safety controller additionally indicates both faults via the ERROR LED.

5.3.3 Behavior in the event of external short circuit or overload

The controller can still be tested in the event of a short circuit of the output to 0V24 or overload. Shutdown via the safety controller is not necessary.

The total current consumption of the safety controller is monitored. Once the threshold is exceeded, the safety controller sets all channels to a safe state.

In this state, the safety controller cyclically checks the outputs every few seconds to determine whether the overload is still present. In normal state, the safety controller switches on the outputs again.

5.4 Polled outputs (DO channels of the DI-26 module)

The system comes equipped with 4 non-safety related, current-limited digital outputs (24 V).

The outputs are not electrically isolated from the supply unit. The shunt current monitoring function (line control) of the 24 V outputs can be used to detect line break and open circuit detection. For this purpose, the individual polled outputs are briefly de-energized and the signals are read on the associated digital inputs. Different polled outputs must be used for shunt current monitoring.

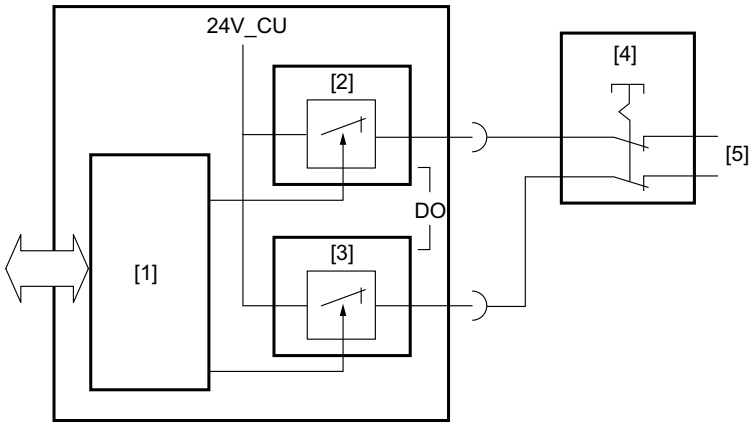
The following parameters can be set for the polled outputs (together with the digital inputs) in SILworX®:

- Assignment between polled output and digital input
- Waiting period (400 µs minimum) between shutting down the polled output and reading the input, can be adjusted using the parameter *DI cycle delay [µs]*.

  The wait time prolongs the cycle time by the set value.

21230595 / EN – 05/2014

The following figure shows the principle of line monitoring:



9007204202753163

[1] Connection to I/O bus

[2] Channel 1

[3] Channel 2

[4] Emergency stop switch

[5] Interface to the digital inputs

INFORMATION

Observe the following points during project planning:

- If the controller polls DO02, then also DO01 is polled.
- If the controller polls DO04, then also DO03, DO02 and DO01 are polled.

⚠ WARNING

Loss of safety category (performance level) due to incorrect control.

Severe or fatal injuries

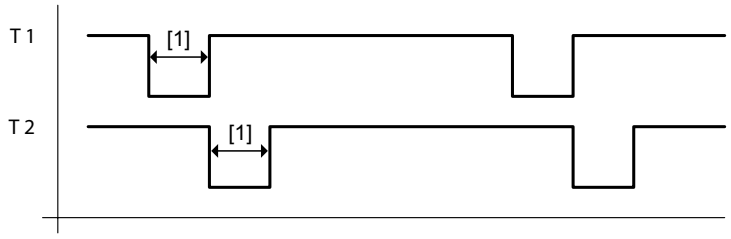
- Polled outputs must not be used as safety-related outputs, for example for controlling safety-related actuators.

You find the specification of the polled outputs in the operating instructions in chapter "Technical Data".

21230595 / EN – 05/2014

5.4.1 Polled output

The controller polls the digital outputs in order to recognize line faults and line breaks in the cables connecting the digital inputs. For this purpose, set the parameters for the system variable *Value [BOOL]* in SILworX®. The variables must start with channel 1 and be placed in consecutive order (see system variable in system manual).



4784626827

[1] Configurator 400 – 2000 µs

6 Software for the MOVISAFE® HM31 safety controller

The software of the safety controller comprises the following parts:

- Operating system
- User program
- Programming tool according to IEC 61131-3

The operating system is loaded into the central part of the controller (CPU) and must be used in the current version certified by TÜV (German Technical Inspection Association) for safety-related applications.

The programming tool is used to create the user program with the system-specific functions to be performed by the automation device. The programming tool is also used to configure and operate the operating system functions.

The code generator of the programming tool compiles the user program into machine code. The programming tool transfers this machine code to the flash EPROMs of the automation devices via Ethernet interface.

6.1 Safety-related aspects of the operating system

Each approved operating system is identified by its designation. The version number and CRC signature are indicated to help distinguish the systems from one another. The valid operating system versions and associated signatures (CRCs), which are approved by TÜV for use in safety-related automation devices, are subject to a revision control and are documented in a list generated together with TÜV.

The current operating version can be read using the programming tool. The user has to verify this (see chapter "Checklist for creating a user program").

6.2 Operation and functions of the operating system

The operating system executes the user program cyclically. It basically performs the following functions:

- Read input data
- Process logic function programmed in accordance with IEC 61131-3
- Write output data

The following main functions are also performed:

- Comprehensive self tests
- Tests of inputs and outputs during operation
- Data transmission
- Diagnostics

6.3 Safety-related aspects of programming

6.3.1 Safety concept of the programming tool

Safety concept of the SILworX® programming tool:

21230595 / EN – 05/2014

- When installing the programming tool, a CRC checksum ensures the integrity of the program package from the manufacturer to the user.
- The programming tool performs plausibility checks to reduce the likelihood of incorrectly entered data.
- Compiling the program twice and comparing the generated CRC checksums ensures the detection of corrupt data in the application resulting from temporary malfunctions of the PC in use.

Compiling the program twice and comparing the results:

1. Start compilation.

   After successful compilation, the programming tool displays a CRC checksum.

2. Restart compilation.

   After successful compilation, the programming tool displays a CRC checksum.

If both CRC checksums are identical, the data have not been corrupted during compilation.

When starting up a safety-related controller for the first time, perform a comprehensive function test to verify the safety of the entire system.

Function test of the controller

3. Verify that the tasks to be performed by the controller were properly implemented using the data and signal flows.
4. Perform a comprehensive function test of the logic by trial (see "Testing the configuration and the user program).

The controller and the user program are sufficiently tested.

If a user program is modified, only the program sections affected by the change have to be tested.

The safe revision comparator of SILworX® can be used to determine and display all changes made since the previous version.

21230595 / EN – 05/2014

6.3.2 Checking the configuration and the user program

To verify that the generated user program performs the specific safety function, suitable test cases have to be created that cover the specification.

It is usually sufficient to test each loop independently (consisting of input, the most important connections from perspective of the user, and output). The programming tool and the measures defined in this safety manual make it sufficiently improbable that a code, which was properly generated semantically and syntactically, still contains undetected systematic faults resulting from the code generation process.

Suitable test cases also have to be generated for the numerical evaluation of formulas. Suitable tests are equivalence class tests. This are tests within defined value ranges, at the limits of or within invalid value ranges. The test cases have to be selected in such a way that the program logic can be proven to be correct. The required number of test cases depends on the program logic used and must include critical value pairs.

An active simulation with data sources is the only way to prove that sensors and actuators in the system (also those connected to the system via remote I/Os) are wired properly. This is also the only way to verify the system configuration.

This procedure applies to creating a user program for the first time and to modifying it.

6.3.3 Archiving a project

SEW-EURODRIVE recommends to archive the project every time the program is loaded to the controller. This applies to downloading and reloading.

Creating a project archive:

1. Print out the user program to compare the logic with the specifications.
2. Compile the user program to generate the configuration CRC of the CPU.
3. Write down the version of the configuration CRC of the CPU.
4. Create a project archive with the user program name, the configuration CRCs of the CPUs, and the date and store it on a storage medium. This recommendation does not replace the user's internal documentation requirements.

The project archive was successfully completed.

SILworX® creates a project in a project file. The project file can be saved on a storage medium (such as USB stick).

6.3.4 Option for identifying the program and the configuration

User programs are identified unambiguously by the configuration CRC of the project. The configuration CRC of the project can be compared with the configuration CRC of the loaded project.

To ensure that the saved project file remains unchanged, compile the corresponding resource and compare the configuration CRC with the CRC of the loaded configuration. The CRC can be displayed with SILworX®.

21230595 / EN – 05/2014

6.4 Parameters of the resource

⚠ WARNING

Faulty configuration.

Severe or fatal injuries.

- System ID
- Safety time
- Watchdog time
- Main enable
- Autostart
- Start allowed
- Loading allowed
- Reload allowed
- Global forcing allowed

The following parameters are defined in the programming tool for the operations permitted in the safety-related operation of the automation device and are referred to as safety-related parameters.

Parameters that might be defined during safety-related operation are not bound to any specific requirement class but have to be agreed upon with the responsible test authority for each separate implementation of the controller.

A distinction is made between system parameters of the resource and system parameters of the hardware.

6.4.1 System parameters of the resource

These parameters define the behavior of the controller during operation. They are set in SILworX.

Parameter/switch	Description	Default	Setting for safe operation
Name	Name of the resource		Any
System ID [SRS]	System ID of the resource 1 – 65 535 The system ID must have another value than the default value, else the project cannot be executed.	60 000	Unique value within the network of controllers that may be connected to each other.
Safety time [ms]	Safety time in milliseconds. 20 – 22 500 ms	600 ms	Application-specific
Watchdog time [ms]	Watchdog time in milliseconds. 8 – 5000 ms	200 ms for controllers	Application-specific

21230595 / EN – 05/2014

Parameter/switch	Description	Default	Setting for safe operation
Main enable	**ON:** The following switches/ parameters can be changed during ongoing operation (= RUN) using the PADT: • System ID • Watchdog time of the resource • Safety time • Target cycle time • Target cycle time mode • Autostart • Global forcing allowed • Global force timeout response • Loading allowed • Reload allowed • Start allowed **OFF:** The parameters cannot be changed during operation. **Note:** *Main enable* can only be set to ON when the PES is stopped.	ON	OFF recommended
Autostart	**ON:** The user program starts automatically when the processor system is connected to the supply voltage. **OFF:** The user program does not start automatically when connecting the system to the supply voltage.	OFF	Application-specific
Start allowed	**ON:** Cold start or warm start using the PADT is permitted in RUN or STOP condition. **OFF:** Start not allowed.	ON	Application-specific

21230595 / EN – 05/2014

Parameter/switch	Description	Default	Setting for safe operation
Loading allowed	**ON:** Downloading the user program is permitted. **OFF:** Downloading the user program is not permitted.	ON	Application-specific
Reload allowed	**ON:** Reloading the user program is permitted. **OFF:** Reloading the user program is not permitted. An ongoing reload process is not aborted when switching to OFF.	ON	-
Global forcing allowed	**ON:** Global forcing permitted for this resource. **OFF:** Global forcing not permitted for this resource.	ON	Application-specific
Global force timeout response	Specifies how the resource behaves when the timeout of global forcing has expired: • Stop forcing • Stopping the resource	End forcing	Application-specific
Max. com. time slice ASYNC [ms]	Highest value in ms for the time slice used for communication during a resource cycle, 2 – 5000 ms	60 ms	Application-specific
Max. duration of configuration connections [ms]	Defines how much time is available within a CPU cycle for process data communication, 6 – 5 000 ms	6 ms	
Target cycle time [ms]	Required or maximum cycle time, see *Target cycle time mode*, 0 – 7 500 ms. The maximum target cycle time must not exceed the defined watchdog time (6 ms), else it is rejected by the PES.	0 ms	-

21230595 / EN – 05/2014

Parameter/switch	Description	Default	Setting for safe operation
Multitasking mode	**Mode 1:** The duration of a CPU cycle depends on the execution time required by all user programs. **Mode 2:** Execution time not required by user programs with a lower priority are made available to user programs with a higher priority by the processor. Operating mode for high availability. **Mode 3:** The processor waits for execution time not required by user programs and in this way extends the cycle.	Mode 1	
Target cycle time mode	Using the *Target cycle time [ms]*. **Fixed:** The PES adheres to the target cycle time and extends the cycle, if necessary. This is not the case when the processing time of the user programs exceeds the target cycle time. **Fixed tolerant:** Similar to fixed, but the target cycle time is ignored during the first reload activation cycle. **Dynamic/liberal:** The PES adheres to the *target cycle time* but executes the cycle as quickly as possible. In the first activation cycle of the reload, the *target cycle time* is not relevant.	Fixed	-
Maximum configuration version	The configuration files and code generation are structured as in the mentioned SILworX® version (except for newer functions). This setting ensures compatibility with later versions.	SILworX V4	-

21230595 / EN – 05/2014

Parameter/switch	Description	Default	Setting for safe operation
Maximum system bus latency [µs]	May not be used for the MOVISAFE® HM31 safety controller.	0 ms	-
safeethernet CRC	**Current version:** The CRC for safeethernet is created with the current algorithm.	Current version	Application-specific

6.4.2 System variables of the hardware

These variables are used to change the behavior of the controller during operation if specific states occur. The variables can be set in the detailed view of the hardware in the Hardware Editor of SILworX®.

Parameter/switch	Function	Default	Setting for safe operation
Force deactivation	Is used to prevent forcing and stop it immediately.	FALSE	Application-specific
Spare 0 – spare 16	No function.	-	-
EMERGENCY STOP 1 – EMERGENCY STOP 4	Emergency stop switch to shut down the controller in the event of error detected by the user program.	FALSE	Application-specific
Read only in RUN	After starting the controller, no operating action (stop, start, download) is permitted in SILworX®. Exceptions: Forcing and reload.	FALSE	Application-specific
Reload deactivation	Prevent loading the controller via reload.	FALSE	Application-specific
User LED 1 – 2	Activates the corresponding LED, if present.	FALSE	Application-specific

Global variables can be assigned to these system variables. The value of a global variable is modified using a physical input or the user program logic.

Example: A key switch is connected to a digital input. The digital input is assigned a global variable, which is assigned to system variable *Read only in Run*. This means the owner of a key can activate or deactivate operating actions, such as stop, start, and download.

6.5 Protection against manipulation

Together with the responsible test authority, the user has to define the measures to be taken to protect the system against manipulation.

Protective mechanisms are integrated in PES and programming tool to prevent accidental or unauthorized modifications of the safety system:

- Changing the user program or the configuration will create a new CRC.

21230595 / EN – 05/2014

- The operating options depend on the user login for the PES.
- The programming tool prompts the user to enter a password to establish a connection to the PES.
- During RUN operation, no connection is required between PADT and PES and can be interrupted.

Adhere to the requirements about manipulation specified in the safety and application standards. The operator is responsible for authorizing personnel and for implementing the required protective measures.

INFORMATION

Only authorized personnel may be granted access to the safety controller.

Take the following measures to protect the controller from unauthorized modifications:

- Change the default settings for user name and password.
- Users must keep their passwords secret.
- Once startup is complete, disconnect the PADT from the controller and only connect it again if changes have to be made.

Access to data of the PES is only possible if the PADT used has the programming tool and the user project runs with the current version (archive maintenance).

A connection between PADT and PES is only needed for downloading the user program or for reading variables. The PADT is not required for normal operation. Disconnecting PADT and PES during normal operation protects against unauthorized access.

21230595 / EN – 05/2014

7 Safety-related aspects of the user program

General procedure for programming the MOVISAFE® HM31 safety controller for safety-related applications:

- Specify the control function
- Write the user program
- Compile the user program with the C-code generator
- Compile the user program a second time to compare the results (CRC)
- The program has been successfully created and can run
- Verify and validate the user program

The PES can now commence its safety-related operation.

7.1 Conditions for safety-related use

(For specifications, rules, and explanations regarding safety conditions, refer to chapter "Safety conditions").

Enter the user program with the permitted SILworX® programming tool.

For information about approved operating systems for personal computers, refer to the release notes of the programming tool.

The SILworX® programming tool includes:

- Input (Function Block Editor), monitoring and documentation
- Variables with symbolic names and data type (BOOLEAN, UINT, etc.)
- Assignment of controllers
- Code generator (for compiling the user program into machine code)
- Hardware configuration
- Hardware configuration

7.1.1 Programming basics

The tasks to be performed by the controller should be described in a specification or performance specification. This documentation serves as the basis for verifying its proper implementation in the user program. The format of the specification depends on the task to be performed. These may include:

- Combinational logic
  - Cause/effect diagram
  - Logic of the connection with functions and function blocks
  - Function blocks with specified characteristics
- Sequential controllers (sequence control systems)
  - Written description of the steps and their enabling conditions as well as of the actuators to be controlled
  - Flow charts
  - Matrix or table form of the step enabling conditions and the actuators to be controlled
  - Definitions of constraints, such as operating modes, EMERGENCY STOP, etc.

21230595 / EN – 05/2014

The I/O concept of the system must include an analysis of the field circuits, i.e. of the type of sensors and actuators:

- Sensors (digital or analog)
  - Signal during normal operation (normally energized principle with digital sensors, life zero with analog sensors)
  - Signal in the event of an error
  - Definition of required safety-related redundancies (1oo2, 2oo3)
  - Discrepancy monitoring and response
- Actuators
  - Position and activation during normal operation
  - Safe response/position in the event of shutdown or power failure

Objectives for programming the user program:

- Easy to understand
- Easy to follow
- Easy to modify
- Easy to test

7.1.2 Functions of the user program

Programming is not subject to restrictions by the hardware. The functions of the user program can be programmed freely.

- Only elements complying with IEC 61131-3 and their functional requirements are permitted within the logic.
- The physical inputs and outputs usually operate according to the normally energized principle. This means their safe state is 0. You have to take this into account during programming.
- The user program contains meaningful logic and/or arithmetic functions irrespective of the normally energized principle of the physical inputs and outputs.
- The program logic should be clear and easy to understand. It should be documented to facilitate debugging. This includes the use of functional diagrams.
- Any kind of negation is permitted.
- Error signals from inputs/outputs or from logic blocks have to be evaluated.

It is important that functions are encapsulated in user-defined function blocks and functions consisting of standard functions. Doing so helps ensure that a program can be clearly structured in modules (functions, function blocks). Each module can be regarded individually. The individual modules can be grouped to form a larger single module or a program resulting in a comprehensive, complex function.

21230595 / EN – 05/2014

7.1.3 Variable declaration

A variable is a placeholder for a value in the program logic. The variable name (max. 31 characters) is used to symbolically address the storage location with the stored value. A variable is created in the variable declaration of the program or function block.

Using symbolic names instead of the physical address has the following two advantages:

- The system designations of inputs and outputs can be used in the user program.
- Changes made to the assignment of variables to input and output channels do not affect the user program.

The initial value of variables that are not initialized is 0 or FALSE after a cold or warm start. This does not apply if the variables have RETAIN attributes.

Variables with invalid source, for instance caused by a hardware error in a physical input, adopt the configured initial value.

7.1.4 Acceptance by approving authorities

SEW-EURODRIVE recommends that you involve the approving authority as early as possible when designing a system that is subject to approval.

7.2 Procedures

This chapter describes the typical procedure for developing user programs for MOVISAFE® HM31 safety controllers.

7.2.1 Assigning variables to inputs/outputs

The operating system automatically performs the test routines required for safety-related inputs and outputs.

Assigning a variable to an I/O channel:

1. Define a global variable of a suitable type.
2. Enter a suitable initial value during definition.
3. Assign the global variable to the channel value of the I/O channel.
4. In the user program, evaluate the error code → *Error code [byte]* and program a safety-related response.

The global variable is assigned to an input/output channel.

7.2.2 Locking and unlocking the controller

Locking the controller means all functions are locked and users cannot access them during operation. The purpose is to protect the user program from being manipulated. The scope of locking depends on the safety requirement for using the PES but can also be coordinated with the test authority responsible for final system acceptance.

Unlocking the controller means previously locked functions are enabled, for instance to perform work on the controller.

21230595 / EN – 05/2014

Three system variables are used for locking:

Variable	Function
Read only in run	ON: Starting, stopping, downloading the controller is locked. OFF: Starting, stopping, downloading the controller is possible.
Deactivate reloading	ON: Reload is locked. OFF: Reload is possible.
Deactivate forcing	ON: Forcing is disabled. OFF: Forcing is possible.

When all three system variables are set to ON, the controller can no longer be accessed. In this case, the only way to have the controller adopt STOP/VALID CONFIGURATION state is to restart it. It is then possible to reload a user program.

Example of how to use these system variables:

Making a controller lockable

1. Define a global variable of the type BOOLEAN and set its initial value to OFF.
2. Assign global variables to the three system variables *Read only in run*, *Reload deactivation* and *Force deactivation*.
3. Assign the global variable to the channel value of a digital input.
4. Connect a key switch to the digital input.
5. Compile the program, load it to the controller, and start it.

The owner of a matching key can now lock and unlock the controller. The controller is unlocked when a fault occurs in the corresponding digital input device or input module.

7.2.3 Generating the code

The code is generated after having successfully entered the user program and the I/O assignment of the controller. The code generator generates the configuration CRC. This CRC is a signature for the entire configuration of the CPU, inputs/outputs and communication. It is issued as a 32-bit, hexadecimal code. The signature comprises all configurable or modifiable elements, such as the logic, variable, or switch settings.

Generate the code a second time to rule out any influence of the non-safe PC on the process. The resulting two configuration CRCs must be identical.

Generating the code for safety-related operation

1. Start the code generator to generate the code with the configuration CRC.

   Executable code 1 with CRC 1.
2. Start the code generator again to generate the code with the configuration CRC.

   Executable code 2 with CRC 2.
3. Compare CRC 1 with CRC 2.

   Both CRCs are identical.

The generated code can be used for safety-related operation and for the system's certification through test authorities.

21230595 / EN – 05/2014

7.2.4 Loading and starting the user program

A PES in the MOVISAFE® HM31 controller can only be downloaded if it was set to STOP before.

Number of user programs per controller
1 – 32

The system monitors that the user program is loaded completely. Next, you can start the user program. The routine is then processed cyclically.

INFORMATION

SEW-EURODRIVE recommends that you make a backup of the project data (for example on a removable medium) every time you have loaded a user program to the controller. The reason is to ensure that the project data matching the configuration loaded to the controller will be available in the event of a PADT failure.

SEW-EURODRIVE recommends to make backups on a regular basis irrespective of whether a program is loaded or not.

7.2.5 Optional functions – multitasking and reload

INFORMATION

In MOVISAFE® HM31, the optional functions can be used for testing purposes without activation for 5000 operating hours. The “ERROR” system LED lights up red continuously when functions are used that were not enabled.

After the 5000 operating hours have elapsed, the controller no longer starts.

- Therefore order the license for enabling the required functions in time.

- **Multitasking:**

  Multitasking refers to the capability of the safety controller to process up to 32 user programs within the processor module.

  In this way, sub-functions of a project can be separated from one another. Individual user programs can be started, stopped and reloaded independently of each other.

NOTICE

Reciprocal influence of user programs.

Using the same global variable in several user programs might result in reciprocal influence of the user programs and have various consequences.

- Carefully plan the use of same global variables in several user programs.
- Use cross references in SILworX® to check the use of global data. Global data may only be assigned values by one entity, either in a user program, by safety-related inputs, or through safety-related communication protocols.

21230595 / EN – 05/2014

NOTICE

Reciprocal influence of user programs

Using the same global variable in several user programs might result in reciprocal influence of the user programs and have various consequences.

- Carefully plan the use of same global variables in several user programs.
- Use cross references in SILworX® to check the use of global data. Global data may only be assigned values by one entity, either in a user program, by safety-related inputs, or through safety-related communication protocols.

- **Reload:**

  If changes were made to the user programs, these changes can be transferred to the PES during ongoing operation. The operating system verifies and activates the modified user program, which then takes over the control function.

INFORMATION

Adhere to the following information when reloading step chains:

The reload information for step chains does not take account of the current state of the chain. This is the reason why the step sequence might be changed accordingly and set to an undefined state when performing a reload. The user is responsible for this action.

- Deleting the active step. As a result, no step of the step chain is in active state.
- Renaming the initial step while another step is active. As a result, the step chain has two active steps.

INFORMATION

Adhere to the following information when reloading actions:

During reload, actions are loaded with their entire data. Analyze the consequences carefully before performing a reload.

- Deleting a timer action qualifier due to the reload causes the timer to expire immediately. As a result, the Q output can change to TRUE depending on the other settings.
- Deleting the action qualifier for a set element (such as the S action qualifier) causes the elements to remain set.
- Deleting a P0 action qualifier that is set to TRUE will initiate the trigger.

7.2.6 Forcing

Forcing means that the present value of a variable is replaced with a force value. A variable can obtain its present value from a physical input, communication, or logic operation. When the variable is forced, its value no longer depends on the process but is specified by the user.

21230595 / EN – 05/2014

⚠ WARNING

Using forced values can disrupt safety-related operation.

Severe or fatal injuries.

- Forced values can lead to incorrect output values.
- Forcing extends the cycle time. The watchdog time might be exceeded as a result.

For more information, refer to the system manual.

7.2.7 Changing system parameters online

Some system parameters/switches can be changed online (during operation) in the controller. For example, to temporarily increase the watchdog time to be able to perform a restart.

Parameters that can be changed online:

- System ID
- Watchdog time of the resource
- Safety time
- Target cycle time
- Target cycle time mode
- Main enable
- Autostart
- Start allowed
- Loading allowed
- Reload allowed
- Global forcing allowed
- Global force timeout response

Before setting the parameters using an online command, make sure that the changed parameter setting will not lead to a hazardous state. If necessary, take organizational and/or technical measures to prevent any damage.

Main enable lets you change the remaining parameters. *Main enable* can only be set to TRUE in STOP condition.

The values of the *safety time* and *watchdog time* must be checked and compared with the safety time required by the application and with the actual cycle time. These values cannot be verified by the PES. Another way of changing system parameters during operation is to perform a reload.

7.2.8 Program documentation for safety-related applications

The programming tool lets you automatically print the documentation of a project. The most important documents are:

- Interface declaration
- Variable list
- Logic
- Description of data types

21230595 / EN – 05/2014

- Configurations for system, modules and system parameters
- Network configuration
- Cross reference list for variables
- Code generator information

The documentation is required for the acceptance test of a system subject to approval by a test authority (such as TÜV). The acceptance test only refers to the user function, not to the safety controller that has already been prototype examined.

7.2.9 Acceptance by approving authorities

SEW-EURODRIVE recommends that you involve the approving authority as early as possible when designing a system that is subject to approval. The acceptance test only refers to the user function, not to the safety controller that has already been prototype examined.

21230595 / EN – 05/2014

8 Configuring the communication

In addition to physical input and output variables, variables can also be exchanged with another system via data connection. For this purpose, the variables of the respective resource are declared in the Protocol Editor of the programming tool. Data can be exchanged in read-only or read/write mode.

8.1 Standard protocols

Many communication protocols only allow for non-safety related data transmission. These protocols can be used for the non-safety related parts of an automation task.

⚠ WARNING

Using unsafe import data.

Severe or fatal injuries.

The following standard protocols are available for the safety controller:

- SNTP server/client
- Modbus TCP master

8.2 Safety-related protocol (safeethernet)

Safety-related communication via safe**ethernet** is certified up to SIL 3. The safe**ethernet** Editor is used to configure how safety-related communication is monitored.

INFORMATION

Your find additional information in the "MOVISAFE® HM31" system manual in the "safeethernet" chapter.

The following condition applies for calculating the safe**ethernet** parameters *Receive Timeout* and *Response Time*:

The communication time slice must be large enough to process all safe**ethernet** connections during one CPU cycle.

For safety-related functions which are implemented via safe**ethernet,** only the *Use initial data* setting may be used.

INFORMATION

An unintentional change to safe state is possible.

ReceiveTMO is a safety-related parameter.

If all values are to be transferred, the value of a variable must either be present for longer than *ReceiveTMO* or must be monitored using loop-back.

ReceiveTMO is the monitoring time of controller 1 during which a valid response must be received from controller 2.

21230595 / EN – 05/2014

8.2.1 Receive timeout

ReceiveTMO is the monitoring time in milliseconds (ms) during which a correct answer must be received from the communication partner.

If the communication partner does not receive a valid response during the *ReceiveTMO*, safety-related communication is terminated. The input variables of this safe**ethernet** connection behave according to the setting made for *Freeze data on lost connection [ms]*.

For safety-related functions which are implemented via safe**ethernet,** only the *Use initial data* setting may be used.

Because *ReceiveTMO* is a safety-relevant component of the worst case response time T_R (for maximum response time, see safety manual, chapter 8.2.4), the *ReceiveTMO* must be calculated as described below and entered in the safe**ethernet** Editor:

ReceiveTMO ≥ 4 × delay + 5 × max. cycle time

Condition: The communication time slice must be large enough to process all safe**ethernet** connections during one CPU cycle.

Delay: Delay on the transmission path, for instance due to switch or satellite

Max. cycle time: Maximum cycle time of both controllers

INFORMATION

- A desired error tolerance of the communication can be achieved by increasing *Receive TMO* provided this is permitted for the application process in terms of time.
- The maximum value permitted for *ReceiveTMO* depends on the application process and is set in the safe**ethernet** Editor together with the maximum expected *response time* and the profile.

8.2.2 Response time

The *ResponseTime* is the time in milliseconds (ms) that elapses until the sender of a message receives an acknowledgement from the recipient.

To set parameters using a safe**ethernet** profile, you have to specify an expected *ResponseTime* based on the physical conditions of the transmission path.

The specified *ResponseTime* affects the configuration of all parameters for the safe**ethernet** connection. These parameters must be calculated as follows:

ResponseTime ≤ ReceiveTMO / n

n = 2, 3, 4, 5, 6, 7, 8.....

The ratio of *ReceiveTMO* to *ResponseTime* affects the capability to tolerate faults, for instance if packets are lost (resending lost data packets) or there are delays along the transmission path.

In a network where packets could be lost, the following condition must be met:

Min. response time ≤ receiveTMO / 2 ≥ 2 × delay + 2.5 × max. cycle time

If this condition is met, the loss of at least one data packet can be compensated without interrupting the safeethernet connection.

21230595 / EN – 05/2014

INFORMATION

- If this condition has not been met, the availability of a safeethernet connection can only be guaranteed in a network free of collisions and interference. However, this does not mean that the processor module has a safety problem.
- Make sure that the communication system complies with the set *ResponseTime*. In cases where this cannot always be guaranteed, a corresponding system variable for the connection is available to monitor the *ResponseTime*. If the *ResponseTime* measured is exceeded by half of the *ReceiveTMO* more often than in exceptional cases, then the *ResponseTime* set must be increased. The *Receive Timeout* must be adjusted to the newly set *ResponseTime*.
- In the examples below, the formulas for calculating the maximum response time for a connection with the safety controller only apply if the safety time for these has been set to = 2 × watchdog time.

8.2.3 Maximum cycle time of the safety controller

SEW-EURODRIVE recommends the following method for determining the maximum cycle time of a MOVISAFE® HM31 safety controller.

Determining the maximum cycle time of the MOVISAFE® HM31 safety controller:

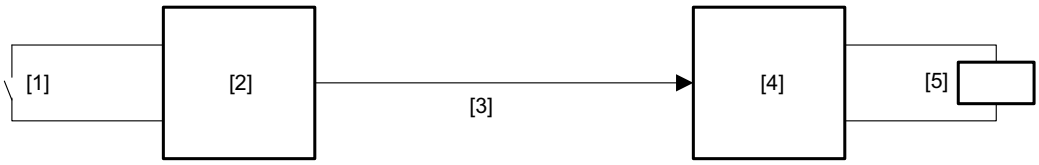
1. Operate the system under maximum load. All communications connections must be operating via safe**ethernet** and via standard protocols. Frequently read the cycle time from the control panel and note the maximum cycle time.
2. Repeat step 1 for the communication partner (second safety controller).
3. The required maximum cycle time is the greater of the two determined maximum cycle times.

The maximum cycle time has now been determined and is used in the calculations below.

21230595 / EN – 05/2014

8.2.4 Calculating the maximum response time

The maximum response time T_R (worst case) from the change of an input in PES 1 until the response of the output in PES 2 can be calculated as follows:



4784751883

[1] Input

[2] Safety controller PES 1

[3] Safety-related protocol

[4] Safety controller PES 2

[5] Output

$T_R = t_1 + t_2 + t_3$

T_R Worst case reaction time

t_1 2 × watchdog time of safety controller 1

t_2 ReceiveTMO

t_3 2 × watchdog time of safety controller 2

The maximum response time depends on the process and has to be agreed with the test authority responsible for final acceptance.

8.2.5 Terms

Term	Description
ReceiveTMO	Monitoring time in controller 1 during which a valid response must be received from controller 2. When the time has elapsed, safety-related communication is terminated.
Production rate	Minimum interval between two data transmissions.
Watchdog time	Maximum permitted duration of a RUN cycle of a controller.
Worst case response time	Maximum response time for transmitting the state change of a physical input of controller 1 until the change of a physical output of controller 2.

21230595 / EN – 05/2014

8.2.6 Assigning safeethernet addresses

Observe the following information when assigning network addresses (IP addresses) for safeethernet:

- The addresses must be unique in the network used.
- When connecting safeethernet to another network (company-internal LAN, etc.), make sure no disturbances can occur. Potential sources of disturbance:
  - Data traffic
  - Coupling with other networks (such as Internet)

In these cases, take suitable measures to eliminate such disturbances using Ethernet switches, firewall, and similar.

21230595 / EN – 05/2014

9 Appendix

9.1 Glossary

Term	Description
DC 24 V	The safety controller has the following DC 24 V input voltage potential: 24V_CU: DC 24 V input – controller 24V_L: DC 24 V input – load 24V_S: DC 24 V input – sensor supply Reference potential 0V24
ARP	Address resolution protocol (network protocol for assigning network addresses to hardware addresses)
BS	Operating system
BL	Boot loader
BWS	Contactless protection device
COM	Communication module
COE	CANopen software module
CRC	Cyclic redundancy check (checksum)
CUT	Com user task
DCS	Distributed control system (process control system)
DI	Digital input (binary input)
DO	Digital output (binary output)
EMC	Electromagnetic compatibility
EN	European standard
ESD	Electrostatic discharge
FB	Fieldbus interface of the controller
FBD	Function block language
FIFO	First-in first-out (data memory)
FTA	Field termination assembly
FTT	Fault tolerance time
ICMP	Internet control message protocol (network protocol for status and error messages)
IEC	International Electrotechnical Commission
IF	InterFace
MAC address	Media access control address (hardware address of a network connection)

21230595 / EN – 05/2014

Term	Description
PADT	Programming and debugging tool (in accordance with IEC 61131-3), PC with SILworX®
NVRAM	Non volatile random access memory
PE	Protective earth
PELV	Protective extra low voltage
PES	Programmable electronic system
POU	Program organizational units (in accordance with IEC 61131-1)
PFD	Probability of failure on demand
PFF-HM31A	Safety controller
PFH	Probability of failure per hour
R	Read (system variable provides a value, for example to the user program)
Non-reactive	Supposed two input circuits are connected to the same source (e.g. a transmitter). In this case, an input circuit is referred to as non-reactive if it does not distort the signals of the other input circuit
R/W	Read/Write (column title for system variable type)
SB	System bus (module)
SELV	Safety extra low voltage
SFF	Safe failure fraction
SIL	Safety integrity level (according to IEC 61508)
SILworX®	Programming tool for PFF-HM31A safety controller
SNTP	Simple network time protocol (RFC 1769)
S.R.S	System.Rack.Slot (addressing of a module)
SW	Software
S&R	Send and Receive; in connection with TCP protocols
TMO	Timeout
W	Write (system variable is provided with a value, for example from the user program)
Watchdog (WD)	Time monitoring for modules or programs. A fault stop will occur in the module or program if the watchdog time is exceeded.
WDT	Watchdog time

21230595 / EN – 05/2014

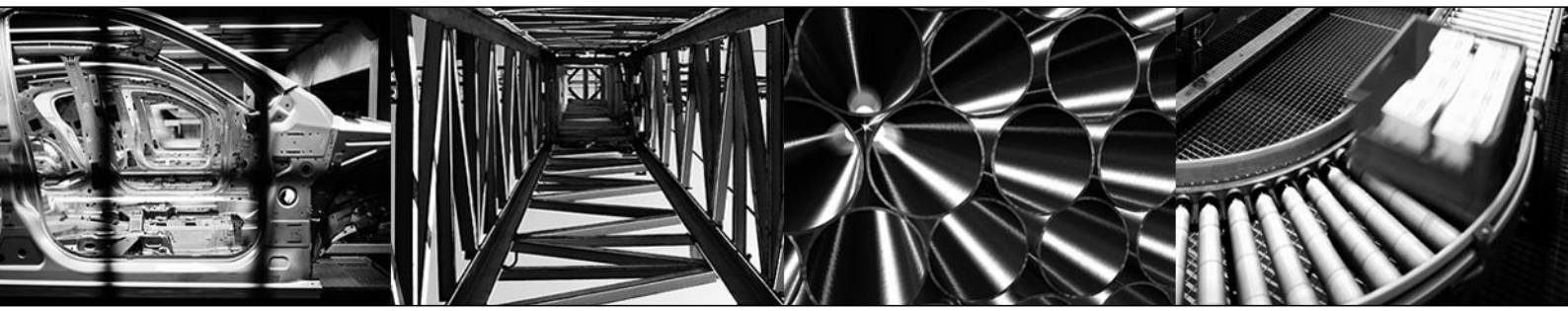
Index

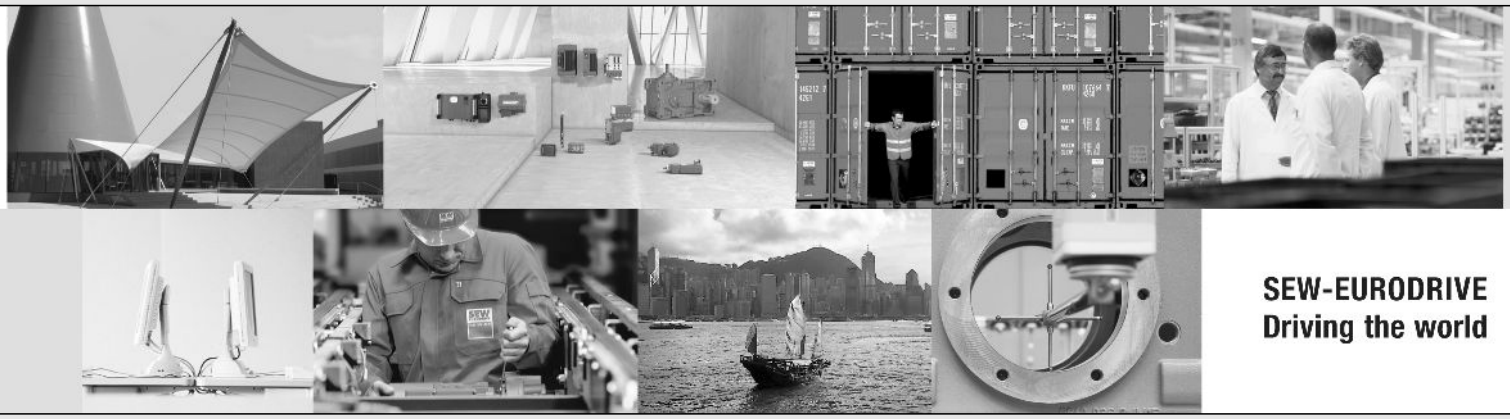
21230595 / EN – 05/14

T

W

21230595 / EN – 05/14





SEW-EURODRIVE
Driving the world

SEW-EURODRIVE GmbH & Co KG
P.O. Box 3023
76642 BRUCHSAL
GERMANY
Phone +49 7251 75-0
Fax +49 7251-1970
sew@sew-eurodrive.com
➞ **www.sew-eurodrive.com**