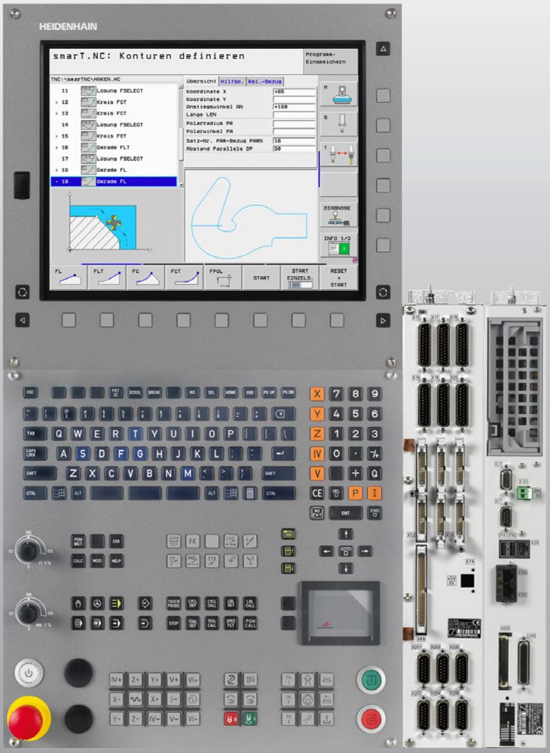
HEIDENHAIN

Functional Safety



Technical Manual

Functional Safety (FS)

NC Software
606 420-01 SP 05
606 421-01 SP 05

July 2011

Subject

4 Realization and Safety Functions

5 Safety-Related MPs and Signals

8 SPLC – Safety-Related PLC

1 Update Information

1.1 General Information

Update Information for the Functional Safety Technical Manual appears at irregular intervals, often as part of a new software version. This is preliminary information in PDF format, containing brief descriptions of new software functions as well as new hardware components. After the Update Information has been published, the new items are included in the Functional Safety Technical Manual.

The Technical Manual and each Update Information are saved in the HEIDENHAIN FileBase on the Internet, where registered users can access them at http://portal.heidenhain.de.

Registered users of the HEIDENHAIN FileBase on the Internet receive an e-mail notification when a new Update Information appears.

This version of the Technical Manual includes all Update Information notifications up to and including number 01, meaning that the contents of this Functional Safety (FS) Technical Manual correspond to the scope of functions of software version 606 42x-01 with Service Pack 05.

1 Update Information No. 01 – Functional Safety

1.1 Overview

1.1.1 Released service packs

The following service packs were released for **606 42x-01**:

Service pack 01:	August 2010
Service pack 02:	December 2010
Service pack 03:	February 2011
Service pack 04:	March 2011 (not for functional safety)
Service pack 05:	May 2011 (full version)

1.2 NC Software 606 42x-01 SP 05

1.2.1 Important notes

New test of the safe outputs:

Service pack 05 expands the safety selftest as regards the safe outputs. This new safety test for safe PL outputs is necessary for certification of the functional safety.

During the test all safe, dual-channel PL outputs are specifically switched off. This state is checked to ensure that all dual-channel outputs assume this state (= 0) and remain in it.

However, the PLD-H 04-08-00FS modules with ID 727 219-01 do not fulfill the requirements of this test yet, and must therefore be modified. Other PL modules already support this test.

If PLD modules with ID 727 219-01 are in the electrical cabinet when the new test is performed, the test is aborted with the error message "E031 error xxxxxxxx…".

Further procedure:

HEIDENHAIN started building the PLD-H 04-08-00FS modules with the appropriate modification in April 2011, and changed the variant to 02 (ID 727 219-02).

Starting immediately, please ship all machines with HSCI and functional safety only with the 02 variant of PLD-H 04-08-00FS PL modules. The modules must also be exchanged for affected machines already in the field, so that the test can be performed. Please get in touch with your contact partner at HEIDENHAIN first, in order to coordinate the exchange action in the best possible manner.

The test can be deactivated via SMP560 bit 12 = 1 until the PL modules have been exchanged. The test must be reactivated once the modules have been exchanged!

Attention

- On machines with PLD-H 04-08-00FS (ID 727 219-02) PL modules, or without PLD-H 04-08-00FS, the test must be activated with SMP560 bit 12 = 0.

dv/dt monitoring of the spindle

dv/dt monitoring of the spindle during SS1 reaction

dv/dt monitoring of the spindle is being introduced as a new safety function in service pack 05. The safety function monitors braking of the spindle during an SS1 reaction.

After an SS1 reaction has been initiated, the SKERN monitors the spindle speed to ensure that it continually decreases. Should the monitoring determine that the speed remains constant or even increases, an SS0 reaction is initiated for the spindle. SS1F is initiated for all other axes. This monitoring can be deactivated with SMP560 bit 11 for commissioning purposes. However, this monitoring is essential to the HEIDENHAIN safety strategy, and must be reactivated after commissioning.
Input for SMP560 bit 11:

0: dv/dt monitoring of the spindle active
1: dv/dt monitoring of the spindle inactive

2 Introduction

2.1 Meaning of the Symbols Used in this Manual

⚠ Danger

Failure to comply with this information could result in most serious or fatal injuries, and/or in substantial material damage.

⚠ Attention

Failure to comply with this information could result in injuries and interruptions of operation, including material damage.

➡ Note

Tips and tricks for operation as well as important information, for example about standards and regulations as well as for better understanding of the document.

2.2 Warnings

Danger

The functional safety as provided by HEIDENHAIN only handles the safety functions stated and described in this manual. Functional safety can reduce the inherent risks of machine tools. However, it is impossible to implement safety measures that ensure that nothing will ever go wrong with a machine tool.

In order for functional safety to take effect, the machine manufacturer must:

- verify the theoretical and actual setup of the machine tool, the necessary (S)PLC programs and the machine-parameter settings with a thoroughly documented acceptance test. This acceptance test must be performed by qualified personnel.
- thoroughly understand the information contained in this manual and other documentation for the control and other electronic components being used (such as inverters and motors), as well as understand and enforce the safety instructions, constraints and relevant standards.
- draw up a risk analysis, as required by the EC machinery directive.
- implement all measures deemed necessary based on the risk analysis of the machine. These measures may be implemented as a part of functional safety, or with other suitable equipment or procedures. All measures must be validated.

Danger

Many safety-related machine parameters (SMP) and the safety-related PLC program (SPLC program) are important for ensuring the safety of the machine when it is controlled by an iTNC 530 with integrated safety strategy.
Changing these safety-related machine parameters or the SPLC program can result in loss of the machine safety as specified in the applicable standards!

Safety-related machine parameters are therefore protected by a special **OEM password** that is only known to the machine manufacturer.

Changes to the safety-related machine parameters and the SPLC program may only be performed by trained personnel of the OEM. He is responsible for the safety of the machine and compliance with the applicable standards, in particular with **EN 12417**.

The HEIDENHAIN safety strategy cannot detect erroneous parameterization or programming by the OEM. The necessary level of safety can only be achieved with thorough acceptance testing of the machine.

When exchanging a power module or motor, the same type must be used, since otherwise the settings of the machine parameters could lead to different reactions by the safety functions. If an encoder is exchanged, the affected axis must be recalibrated.

Hardware components of the machine tool may only be exchanged by trained personnel.

Attention

Prior to the initial operation or shipping of a machine tool, the machine manufacturer must conduct a complete acceptance test.
All of the machine's safety functions must be tested. Furthermore, the input values of the safety-related machine parameters and the entire SPLC program must be checked for correctness.

If the SPLC program is changed subsequently, the entire acceptance test must be repeated.
If individual machine parameters are changed subsequently, a partial acceptance test is required.

Upon subsequent changes the safety functions affected by the respective change must be tested. The changes and the necessary acceptance tests may only be performed by trained personnel of the OEM.

Attention

- The machine tool is not in a safe state until after it has booted completely and the safety self-test was passed successfully!
- During start-up or the reset phase, the control is not in a safe state (e.g. installation of a service pack). Axes and spindles are without torque during this time!
- When exchanging hardware components, also use the same model. If an encoders is exchanged, then the motor affected must be referenced and tested again.
- Depending on the changes during an exchange or update of the software, either a partial or complete acceptance test becomes necessary. The following must be ensured before or during an exchange or update of the software:
  - All openings (e.g. doors) to the working space must be closed
  - Emergency stop must be activated
  - There must be no tools in the spindle
  - Vertical axes must be protected against falling
  - No persons are permitted in the danger zone
- The control must be shut down correctly before the machine is switched off via the main switch. Should this not be possible due to an error, an emergency stop is to be initiated via the man switch before removing power from the machine.

2.3 Proper Operation

The described components may only be installed and operated as described in this manual. Commissioning, maintenance, inspection and operation are only to be performed by trained personnel.

HEIDENHAIN contouring controls and their accessories are designed for integration in milling, drilling and boring machines, and machining centers.

2.4 Trained Personnel

Trained personnel in the sense of this manual means persons who are familiar with the installation, mounting, commissioning, and operation of the HEIDENHAIN components. Furthermore, electrical engineering work on the system may be carried out only by trained electrical engineering technicians or persons trained specifically for the respective application.

Basically, persons who perform work on HEIDENHAIN components must meet the following requirements:

- They must have been trained or instructed in the standards of safety engineering.
- They must have appropriate safety equipment (clothing, measuring systems).
- They should be skilled in first-aid practice.

2.5 General Information

⚠ Danger

Please note the following during initial operation of your new machines with the new HSCI hardware generation of the iTNC 530:

With the introduction of this hardware, the new functional safety (FS) is available for the first time, featuring the following properties:

- Safety category 3 (Performance Level d) in accordance with EN ISO 13849-1:
  December 2008
- SIL 2 as per DIN EN 61508
- Operating modes as per EN 12417
- Integrated SPLC for adaptation to the machine

The enhancements regarding functional safety to the NC software are fundamental new developments by HEIDENHAIN. This means that the necessary software tests have been performed only partially, and that the complete system does not yet have sufficient functional tests. This means that special care must be taken when working with the affected new machines, since faulty operation of the integrated safety functions of the software cannot be ruled out.

Please inform your colleagues and employees using these machines of these possible dangers. No persons should be within the traverse range of the axes.

⚠ Danger

- Only the iTNC 530 HSCI control with NC software 606 42x may currently be used for applications with functional safety. Other controls (e.g. the TNC 6xx NCK-based controls) and NC software versions do not yet support the use of functional safety!
- However, NC software 606 42x has not yet been generally approved for applications that use the integrated functional safety (FS) of the control. Separate approval by HEIDENHAIN is required for the use of integrated functional safety (FS) according to EN ISO 13849-1!

Every machine tool operator is exposed to certain risks.
Although protective devices (safeguards) can prevent access to dangerous points, the operator must also be able to work with the machine without this protection (e.g. if the guard door is open).
Several guidelines and regulations to minimize these risks have been developed in recent years.

Machinery Directive 2006/42/EC obligates you as a machine-tool manufacturer to perform detailed risk assessments in order to prove operator safety during the various operating phases of the machine. The combination of hazard analysis and risk evaluation leads to the determination of how much risks must be reduced by design measures or control methods in order to achieve an appropriate level of safety.

In accordance with EN 12417, the electronic controls of universal machines, milling machines, lathes and machining centers must fulfill the requirements of EN 13849-1 category 3 (previously EN 954-1) for their safety-related parts. In particular this means that the control must be designed such that an individual fault does not lead to loss of the safety function, and that any individual fault is detectable if this is possible in an acceptable manner.

According to EN ISO 12100-1/2 (Safety of Machinery), it is important for safe operation of the machine that the safety measures permit simple and continuous use of the machine and that they do not impair its correct and intended operation. If this is not the case, then this can lead to the safety measures being circumvented in order to attain the simplest possible operation of the machine.

The HEIDENHAIN safety strategy integrated in the iTNC 530 HSCI complies with Category 3 as per EN 13849-1 and SIL 2 as per IEC 61508, features safety-related operating modes in accordance with EN 12417, and assures extensive operator protection.

The basis of the HEIDENHAIN safety strategy is the dual-channel processor structure, which consists of the main computer (MC) and one or more CC drive controller modules (CC = control computing unit).
All monitoring mechanisms are designed redundantly in the control systems. Safety-related system data is subject to a mutual cyclic data comparison, see page 4–46.
Safety-related errors always lead to safe stopping of all drives through defined stop reactions.

Defined safety reactions are triggered and safe operating statuses are achieved via safety-related inputs and outputs (in two channels) which have an influence on the process in all operating modes.

Additional information

- **Documentation**
  This manual is a supplement to the Technical Manual of your control, and describes the functions of the functional safety (FS) and the SPLC from HEIDENHAIN. Therefore, please also refer to the following documentation:
  - Technical Manual of your control
  - "Inverter Systems and Motors" Technical Manual
  - Online help of the PLCdesignNT development environment for (S)PLC programming
- **Documentation for NC software 606 42x-01**
  For the documentation of the new iTNC 530 HSCI hardware generation, please refer to the iTNC 530 HSCI Technical Manual.

Note

Update Information No. 25 loses its validity as soon as the iTNC 530 HSCI Technical Manual for NC software 606 42x becomes available.

Note

You can download manuals, other documentation and PC software tools for machine manufacturers from the HEIDENHAIN FileBase.

- **Specifics and constraints**
  The first software versions for functional safety of the iTNC 530 HSCI do not include the full range of features necessary to provide functional safety for all machine models. Please see page 4–88. Your contact person at HEIDENHAIN will be glad to answer any questions concerning the iTNC 530 HSCI with functional safety.

Note

Before planning a machine with functional safety, please inform yourself of whether the current scope of functional safety features suffices for your machine design.

In practice, and in the sense of this document, a HEIDENHAIN control system for a machine tool consists of:

- a HEIDENHAIN NC control with integrated safety and HSCI, an MC main computer and CC controller units
- peripheral units such as screen, keyboard, machine operating panel and handwheel
- the SPL or PL assemblies with their I/O modules for connecting safety and standard inputs and outputs
- synchronous and asynchronous feed and spindle motors
- position and speed encoders
- supply modules and inverters

A prerequisite for the functional safety of HEIDENHAIN controls is the connection of the actual control components via the common HSCI connection (HSCI = HEIDENHAIN Serial Controller Interface).

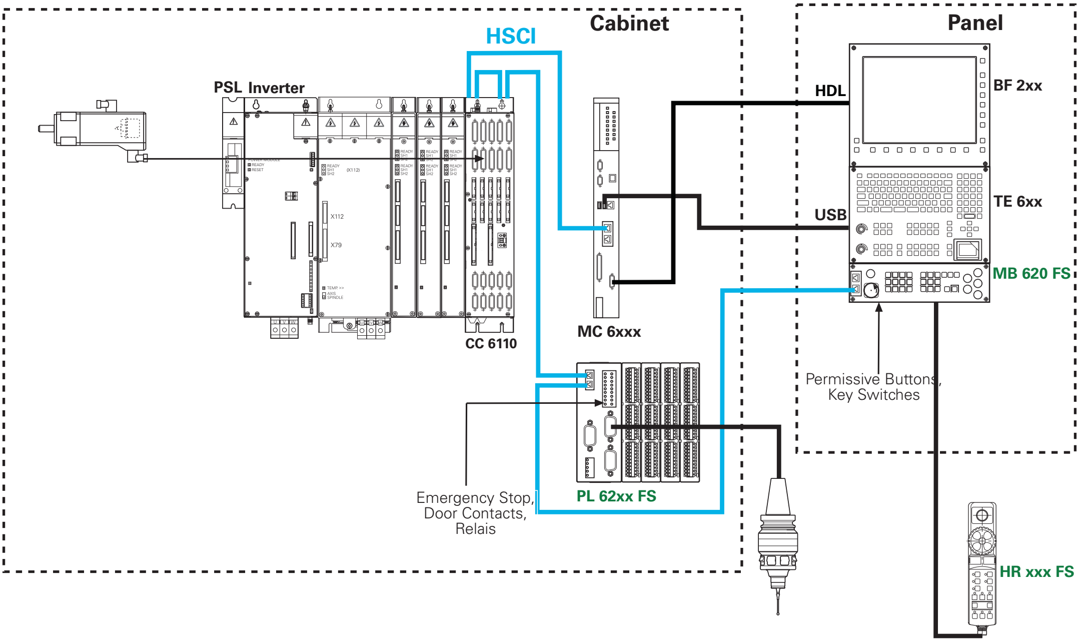


Figure 3.1: Possible setup of an HSCI system

HEIDENHAIN control components for setting up a system with functional safety:

Series	Component of the control system
MC 6xxx	MC main computer with HSCI interface for the HEIDENHAIN NC control
CC 6xxx	CC controller units with HSCI interface and support for a variable number of control loops
PLB 6xxx FS	Functional safety (FS) version of a bus module, serves as carrier for several PLD-H xx-xx-xx (FS) I/O modules. Designated SPL in this document.
PLD-H xx-xx-xx FS	Functional safety (FS) version of an I/O module. Designated SPLD in this document.
MB 6xx FS	Functional safety (FS) version of a machine operating panel. Designated SMOP in this document.
TE 6xx	Keyboard unit (ASCII keyboard, keys for supporting the operator) without safety-relevant tasks.
TE 6xx FS	Functional safety (FS) version of a keyboard unit with an integrated MB 6xx FS machine operating panel. The MB is designated SMOP in this document.
HR xxx FS	Functional safety (FS) version of an HR handwheel.
BF xxx	Screen with HDL connection.
Position and speed encoders	HEIDENHAIN encoders with analog, EnDat 2.1 and EnDat 2.2 interface.
UM 1xxD, UVR 1x0D, UV 130D, UR 2xxD, UE 2xxD and UE 1xx	HEIDENHAIN power modules (UM), supply modules (UV), regenerative supply modules (UVR), inverter units (UE) and regenerative inverters (UR).
SIEMENS-SIMODRIVE 611	The use of modules from Siemens' SIMODRIVE 611 power module product family or other non-HEIDENHAIN inverters has not been approved for the integrated functional safety!

The HEIDENHAIN safety strategy enables you to implement the protection objectives defined in Directive 2006/42/EC easily and enjoy economic benefits at the same time.
The following items may no longer be required:

- Safety contactor combinations for emergency stop and guard door control
- Time delay relays and auxiliary relays
- Limit switches
- Wiring effort

2.6 Overview of FS Components

One of the priorities of software release 606 42x-01 is the support of the new digital real-time bus system HSCI (HEIDENHAIN Serial Controller Interface) from HEIDENHAIN. HSCI combines the communication between axis system and automation into one bus system between control components. Along with simplifying the connection technology, HSCI is also the basis for safe, dual-channel, digital communication, which is the technical prerequisite for future integrated safety functions, referred to as "functional safety." The official release of HSCI with integrated functional safety will be announced in a separate Update Information once the FS system has been certified.

The following tables give an overview of the HSCI, FS and inverter components of the iTNC 530 HSCI. The individual HEIDENHAIN components are described in the iTNC 530 HSCI Technical Manual and the Inverters and Motors Technical Manual.

In systems with functional safety, certain hardware components assume safety-relevant tasks. Approval for these components must be granted for each variant individually by HEIDENHAIN. In the following tables you will find the basic ID number and variant for those hardware components that have safety-relevant tasks.

Note

The following lists, consisting of hardware components and their variants, contain all hardware components that may be used in systems with functional safety.
In HSCI systems with integrated functional safety (FS) you may use only devices or variants that have been certified for use in such systems.

Please take the following lists into account when configuring your machine and in case servicing is required. The right-most table column contains the approved ID numbers of these components.

2.6.1 List of approved control components

In systems with functional safety, certain hardware components assume safety-relevant tasks. Approval for these components must be granted for each variant individually by HEIDENHAIN. In the following tables you will find the basic ID number and variant for those hardware components that have safety-relevant tasks.

Note

Systems with FS may consist of only those safety-relevant components for which the variant is listed in the table below (e.g. xxx xxx-03).

Components indicated in this list with -xx do not assume any safety-relevant task in the sense of functional safety (FS). You can use any variant of these components.

Components indicated in this list with "Not yet approved for FS" are not approved for use in systems with functional safety.

The list will be expanded or revised correspondingly when new components are approved for use in systems with functional safety (FS). Should a component you wish to use not be listed, please ask your contact person at HEIDENHAIN if the component may be used.

Hardware component		ID
MC 6241	Main computer 1.8 GHz with HDR, electrical cabinet version, without Profibus	573 398-03
MC 6241	Main computer 1.8 GHz with HDR, electrical cabinet version, with Profibus	653 220-03
MC 6222	Main computer with 15-inch TFT display, 1.8 GHz with SSDR, operating-panel version, without Profibus	634 109-02
MC 6222	Main computer with 15-inch TFT display, 1.8 GHz with SSDR, operating-panel version, with Profibus	634 113-02
MC 6341	Main computer with 15-inch TFT display, 2.2 GHz dual core with HDR, electrical-cabinet version	Not yet approved for FS
MC 6341	Main computer with 15-inch TFT display, 2.2 GHz dual core with HDR, electrical-cabinet version, with Profibus	Not yet approved for FS
HDR iTNC	Hard disk for MC 6x41, 80 GB, NC software 606 420-01	682 272-01
HDR iTNC	Hard disk for MC 6x41 (export version), 80 GB, NC software 606 421-01	682 272-51
SSDR iTNC	Solid State Disk for MC 6222, 32 GB, NC software 606 420-01	736 591-01
SSDR iTNC	Solid State Disk for MC 6222 (export version), 32 GB, NC software 606 421-01	736 591-51
SIK iTNC	SIK for MC 62xx, single-processor version, incl. SW option 2	586 084-xx
SIK iTNC	SIK for MC 62xx, single-processor version, incl. SW option 2 (export version)	586 084-xx
SIK iTNC	SIK for MC 63xx, single-processor version, incl. SW option 2	Not yet approved for FS
SIK iTNC	SIK for MC 63xx, single-processor version, incl. SW option 2 (export version)	Not yet approved for FS

Hardware component		ID
BF 250	15-inch TFT display with HDL connection	599 916-xx
BF 260	19-inch TFT display with HDL connection	617 978-xx
CC 6106	Controller unit for HSCI for max. 6 control loops	662 636-01
CC 6108	Controller unit for HSCI for max. 8 control loops	662 637-01
CC 6110	Controller unit for HSCI for max. 10 control loops	662 638-01
UEC 111	Controller unit with inverter and PLC, 4 control loops	625 777-xx
UEC 112	Controller unit with inverter and PLC, 5 control loops	625 779-xx
UEC 111 FS	Controller unit with inverter and PLC, 4 control loops, functional safety	Not yet approved for FS
UEC 112 FS	Controller unit with inverter and PLC, 5 control loops, functional safety	Not yet approved for FS
UMC 111 FS	Controller unit with inverter and PLC for power supply via external DC link, 4 control loops, functional safety	Not yet approved for FS
CMA-H 04-04-00	SPI expansion module for analog nominal-value outputs	688 721-xx
PSL 130	Low-voltage power supply unit, 750 W, for +24 V NC and +24 V PLC	575 047-xx
PSL 135	Low-voltage power supply unit, 750 W, for +24 V NC, +24 V PLC and +5 V NC	627 032-xx
MS 110	Mounting case for multi-row configuration	658 132-xx
MS 111	Mounting case for multi-row assembly, additional connection for 24 V supply to the fan	673 685-xx
TE 620	Keyboard unit without touchpad	625 806-xx
TE 630	Keyboard unit with touchpad	617 976-xx
TE 635Q FS	TE with touchpad and integrated MB for HSCI connection, functional safety	662 255-01
TE 645Q FS	TE with touchpad and integrated MB for HSCI connection, functional safety (19-inch)	685 394-01
MB 620 FS	Machine operating panel for HSCI connection, functional safety	660 090-01
PLB 6001 FS	HSCI adapter for OEM-specific machine operating panel, functional safety	Not yet approved for FS
HR 410 FS	Portable electronic handwheel with cable connection	337 159-11, 578 114-03
HR 520 FS	Portable electronic handwheel with cable connection and display	670 304-01, 670 305-01
HR 550 FS	Portable electronic handwheel with wireless transmission and display	598 515-02, 606 622-02
HRA 551 FS	Handwheel adapter with integrated charger	731 928-01

Hardware component		ID
HRA 550 FS	Handwheel adapter with integrated charger	633 108-02
PLB 6104	PLB for HSCI, 4 slots	591 828-xx
PLB 6106	PLB for HSCI, 6 slots	630 058-xx
PLB 6108	PLB for HSCI, 8 slots	630 059-xx
PLB 6204	PLB for HSCI, 4 slots, with system module	591 832-xx
PLB 6206	PLB for HSCI, 6 slots, with system module	630 054-xx
PLB 6208	PLB for HSCI, 8 slots, with system module	630 055-xx
PLB 6104 FS	PLB for HSCI, 4 slots, functional safety	590 479-03
PLB 6106 FS	PLB for HSCI, 6 slots, functional safety	804 755-01
PLB 6108 FS	PLB for HSCI, 8 slots, functional safety	804 756-01
PLB 6204 FS	PLB for HSCI, 4 slots, with system module, functional safety	586 789-03
PLB 6206 FS	PLB for HSCI, 6 slots, with system module, functional safety	622 721-03
PLB 6208 FS	PLB for HSCI, 8 slots, with system module, functional safety	620 927-03
PLD-H 16-08-00	PL for PLB 6xxx: 16 digital inputs, 8 digital outputs	594 243-xx
PLD-H 08-16-00	PL for PLB 6xxx: 8 digital inputs, 16 digital outputs	650 891-xx
PLD-H 08-04-00 FS	PL for PLB 6xxx FS: 8 digital inputs, 4 digital outputs, functional safety	598 905-01, 598 905-02
PLD-H 04-08-00 FS	PL for PLB 6xxx FS: 4 digital inputs, 8 digital outputs, functional safety	727 219-02
PLA-H 08-04-04	PL for PLB 6xxx, eight ±10 V inputs, four ±10 V analog outputs, four PT 100 inputs	675 572-xx

If other low-voltage power supply units are used for +24 V NC and +24 V PLC, the output voltages must fulfill the requirements for Protective Extra Low Voltage (PELV) with double basic insulation according to EN 50 178, also see the iTNC 530 HSCI Technical Manual, chapter 3.8.

2.6.2 List of approved inverter components

Danger

In HSCI systems with integrated functional safety (FS) you may use only inverters or power supply modules that have been approved for use in such systems.

Please take this into account when configuring your machine and in case servicing is required. Suitable devices are listed below in the right column of the table.

Components indicated in this list with "Not yet approved for FS" are not yet approved for use in systems with functional safety.

The list will be expanded or revised correspondingly when new components are approved for use in systems with functional safety (FS). Should a component you wish to use not be listed, please ask your contact person at HEIDENHAIN if the component may be used.

Below you will find an overview of the devices that—according to ISO 13849— are permitted for use in systems with FS:

Hardware component	**Device ID for systems with integrated FS**
Inverter modules	
UM 117DW	Not yet approved for FS
UM 116D	Not yet approved for FS
UM 116DW	Not yet approved for FS
UM 115D	671566-01
UM 114D	671288-01
UM 113D	730435-01
UM 112D	731984-01
UM 122D	667633-01
UM 121BD	667942-01
UM 111BD	671968-01
UM 121D	667838-01
UM 111D	667945-01
Power supply modules	
UVR 120D	728252-01
UV 130D	Not yet approved for FS
UVR 130D	728248-01
UVR 140D	728253-01
UVR 150D	728255-01
UVR 160D	728257-01
UVR 160DW	728258-01
UVR 170DW	Not yet approved for FS

Hardware component	Device ID for systems with integrated FS
Non-regenerative compact inverters	
UE 210D	Not yet approved for FS
UE 211D	Not yet approved for FS
UE 212D	Not yet approved for FS
UE 230D	Not yet approved for FS
UE 240D	Not yet approved for FS
UE 241D	Not yet approved for FS
UE 242D	Not yet approved for FS
UE 110	Not yet approved for FS
UE 111	Not yet approved for FS
UE 112	Not yet approved for FS
Regenerative compact inverters	
UR 242D	Not yet approved for FS
UR 230D	Not yet approved for FS
UR 240D	Not yet approved for FS

2.6.3 Differences between systems with and without functional safety (FS)

With the following HSCI control components, you must make a distinction between those that are required in a system with functional safety and those that can be used in a system without functional safety. Devices with FS are listed below in the middle column:

Note

Please refer to the lists of components approved for FS.

Device designation	Device ID for systems with integrated FS	Device ID for systems without integrated FS
Machine operating panels and keyboard units In systems with FS you must use a machine operating panel for functional-safety applications. In these operating panels, all keys have twin channels. A movement can therefore be executed without additional permissive button/key.		
MB 620 (FS)	660 090-xx	617 973-xx
TE 635Q (FS)	662 255-xx	617 975-xx
TE 645Q(FS)	685 394-xx	682 104-xx
PLB basic modules In FS systems, mixed use of PLB basic modules with and without FS is possible. However, at least one PLB 62xx FS must be used in systems with FS.		
PLB 6104 (FS)	590 479-xx	591 828-xx
PLB 6106 (FS)	804 755-xx	630 058-xx
PLB 6108 (FS)	804 756-xx	630 059-xx
PLB 6204 (FS)	586 789-xx	591 832-xx
PLB 6206 (FS)	622 721-xx	630 054-xx
PLB 6208 (FS)	620 927-xx	630 055-xx
PLB 6001 (FS)	Not yet available	668 792-xx
PLD-H I/O modules In systems with FS, the mixed use of PLD-H modules with and without FS is possible in PLB basic modules with FS. However, do not insert PLD-H modules with FS in PLB basic modules without FS. Furthermore, the modules with FS must always be inserted into the PLB with FS starting from the left.		
PLD-H 16-08-00, PLD-H 08-04-00FS	598 905-xx	594 243
PLD-H 08-16-00, PLD-H 04-08-00FS	727 219-xx	650 891-xx
Handwheels In FS systems, handwheels with cross-circuit proof permissive buttons must be used. Handwheels for which this has been implemented are identified with FS.		
HR 410(FS)	337 159-xx, 578 114-xx (with detent)	296 469-xx, 535 220-xx (with detent)
HR 520 (FS)	670 304-xx, 670 305-xx (with detent)	670 302-xx, 670 303-xx (with detent)

3 Directives and Standards

3.1 Applicable Directives

Compliance with the following directives is mandatory for the design of machine tools:

Directives	Applicable since
Machinery Directive 2006/42/EC	December 29, 2009
EMC Directive 2004/108/EC	July 20, 2007
Low Voltage Directive 2006/95/EC	January 16, 2007

HEIDENHAIN controls with integrated safety strategy fulfill their share of the requirements as specified in the above directives, thus enabling you as the manufacturer to produce your machines in accordance with the machinery directives.

HEIDENHAIN controls with integrated functional safety (FS), for which safety-relevant specifications (suitability for certain PL or SIL levels) will be indicated in the future, are not considered safety components in the sense of Machinery Directive 2006/42/EC (article 2, letter c). Since these controls are also not "partly completed machinery" (article 2, letter g), they do not fall under the provisions of the Machinery Directive. For this reason we do not issue any EC Declaration of Conformity nor a Declaration of Incorporation in the sense of the Machinery Directive.

3.2 Basis for Testing

The safety functions described as well as the devices for controls with functional safety (FS) are tested by TÜV Süd. The directives and standards serving as the basis for testing are listed below:

European directives

Directives	Applicable since
Machinery Directive 2006/42/EC	December 29, 2009
EMC Directive 2004/108/EC	July 20, 2007
Low Voltage Directive 2006/95/EC	January 16, 2007

Functional safety

Safety standards	Requirement	Meaning / Designation
DIN EN 61508-1 to 4 (2001)	SIL 2	Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-Related Systems
EN 954-1 (1996)	Cat 3	Safety of Machinery – Safety-Related Parts of Control Systems
DIN EN ISO 13849-1 (2008)	Cat 3 / PL d	Safety of Machinery – Safety-Related Parts of Control Systems

Due to the applications of the device or system, the following directives and standards are also valid:

Safety standards	Meaning / Designation
IEC 61800-5-2 (FDIS) (2006)	Adjustable Speed Electrical Power Drive Systems – Part 5-2: Safety Requirements – Functional
DIN EN 60204-1 (2007)	Safety of Machinery – Electrical Equipment of Machines – Part 1: General Requirements

Primary safety

Safety standards	Meaning / Designation
DIN EN 50178	Electronic Equipment for Use in Power Installations

Electromagnetic compatibility

Safety standards	Meaning / Designation
DIN EN 61800-3	EMC product standard including specific test methods for electrical power drive systems
"EMC and functional safety for power drive systems with integrated safety functions" principle for testing dated February 2007	

Requirements of IEC 61508 SIL 2

The goal is to control or avoid errors in the control, and to limit the probability of dangerous failures to defined values. Safety integrated levels (SIL) have been defined to measure the achieved level of safety-related performance. The entire system, including all associated components, must achieve the required safety integrated level. For systems with programmable electronics, the SIL capability and the limited failure rate PFH (probability of dangerous failure per hour) result from applying IEC 61508 during the development and manufacture of these systems.
A safety integrated level corresponds to a defined range of probability for the dangerous failure of safety functions. By achieving SIL 2, which the HEIDENHAIN controls with functional safety do, the probability of failure of the safety functions is between 10^{-6} and 10^{-7} failures per hour.

Requirements of EN 13849-1 Category 3, Performance Level d

The EN 13849 standard (previously EN 954) is of special importance.
This standard groups the requirements for safety-related control components into categories (B, 1, 2, 3, 4) and performance levels (a, b, c, d, e) in ascending degrees of safety-related effectiveness.

Category B must always be fulfilled. It requires the following:
In accordance with the applicable standards, the design of safety-related parts of machine controls and their safeguards must ensure that they can withstand the influences to be expected.

To attain category 3, the occurrence of an individual fault must not result in the loss of the safety function. The system must reliably detect individual faults. The safety function must always remain in effect if an individual fault occurs.

The performance level determines the capability of the safety-related parts of the control to perform a safety function. Performance Level d corresponds to SIL 2 of IEC 61508 (see above), but is determined using a risk graph.

Fulfillment of the requirements

HEIDENHAIN controls with functional safety operate according to the following principles in order to fulfill the requirements for category 3:
The control is structured in such a way that individual faults are detected, and that an individual fault in the control does not result in loss of the safety function.
Redundant structures, reciprocal data comparison and dynamic sampling of safety-related signals are used for error detection.

The principles below are followed in order to fulfill the requirements of SIL 2:
In order to avoid faults in safety-related software, HEIDENHAIN adheres to annexes A and B of IEC 61508-3.
Tables A.2 to A.15 and A.16 to A.19 of IEC 61508-2 are used to control random faults and to avoid systematic faults.

3.3 Requirements on Safety Integrity

3.4 SIL and Target Failure Measures

A complete system from HEIDENHAIN, consisting of control, encoder and drive, fulfills SIL 2. This corresponds to a PFH_total (probability of dangerous failure per hour) of 10^{-7} to 10^{-6}.

Summary of the fulfilled safety categories and levels for the safety functions described in this manual:

- Complete system: SIL 2 and category 3
- PFH_total: 10^{-7} to 10^{-6}
- Performance level: d

The safety functions and hardware components for functional safety (FS) are certified by independent institutes. Upon request, your contact partner at HEIDENHAIN can provide you with the safety-related characteristic values needed for calculations as per EN ISO 13849-1.

3.5 Storage and Operating Temperatures

The limit values for the individual HEIDENHAIN components are stated in the iTNC 530 HSCI Technical Manual.

3.6 Limit Values for EM Noise Immunity

According to the current standards, safety related power drive systems with integrated safety functions, abbreviated as PDS(SR), must have an increased noise immunity to electromagnetic phenomena (electromagnetic compatibility (EMC)). HEIDENHAIN complies with the limit values specified in the "EMC and functional safety for power drive systems with integrated safety functions" principle for testing dated February 2007. This specification is used when testing and certifying the iTNC 530 HSCI with integrated safety.

3.7 Mission Time

An average life limit of 20 years is assumed for these controls.

4 Realization and Safety Functions

4.1 Glossary

A channel and B channel	All safety-related areas of the control (hardware and software) have a dual-channel design. The two channels are designated as the A channel and B channel. Areas covered by the A channel are colored blue in this document. Areas covered by the B channel are colored red in this document.
STL	Statement list of the (S)PLC program
API	Application programming interface Interface between the (S)PLC program and the respective safety-kernel software (SKERN MC, SKERN CC) or the standard functions of the NC software.
CC	Controller computer: Modular HSCI slaves, for servo drive control CCs also assume safety-related tasks (see SPLC/SKERN below). The MC determines the master CC on the basis of the relative positions in the HSCI system. The first CC in the HSCI system (nearest the MC) becomes the master CC.
Master CC	Master controller computer: Modular HSCI slaves, for servo drive control In a safety-related control system, the master CC alone assumes the following special tasks in addition to the usual tasks of every CC: ■ Represents the B channel of a safety-related control system ■ Generates the output states of the SPLC of the B channel (for the safety-related outputs on the SPL), such as the outputs for controlling the brakes ■ Monitors the controlling of the motor holding brakes of the B channel (via power module or SPLC) and the disabling of power modules for all axes in the system ■ Supplies the B-channel data for cross comparison ■ Supplies the actual position values for the SPLC

CC-CC communication	Special HSCI telegram for exchanging the following data between two or more CCs: ■ States of the individual axes (at standstill or in motion) ■ Axis-group assignment ■ Actual position values of the axes ■ Status of brake control ■ Status of the axis-specific cutout ports of the B channel ■ Information about fatal fault
FPGA	Field programmable gate array: Freely programmable logic circuit.
HDL	HEIDENHAIN display link: HDL is a data connection between the MC and the screen/keyboard.
HR	Handrad HR (German) = Handwheel HW Handwheel for operating the machine.
HSCI	HEIDENHAIN serial controller interface: HSCI is a field bus system that is based on Ethernet hardware and has a line structure according to the master-slave principle. There is one master in the system; all other devices are slaves. All data transfers are initiated by the master; however, direct communication between the slaves is also possible.
IOC file	Configuration file of the HSCI system: Configuration of all participants in the HSCI system, their sequence and configuration of the inputs and outputs of the (S)PLC.
LIFT-OFF	Function that lifts off the tool automatically from the contour by a defined distance in the tool-axis direction in order to protect the workpiece (e.g. in a power failure).
MC	Main computer: Control hardware that also functions as a master for HSCI.
PLC	Programmable logic control: The main task of the PLC program is the processing of the input information from the PLs and the generation of output states for the PLs (see page 4–42).
SKERN	Safety-kernel software: The software process of the safety-kernel software (SKERN) runs in parallel to the SPLC. Basic safety functions are permanently defined in the SKERN software and cannot be changed (see page 4–45).

SMOP	Safe machine operating panel: The (safety-related) machine operating panel is an HSCI slave to which safety-related keys for controlling a machine tool are attached and to which further (safety-related) inputs/outputs are connected (see page 6–152). The safety-related data is transmitted from the SMOP to the MC and CC over two channels via the HSCI connection. The safety-related data is transferred from there to the respective SPLC.
SPLC	Safe programmable logic control: The main task of the SPLC program is the processing of the input information from the SPLs and the generation of output states for the SPLs. This can be configured flexibly using the SPLC program. (see page 4–43)
SPL and PL	(Safe) programmable logic unit: A PL is an HSCI slave equipped with multiple I/O modules. Each I/O module provides digital ((S)PLD) and/or analog (PLA) inputs and/or outputs (I/Os). These I/Os are read and controlled by the PLC and SPLC during normal operation (see page 4–43). An SPL is a dual-channel PL, which is equipped with controllers for the A channel and the B channel. The safety-related data is transmitted from the SPL to the MC and CC over two channels via the HSCI connection. The safety-related data is transferred from there to the respective SPLC. A safety-related control generally uses both SPLs and single-channel PLs. Safety-functions require the use of SPLs. An (S)PL is structured as follows: ■ Bus module All (S)PLs have a bus module. The bus module can have only one controller (for the A channel), or two controllers (for the A channel and the B channel) in the case of a control with integrated safety. ■ System module A system module has control-specific I/Os and connections for touch probes. At least one system module is present in every system. ■ I/O module – (S)PLD, PLx One S(PL) has slots for four, six or eight I/O modules. Both (safety-related) digital ((S)PLD) I/Os and, for example, analog (PLA) I/Os can be inserted. ■ System PL SPL with system module

SPLD and PLD	One SPL or PL has slots for four, six or eight digital I/O modules. A safety-related control generally uses both SPLDs and single-channel PLDs. Safety-functions require the use of SPLDs.
FS inputs, FS outputs	Safety-related dual-channel inputs/outputs. One FS input/output consists of two physical terminals.
(S)MP	(Safety) machine parameters: Parameters for adapting the control to the respective machine tool (see page 5–95).
S status	Safe status range of the HSCI telegram. The safe status range contains bits for the status of watchdogs, emergency stop and power-fail information, etc. of the individual HSCI participants. The bits of the safe status range provide the basic safety-related information of the A channel (see page 4–75).
TM	Tool magazine: Tool magazine for the storage and management of different tools.
SSt	Safety self-test: Safety self-test (see page 7–157)
WD	Watchdog: Counter for monitoring the status of other functions or components.

4.2 Realization of the HEIDENHAIN Safety System

The dual-channel safety system of HEIDENHAIN controls is achieved by a dual-channel control architecture. The two computers are located in the MC main computer and CC controller unit components, where two independent software processes run. These two processes realize two safety channels, which capture and evaluate all safety-relevant signals in the two channels. Faults are detected by mutual comparison of the states and data (cross comparison) in the two channels. This way, the occurrence of just one fault in the control does not lead to the safety functions being incapacitated.

The SPLC (safety-related PLC) and SKERN (safety-kernel software) software processes are the basis of the two redundant channels. The two software processes run on the MC (CPU) computer and the CC (DSP) controller unit computer.

The dual-channel structure of the MC and CC is also used in the PL 6xxx FS input/output systems and the MB 6xx FS machine operating panel. This means that all safety-relevant signals (e.g. permissive buttons and keys, door contacts, emergency stop button) are captured via two channels, and are evaluated independently of each other by the MC and CC. The MC and CC use separate channels to address the power modules, and to stop the drives in case of a fault.

Furthermore, HEIDENHAIN controls with functional safety offer four safety-related operating modes as per the EN 12 417 standard (Machine Tools–Safety–Machining Centers). The application-oriented operation offered by this promises a high level of acceptance, and therefore safety.

4.3 Activation of Functional Safety (FS)

Functional safety is not a software option that must be enabled. If the control identifies a PLB 62xxFS in the HSCI system during booting, functional safety is activated. In this case, the following prerequisites must be fulfilled:

- Functional safety versions of safety-related control components (e.g. MB 620FS, HR 520FS)
- Safety-related SPLC program
- Configuration of safe machine parameters
- Wiring of the machine for systems with functional safety

4.4 (S)PLC Programs

The main task of the (S)PLC program is the processing of the input information from the (S)PLs and the generation of output states for the (S)PLs.
To do so, it edits the PLC memory via PLC commands with memory operands. Logical states and signed bytes, words (16 bits) and doublewords (32 bits) are saved in this memory.

Specific areas have different tasks:

- Memory mapping the status of the inputs
- Memory for timers and counters
- Memory for internal states and calculations
- Memory for the interface to the software of the MC and CC
- Memory defining a map of the outputs to be set

This division of the memory is also called a memory map.

On a control with integrated safety, three different PLC programs with separate memory maps are run simultaneously:

- Standard PLC program on the hardware of the MC
- SPLC program on the hardware of the MC
- SPLC program on the hardware of each CC

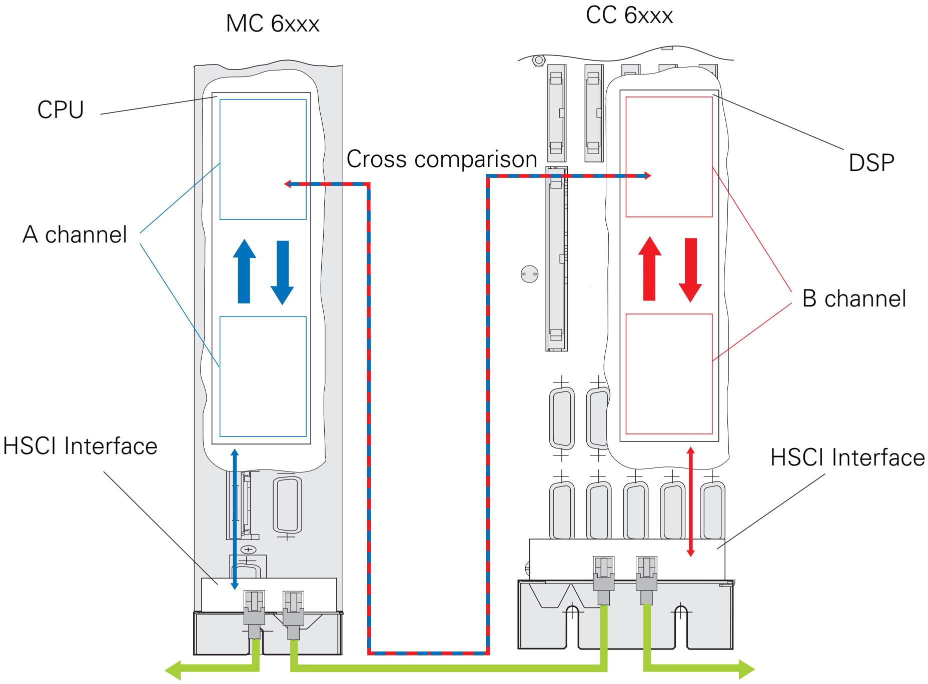


Figure 3.2: SKERN and SPLC

4.5 SPLC

The safe PLC program (= SPLC program), the PL 6xxx FS (= SPL) input/output modules and the MB 6xx FS (= SMOP) machine operating panel provide the machine tool builder with a flexible configuration of the safety system. The SPLC consists of the SPLC runtime system and the SPLC program. The SPLC runtime system is part of the software supplied by HEIDENHAIN. It executes the SPLC program that must be written by the machine tool builder. The safety-related inputs and outputs as well as additional safety functions can be programmed flexibly in the SPLC program. The SPLC is also responsible for the import and processing of FS inputs, as well as for the output of FS outputs.

The SPLC software runs both on the MC (SPLC MC) and on every CC (SPLC CC) completely independently. The SPLC MC is assigned to safety channel A, and the SPLC CC to safety channel B. Every SPLC communicates with further HSCI participants (e.g. SPL, SMOP) via HSCI. The evaluated data is then transmitted to the respective SKERN (MC/CC). The SPLC requests the execution of safety functions from the SKERN. However, the SKERN can activate safety functions that provide an even higher degree of safety for the operator.

The physical FS inputs (terminals on SPL or SMOP) of the A channel and the B channel are first gated with AND; only the result of the AND operation is then forwarded to the SPLC as input status. Consequently, the SPLCs of the A channel and the B channel will receive the value 0 as input information if two inputs have different states (e.g. A channel = 0, B channel = 1).

As with the standard PLC program, the PLCdesignNT PC software from HEIDENHAIN is used to create the SPLC program. For requirements to be met by the SPLC program, see page 184.

Tasks of the SPLC:

- Flexible adaptation of the safety functions to the respective machine tool by the machine tool builder
- Import (reading in) of FS inputs
  This includes, for example:
  - External EMERGENCY STOP
  - Axis-group-specific "Control Voltage ON" key
  - Door contacts of the guard doors
  - Permissive buttons and keys (on the handwheel, operating panel and tool magazine)
  - Keylock switches for the safety-related operating modes (SOM_1, SOM_2, SOM_3, SOM_4)
  - Test input for motor holding brake
  - Feedback from chain of normally closed contacts
  - Axis-direction keys
  - Other keys with a Start function (NC start, spindle start, spindle jog)
  - Keys with Stop function (NC stop, spindle stop)
- Gating of FS inputs/outputs

- Realization of machine-specific safety functions
- Realization of timer functions
- Data transfer from the SPLC to the safety-kernel software (see also page 8–193)
  - Request for the safety-related operating mode (SOM_1, SOM_2, SOM_3, SOM_4)
  - Axis-group-specific request for monitoring the safely limited speed (SLS) in the respectively active, safety-related operating mode
  - Axis-specific and axis-group-specific activation of a permissible movement after the evaluation of the inputs of axis-direction keys (of SMOP, HW, TM)
  - Axis-group-specific request for stop reactions (SS1, SS1F, SS2)
  - Axis-group-specific state of the permissive buttons and keys
  - Status of the chain of normally closed contacts
  - Status of the "Control Voltage ON" (CVO) key
  - Axis-group-specific drive enable (PDO = Permit Drive On)
  - At least one machine operating key is pressed
  - Status of the test input of the motor holding brakes
- Controlling of outputs that are commanded by the safety-kernel software (e.g. SBC safety function), or of safety-related outputs defined by the machine tool builder.
  The SPLC program of the master CC controls the SPLC outputs of the B channel of each SPL; the SPLC program of the MC controls the SPLC outputs of the A channel.

4.6 SKERN

The software process of the safety-kernel software (SKERN) and the SPLC run in parallel on the MC and CC. Basic safety functions are permanently defined in the SKERN software and cannot be changed by the machine tool builder. The safety-kernel software receives status information and requests for safety functions from the SPLC. The SKERN initiates safety functions and monitors them. Furthermore, all dynamic tests are controlled by the safety-kernel software.

The safety-kernel software is responsible for the realization of all basic safety functions:

- Initiation and monitoring of the stop reactions (SS0, SS1, SS1F, SS2)
- Standstill monitoring in SOS state
- Monitoring of the safely limited speeds (SLS) in the various safety-related operating modes
- Initiation of safe brake control (SBC)
- Safely-limited position (SLP)
- Nominal-actual value comparison of position values or speed values
- Control of dynamic tests
- Carrying out the cross comparison
- Commanding the control of safety-related outputs of the SPLC (e.g. control of motor holding brakes)
- Transfer of axis-group states (STO, SOS, AUTO (AUTO = operation if the guard doors are closed) or of the safety function in direct connection with the operating mode: SLI_2 through SLI_4, SLS_2 through SLS_4) to the SPLC
- Transfer of the axis states (at standstill or in motion) to the SPLC
- Transfer of the axis positions to the SPLC
- Performing the safety self-test (SSt)

4.7 Cross Comparison

During the cross comparison, safety-related signals and operating states (active safety functions) are exchanged between the MC and the CC, and compared in both units. The cross comparison is performed by the SKERN of the MC and the CC in a safety cycle (3 ms).

If one of the CCs or the MC detects a fault, an SS1 reaction is initiated.

The cross comparison contains the following data:

- All output signals from the SPLC that are transferred to the safety-kernel software.
- Status information of the safety-kernel software in the MC and CC.
- Output signals from the SPL that are fed back to the safety-kernel software (outputs can be read back).
  Each of the dual-channel hardware outputs has a feedback mechanism on the I/O modules of the SPL, which can be used to read the status of the output. This dual-channel information is sent from the SPL to the SPLCs via the HSCI, and transferred to the safety-kernel software of the MC and CC. The cross comparison is always active for all safety-related outputs.
- Status information of the SPLC program on both the MC and CC (SPLC program is being executed).
- SS1F stop reactions requested by the SPLC runtime system

The gated and, where applicable, fed-through signals, which are the output signals from the SPLC of the MC and CC to the respective SKERN, are compared.

In the HEIDENHAIN system the SPLC output statuses mapped from the physical inputs, and not the physical inputs themselves, are used for the cross comparison during forced dynamic sampling. During forced dynamic sampling the physical inputs are checked only for a short-circuit to +24 V. A real cross comparison of the physical inputs is only performed during the safety self-test to avoid problems with dual-channel keys that do not switch simultaneously.

Note

A direct cross comparison of the physical input signals of the SPLC does not take place.

4.8 Description of the Safety/Monitoring Functions

Danger

The risk analysis you have to carry out for the machine must state the requirements to be fulfilled by the individual safety function.

Before using the control, you must check whether the safety functions realized by HEIDENHAIN meet the requirements of your risk analysis.

All components (e.g. control hardware, control software, emergency stop button, safety relays) that are involved in the individual safety functions must meet the requirements for the safety function. The hardware of the individual safety functions, including the wiring, must also be structured according to the determined requirements.

4.8.1 Overview of the safety functions

In order to ensure operator protection, the control and drive system with integrated HEIDENHAIN safety design provides a number of safety functions you can request and initiate through the SPLC program, and parameterize through SMPs. These safety functions to be complied with correspond to the draft of the new DIN IEC 61800-5-2 standard.

Overview of definitions	Brief description
Safe stop 0 (SS0)	The current to the drives is cut off. The STO and SBC functions are initiated immediately. The drives are switched back on by turning the machine off and on. The stop reaction is carried out via two channels.
Safe stop 1 (SS1)	The drives are stopped along the emergency braking ramp. The STO and SBC functions are initiated after standstill. The drives are switched back on via Control Voltage ON. The stop reaction is carried out via two channels.
Safe stop 1D (SS1D)	Same as SS1, but axis-group-specific switch-off with delay.
Safe stop 1F (SS1F)	The drives are stopped along the emergency braking ramp. The STO and SBC functions are initiated after standstill. The drives are switched back on by turning the machine off and on. The stop reaction is carried out via two channels.

Overview of definitions	**Brief description**
Safe stop 2 (SS2)	The axes and spindles are stopped along the braking ramp. At standstill the STO function is initiated for the spindles, and the SOS function for the axes. The stop reaction is carried out via two channels.
Safe torque off (STO)	The energy supply to the motor is interrupted via two channels (by MC and CC).
Safe operating stop (SOS)	The drives remain under position control and are monitored for standstill via two channels (by MC and CC).
Safely limited speed (SLS)	The SS1 safety function is initiated if defined speed limit values are exceeded. Monitoring takes place via two channels (by MC and CC).
Safely limited position (SLP)	The SS1 safety function is initiated if an absolute position limit value is exceeded. Monitoring takes place via two channels (by MC and CC).
Safe brake control (SBC)	Dual-channel control of external motor holding brakes (by MC and CC).
Safely limited increment (SLI)	The function must be realized via the SPLC program.

4.8.2 Overview of monitoring functions

Further monitoring functions are integrated in addition to the safety functions. These monitoring functions can be programmed through SMPs to a certain extent.

Overview of definitions	Brief description
Nominal-actual value comparison of position values	Dual-channel comparison (by MC and CC) of the actual position values (speed encoder, position encoder) to the nominal position value.
Nominal-actual value comparison of speed values	Dual-channel comparison (by MC and CC) of the actual speed values (speed encoder, position encoder) to the nominal speed value.
Monitoring of the encoder amplitudes	Dual-channel monitoring (by MC and CC) of the signal amplitudes of the encoders.
Monitoring of the encoder frequency	Dual-channel monitoring (by MC and CC) of the input frequency of the encoders.
Protection against unexpected start-up	If all axes or spindles of an axis group do not move for more than 3 seconds during SLS, an automatic axis-group-specific transition to SOS or STO is carried out.
dv/dt monitoring of the axes/ spindle by the MC/CC	During deceleration the axes and the spindle are monitored via two channels (by MC and CC) for a decrease in speed.
Temperature monitoring	Monitoring of the internal temperature of HSCI components.
Monitoring of rotational speed of fan	Dual-channel monitoring (by MC and CC) of the rotational speed of the internal fans of HSCI components.
Monitoring of the supply voltages	On each board, the supply voltages are monitored via two channels.

4.8.3 Safe stop 0 (SS0)

An SS0 reaction is initiated in the event of a fault.

An SS0 reaction is initiated by the SKERN. The SPLC cannot request an SS0 reaction from the SKERN.

If an SS0 is initiated, the STO (see page 4–60) and SBC (see page 4–66) safety functions are activated for the affected axis (axes) and spindle(s) via two channels.

The switch-off of safe outputs must be realized through the SPLC program (see page 8–197). The behavior of normal PLC outputs can be configured via IOconfig.

Danger

- Axes and spindles that do not have mechanical motor holding brakes coast to a stop.
- The measures to be taken against external force (e.g. sagging of hanging axes) must be in accordance with Information Sheet No. 005 "Gravity-loaded axes (vertical axes)" issued by the engineering technical committee of the BGM (German Employer's Liability Association in the metal industry).

After SS0, the drives can be restarted **only by turning the main switch off and back on** (power supply voltage of the machine).

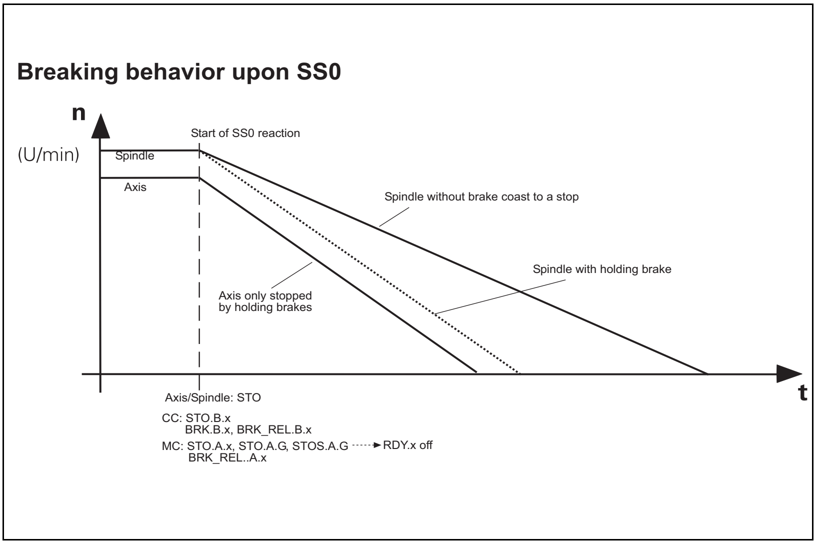


Figure 3.3: Braking behavior upon stop 0
(For signal designations, see page 5–120)

4.8.4 Safe stop 1 (SS1) – Fastest possible stopping

An SS1 reaction is initiated if a fault or an emergency stop occurs.

An emergency stop can be initiated internally by the SKERN itself, or can be initiated depending on the safety-related inputs for emergency-stop buttons.

An SS1 reaction is initiated by the SKERN. The SPLC can request an axis-group-specific SS1 reaction from the SKERN (for axis groups, see page 6–136).

If an SS1 is initiated, the affected axis (axes) and spindle(s) are decelerated by the respective CC as quickly as possible along the emergency braking ramp.

When the SS1 reaction starts, the monitoring timers with the time defined in SMP525.x for the axes and in SMP526.x for the spindles are started. The initiated deceleration process is additionally monitored via dv/dt monitoring (see page 4–69).

The steepness of the emergency braking ramp (ramp for deceleration) is defined in MP2590. The greater the value entered in MP2590, the steeper the emergency braking ramp. The maximum value for MP2590 is limited by the output power of the inverter. The minimum value is defined in MP1060. The permissible acceleration of the axis during normal machining operation is defined in MP1060. If the value in MP2590 is less than the value in MP1060, the value from MP1060 will be used.
A special case is the value of 0 in MP2590, which results in deceleration at the limit of current.

After the values for MP2590 and MP1060 have been defined, the collective braking behavior of all axes must be checked by the machine tool builder by initiating an emergency stop. It must be ensured that this does not lead to an overload and, as a result, to the switch-off of the inverters. The maximum permissible deceleration time of all axes must not be exceeded.

The switch-off of safe outputs must be realized through the SPLC program (see page 8–197). The behavior of normal PLC outputs can be configured via IOconfig.

A distinction is made between the following cases for SS1 reactions:

- **Normal deceleration process (timer monitoring and dv/dt monitoring do not respond):**
  If a standstill of the axes (feed rate < 50 mm/min) or spindles (speed < 10 rpm) within the time defined in SMP525.x or SMP526.x is detected by a CC, this CC initiates the SBC safety function. After the time defined in MP2308 (default: 200 ms) has expired, this CC then initiates the STO safety function. If the MC detects that the CC is in STO, the MC also initiates the STO and SBC safety functions.
- **Faulty deceleration process (timer monitoring responds)**
  If the time set in SMP525.x or SMP526.x is exceeded in the timers on the MC and CC during the deceleration process, the MC and CC initiate the SS0 safety function independently of each other.

Danger

- Axes and spindles without mechanical motor holding brakes coast to a stop if an SS0 is initiated.
- The measures to be taken against external force (e.g. sagging of hanging axes) must be in accordance with Information Sheet No. 005 "Gravity-loaded axes (vertical axes)" issued by the engineering technical committee of the BGM (German Employer's Liability Association in the metal industry).

- **Faulty deceleration process (dv/dt monitoring responds)**
  The fault reaction is in accordance with the description of dv/dt monitoring (see page 4–69).

After SS1, the restart of the drives is enabled **by switching on the machine control voltage** (CVO) via the `Control Voltage ON` button (see page 4–81).

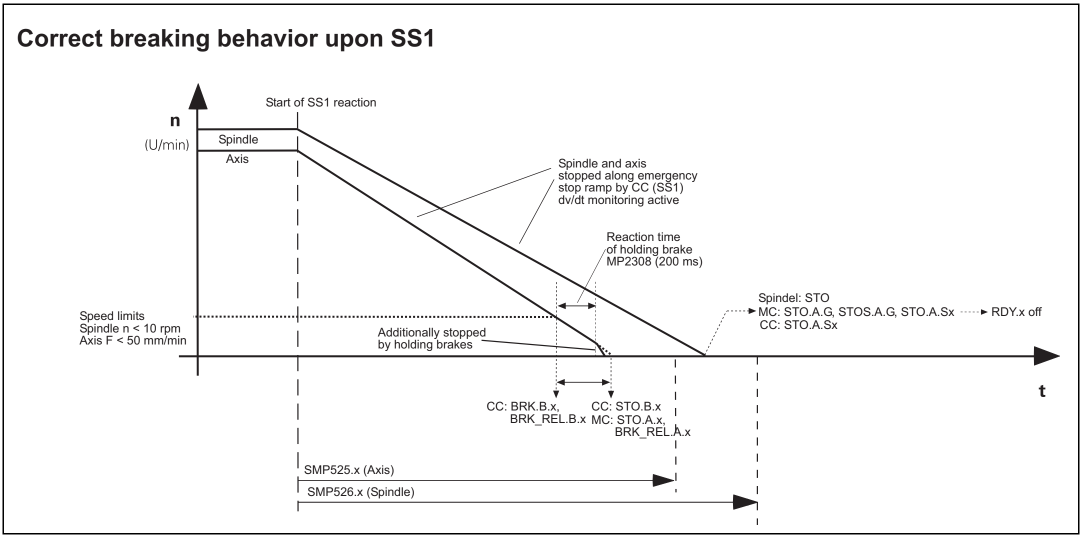

Correct breaking behavior upon SS1
n
(U/min)
Start of SS1 reaction
Spindle
Axis
Spindle and axis stopped along emergency stop ramp by CC (SS1) dv/dt monitoring active
Reaction time of holding brake MP2308 (200 ms)
Speed limits
Spindle n < 10 rpm
Axis F < 50 mm/min
Additionally stopped by holding brakes
Spindel: STO
MC: STO.A.G, STOS.A.G, STO.A.Sx
RDY.x off
CC: STO.A.Sx
t
CC: BRK.B.x, BRK_REL.B.x
CC: STO.B.x
MC: STO.A.x, BRK_REL.A.x
SMP525.x (Axis)
SMP526.x (Spindle)

Figure 3.4: Braking behavior upon stop 1

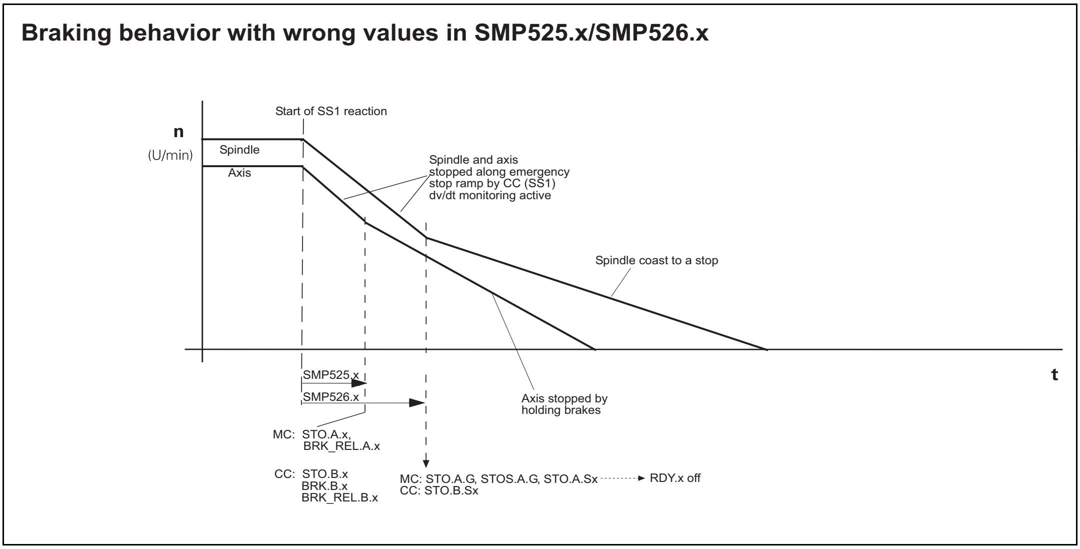


Figure 3.5: Braking behavior upon stop 1 with incorrect parameters

4.8.5 Safe stop 1D (SS1D) – Delayed SS1

The SS1D stop reaction is a delayed SS1, in which, for example, the axis group of the spindle is not decelerated until the axis groups of the NC axes have been stopped.

The braking sequence of the axis groups for SS1D is defined in MP610.x.

The switch-off of safe outputs must be realized through the SPLC program (see page 8–197). The behavior of normal PLC outputs can be configured via IOconfig.

4.8.6 Safe stop 1F (SS1F) – Fastest possible stopping

An SS1F reaction is initiated in the event of a fatal fault.

An SS1F corresponds to an SS1 reaction, but it is initiated globally for all drives of the machine tool. The switch-off of safe outputs must be realized through the SPLC program (see page 8–197). The behavior of normal PLC outputs can be configured via IOconfig.

After SS1F, the drives can be restarted **only by turning the main switch off and back on** (power supply voltage of the machine)!

4.8.7 Safe stop 2 (SS2) – Controlled stopping

An SS2 reaction is initiated by the SKERN. The SPLC can request only axis-group-specific SS2 reactions from the SKERN (see page 6–136 for axis groups).

A distinction is made between the following cases for SS2 reactions:

Normal deceleration process
(timer monitoring and path monitoring do not respond):

An SS2 reaction is initiated by the SKERN or must be initiated by the SPLC program upon:

- Releasing an axis-direction key (axis-specific SS2 by the SKERN; the SPLC program must set the attribute **`PP_AxFeedEnable`** = 0, see page 208)
- Releasing the permissive button or key while the spindle is running (Figure 3.6) (axis-group-specific SS2 by the SKERN; permissive button/key information is passed on by the SPLC program)
- Releasing the permissive button or key during programmed movements in the SOM_2 or SOM_3 operating mode (axis-specific SS2 by the SKERN; the SPLC program must set the marker **`MG_Program_Running`** = 0, see page 205)
- Pressing the NC stop key (SS2 reaction must be initiated through the SPLC program)
- Switching between safety-related SOM_x operating modes (SS2 reaction must be initiated through the SPLC program)
- Opening the guard door of an axis group during programmed movements without pressing a permissive button or key (SS2 reaction must be initiated through the SPLC program).
- Selection of or switching to one of the following machine modes of operation (SS2 reaction is initiated by the SKERN)
  - Switching to the El. Handwheel mode of operation (El. Handwheel mode of operation or activation of an HR 5xx handwheel)
  - Switching to operation through machine operating panel
  - Switching to the Reference run mode of operation

If an SS2 is initiated for the axes, the SKERN instructs the NC software to decelerate the drives of the affected axis (axes) on the contour until standstill. This ensures that the nominal contour is not departed from during the deceleration process (workpiece protection). To do this, the axes are stopped using interpolation.
When an SS2 reaction starts, the SKERN monitoring timers with the time defined in SMP527.x for the axes are started, and path monitoring for the permissible axis-specific path of traverse defined in SMP550.x is activated. When the axes have come to a standstill (SKERN monitors for feed rate < 50 mm/min), the safe operating stop (SOS) safety function is initiated for the affected axes.
If the spindle is running at the same time, the SKERN initiates an SS1 for the spindle of the working space after the axes have been brought to a standstill through SS2. This must be realized in the SPLC program. On a machine with multiple spindles, it is possible that a spindle can already be decelerated before all axes have been stopped. This behavior can be achieved through a suitable configuration of axis groups (see page 6–136).

An SS2 reaction for the spindle must be initiated by the SPLC program upon:

- Pressing the spindle stop key
- Releasing the spindle jog key

If an SS2 is initiated for the spindle, the SKERN instructs the NC software to decelerate the spindle of the axis group.
When an SS2 reaction starts, the SKERN monitoring timers with the time defined in SMP528.x for the spindles are started.
When the spindles have come to a standstill (SKERN monitors for speed < 10 rpm), the safe torque off (STO) safety function is initiated for the affected spindles.

SMP549.x can be used to activate the same behavior for the spindles as for the axes. The spindles will then also change to the SOS state as part of an SS2 reaction. This may be required for the configuration of lathes. However, the change to SOS instead of STO is only possible if the SS2 reaction was triggered by pressing the spindle stop key. If the SS2 reaction was triggered by a different event, then the STO state is maintained at the end of a stop reaction.

Faulty deceleration process (timer monitoring responds)
If the time defined in SMP527.x for the axes or the time defined in SMP528.x for the spindles is exceeded in the SKERN timers during the deceleration process, the SKERN initiates the SS1 safety function.

Faulty deceleration process (path monitoring responds)
If the axis-specific maximum permissible path defined in SMP550.x for the SS2 reaction is exceeded, the SKERN initiates the SS1 safety function.

The machine control voltage (CVO) is not switched off at the end of an SS2 reaction! The drives can therefore be restarted directly.

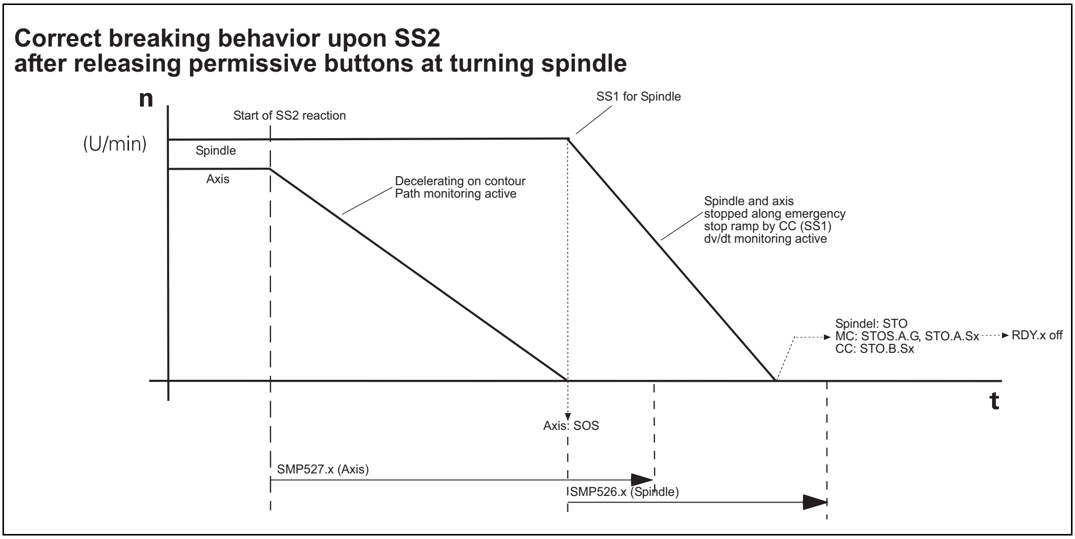


Figure 3.6: Braking behavior upon stop 2 (releasing the permissive button or key while the spindle is running)

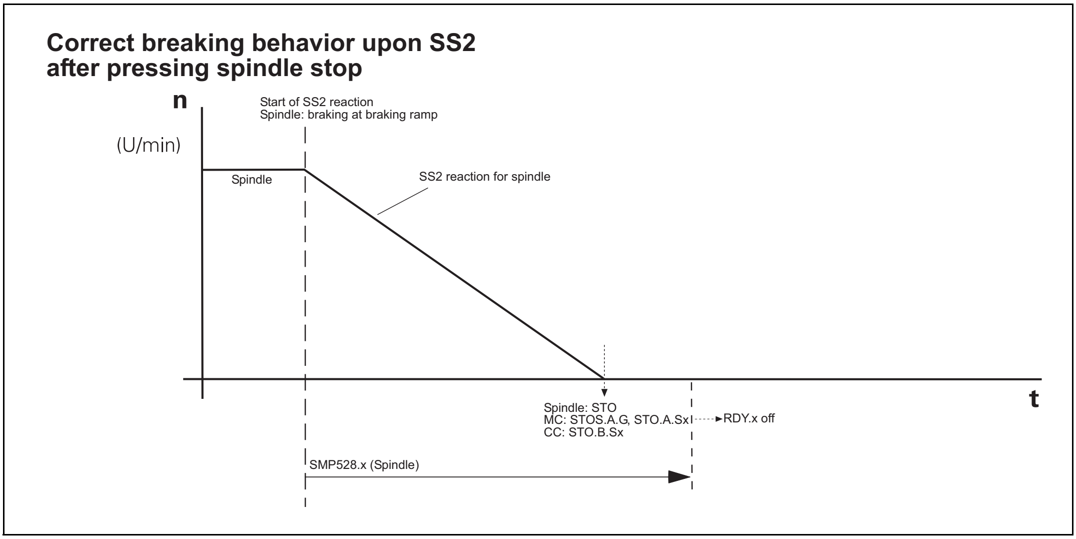


Figure 3.7: Braking behavior upon stop 2 (pressing the spindle stop key)

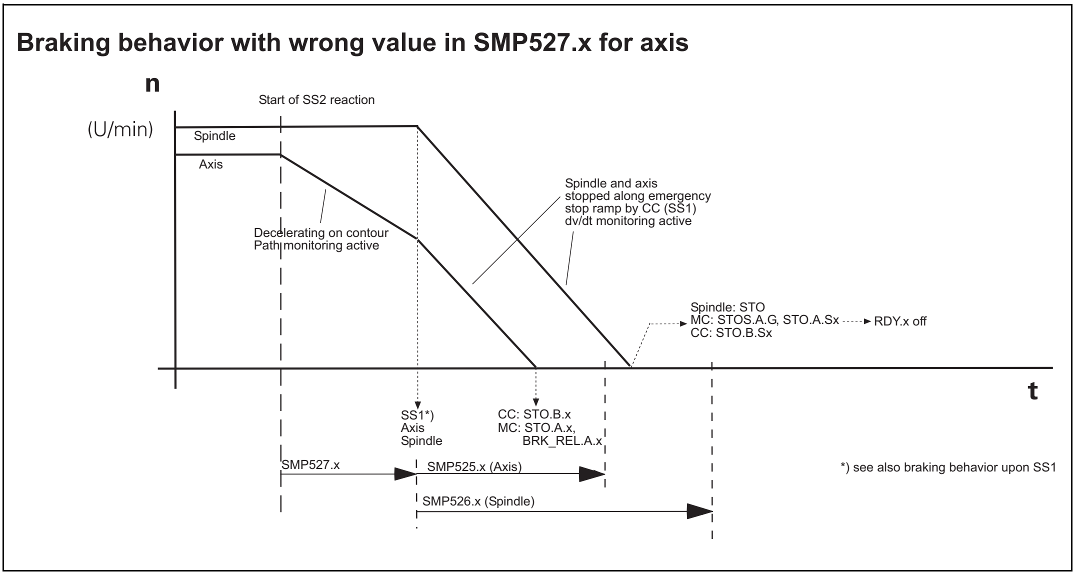


Figure 3.8: Braking behavior upon stop 2 with incorrectly set parameters

4.8.8 Summary of the stop reactions

	MC	CC
Stop 0 (SS0)	**Immediate initiation of STO and SBC:** Clearing of WD.A.STO, WD.A.SMC and STO.A.P.x Activation of motor holding brakes Status of the signals: –STO.A.G = 0 –STOS.A.G = 0 –STO.A.x = 0 –BRK_REL.A.x = 0 Restart: main switch Off/On	**Immediate initiation of STO and SBC:** Clearing of STO.B.P.x Activation of motor holding brakes; error code to MC Status of the signals: –STO.B.x = 0 –BRK.B.x = 0 –BRK_REL.B.x = 0 Restart: main switch Off/On
Stop 1 (SS1)	**Stopping along the emergency braking ramp:** "Drives Off" command for axes and spindle to the CC. Wait until all drives have been switched off by the CC: --> STO and activation of motor holding brakes For status of the signals, see above. Restart: with Control Voltage ON (CVO) The deceleration process is monitored by timers according to SMP525.x/SMP526.x, and dv/dt monitoring	**Stopping along the emergency braking ramp:** A command from the MC or detection of the fault by the CC itself leads to axis-specific electrical deceleration along the emergency braking ramp until standstill; then axis-specific activation of the mechanical brakes; After 200 ms --> STO For status of the signals, see above. Restart: with Control Voltage ON (CVO) The deceleration process is monitored by timers according to SMP525.x/SMP526.x, and dv/dt monitoring (If the fault is detected by the CC itself, an error message is sent to the MC beforehand)
Stop 1F (SS1F)	**Fault reaction:** Corresponds to stop 1 (SS1), but: Restart: main switch Off/On	**Fault reaction:** Corresponds to stop 1 (SS1), but: Restart: main switch Off/On

	MC	CC
Stop 2 (SS2)	**Deceleration along the contour:** Instruction to the NC software: Stop the axes and spindles along the braking ramp; In addition, SS2 is reported to the PLC. The PLC then issues an NC stop or spindle stop. Upon standstill: --> SOS for axes, STO for spindles (depending on SMP549.x) Restart: direct restart possible Deceleration process is monitored by the timers according to SMP527.x/ SMP528.x, and path monitoring according to SMP550.x	**Stopping with delay:** Sets monitoring timers with time defined in SMP527.x Upon standstill of axes or spindles: --> SOS for axes, STO for spindles (depending on SMP549.x) Restart: direct restart possible Deceleration process is monitored by the timers according to SMP527.x/ SMP528.x, and path monitoring according to SMP550.x

The switch-off of dual-channel safety-related FS outputs due to a stop reaction must be realized through the SPLC program (see page 8–188).

4.8.9 Safe torque off (STO)

The STO function provides protection against unexpected start-up of the drives and against faulty reactions of axes and spindles (e.g. unexpected increase in speed or unexpected direction of traverse).
In STO, the power supply to the motor is safely interrupted via two channels (CC and MC). The drive cannot generate a torque, and is therefore unable to execute any hazardous movements.

The safety function is realized in the HEIDENHAIN safety design by safely disabling the pulses (PWM signals) for the power switches via two channels. The PWM signals to the power output stages of the axes and spindles are switched off immediately by the CC (–STO.B.x) and MC (–STO.A.x) (for signal designations, see page 5–120). On the MC, the global signals –STO.A.G and –STOS.A.G are also switched off.

If wired, the MC switches off the safety relays in the power supply units or compact inverters (–STO.A.G, –STOS.A.G). This wiring was safety-relevant for inverters of the old generation; when inverters of the new generation (new ID numbers) are used, however, this wiring is not obligatory. However, control systems with FS absolutely require the use of inverters and power supply units that are approved for use in systems with functional safety (FS). The wiring of the safety relays in the compact inverters or power supply units via STO.A.G and STOS.A.G is then optional.

There is the additional possibility of using the main contactor to cut off power to the drive system. However, this possibility is not safety-relevant for the HEIDENHAIN safety design.

Standstill monitoring is not active in the STO safety function. The only exception is the following function:

- Test of the cut-out channels
  If the STO function is active only in the CC, the MC monitors the standstill position. Conversely, the CC monitors the standstill position if the STO function is active only in the MC.

Note

The safe torque off (STO) safety function must automatically switch off the machine control voltage (CVO) via –STO.A.G. Therefore, the –STO.A.G signal must be connected to the latch circuit of the machine control voltage via a relay contact.

Please refer to the basic circuit diagram from HEIDENHAIN. The line voltage of the machine is not switched off.

Danger

When the STO function is activated, the motor cannot generate a torque anymore. This can result in a hazardous movement, such as may occur with:

- Axes and spindles without mechanical motor holding brakes (coasting to a stop)
- Vertical and inclined axes without weight compensation
- Direct drives with low friction and self-retention
- External force on the drive axes
- The measures to be taken against external force (e.g. sagging of hanging axes) must be in accordance with Information Sheet No. 005 "Gravity-loaded axes (vertical axes)" issued by the engineering technical committee of the BGM (German Employer's Liability Association in the metal industry).

It is your duty as a machine tool builder to carry out a risk analysis and use it as a basis to minimize the risks by taking suitable measures.

4.8.10 Safe operating stop (SOS)

The SOS function provides protection against unexpected start-up of the drives.
In SOS, all feedback control functions (speed, position, etc.) are maintained. While the SOS function is active, control measures prevent the drive from performing hazardous movements resulting from faults.
After the SOS function has been deactivated, e.g. by closing a guard or by a start command, the machining motion of the drive can be restarted at the point of interruption.

When the SOS safety function is active, dual-channel standstill monitoring is performed by the MC and the CC.
Standstill is considered to be achieved if the spindle speed / axis feed rate falls below the following limit values:

- Spindle speed < 10 rpm
- Axis feed rate < 50 mm/min

If these limit values for spindle speed and axis feed rate are exceeded when the SOS function is active, the SS1 safety function is initiated.

If, however, the maximum permissible path defined in SMP545.x (limit value for standstill monitoring in [mm] or [°]) is exceeded while adhering to the limit values for the spindle speed and axis feed rate in SOS, the SS0 safety function is initiated.

In the safety-related SOM_1 operating mode, the SOS safety function becomes active when the guard door is opened.

Also, the nominal-actual value comparison of position values or speed values is performed via two channels if the SOS safety function is active.

In control systems without FS, the axes of an axis group were disconnected from power when the "axis group enabling (X150/X151 or MP4132) signal was reset (= 0). This was the only possibility of preventing any further axis motions. In systems with FS, you can ensure that the axes of an axis group are at a standstill without disconnecting the axes from power. You can monitor the axes for SOS instead—this is sufficient to ensure that they are at a standstill.

4.8.11 Safely limited speed (SLS)

The safely-limited speed safety function is active in all operating modes (except SOM_1) when the guard door is open. SLS monitors whether the drives exceed the specified speed limit values.

In the HEIDENHAIN safety design, the speed limit values are monitored via two channels by the MC and the CC, and a safe stop is initiated via SS1 if these values are exceeded.

Attention

- The speed limit values for the axes and spindle are defined in EN 12417:2007 for the various safety-related operating modes, and are stored in safe machine parameters in the HEIDENHAIN controls.
- The monitoring for SLS is always axis-specific. During interpolating movements (movements in which more than one axis is involved) the resulting contour speed of the tool center point or tool can assume higher values than the defined axis-specific limit values.
- The machine tool builder must enter the axis-specific speed limit values for SLS of the various safety-related operating modes in the SMPs such that the permissible speed limit values of the standard are not exceeded even when interpolating movements are executed. The resulting contour speed of the tool center point must not exceed the permissible speed limit values of the standard.

If the safely-limited speed (SLS) safety function is activated when the speeds are already above the speed limit values (e.g. by opening the guard doors), SS1 will be initiated immediately. Pressing the F LIMITED soft key enables you to open the guard doors without initiating an SS1 reaction.

If you press the F_LIMITED soft key, the maximum permissible speed of the axes and of the spindle is limited to the defined safely-limited speed. The limitation depends on the safe SOM_x operating mode selected by keylock switch. The speed of axes and spindles is reduced to the limit values for "safely limited speeds." If SOM_1 is active, the axes and spindles are brought to a stop, because only then will you be allowed to open the guard doors in SOM_1.

4.8.12 Safely limited position (SLP)

The safely-limited position safety function replaces the conventional hardware limit switches and is active in all operating modes.

Control measures ensure that an SS1 reaction is initiated if a defined absolute position limit value (SMP650.x and SMP670.x) is exceeded. This is done by a dual-channel comparison of the actual position to the position limit value. The associated limit values are stored in safe machine parameters.

Attention

- The technologically maximum possible overtravel of the axes must be taken into account when setting the absolute position limit values.
- The positive and negative absolute position limit values should be selected such that during traverse to these positions the standard software limit switches are reached first.

The first time the SLP safety function is initiated, the operator has the possibility of returning the axes to the permissible area after switching the machine back on.
If he uses this possibility and moves the axes in the wrong direction, the drives will be stopped via SS1. Then the drives cannot be moved until the limit values have been changed in the safe machine parameters.

The absolute position of the machine axes must be captured via two channels in order to ensure the safely-limited position (SLP) function:

- **Axis reference run**
  After switching on the control, the absolute position is determined by means of the "Traversing the reference marks" function.
  For example, for position encoders with distance-coded reference marks you must traverse two reference marks in order to determine the absolute value of the position, and for absolute encoders with EnDat interface the position value is read out when the control is switched on.
  In the "Traversing the reference mark" machine mode of operation, only one axis can be moved at any one time. If the control is in the Reference Run mode, and more than one NC axis or auxiliary axis whose associated axis groups are not in the AUTO or SOM_1 monitoring states are moving, then the SKERN initiates an SS2 for all axis groups that are not in AUTO or SOM_1.
  If the guard door is open, an automated reference run can only be executed by means of NC start and the permissive button or key.
  If the guard door is closed, the reference run can be executed both by means of NC start and directly by means of the axis-direction keys.
  As long as the axes have not been homed, it is not possible to traverse the axes in another machine mode of operation (such as Manual Operation or El. Handwheel).
  The absolute positions determined in this manner are compared to the last axis positions stored in the control. If a difference between the two values is found, the axes must be checked. If an axis that has not been checked is not in the "Traversing the reference marks" mode of operation, the axis can be moved only if the guard door is closed (independent of the active mode of operation).

- **Axis check**
  Checking the axes is also required when the machine is commissioned or, for example, after an encoder has been replaced. In addition, the axes must be checked if an SMP, or an MP with an indirect influence on the safety functions (e.g. MP960.x) has been changed. This is done by comparing the actual value display to the actual position of the machine axes. The end user is prompted to move the machine axes via soft key to a reference position defined by you. After checking the markings applied to the machine table and at fixed points, the end user must press the dual-channel permissive key (PB) of the machine operating panel to confirm that the reference position has actually been reached (end user's confirmation).
  If the guard door is open, the axes can only be checked automatedly by means of NC start.
  If the guard door is closed, the axes can be moved to the test position both by means of NC start and by means of the axis-direction keys. SOM_2, SOM_3 or SOM_4 must be active for checking the axis. In SOM_1 the axes cannot be checked.
  As a machine tool builder, you must establish the assignment of the position of the limit switches to the reference marks. In order to be able to verify this assignment, a marking for every axis must be applied to the machine table and the machine base at a clearly visible location. The marking corresponds to a certain reference position and must be entered in SMP646.x.

Attention

- The assignment of the axis position to the position of the limit switches is ensured only if the axes have been checked, i.e. the limit switches at the end of the traverse range (absolute position limit values) become effective only for checked axes.
- The safe operation of a machine requires that all axes have the "checked" status. The axis display must not show any axis marked by the warning symbol for "unchecked axis"!
- Axes must be checked only by trained personnel.

The positions of the axes are saved before the machine is shut down and are used as start positions after the machine is switched back on.
After the reference marks have been traversed or the absolute value has been read out, the SKERN compares the position determined in this manner to the respective position saved (in the MC and CC). If the deviation exceeds the value saved in machine parameter SMP642.x because, for example, an axis was moved manually while the control was inactive, the confirmation is requested again, as during commissioning. The "Check axis positions" prompt appears. After approaching the test position, the SKERN compares the currently determined position to the reference position in SMP646.x. The "Check axes" state cannot be left as long as the positions determined by the SKERN MC and SKERN CC deviate from the reference position in SMP646.x by more than the value in SMP642.x.

The machine parameters for defining the safe limit switches (SMP650.x, SMP670.x) are referenced to the machine datum. The machine datum is defined by the non-safe machine parameter MP960.x. Any changes made to MP960.x are assumed by functional safety after the control has been rebooted, and therefore affect the safe position limit values, which are shifted according to the changes made to MP960.x. If major changes are made to the value in MP960.x, this might lead to the position limit values being shifted to such that the safety of the machine is affected. In order to prevent the user from accidentally changing this value, a confirmation is requested, as during commissioning. If the user notices that the change might affect the safety of the machine, MP960.x must be reset to its original value. The actual value of the axis must match the actual position.

4.8.13 Safe brake control (SBC)

In the SBC safety function, axis-specific dual channel control of the existing motor holding brakes is carried out by the MC and CC. The SBC safety function is requested by the respective SKERN and must then be executed by the SPLC.

The existing mechanical motor holding brakes of axes and spindles are activated via two channels:

- After the request from the SKERN MC, the SPLC MC activates the brakes axis-specifically via the safety-related outputs –BRK_REL.A.x of the SPL and connected safety relays.
- After the request from the SKERN CC, the SPLC CC activates the brakes axis-specifically via the safety-related outputs –BRK_REL.B.x of the SPL and connected safety relays (if present), or
- The SKERN CC activates the brakes via –BRK.B.x if a corresponding inverter interface is present.
- See page 7–164 for the brake control block diagram.

In addition, all brakes are controlled collectively by the MC via the –STO.A.G signal.

Note

Hanging axes must be controlled axis-specifically. Do not combine them into a group of axes whose brakes are controlled collectively rather than individually.

The dual-channel controllability of the motor holding brakes is checked in the safety self-test. In addition, the holding torque of the brakes is tested.

The operation and testing of motor-holding brakes must be in accordance with Information Sheet No. 005 "Gravity-loaded axes (vertical axes)" issued by the engineering technical committee (BGM (German Employer's Liability Association in the metal industry)).

4.8.14 Safely limited increment (SLI)

With the current NC software version, the SLI safety function needs to be realized by the machine manufacturer via the SPLC program. However, the safety function does not monitor the increment itself, but rather the conditions for maintaining the movement. The increment is monitored by the normal NC software; there is no dual-channel monitoring by the SKERN for maintaining the increment.

The increment function is activated with the INCREMENT OFF/ON soft key. This opens an input window in which the user can enter the current increment. When an axis-direction key is pressed, the NC software moves the axis by the defined increment.

The SPLC program is to monitor the conditions for whether the axis movement may exceed the defined increment. The axis-direction key must remain pressed for maintaining the movement. While the axis-direction key is pressed, the axis is moved once by the defined increment and is then stopped automatically. If you want to move the axis by the increment again, you must release the axis-direction key and press it again. In addition, it might be necessary to press the permissive button or key, for example. The conditions to be monitored for maintaining the axis movement must be defined by the machine manufacturer. All necessary conditions must be monitored by the SPLC program. As soon as one of the conditions is no longer fulfilled (e.g. releasing the axis direction key), the SPLC program must initiate an SS2 reaction. Depending on the keylock switch, the respective SLS (safely limited speed) must be active during the increment function.

4.8.15 Nominal-actual value comparison

Depending on the active safety-related operating mode and the type of axis, position values or speed values are used in the nominal-actual value comparison:

	STO active	**SOM_1 active (guard door is closed)**	**SOM_2, SOM_3, SOM_4 active (guard door is open)**
NC axes, auxiliary axes	No nominal-actual value comparison	Comparison with speed values	Comparison with position values
Spindles	No nominal-actual value comparison	Comparison with speed values	Comparison with speed values

Danger

You must ensure that no continuous actual-to-nominal value transfer takes place through W1044 or PLC module 9145, since this would make fault detection through the nominal-actual value comparisons impossible.

4.8.16 Nominal-actual value comparison of position values

The nominal-actual value comparison of position values is active for all position-looped axes in all operating modes. This monitoring function is active only when the guard doors are open; however, no additional delay times for permissible deviations are active.

The maximum permissible deviation between the actual and nominal value can be set in SMP641.x. If the axes are intentionally operated with following error, this does not need to be taken into account in the parameterization of SMP641.x. The following error is automatically considered in position-value monitoring.
If the maximum permissible deviation is exceeded, an SS1 reaction is initiated.

The SKERN CC monitors the motor encoder (rotary encoder), and the SKERN MC monitors the position encoder (if present) or a specifically generated position value of the motor encoder.

4.8.17 Nominal-actual value comparison of speed values

The nominal-actual value comparison of speed values is always active for the speed-controlled axes, regardless of the selected safety-related operating mode or the status of the guard doors. This monitoring function is a plausibility check between the nominal value of the controller and the actual value of the encoder. This monitoring function is to ensure that, for example, a failure or confusion of encoders is detected.

The maximum permissible deviation between the actual and nominal value can be defined in SMP630.x for the axes, and in SMP631.x for the spindle. In SMP632.x or SMP633.x, you additionally define a time window within which the limit values are allowed to be exceeded. The actual speed value must be within the defined tolerance at least once within the time period defined in SMP632.x or SMP633.x. If it is, the time set in SMP632 or SMP633.x, respectively, restarts. If the actual value does not reach the permissible limit values within the time window, an SS1 reaction is initiated.

The monitoring for the deviation defined in SMP630.x is always active, but in SMP632.x and SMP633.x a time window is defined within which the actual speed value must be at least once within the tolerance defined for the nominal value. If this, for example, happens already after 0.5 seconds, the time in SMP632.x already restarts after 0.5 seconds.

The SKERN CC monitors the motor encoder (rotary encoder), and the SKERN MC monitors the position encoder (if present) or a specifically generated position value of the motor encoder.

4.8.18 Protection against unexpected start-up

The SKERN monitors the rotational speed of all axis and spindle motors to provide protection against unexpected start-up. If all motors of an axis group are at a standstill for more than 3 seconds, the safety-kernel software of the MC and the safety-kernel software of the CC initiate an axis-group-specific SS2 independently of each other.

The "Protection against unexpected start-up" safety function is active in the following machine modes of operation when the guard door is open:

- Program Run, Full Sequence operating mode
- Program Run, Single Block operating mode
- Positioning with Manual Data Input (MDI) operating mode

Note

Here are some instances in which the safety function triggers an SS2 reaction in the operating modes mentioned above:

- If the override potentiometer is turned down after the start of an NC block
- During long dwell times (e.g. programmed waiting times) > 3 seconds in an NC block
- Three seconds after the end or cancellation of an NC program, if the axes or spindle remain at a standstill

To prevent this automatic transition from SLS to SOS/STO (such as during very slow movements or for the tapping cycle, etc.), you have to press the permissive key on the machine operating panel. If the guard door is closed, there will be no transition to SOS/STO. This function only provides additional protection when the guard door is open. The same applies to the handwheel when the safety-related operating mode 4 (SOM_4) is active.

4.8.19 dv/dt monitoring of the braking processes

The dv/dt monitoring function performed by the SKERN ensures that there is no further increase in the speed of axes and spindles after an SS1 or SS1F has been initiated.

The dv/dt monitoring of axes verifies that the axes are not accelerated anymore after the waiting time defined in SMP530.x has expired. If a fault occurs, an axis-specific SS0 is initiated for the affected axis, and an SS1F for all other axes and spindles.

The dv/dt monitoring function does not respond if an axis coasts to a stop, e.g. after an SS0 reaction.

If the time defined in SMP525.x is exceeded during the deceleration process, an SS0 reaction is initiated.

dv/dt monitoring of the spindle is being introduced as a new safety function in service pack 05. The safety function monitors deceleration process of the spindle during an SS1 reaction. The waiting time for dv/dt monitoring of the spindle is permanently defined and cannot be configured via an SMP.

After an SS1 reaction has been initiated, the SKERN monitors the spindle speed to ensure that it continually decreases. Should the monitoring determine that the speed remains constant or even increases, an SS0 reaction is initiated for the spindle. SS1F is initiated for all other axes.

4.8.20 Response times, definitions, demand rates

The following data apply to stop reactions:

- Response times
  The data applies to all safety functions.
  - Response time of the SKERN:
    The corresponding stop reaction is initiated no later than two HSCI cycles (2 * 3 ms) after the fault has occurred.
  - Response time of the SPLC:
    The corresponding stop reaction is initiated no later than 22 HSCI cycles (22 * 3 ms = 2 * SPLC cycle + 2 * HSCI cycle; SPLC cycle = max. 30 ms, HSCI cycle = 3 ms) after the fault has occurred.
  - Response time of the CC:
    CC-CC communication
    Data is transmitted between the CCs at an interval of 3 ms. If the CC software detects a telegram to be faulty, a fault reaction is initiated within 4 * 3 ms.
  - The time until the axes come to a standstill after the stop reaction has been initiated must be added to the response time of the control. The times resulting from the corresponding MPs (e.g. acceleration) and the behavior of the CC (deceleration at the limit of current) must be used for this calculation.
  - HEIDENHAIN specifies a target value of 150 ms within which the axes must come to a standstill (finger protection).
- Definitions and monitoring ranges
  - Speed: SLS + 5 %
  - Absolute position: > SMP650 and < SMP670
  - Standstill of the axes: < 50 mm/min
  - Standstill of the spindle: < 10 rpm

Worst-case consideration of response times

Response times after initiation of emergency stop:

Time	Reactions of HSCI participants	**Signal involved**
t = 0	Emergency stop initiated via emergency stop button ES.SMOP on SMOP	–ES.A.SMOP = 0 –ES.B.SMOP = 0
t = 200 µs	Safe status bits of all HSCI participants are set correspondingly	–ES.A = 0 –ES.B = 0
	Reaction of MC	
Safe/Fastest reaction: t = 200 µs + 3 ms	The MC detects –ES.A = 0 and initiates an emergency stop reaction (SS1)	–ES.A = 0
t = 200 µs + 3 ms + reaction of CC	**"Normal" time** until switch-off by MC: The MC is informed about the switch-off of the CC through a message from the CC and initiates STO.A and SBC. After the SS1F reaction has been performed, the SKERN MC demands that the SPLC program activate the brakes and switch off the FS outputs (the machine manufacturer is responsible for the implementation).	At standstill the MC sets: –STO.A.x = 0, –BRK_REL.A.x = 0
t = 200 µs + 3 ms + time from SMPs	**"Maximum" time** until switch-off by MC: The time of the monitoring timers defined in SMP525.x for the SS1 reaction for axes, or in SMP526.x for the SS1 reaction for spindles is exceeded. The MC initiates STO.A and SBC. After the SS1F reaction has been performed, the SKERN MC requests the SPLC program to activate the brakes and to switch off the FS outputs (the machine manufacturer is responsible for the implementation).	At standstill the MC sets: –STO.A.x = 0, –BRK_REL.A.x = 0
	Reaction of CC	
Fastest reaction: t = 200 µs + 3 ms	The CC detects –ES.B = 0 in the safe state and initiates an emergency stop reaction (SS1). Deceleration process along the emergency braking ramp (MP2590).	–ES.B = 0

Time	Reactions of HSCI participants	**Signal involved**
t = 200 µs + 3 ms + max. 100 ms[a]	**"Normal" time** from the start of the SS1 reaction by the CC to the standstill of the axes	At standstill the CC sets: –BRK_REL.B.x = 0
t = 200 µs + 3 ms + max. 100 ms + MP2308	After the standstill of the axes and SBC, the CC initiates STO.B with a delay (by the time in MP2308). After the SS1F reaction has been performed, the SKERN CC requests the SPLC program to switch off the FS outputs (the machine manufacturer is responsible for the implementation).	The CC sets: –STO.B.x = 0
Safe reaction: t = 600 µs + 6 ms	The CC receives an HSCI telegram with information about –ES.B = 0 from the µC.B of the SMOP	–ES.B = 0
t = 600 µs + 6 ms + 3 ms	The CC detects –ES.B = 0 in the telegram and initiates an emergency stop reaction (SS1). Deceleration process along the emergency braking ramp (MP2590).	–ES.B = 0
t = 600 µs + 6 ms + 3 ms + max. 100 ms[a]	**"Normal" time** from the start of the SS1 reaction by the CC to the standstill of the axes	At standstill the CC sets: –BRK_REL.B.x = 0
t = 600 µs + 6 ms + 3 ms + max. 100 ms + MP2308	After the standstill of the axes and SBC, the CC initiates STO.B with a delay (by the time in MP2308). After the SS1F reaction has been performed, the SKERN CC requests the SPLC program to switch off the FS outputs (the machine manufacturer is responsible for the implementation).	The CC sets: –STO.B.x = 0
t = 600 µs + 6 ms + time from SMPs	**"Maximum" time** until switch-off by CC: The time of the monitoring timers defined in SMP525.x for the SS1 reaction for axes, or in SMP526.x for the SS1 reaction for spindles is exceeded. The CC initiates STO.B and SBC. After the SS1F reaction has been performed, the SKERN CC requests the SPLC program to switch off the FS outputs (the machine manufacturer is responsible for the implementation).	The CC sets: –STO.B.x = 0, –BRK_REL.B.x = 0

[a] Time that is assumed by HEIDENHAIN to be the maximum deceleration time for feed axes. An axis speed of 5 m/min and a braking acceleration of 1 m/s^2 were assumed.

Response times after opening the guard door at speeds > SLS:

Time	Reactions of HSCI participants	**Signal involved**
t = 0	Activation of SD guard door contacts at the SPL inputs	–SD.A.x = 0 –SD.B.x = 0
t = max. 22 ms	Capturing the signals of the SPL inputs of the µC.A and µC.B of the SPL via PICs.	–SD.A.x = 0 –SD.B.x = 0
Safe reaction: t = 22 ms + 6 ms	The MC and the CC receive an HSCI telegram with information about –SD.A.x = 0 from the µC.A and –SD.B.x = 0 from the µC.B of the SPL	–SD.A.x = 0 –SD.B.x = 0
	Reaction of MC	
t = 22 ms + 6 ms + 2*SPLC cycle	The SKERN of the MC receives information about the open guard door because the SLS axis-group status was set by the SPLC	
t = 22 ms + 6 ms + 2*SPLC cycle + 3 ms	The SKERN of the MC monitors for the SLS safety function and detects that the limit values have been exceeded: Initiation of SS1 stop reaction	
t = 22 ms + 6 ms + 2*SPLC cycle + 3 ms + cut-out time of CC	**"Normal" time** until switch-off by MC: The MC is informed about the switch-off of the CC through a message from the CC and initiates STO.A and SBC. After the SS1F reaction has been performed, the SKERN MC requests the SPLC program to activate the brakes and to switch off the FS outputs (the machine manufacturer is responsible for the implementation).	At standstill the MC sets: –STO.A.x = 0, –BRK_REL.A.x = 0
t = 22 ms + 6 ms + 2*SPLC cycle + 3 ms + time from SMPs	**"Maximum" time** until switch-off by MC: The time of the monitoring timers defined in SMP525.x for the SS1 reaction for axes, or in SMP526.x for the SS1 reaction for spindles is exceeded. The MC initiates STO.A and SBC. After the SS1F reaction has been performed, the SKERN MC requests the SPLC program to activate the brakes and to switch off the FS outputs (the machine manufacturer is responsible for the implementation).	At standstill the MC sets: –STO.A.x = 0, –BRK_REL.A.x = 0

Time	Reactions of HSCI participants	**Signal involved**
	Reaction of CC	
t = 22 ms + 6 ms + 1*SPLC cycle	The SKERN of the CC receives information about the open guard door because the SLS axis-group status is set by the SPLC	
t = 22 ms + 6 ms + 1*SPLC cycle + 3 ms	The SKERN of the CC monitors for the SLS safety function and detects that the limit values have been exceeded: Initiation of SS1 stop reaction. Deceleration process along the emergency braking ramp (MP2590).	
t = 22 ms + 6 ms + 1*SPLC cycle + 3 ms + max. 100 ms[a]	**"Normal" time** from the start of the SS1 reaction by the CC to the standstill of the axes.	At standstill the CC sets: –BRK_REL.B.x = 0
t = 22 ms + 6 ms + 1*SPLC cycle + 3 ms + max. 100 ms[a] + MP2308	After the standstill of the axes and SBC, the CC initiates STO.B with a delay (by the time in MP2308). After the SS1F reaction has been performed, the SKERN CC requests the SPLC program to switch off the FS outputs (the machine manufacturer is responsible for the implementation).	At standstill the CC sets: –STO.B.x = 0
t = 22 ms + 6 ms + 1*SPLC cycle + 3 ms + time from SMPs	**"Maximum" time** until switch-off by CC: The time of the monitoring timers defined in SMP525.x for the SS1 reaction for axes, or in SMP526.x for the SS1 reaction for spindles is exceeded. The CC initiates STO.B and SBC. After the SS1F reaction has been performed, the SKERN CC requests the SPLC program to switch off the FS outputs (the machine manufacturer is responsible for the implementation).	At standstill the CC sets: –STO.B.x = 0, –BRK_REL.B.x = 0

[a] Time that is assumed by HEIDENHAIN to be the maximum deceleration time for feed axes. An axis speed of 5 m/min and a braking acceleration of 1 m/s^2 were assumed.

4.8.21 Safe status bits

The safe status bits are transmitted to every HSCI participant via the HSCI telegram. The individual HSCI participants (MC, CC, SPL, SMOP) themselves can set the safe status bits, evaluate the received bits and react to them. The fault reactions defined for the individual safe status bits vary depending on the type of HSCI participant, see page 4–78.

Safe status bit	Signal	Meaning
0	–ES.A	Emergency stop channel A The control has initiated the SS1 alarm reaction.
1	–ES.B	Emergency stop channel B The control has initiated the SS1 alarm reaction.
2	–ES.A.HW	Emergency stop channel A, handwheel; no function in controls without functional safety. The control has initiated the SS1 alarm reaction.
3	–ES.B.HW	Emergency stop channel B, handwheel; no function in controls without functional safety. The control has initiated the SS1 alarm reaction.
4	–STO.A.MC.WD	Watchdog of MC software, switch-off of inverters, A channel (with functional safety: switch-off of FS outputs). The control has initiated the SS1 alarm reaction.
5	–STOS.A.MC	Spindle is switched off by the MC, A channel, STOS.A.G is initiated (CC: switch-off of spindle); no function in controls without functional safety.
6	–STO.B.CC.WD	Watchdog of CC software, switch-off of inverters, B channel The control has initiated the SS1F alarm reaction.
7	–SMC.A.WD	"Fast" watchdog of MC software; alarm on CC, which initiates the deceleration of the axes. The control has initiated the SS1 alarm reaction.
8	–SPL.WD	With FS: Multi-channel watchdog of SPL firmware (A/B channel); serious error of PL. Without FS: Single-channel watchdog of PL firmware. The control has initiated the SS1F alarm reaction.

Safe status bit	Signal	Meaning
9	–SMOP.WD	With FS: Multi-channel watchdog of SMOP firmware (A/B channel); serious error of MOP machine operating panel (SS1F). Without FS: Single-channel watchdog of MOP firmware (machine operating panel)
10	–PF.PS.AC	Power supply of inverter too low (parameterized LIFT OFF function in some cases).
11	–PF.PS.DC	DC-link voltage U_Z too low The control has initiated the SS1 alarm reaction.
12	–PF.BOARD	Fault in the supply voltage of the respective module. The control has initiated the SS1F alarm reaction.
13	–N0	Internal safe status bit The control has initiated the SS1 alarm reaction.
14	–REQ.SS2	The control has initiated the SS2 alarm reaction. Possible causes include: ■ Speed of MC fan or CC fan outside the tolerance ■ Temperature of MC, CC, UEC, UMC, PL or MB outside the tolerance ■ CC has detected an internal fault
15	–	Reserved

The following additional status bits are available for an external PL:

Safe status bit	Signal	Meaning
16	–SPL.A.WD	SPL watchdog, channel A
17	–SPL.B.WD	Only in controls with functional safety (FS): SPL watchdog, channel B
18	PGOOD.NC	Voltage monitoring of NC reports a fault
19	PGOOD.PLC	Voltage monitoring of PLC reports a fault
20	–INT	Internal interrupt
21..31	1	Reserved

The following additional status bits are available for an external MB machine operating panel:

Safe status bit	Signal	Meaning
16	–SMOP.A.WD	SMOP watchdog, channel A
17	–SMOP.B.WD	Only in controls with functional safety: SMOP watchdog, channel B
18	PGOOD.A	Voltage monitoring of channel A reports a fault
19	PGOOD.B	Voltage monitoring of channel B reports a fault
20	1	Reserved
21..31	1	Reserved

4.8.22 Fault reaction to safe status bits

An entry consisting of "- - -" in the following table means that the dual-channel outputs are not switched off based on the safe status bits. They are only switched off automatically if the control crashes, if an internal fault of the component occurs, or if there is a fault in the HSCI communication.

Note

The SPLC program must switch off the FS outputs.

The SKERN demands via the interface signal **`NN_GenOutputEnable`** that the SPLC program switch off the FS outputs in case of a fault, also see page 8–188.

Name	Evaluation and reaction			
	MC	CC	SPL	SMOP
- - -				
–REQ.SS2	SS2	SS2	- - -[e]	
–N0	- - -[d]	SS1	- - -[e]	
–PF.BOARD	SS1F	SS1F	Switch-off of FS outputs[c]	
–PF.PS.DC[a]	- - -[b]	SS1	- - -[e]	
–PF.PS.AC[a]	LIFT-OFF	LIFT-OFF	- - -[e]	
–SMOP.WD	SS1F	SS1F[f]	- - -[e]	Switch-off of FS outputs[c]
–SPL.WD	SS1F	SS1F[f]	Switch-off of FS outputs[c]	- - -[e]
–SMC.A.WD	SS1	SS1	- - -[e]	
–STO.B.CC.WD	SS1F	SS1F	- - -[e]	
–STOS.A.MC	- - -[d]	Detection (test)	- - -[e]	
–STO.A.MC.WD	SS1	SS1	- - -[e]	
–ES.B.HW	SS1[f]	SS1[f]	- - -[e]	
–ES.A.HW	SS1	SS1[f]	- - -[e]	
–ES.B	SS1f	SS1[f]	- - -[e]	
–ES.A	SS1	SS1[f]	- - -[e]	

[a] The evaluation of these signals and their reactions can be deactivated via a PLC module.

[b] If –PF.PS.DC is active, the watchdogs of the MC are not retriggered anymore. The other HSCI participants therefore detect the MC as being defective.

[c] The FS outputs are switched off automatically only on the HSCI participant on which the fault occurs (locally). Local fault detection by evaluating the internal fault bits (control crash, internal fault of the component, fault in the HSCI communication).

d. The outputs are not switched off based on the safe status bits. They are only switched off automatically if the control crashes, if an internal fault of the component occurs, or if there is a fault in the HSCI communication.
e. No reaction
f. Fast reaction, not relevant for safety. The CC receives safety-relevant information via the HSCI telegram.

4.8.23 Behavior when a fault is detected

General information

If an emergency stop or an error occurs, specific stop functions are used to bring all drives to a safe standstill as quickly as possible.

Once a stop function has been initiated it is always run in its entirety, even if the cause of its initiation is no longer applicable. This applies regardless of the Control Voltage ON (CVO) status. The machine cannot be restarted until the stop function and the associated braking reaction have been run in their entirety.
However, a stop reaction that has been initiated can be replaced by a higher-priority stop.

The cause of SS0/SS1F/SS1/SS2 reactions is displayed on the screen.

The stop reaction with the highest priority is the SS0 reaction, followed by SS1F and SS1. The SS2 stop reaction has the lowest priority. These stop functions can be initiated by every monitoring channel (MC/CC).

Stop reactions

Stop reactions are defined and divided into categories in EN 60204-1. The stop reactions and all further safety functions are described in detail under **Safety Functions** (see page 4–47). The table below shows the assignment of the stop reactions to the categories.

EN 60204-1	HEIDENHAIN	Priority
Category 0	Safe stop 0 (SS0)	Highest priority
Category 1	Safe stop 1F (SS1F)	
	Safe stop 1 (SS1)	
Category 2	Safe stop 2 (SS2)	Lowest priority

Safety function states

The safety functions are described in detail under **Safety Functions** (see page 4–47). The table below shows which safety function provides which safety level to the end user.

For the initiation of safety functions by the SPLC and SKERN, it always applies that the safety function providing the higher level of protection to the machine operator is active.

Safety function	Level
Safe torque off (STO)	Highest safety
Safe operating stop (SOS)	
Safely-limited speed (SLS)	Lowest safety

Restarting the drives after stop reactions

After **SS1F** or **SS0**
(i.e. the **STO** safety function is active), the restart of the drives can only be enabled by switching the main switch off and back on.
For safety reasons, switching the main switch back on leads to a new safety self-test.

> Danger
>
> There is an increased risk when the machine is switched on (booting), and especially when the drives are switched on. It must be ensured that there are no persons in the immediate danger zone!

If an **SS1** was initiated, the drives can be restarted by simply switching on the machine control voltage, without actuating the main switch. All logic functions of the machine are retained while the control voltage is switched off, and continue to run unimpeded.
An unexpected restart by resetting the emergency stop button is not possible, since the **safe torque off** (STO) operating status was initiated via two channels.

> Danger
>
> For large machine tools whose work zone cannot be fully seen, the use of an additional reset button in accordance with EN 954 or EN 13849 is compulsory.

The reset button must be situated outside the danger zone in a safe position from which there is good visibility for checking that no person is within the danger zone. Switching the machine back on by using Control Voltage ON (CVO) is not permissible until the reset button has been pressed. This functionality must be realized in the SPLC program.

After an **SS2** (SOS), a restart is possible without actuating the main switch and without switching on the machine control voltage.

4.8.24 Stop reactions depending on the fault situations

The following tables show which stop reactions, depending on the fault that occurred, are triggered by the MC or the CC:

Safe stop 0 (SS0)

Active state:	Fault situation:	SS0 reaction initiated by:
SOS	Axis is moving at < 50 mm/min, but the path from SMP545 has been exceeded	MC, CC (axis-specific)
SS1	Limit values for dv/dt monitoring according to SMP530.x during the SS1 reaction have been exceeded (alarm code of the CC: E240)	MC, CC (axis-specific)
SS1	Limit value for timer monitoring according to SMP525 or SMP526 during the SS1 reaction has been exceeded (alarm code of the CC: E200)	MC, CC (axis-specific)

Safe stop 1F (SS1F)

Active state:	Fault situation:	SS1F reaction initiated by:
NM (normal mode = normal operation)	SS0 reaction requested by the SPLC program	MC, CC
NM	Error while checking the watchdog counters	MC, CC
NM	Internal safety-relevant software error	MC
NM	One of the device-specific monitored voltages exceeds the defined limit values (signal –PF.BOARD)	MC, CC
NM	Monitoring detects that the voltages exceed or fall below the defined limit values	MC, CC
NM	Error during the "Axis checked" status comparison between the MC and CC	MC
NM	Fatal system error occurred	MC, CC
NM	Active safe status bit: –STO.B.CC.WD, –SPL.WD, –SMOP.WD and –PF.BOARD	MC, CC
NM	Error while monitoring the CRC checksums (applies to all CRC checksums)	MC, CC
Booting	Different types of axes assigned to the same axis group	MC, CC
NM	dv/dt monitoring responds for an axis or spindle, and SS0 is initiated for the respective axis. SS1F is initiated for all other drives.	MC, CC
NM	SSO has been requested for an axis group. As a result, SS1F follows for all other axis groups.	MC, CC
NM	SS1F has been requested for an axis group. As a result, SS1F also follows for all other axis groups.	MC, CC
NM	Invalid axis-group state	MC, CC
NM	Invalid stop reaction requested	MC, CC
NM	Invalid safety function requested	MC, CC
SOM_2, SOM_3	Operating mode switched to SOM_4 for an axis group	MC, CC
SOM_4	Operating mode switched to SOM_2 or SOM_3 for an axis group	MC, CC
NM	Axis group without spindle requests SLI for a spindle (= operating mode SOM_S requested)	MC, CC
NM	Spindle axis group requests SLI for axes	MC, CC
NM	Invalid SMP checksum	MC, CC
Booting	The motor shaft speed entered in or transferred for MP3210 is not between 0 and 100 [* 1000 rpm]	CC
Booting	The rated speed for gear ranges entered in or transferred for MP3510 is less than or equal to 0 rpm	CC
STO	SMP1054.x parameterized incorrectly (SMP = 0)	CC
NM	Watchdog WD.A.HSCI is reset	MC, CC or SPL

Safe stop 1 (SS1)

Active state:	Fault situation:	SS1 reaction initiated by:
STO	Test of the chain of normally-closed contacts before retriggering the MC watchdogs, to see whether all contacts are closed	MC
NM	Limit values for safely limited position (SLP) exceeded	MC, CC
NM	Limit values for safely limited increment (SLI) exceeded	MC, CC
NM	Limit values for amplitude monitoring exceeded	MC, CC
NM	Error reported by encoder-frequency monitoring	MC, CC
SS2	Limit values for path (SMP550.x) or time (SMP527.x, SMP528.x) exceeded during SS2 reaction	MC, CC
SOM_S	When the guard door is open: Limit value of < two revolutions (SLI) or speed of < 50 rpm (SLS) exceeded	MC, CC
SOM_2, SOM_3, SOM_4	When the guard door is open: Speed of the axes exceeds the respective limit values for SLS	MC, CC
SOM_2, SOM_3, SOM_4	When the guard door is open: Spindle shaft speed exceeds the respective limit values for SLS	MC, CC
SOM_2, SOM_3, SOM_4	SMPs for limit values for SLS parameterized incorrectly (SMP = 0)	CC
NM	Emergency stop initiated via one of the emergency stop buttons	MC, CC
NM	Internal emergency stop initiated via the SKERN (e.g. by IPO, CC)	MC, CC
NM	Error during nominal-actual value monitoring with position or speed values	MC, CC
NM	Error while performing forced dynamic sampling	MC, CC
SOS	Limit values for the safe operating stop SOS exceeded: Axis movements > 50 mm/min or > 10 rpm	MC, CC
NM	Bit 0 of SMP560 is not set to enable SOM_4 when that operating mode is switched to	MC, CC
NM	Error found during cross-comparison	MC, CC
NM	Active safe status bit: –SMC.A.WD, –STO.A.MC.WD, –ES.A.x, –ES.B.x, –PF.PS.DC and –N0 (–N0 and –PF.PS.DC only CC reaction)	MC, CC
SOM_1	Moving a safe axis with open guard door	MC, CC
NM	SS1 reaction initiated by the SPLC program	MC, CC

Safe stop 2 (SS2)

Active state:		SS2 reaction initiated by:
NM	The temperature exceeded or fell below the limit values	MC, CC
NM	The fan speed fell below the limit values	MC, CC
SOM_2, SOM_3, SOM_4	No valid permissive button or key active for switching on the spindle while NC program is running	MC, CC
SOM_2	Number of axes permitted to move in SOM_2 exceeded. Only one axis may be moved.	MC, CC
SOM_3, SOM_4	Number of axes permitted to be moved by the handwheel (e.g. with axis-direction keys) exceeded. Only one axis may be moved if SMP560 bit 9 = 0.	MC, CC
NM	Maximum time in SMP511 for performing the safety self-test (with open guard door) exceeded	MC, CC
SLS	Protection against unexpected start-up becomes active (switches to SOS state)	MC, CC
SOM_2, SOM_3	No valid permissive button or key, or permissive button or key released during movement	MC, CC
SOM_2, SOM_3, SOM_4	NC stop or spindle stop key is pressed, and the SPLC program requests an SS2 reaction	MC, CC
SOM_2, SOM_3, SOM_4	Axis-direction key was released during movement	MC, CC
SOM_2, SOM_3, SOM_4	Spindle jog key released while spindle was active	MC, CC
SOM_2, SOM_3, SOM_4	Switch between machine operating modes (e.g. from El. Handwheel to Manual Operation mode)	MC, CC
NM	Active safe status bit –REQ.SS2	MC, CC
NM	Untested axis moved	MC, CC
NM	SS2 reaction initiated by the SPLC program	MC, CC

Reaction upon errors during the safety self-test (SSt)

Active state:	Fault situation:	Reaction upon error:
STO	Illegal start of the SSt by the PLC: Guard doors not closed	MC, CC wait
STO	Illegal start of the SSt by the PLC: Not all drives had been switched off by the MC after the brake test before the SSt (alarm code of the CC: C037)	SS1F initiated by CC
STO	Emergency-stop circuit not closed	MC, CC wait
STO	Request that the chain of normally-closed contacts is not closed (alarm code of the CC: E001)	SS1F initiated by MC, CC
STO	Request that the chain of normally-closed contacts is not open (alarm code of the CC: E001)	SS1F initiated by MC, CC
STO	The guard doors are not closed during the safety self-test	MC, CC wait
STO	CVO key active before such a request is placed. The message "Switch off external dc voltage" is displayed.	MC waits
STO	CVO key is not pressed after "Switch on external dc voltage" prompt	MC, CC wait
SOS	During the SSt, SOS is active on the MC and CC, unless you activate STO for test purposes. If SOS is active, then a safe operating stop is watched for. However, only the path is monitored, but not the speeds.	SS0 initiated by MC, CC
STO	MC does not test the motor brake control although the parameter setting requires it	SS1F initiated by CC
STO	Error during test of motor brake control	SS1F initiated by MC
NM	Limit values for the safe operating stop (SOS) exceeded during test of motor brake control	MC requires that a safe position be moved to
STO	No machine operating key may be pressed	MC, CC wait
STO	Error while switching on all spindle power modules via a global signal. The power modules do not report readiness within 10 seconds.	SS1F initiated by MC, CC
STO	Error while switching on all axis power modules via a global signal. The power modules do not report readiness within 10 seconds.	SS1F initiated by MC, CC
STO	Error while switching off all spindle power modules via a global signal STOS.AG. The power modules are still ready although the time in SMP2172 has expired.	SS1F initiated by MC, CC

STO	Error while switching off all axis power modules via a global signal STO.AG. The power modules are still ready although the time in SMP2172 has expired.	SS1F initiated by MC, CC
STO	Error during axis-specific switch-on of the power modules. The power modules do not report readiness within 10 seconds.	SS1F initiated by MC, CC
STO	Error during axis-specific switch-off of the power modules via STO.A.x and STO.B.x. The power modules are still ready although the time in SMP2172 has expired.	SS1F initiated by MC, CC
STO	Error while checking the internal watchdogs during the self-test	SS1F initiated by MC, CC; MC aborts SSt

4.9 Special Features of Software Version 606 42x-01

The first software versions for functional safety of the iTNC 530 HSCI do not include the full range of features necessary to provide functional safety for all machine models.

Note

Before planning a machine with functional safety, please inform yourself of whether the current scope of functional safety features suffices for your machine design.

Your contact person at HEIDENHAIN will be glad to answer any questions concerning the iTNC 530 HSCI with functional safety.

The current constraints and specifics are listed below:

Switching of safe machine parameters (SMPs)

For reasons of safety, safe machine parameters cannot be switched or changed without entering the OEM password. The changes do not become active until the OEM password has been entered. Also, if safe machine parameters are changed, a partial acceptance test is required. This mechanism in software version 606 42x-01 prevents you from switching between different parameter sets of safe machine parameters. This mechanism has the following consequences:

- Exchanging axes while the PWM output remains the same is not possible
- Interchangeable heads cannot be realized at present

It is possible, however, to create a parameter set for a maximum configuration of the machine. Axes can then be activated or deactivated via MP10. This is possible without the OEM password, but it requires rebooting the control and checking the switched axis (axes) again. This means that the deactivation/activation of optional axes or indexing fixtures is possible. Save the maximum configuration in the safe machine parameters. Then use MP10 to switch the axes.

Master-slave-torque and gantry modes

In software 606 42x-01, only the master axis can be configured as a safe axis. The slave axis must be configured as a non-safe axis. As a result, all safety functions for axis monitoring are active only for the master axis.

Switch-off
The master axis is switched off via two channels (by the SKERN MC and SKERN CC). The slave axis is switched off once by the SKERN MC (STO.A.x signal), and also through the standard functions of the NC software in the MC and CC. The CC also uses the STO.B.x PWM interface signal.

Brake test
See "Brake test for synchronized axes" on page 7 – 168

Master-slave operation is nevertheless possible, depending on the machine design. The machine tool builder is responsible for the implementation.

This absolutely requires that the master axis and the slave axis be firmly connected with each other via a mechanical connection. All movements of the slave axis must always affect the master axis. Problems of the slave axis (such as axis "runaway") can then be detected by the FS monitoring functions of the master axis as long as the master axis is not in the STO state. No safe monitoring functions are active while the STO safety function is active. In the STO state, movements of the slave are detected by the normal NC software (e.g. following-error monitoring of the master), and not by functional safety.

Note

The machine tool builder's risk analysis of the master-slave axes must ensure that the master axis and the slave axis are mechanically firmly connected with each other, and that the motor holding brake of the master axis suffices as motor holding brake for the synchronized axes.

The risk analysis of the synchronized master-slave axes must prove whether this type of master-slave operation is sufficient for the safety design of the machine.

C-axis operation

This version of the FS software does not yet support safe C-axis operation. It is not possible to operate an axis and a spindle alternately with a common drive.

Traverse ranges

Switching the traverse range with MP100.x does not affect functional safety. Machine parameter MP100.x is used to operate axes alternately as NC or PLC axes. The SKERN derives this axis status solely from the entry in MP100.0. The indices of MP100.x can only be used to switch the standard functions of the NC software. For the SKERN the configuration in MP100.0 remains decisive. In software version 606 42x-01, the safety-related examination of the axes is inextricably linked to MP100.0. Therefore, the safety-related examination of an axis always remains the same. PLC axes are sometimes subject to more stringent safety requirements (e.g. movement possible only in connection with permissive button or key).

Safe traverse-range switchover with MP100.x is not possible if software version 606 42x-01 is being used.

Alternating table operation

Here, you must first remember the constraints regarding the ranges of traverse. For alternating table operation, an axis (e.g. two rotary tables as "A axis" and "a axis", respectively) must usually be operated alternately as NC axis and PLC axis. This switchover is still possible for the NC software, but not for the safety-related examination of the axis. Also, in functional safety, this axis must be defined in a separate axis group. As a result, for example, the axes X, Y, Z must be configured in an axis group for NC axes, and the two rotary tables (A axes) must also each be defined in a separate axis group. This results in three axis groups.

This leads to a problem if the axis group of the NC axes and one of the two A-axis groups are to be interpolated and moved together. The problem is caused by the "Protection against unexpected start-up" safety function.

The "Protection against unexpected start-up" function sets an axis group consisting of axes to the SOS status, and an axis group consisting of spindles to the STO status (as a result of an SS2 reaction, configurable via SMP549.x) if the axes/spindles of this axis group are not moved for more than three seconds. Once the axes of this axis group are in the STO state, this state cannot be left automatically anymore.

The NC axes and the A axis are in two separate axis groups. In an NC program it is not unusual that especially the A axis is at a standstill for more than three seconds, and this results in the "Protection against unexpected start-up" function becoming active. Later in NC program run, however, the A axis should be moved again, which is then no longer possible. The same problem occurs with an SS2 reaction (deceleration along the contour). In this case, standstill monitoring may prevent you from moving up to the end of the contour.

Version 606 42x-01 of the FS software does not support alternating table operation if the different axis groups are to be interpolated and moved together.

EnDat 2.2

Version 606 42x-01 of the FS software does not support EnDat 2.2 encoders. This applies to all EnDat 2.2 encoders with or without functional safety (FS).

Non-HEIDENHAIN inverters

The use of modules from Siemens' SIMODRIVE 611 power module product family or other non-HEIDENHAIN inverters has not been approved for the integrated functional safety!

Spindles with gear ranges

Spindles with gear ranges and only one motor encoder (single-encoder system) are not supported. Spindles with a gear ratio (one or more than one gear range) can be used as safe spindles only if they have a motor encoder and a position encoder. The position encoder must be mounted behind the gearbox or the transmission so that it returns the actual speed of the spindle, i.e. of the tool.

Variable gear ratio

Safe axes with a variable gear ratio in MP1054.x (distance per motor revolution) cannot be operated with software version 606 42x-01. A variable gear ratio is a formula in MP1054.x, which does not provide a constant factor as the result.

4.10 Requirements the Application Must Meet

The machine tool builder uses the basic circuit diagrams as a basis for wiring. This is a non-binding proposal, and must be adapted by the customer to the requirements of the machine that he uses. The machine tool builder is autonomously responsible for adhering to the relevant standards and safety regulations.

It is imperative that the following requirements be fulfilled:

- The normally closed contacts of all relays with safety-relevant functions must be wired to the chain of normally closed contacts. The chains of normally closed contacts are checked when the control is switched on.
- The brakes must be controlled via two channels. In the HEIDENHAIN design this occurs by switching off the motor holding brakes via two channels.
- The temporal demands placed on the safety functions must be checked on the machine and documented.
- A comprehensive test of all safety-relevant functions must be performed before commissioning. The results of this functional test must be documented.
- The safety self-test, including the test of the motor brakes and motor brake control, must be repeated within no more than 168 hours.
- For each specific machine, a calculation of the safety characteristic numbers is to be performed in accordance with ISO 13849-1 for all components used, including external safety components.
- When installing and operating HEIDENHAIN components, please refer to the Technical Manual of the respective control as well as to the "Inverter Systems and Motors" Technical Manual.

Encoders

The following encoder configurations can be used on HEIDENHAIN control systems with functional safety in order to monitor safe axes:

- Two-encoder systems (speed and position encoders) with analog encoder signals (1 V_{PP}, EnDat 2.1)
- Single-encoder systems (speed encoder) with analog encoder signals (1 V_{PP}, EnDat 2.1)
- Single-encoder systems (speed encoder) with certified EnDat 2.2 FS encoder (as soon as these are supported)
- Two-encoder systems (speed and position encoders) with EnDat 2.2 encoders without certified encoder or with certified EnDat 2.2 FS encoder (as soon as these are supported)

Danger

External devices used in safety functions of the control must meet the following requirements:

- **Safety contactor combinations (SCC) or corresponding devices**
  Only devices that correspond to EN ISO 13849-1 Category 3, Performance Level d or EN 61508 SIL 2 may be used as safety contactor combinations (SCC) or corresponding devices (e.g. safety-relevant PLC).
- **Safety relays**
  Only devices that correspond to EN ISO 13849-1 Category 3, Performance Level d and EN 61508 SIL 2 and have a positively-driven normally closed relay contact may be used as safety relays.
- **Encoders**
  The control system with FS performs plausibility checks in order to detect faults in encoders. However, the plausibility checks can detect faults only if the drive moves. But, in the SOS safety function, the drive is kept in its current position, and there is no movement. If the connection between the drive and the encoder loosens at this point in time, this fault cannot be detected by the control system.
  For safe axes/spindles with a single-encoder system, this results in the following requirement for the encoder used:
  Use only encoders for which the loosening of the connection between the drive and encoder at standstill is ruled out. The encoder manufacturer must be able to exclude the "loosening of the mechanical coupling" fault for the chosen encoder. The "mechanical coupling" characteristic value provides information on the "loosening of the mechanical connection" fault.
  Dual-encoder systems and non-safe axes/spindles are not affected by this requirement.

4.11 Remaining Risks

Please keep the following in mind in addition to the information given in chapter (2–14) 2:

- If the machine is switched off via the main switch and wired as suggested in the basic circuit diagram, the main contactor of the UV(R) power supply unit is switched off through the leading main-switch contact. This results in the immediate switch-off of the PWM pulses to the inverters. The torque is removed from the axes and spindles, and the available holding brakes of the drives are activated at the same time. The delay times caused by the wiring and the brake relays can lead to a a slight sagging of hanging axes until the holding brakes engage.
  This causes a problem only if the machine is switched off via the main switch while the drives are in closed-loop control.
- If an inverter is defective, in rare cases this can lead to the drives being no longer controlled. The torque is removed from the axes and spindles. The delay times until the detection of the failure can lead to a a slight sagging of hanging axes until the holding brakes engage.
  This causes a problem only if the defect occurs while the drives are in closed-loop control.

5 Safety-Related MPs and Signals

5.1 Safety-Related Machine Parameters (SMPs)

A machine parameter is safety-relevant if it has an effect on the safety-related software, and therefore on the safety of the machine. SMPs are firmly linked with the safety-related software. They are monitored via a checksum and can be changed only after entering a separate code number and the OEM password (see page 5–99).

The input values of the safe machine parameters are defined and entered during commissioning of the machine.

The safe machine parameters are protected from unauthorized changes to ensure that the safety of the machine is not endangered. For this purpose, a machine parameter file (*.mpl) containing the machine parameters to be protected is defined in the **PLC:\OEM.SYS** file using the **MPLOCKFILE = ...** keyword. These parameters are specified in the same way as in a normal machine parameter file, except that no values are assigned.

The MPLOCKFILE indicates the MPs that require the corresponding code number in order to be edited. The machine tool builder can add any number of MPs to the MPLOCKFILE in order to protect them from being changed by the end user. MPs that have been added by the OEM can be edited without entering the OEM password.

However, only the SMPs that have been defined as such by HEIDENHAIN are used for generating the checksum for SMPs. This is an internal list of machine parameters that cannot be edited by the machine tool builder. You will find a list of these machine parameters on page 5–99 ff. If one of these MPs is changed, the control reboots. The OEM password must be entered for the new machine parameter value to go into effect. Then a partial acceptance test must be performed.

Danger

- The machine parameter file for SMPs, *.MPL ("MPLOCKFILE"), must be activated in the OEM.SYS file.
- The machine tool builder is autonomously responsible for any changes to the *.MPL file ("MPLOCKFILE").
  Changes can lead to the loss of safety!

After entering the code number 95148 or in the **Machine parameter programming** mode of operation, you can only edit the machine parameters that are not contained in the **MPLOCKFILE** file. Safety-related controls from HEIDENHAIN contain the default entry **MPLOCKFILE = PLC\mp\SGMP.MPL** in the **OEM.SYS** file. This **MPLOCKFILE** contains all machine parameters that are relevant for the safety of the machine, and can have any desired name. The file extension *.mpl is important, however. SMPs are indicated by color in the MP editor.

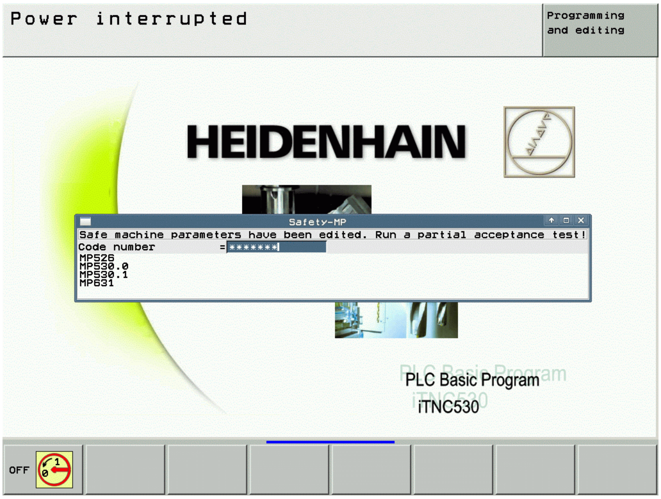
The following code numbers and the OEM password control the access rights to MPs and SMPs in the iTNC 530:

- **Entry of the code number 95148 or 984651 if no MPLOCKFILE is present**
  Reading and editing of all machine parameters. Since there is no **MPLOCKFILE**, there are no SMPs. The code number 95148 or 984651 can be changed using the token **MPPASSWORD** in the OEM.SYS file. After that, the code number 95148 or 984651 only gives you read access to the MP file.
- **Entry of code number 95148 if MPLOCKFILE is present**
  Reading and editing of all machine parameters that are not listed in **MPLOCKFILE**. The machine parameters of **MPLOCKFILE** can only be read, not edited. This code number cannot be changed if **MPLOCKFILE** is present, and is therefore always valid.
- **Entry of code number 984651 and MPPASSWORD if MPLOCKFILE is present**
  Reading and editing of all machine parameters and safety-related machine parameters (MPs in **MPLOCKFILE**). After the control has been rebooted, any changes to the SMPs must be confirmed by entering the OEM password. You can change this code number by means of the keyword **MPPASSWORD =** in the **OEM.SYS** file to protect the machine parameters of **MPLOCKFILE** from unauthorized changes. This renders 984651 invalid for the changing of MPs. After that, the code number 984651 will only give you read access to the machine parameters of **MPLOCKFILE**.
- **OEM password 5038167 and SGMPCHANGE**
  After SMPs have been edited and the control has been rebooted, the OEM password must be entered to confirm the changes.
  You must change this OEM password by means of the keyword **SGMPCHANGE =** in the **OEM.SYS** file to protect the SMPs from unauthorized changes! This will render 5038167 invalid.

> Danger
>
> The password 5038167 must be changed during commissioning of the machine in order to protect the machine parameters of **MPLOCKFILE** and the SMPs from unauthorized changes!

The message **Safe machine parameters have been edited. Run a partial acceptance test!** can appear if an acceptance test of the machine parameters has already been performed (i.e. a valid checksum is stored), but one or more than one SMP was changed later on.

This message displays a list of the SMPs that have been changed. Use this list to check whether the safe machine parameters contained are those safe machine parameters you changed deliberately. For the changes to go into effect, enter the OEM password.



```
Power interrupted
```

```
Safety-MP
Safe machine parameters have been edited. Run a partial acceptance test!
Code number          =*******
MP526
MP530.0
MP530.1
MP631
```

Danger

Only the machine tool builder is permitted to load edited SMPs by entering the OEM password that is known to him (e.g. for optimizing the MPs). Changing any SMPs necessitates a partial acceptance test!

The end user cannot put the control fully into service after changing SMPs, because he does not know the OEM password. If an incorrect password is entered or password entry is canceled, the control returns to the Power Interrupted state.

The following procedure is used to edit SMPs:

The (edited) SMP parameter set is transmitted to the SKERN. The SKERN compares the checksum of the new SMP parameter set with the checksum saved for the last valid SMP parameter set (= reference SMP parameter set).
If the checksum is the same, the control goes into normal operation.
If the checksum has changed, you are prompted by a dialog to perform a partial or complete acceptance test. You must confirm this by entering the OEM password and pressing the permissive key.

Then the SKERN checks for all SMPs whether an SMP has changed compared to its reference SMP parameter set. Each comparison is used to create a list of SMPs that require a partial acceptance test to be performed. After the PLC and the SPLC have been started, the SKERN prompts you to confirm for every SMP in the list of edited SMPs that you will perform a partial acceptance test for this SMP. To confirm the prompt, press the permissive key. After all SMPs in the list have been confirmed, the new checksum of the edited SMPs is loaded and saved in non-volatile memory.

Note

You must perform the partial or complete acceptance test as prompted by the control!

If an SMP has been edited and the OEM password is not available, the SMPs can be corrected to the original value in the **Programming and Editing** mode of operation by pressing the **MOD** soft key and then entering the code number 984651 or, if applicable, by using the password defined in **OEM.SYS > MPPASSWORD= ...**. There is also the possibility of using the code number to reimport and reactivate an SMP set (from the manufacturer) matching the checksum via the file system (with the **PGM MGT** soft key). Changes made to machine parameters in the meantime by the end user, however, will be lost during this process.

The (S)MP set defined by you during commissioning of the machine must be supplied together with the machine when the machine is shipped.
Start-up of the control is successful only if the active SMPs match a checksum saved in the control.

Danger

- Operator protection must be the most important criterion in defining the SMP values. Therefore, the parameterizable tolerances, limit values and delay times must be determined during commissioning depending on the requirements of the machine, and must be optimized regarding operator protection.
- After the acceptance test, you must remove all invalid (old) machine parameter files from the hard disk (so as to avoid old data from being confused with new data).
  The current data that corresponds to the acceptance test must be saved.

Safe machine parameters

SMP (iTNC 530): SMP511

Description: Time until the safety self-test. A test of the HEIDENHAIN control components must be performed after no more than 168 hours.

Input: 1 to 10080 [min]
Default value: 10080 minutes = 168 hours

SMP (iTNC 530): SMP525.x

Description: Default time for stopping the axes along the emergency braking ramp upon SS1 reaction (axis-specific)

Input: 0.000 to 10.000 [s]
Default value: 1 [s]

SMP (iTNC 530): SMP526.x

Description: Default time for stopping the spindles along the emergency braking ramp upon SS1 reaction (axis-specific)

Input: 0.000 to 10.000 [s]
Default value: 1 [s]

SMP (iTNC 530): SMP527.x

Description: Default time for controlled stopping of the axes upon SS2 reaction (axis-specific)

Input: 0.000 to 10.000 [s]
Default value: 1 [s]

SMP (iTNC 530): SMP528.x

Description: Default time for controlled stopping of the spindles upon SS2 reaction (axis-specific)

Input: 0.000 to 10.000 [s]
Default value: 1 [s]

SMP (iTNC 530): SMP530.x

Description: Delay time for dv/dt monitoring

Input: 0.000 to 10.000 [s]
Default value: 0.030 [s]

SMP (iTNC 530): SMP535.x

Description: Run times of the max. 16 timers for the SPLC program

Input: 0.0 to 1 000 000.0 [s]
Default value: 0 [s]

SMP (iTNC 530): SMP540.x

Description: Limit value for the "safely limited speed" (SLS) of the axes in safe operating mode 3 (SOM_3)

Input: 0 to 5000 [mm/min] or [°/min]
Default value: 2000 [mm/min] or [°/min]

SMP (iTNC 530): SMP541

Description: Limit value for the "safely limited speed" (SLS) of the spindle in safe operating mode 3 (SOM_3); MP560=0

Input: 0 to 6000 [rpm]
Default value: 500 [rpm]

Attention

The speed limit values for the axes and spindle are defined in EN 12417:2007 for the different safety-related operating modes.

SMP (iTNC 530): SMP545.x

Description: Axis-specific limit value for standstill monitoring in SOS state

Input: 0.001 to 30.000 [mm] or [°]
Default value: 0.500 [mm] or [°]

SMP (iTNC 530): SMP547.x

Description: Axis-specific limit value for safely limited increment

Input: 0.001 to 10.000 [mm] or [°]
Default value: 2.000 [mm] or [°]

SMP (iTNC 530): SMP549.x

Description: Axis-specific configuration defining whether the spindle (like the axes) is to be switched to SOS instead of STO upon SS2 reaction (used for lathes). Only active via spindle stop key.

Input: 0: Default (spindle in STO, axes in SOS)
1: Axes and spindles in STO upon SS2
2: Axes and spindles in SOS upon SS2
Default value: 0

SMP (iTNC 530): SMP550.x

Description: Axis-specific limit value for maximum permissible path upon SS2 reaction.

Input: 0.0010 to 100.0000 [mm] or [°]
Default value: 0.500 [mm] or [°]

SMP (iTNC 530): SMP551.x

Description: Limit value for the "safely limited speed (SLS)" spindle speed in safe operating mode 4 (SOM_4);
(MP560 bit 0=1 and code number).

Input: 0 to 6000 [rpm]
Default value: 500 [rpm]

SMP (iTNC 530):	SMP552.x
Description:	Limit value for the "safely limited speed (SLS)" axis feed rate in safe operating mode 4 (SOM_4); (MP560 bit 0=1 and code number).
Input:	0 to 5000 [mm/min] Default value: 2000 [mm/min]

Attention

The speed limit values for the axes and spindles are defined in EN 12417:2007 for the various safety-related operating modes.

SMP (iTNC 530):	SMP555.x
Description:	Display mode for rotary axes. The modulo value must be entered for the respective axis in MP810.x, too.
Input:	0.0000 to 99 999.9999 [°] 0 = no modulo display (software limit switches active) Value = modulo value (software limit switches inactive)

Danger

The machine tool builder is autonomously responsible for activating additional functions via **machine parameter MP560**!
If bits are set in **MP560** (bit x=1), and therefore additional functions become active, the safety of the machine no longer complies with the requirements of **EN 12417**!
The safety functions comply with **EN 12417** only if all additional functions of MP560 are deactivated (bit x = 0)!

The following dangers require special awareness:

Increased risk in safe operating mode 4 (SOM_4) (MP560, bit 0):
Higher spindle speeds and feed rates are possible.
The permissive button or key must be pressed only for spindle start, after that the spindle runs without the permissive button or key being held down.
There is a risk of injury by accidental contact with the spindle!
The machine tool builder must check whether this special mode can be permitted for machine operation.

Danger during self-test with open guard doors (MP560, bit 1):
If the commutation angle is measured incorrectly after power ON, there is a risk of rapid and uncontrolled axis movements during the first drive enabling (motor is uncontrollable).
If the guard door is open, the operator may suffer injuries from flying parts!

Danger during brake test with open guard doors (MP560, bit 1):
The sagging of hanging axes cannot be ruled out.
If the guard door is open, the operator may suffer injuries (crushing hazard / danger of collision)!

Unexpected start-up resulting from closing the guard door (MP560, bit 2):
Closing the guard door can lead to an unexpected start-up. The requirements of EN ISO 12100-2 must be complied with.
EN 12417 does not permit an unexpected start-up!

Potential loss of dual-channel controllability of motor holding brakes due to deactivation of brake control test / short-circuit test (MP560, bit 3):
Malfunction of the motor holding brake is detected too late.
The sagging of hanging axes cannot be ruled out.

Potential loss of safety due to deactivation of self-test (MP560, bit 4):
The maximum time for testing the cutout channels can be exceeded.
If a fault has caused the failure of the cutout channel during this time period, this will not be detected.

SMP (iTNC 530): SMP560.x

Description: The machine tool builder is autonomously responsible for additional functions.

Input: %xxxxx

SMP (iTNC 530): SMP560 bit 0

Description: 1 = Enabling of safe operating mode 4 (SOM_4); Permissive key of MB only required for spindle or NC start. Also, max. spindle speed (MP551.x) and max. axis feed rates (MP552.x) can be set separately for SOM_4.

Warning:
Increased risk in safe operating mode 4 (SOM_4): Higher spindle speeds and feed rates are possible. Permissive button or key must be pressed for spindle start. The machine tool builder must check whether operating mode 4 can be permitted for machine operation.

SMP (iTNC 530): SMP560 bit 1

Description: 1 = During the safety self-test the guard doors do not need to be closed.

SMP (iTNC 530): SMP560 bit 2 - not in software version 606 42x-01

Description: 1 = NC start is possible via the PLC by closing the axis/ spindle guard door after external stop state and S=0.

Warning:
Unexpected start-up resulting from closing the guard door. The requirements of EN ISO 12100-2 must be complied with!

SMP (iTNC 530): SMP560 bit 3

Description: 1 = The brake control test is not performed (see page 7–164)

SMP (iTNC 530): SMP560 bit 4 - not in software version 606 42x-01

Description: 1 = No stop2 reaction when the time from MP511 (time by which cutout channel test must be run) has expired, the test has not been run and the guard door T is opened.

SMP (iTNC 530): SMP560 bit 5 - not in software version 606 42x-01

Description: 1 = Measurement of current is inactive during safety self-test

SMP (iTNC 530): SMP560 bit 6

Description: 1 = Test of axis-specific switch-off via PWM output STO.B.x is not possible (two axes on one interface PCB with OR gate). All axes are switched off collectively at the same time.

SMP (iTNC 530): SMP560 bit 7 - not in software version 606 42x-01

Description: 1 = Permissive button of handwheel is only required for spindle start or NC start in operating mode 4 (SOM_4). The permissive button on the handwheel does not need to be held down continuously. This means the behavior is the same as on the machine operating panel. Only possible if operating mode 4 is active (bit 0 = 1).

SMP (iTNC 530): SMP560 bit 8

Description: 1 = There is no wiring of –STO.A.G and –STOS.A.G to the safety relays in the power modules. Switch-off of the power modules over the signals –STO.A.G and –STOS.A.G is not checked in the safety self-test.

SMP (iTNC 530): SMP560 bit 9 - not in software version 606 42x-01

Description: 1 = In the El. Handwheel mode of operation the simultaneous movement of several axes is permitted, e.g. for compensation movements (only relevant in SOM_3, SOM_4).

SMP (iTNC 530): SMP560 bit 10- not in software version 606 42x-01

Description: Reserved for future functions

SMP (iTNC 530): SMP560 bit 11—dv/dt monitoring of the spindle during SS1 reaction

Description: 1 = dv/dt monitoring of the spindle during SS1 reaction not active. Only for commissioning purposes! Monitoring must be reactivated after commissioning (bit 11 = 0).

SMP (iTNC 530): SMP560 bit 12 - Test checking whether safe outputs can be switched off

Description: 1 = Test checking whether safe outputs can be switched off is not active. Only for modules that do not support the test! The test must be reactivated after exchanging the affected modules (bit 12 = 0).

SMP (iTNC 530): SMP585.x

Description: Inverted PLC inputs of the A channel (max. 8 inputs). The inputs are inverted before the logical AND gating of the input information (see page 6–144).

Input: PLC operand address, e.g. 63

SMP (iTNC 530): SMP586.x

Description: Inverted PLC inputs of the B channel (max. 8 inputs). The inputs are inverted before the logical AND gating of the input information (see page 6–144).

Input: PLC operand address, e.g. 63

SMP (iTNC 530): SMP587.x

Description: PLC inputs tested with forced dynamic sampling. The power must therefore be supplied via –TEST.A and –TEST.B. The power is supplied via the test output of the corresponding SPL on which the input is located (max. 16 inputs).

Input: PLC operand address, e.g. 63

SMP (iTNC 530): SMP590.x

Description: Limit value for the axis speed in "safely limited speed" (SLS) mode in SOM_2

Input: 0 to 2000 [mm/min]
Default value: 2000 [mm/min]

SMP (iTNC 530): SMP591

Description: Limit value for the spindle speed in "safely limited speed" (SLS) mode in SOM_2

Input: 0 to 6000 [rpm]
Default value: 500 [rpm]

> Attention
>
> The speed limit values for the axes and spindle are defined in EN 12417:2007 for the different safety-related operating modes.

SMP (iTNC 530): SMP600.x

Description: Assignment of axes to axis groups

Input: Number of axis group
0 to 7
–1: Axis group for non-safe axes

SMP (iTNC 530): SMP601.x

Description: Assignment of spindles to axis groups

Input: 0 to 7
–1: Axis group for non-safe spindles

> Danger
>
> Keep the input values in SMP641.x and SMP642.x as small as possible so that incorrect positioning can be detected as early as possible.

SMP (iTNC 530): SMP641.x

Description: Maximum permissible position deviation for the actual/nominal monitoring-of-position-values safety function

Input: 0.000 to 30.000 [mm] or [°]

SMP (iTNC 530): SMP642.x

Description: Maximum permissible position deviation between:

- The currently determined reference position and the last position saved in the SKERN during the reference run of the axes
- The position in the SKERN and the value in SMP646.x during the test of the axis

Input: 0.000 to 30.000 [mm] or [°]
Default value: 1 [mm] or [°]

SMP (iTNC 530): SMP646.x

Description: Position at which the operator can check the agreement of the actual position with the position values used internally (position of the marking)

Input: –99 999.9999 to +99 999.9999 [mm] or [°]

SMP (iTNC 530): SMP650.x

Description: Positive absolute position limit values (SLP)

Input: –99 999.9999 to +99 999.9999 [mm] or [°]
Input value relative to the machine datum

SMP (iTNC 530): SMP670.x

Description: Negative absolute position limit values (SLP)

Input: –99 999.9999 to +99 999.9999 [mm] or [°]
Input value relative to the machine datum

SMP (iTNC 530): SMP690

Description: Deactivation of CRC check of the SPLC program. This must only be done while commissioning the control.

Input: 0: CRC check is active
1: CRC check is inactive

SMP (iTNC 530): SMP691.0

Description: Checksum through SPLC program's intermediate code

SMP (iTNC 530): SMP691.1

Description: MC checksum through SPLC program's binary code

SMP (iTNC 530): SMP691.2

Description: CC checksum through SPLC program's binary code

SMP (iTNC 530): SMP693

Description: Version of the SPLC-API used to create the SPLC program

Input: Numerical value that corresponds to the API version used (e.g. 100 for version 1.00)

SMP (iTNC 530): SMP1054.x

Description: Linear distance of one motor revolution [mm or °]

Input: Analog axes: No function
Digital axes: Entry of a formula possible

SMP (iTNC 530): SMP2172

Description: Delay time for inhibiting inverter enabling (delayed watchdog of MC for safe status signal – STO.A.MC.WD)
Delay time for removing the enabling of the inverter in the event of serious faults detected by the control (leading to an internal emergency stop)

Input: 0 to 60 [s] as an integer
0: 3 [s] as default value

SMP (iTNC 530): SMP2230.x

Description: Multiplier for motor current during test of motor brake

Input: 0.1 to 30.0 [· motor stall current]
0: No test of motor brakes, or motor without motor holding brakes

SMP (iTNC 530): SMP2232.x

Description: Maximum permissible path during test of motor brakes

Input: 0 to 10.0000 [mm] or [°]

Further machine parameters are included in the checksum in addition to the above-mentioned safe machine parameters, and any changes to them require entering the OEM password. Also, changing the value of certain machine parameters causes the control to reboot. The table below provides an overview of the affected machine parameters and their behavior:

Machine parameter	Meaning	Reboot	OEM password
MP10	Active axes	Yes (if an axis is added)	No
MP12	Axes in demo mode	Yes	Yes
MP100	Assignment of axis designation	Yes	Yes
MP108	Assignment of axes to drive-control motherboards	Yes	Yes
MP109	Assignment of spindles to drive-control motherboards	Yes	Yes
MP110	Assignment of position encoder inputs to axes	Yes (if change to/from value 0)	No
MP111	Assignment of position encoder inputs to spindles	Yes	No
MP120	Assignment of nominal speed value outputs to axes	Yes	Yes
MP121	Assignment of nominal speed value outputs to spindles	Yes	Yes
MP130	y index of the machine parameters MP2xxx.y for the axes	Yes	Yes
MP131	y index of the machine parameters MP2xxx.y for the spindle in operating mode 0	Yes	Yes
MP210	Counting direction of position encoder signals	Yes	Yes
MP331	MP331 = Distance for the counting pulses from MP332 The signal period (automatically calculated by the TNC) = MP331 / MP332	Yes	Yes
MP332	Number of counting pulses in the distance from MP331	Yes	Yes
SMP5xx	For description, see list above	Yes	Yes
SMP6xx	For description, see list above	Yes	Yes

Machine parameter	Meaning	Reboot	OEM password
MP1054	Linear distance of one motor revolution	Yes	Yes
MP2172	Delay time for removing the enabling of the inverter in the event of serious faults detected by the control (leading to an internal emergency stop)	Yes	Yes
MP2200	Type of axis motors	Yes	Yes
MP2230	Test of motor holding brakes: Factor for motor stall current	Yes	Yes
MP3140	Counting direction of encoder signals for spindle	Yes	Yes
MP3142	Line count of the rotary encoder on the spindle	Yes	Yes
MP3210	Motor revolutions at rated speed	Yes	Yes
MP3510	Rated speed for gear ranges	Yes	Yes

Danger

- In all safe machine parameters, you must always enter values that ensure that there is no danger to the operator.
- Monitoring functions that initiate an SS0 reaction if an error occurs must be examined particularly carefully, and must already be parameterized appropriately during the commissioning phase. Axes and spindles without mechanical motor holding brakes coast to a stop after an SS0.

A suitable analysis of the machine and the individual axes/spindles by the machine tool builder results—due to standards and directives—in requirements to be fulfilled by the safety functions, and compliance with these requirements is mandatory.

The limit values to be maintained must be determined by the machine tool builder in a machine-specific risk analysis.

The machine must be configured such that the requirements resulting from the standards and directives for safety functions are always met. The machine tool builder must first consider the machine's limit values and reaction times to be maintained so as to prevent any danger to persons. These considerations and values result in safety functions, safe machine parameters and the SPLC program. The hardware of the machine (e.g. servo drives, power modules) and the software (e.g. normal machine parameters, PLC program) must be designed and configured such that the limit values and reaction times are always observed.

Limit values for SLS

The limit values for SLS in the SMPs are axis-specific values.

Limit values for axes
The limit values for the axes must be set such that, even during interpolating movements with multiple axes, the resulting contour speed is less than the permissible speed limit value specified in the standard EN 12417.

Limit values for spindles
In the safety-related operating modes, the SMPs for the maximum permissible spindle speed must be set such that the spindle comes to a stop within no more than the number of revolutions specified by EN 12417 when an SS1 reaction is initiated. When determining the maximum permissible spindle speeds, you have to take into account that the behavior of the spindle may vary depending on the different tools and the existing gear ranges or wye/delta switchover. It must be ensured that in the worst case the spindle comes to a stop within no more than the specified number of revolutions. You must also keep in mind that the weight or center of gravity differs from tool to tool, for example.

SMP525, SMP526

Default time for axis-specific stopping along the emergency braking ramp upon an SS1 reaction. The braking ramp for SS1 is defined in MP2590 (emergency braking ramp), which is not an SMP.

The machine parameters SMP525 and SMP526 monitor the braking process of an SS1 reaction. The SS1 reaction is defined such that the drives are switched to the STO state (switched off) at the end. This presupposes that the respective brake of the axis (SBC safety function) is active. Therefore, the time set in SMP525 and SMP526 must also include the time until the brake becomes active (= overlap time for braking). An emergency stop is one of the causes that initiate an SS1 reaction.

When the SS1 reaction starts, monitoring timers with the default time defined in SMP525.x for the axes and in SMP526.x for the spindles are started in the MC and CC. The axes or spindles must come to a stop within this time, otherwise an SS0 is initiated by the SKERN.

The braking time of an SS1 reaction (entry in SMP525/526) must be greater than the time needed for electrical braking of the axis/spindle in the worst case. Especially for axes/spindles without mechanical brake, you must ensure that the time entered is greater than the maximum possible braking time for the axis/spindle.
A response of the monitoring function leads to an SS0, i.e. immediate pulse switch-off. Non-decelerated axes/spindles coast to a stop after pulse switch-off. In the worst case, this can cause damage to the machine. Specific operating conditions of the machine, such as maximum feed rate, overload on the axes, etc., must therefore also be taken into account in the time setting.

> Note
>
> A response of the monitoring function (SMP525, SMP526) leads to an SS0. Axes and spindles that do not have mechanical motor holding brakes coast to a stop.

The time for SMP525/526 consists of:

SMP525 = Maximum required braking time until standstill + overlap time for braking (MP2308) + time until there is no more holding current (50 ms) + 70 ms

An SS1 reaction can be initiated while the guard doors are open or closed. The "maximum required braking time until standstill" must therefore be determined independently of the safety-related SOM_x operating modes, taking into account the axis-specific maximum possible feed rate in the AUTO state if the guard doors are closed. The value for the "maximum required braking time until standstill" is determined from the machine tool builder's axis-specific risk analysis. Operator protection is the highest priority in determining the values. In the further configuration of the individual axes (e.g. jerk, acceleration), you must ensure that the time in SMP525.x/SMP526.x is maintained.

Please also note the description of the SS1 reaction and the setting of the emergency braking ramp (see page 4–51). The emergency braking ramp must also be set independently of the SOM_x safety-related operating modes, taking into account the axis-specific maximum possible feed rate in the AUTO state if the guard doors are closed.

After any changes to MP2590, you must check whether the timer monitoring (safety function) for SS1 is exceeded. If this occurs in the relevant worst-case scenario, then the setting for the braking ramp must be changed again. Changing the absolute values of the SMP is not permitted. Entries in SMPs are permanently defined, based on the risk analysis, and may not be retroactively changed for specific machine functions.

Example: Less steep SS1 ramp via MP2590

- Timer monitoring for SS1 reaction responds
- Unwanted reaction by the SKERN
- Correct reaction: The SS1 ramp must be made steeper again

SMP527, SMP528

Default time for controlled stopping upon SS2 reaction (axis-specific). The braking ramp for SS2 is defined in MP1060 (braking ramp), which is not an SMP.

When the SS2 reaction starts, monitoring timers with the default time defined in SMP527.x for the axes and SMP528.x for the spindles are started in the MC and CC. Axes and spindles must come to a stop within this time, otherwise an SS1 is initiated by the SKERN.

An SS2 reaction can be initiated while the guard doors are open or closed. The value for SMP 527.x/SMP 528.x must therefore be determined independently of the SOM_x safety-related operating modes, taking into account the axis-specific maximum possible feed rate in the AUTO state while the guard doors are closed. The values are determined from the machine tool builder's axis-specific risk analysis. Operator protection is the highest priority in determining the values.
In the further configuration of the individual axes (e.g. jerk, acceleration), you must ensure that the time in SMP527.x/SMP528.x is observed.

Keep in mind that in an SS2 reaction the axes are decelerated along the contour. The NC axes involved are interpolated and decelerated. Axis-specific values can be entered in SMP527 and SMP528, but the value of the most critical axis should be entered as the time for all collectively interpolating axes. The axis that is the last to come to a standstill or the slowest one to decelerate is considered to be the most critical axis.

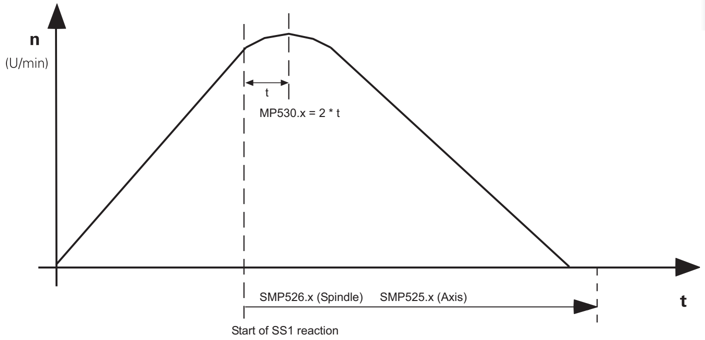
After any changes to MP1060, you must check whether the timer monitoring (safety function) for SS2 is exceeded. If this occurs in the relevant worst-case scenario, then the setting for the braking ramp must be changed again. Changing the absolute values of the SMP is not permitted. Entries in SMPs are permanently defined, based on the risk analysis, and may not be retroactively changed for specific machine functions.

Please also note the description of the SS2 reaction on page 4–55.

SMP530 Delay time for dv/dt monitoring

After the delay time has expired, the dv/dt monitoring function checks whether the speed of the axis has stopped increasing. Therefore, the axis-specific delay time must be set such that, from this point on, the acceleration of the axis actually stops increasing during a normal braking process. To do this, the axis should be accelerated and an SS1 should be initiated during the acceleration phase. The time t from the initiation of the SS1 reaction to the actual deceleration (change in algebraic sign of acceleration) of the axis can be measured in the oscilloscope of the control:

Values for SMP 530.x



The axis-specific value for SMP530.x is derived as follows:

SMP530.x = 2 * t

where: SMP530.x must be less than SMP525.x.

Please note that controller settings can affect the behavior of the dv/dt monitoring function. Machine parameter SMP530 must be set to a value that prevents the operator from being exposed to hazardous situations, even in the worst-case behavior of the machine. You must also keep in mind the varying workpiece loads on the machine, for example.

> Note
>
> A response of the dv/dt monitoring function (SMP530) leads to an SS0. Axes that do not have mechanical motor holding brakes coast to a stop.

The dv/dt monitoring is a possibility for removing energy from an axis if it has been determined that an SS1 reaction has failed. The value in SMP530 should not be parameterized too tightly within the limits resulting from the risk analysis of the machine. HEIDENHAIN finds the default value of 30 ms to be most practical. However, this value must be changed if as a result the dv/dt monitoring responds during regular deceleration procedures.

SMP545

Axis-specific limit value for maximum permissible path during standstill monitoring in SOS state.

If the maximum permissible path defined in SMP545.x (limit value for standstill monitoring in [mm] or [°]) is exceeded in SOS, while adhering to the limit values for the spindle speed and axis feed rate, the SS0 safety function is initiated (see page 4–50).

Operator protection is the highest priority in determining the path limit. Therefore, an axis-specific risk analysis must be performed. Primarily, "finger protection" (7-10 mm) must be considered.

SMP550

Axis-specific limit value for maximum permissible path upon SS2 reaction. Path monitoring is only active in the SOM_2, SOM_3 and SOM_4 operating modes when the guard doors are open. Therefore, the value for SMP550 must be set for the greatest permissible SLS in these operating modes.

If the axis-specific maximum permissible path for the SS2 reaction in SMP550.x is exceeded, the MC and CC initiate the SS1 safety functions independently of each other (see page 4–51).

The axis-specific limit value must be set such that the permissible total path is not even exceeded during interpolating movements.

Operator protection is the highest priority in determining the path limit. Therefore, an axis-specific risk analysis must be performed. Primarily, "finger protection" (7-10 mm) must be considered.

SMP630, SMP631

Maximum permissible speed deviation in % for actual/nominal monitoring of speed values. In SMP632.x (axes) and SMP633.x (spindles) you additionally define time windows within which the limit values are allowed to be exceeded. Actual/nominal monitoring of speed values is active, regardless of the selected safety-related operating mode or the state of the guard doors. Determine the values for these parameters in the SOM_1 operating mode, using the feed rates and rotational speeds possible in that operating mode.

The drive dynamics play an important role in setting the permissible speed deviation. To set these values, consider the nominal speed values (n nominal) and the actual speed values (n actual) in different applications (e.g. roughing, finishing). Define the maximum permissible deviation such that it is greater than the usual differences.

The values in SMP630/SMP631 should not be parameterized too tightly within the limits resulting from the risk analysis of the machine. HEIDENHAIN finds a value of 10 % to be most practical. However, this value must be changed if as a result the nominal/actual value monitoring responds during normal machine behavior.

SMP632, SMP633

Time window for permissible overshoot of the limit values for nominal/actual monitoring of speed values. Determine the values for these parameters in the SOM_1 operating mode, using the feed rates and rotational speeds possible in that operating mode.

Entry in SMP632.x for feed axes:

Determine the maximum start-up time of the individual axes at the acceleration set for the axes. From this, you can calculate the value for SMP632.x as follows:
SMP632.x = start-up time at set acceleration *10

Entry in SMP633.x for spindles:

Determine the maximum reversing time (e.g. from +10000 rpm to –10000 rpm) of the individual spindles at the acceleration set. From this, you can calculate the value for SMP633.x as follows:
SMP633.x = reversing time *2

The values in SMP632/SMP633 should not be parameterized too tightly within the limits resulting from the risk analysis of the machine. HEIDENHAIN finds a value of 4 seconds to be most practical. However, this value must be changed if as a result the nominal/actual value monitoring responds during normal machine behavior.

SMP641

Maximum permissible position deviation for the actual/nominal monitoring-of-position-values safety function This monitoring function is only active if the guard doors are open; there are no additional delay times.

The value for SMP641.x must be determined depending on the maximum safely limited speed (SLS) in the SOM_2, SOM_3 or SOM_4 operating mode.

The drive dynamics play an important role in setting the permissible position deviation. Use the maximum occurring following error of the axis to set this value. From this, you can calculate the value for SMP641.x as follows:

SMP641.x = maximum occurring following error * 10

However, operator protection always is of the highest priority. For the axes, you must define the maximum distance the axis is allowed to move without endangering the operator if the door is open. This value is the maximum value for SMP641.x. The other, non-safe parameters of the axes must be defined such that the occurring following error (including reserve) remains below the value in SMP641.x if the guard door is open.

If the axes are intentionally operated with following error, this does not need to be taken into account in the value defined in SMP641. The following error is automatically considered in position-value monitoring.

MP subfiles

Switching safe machine parameters (SMPs) via subfiles, editing them without repeating the acceptance test, and adaptation by the operator are not possible and not permitted. When using MP subfiles, you must therefore consider the worst case for the operator in the setting of the SMPs. In all safe machine parameters, you must enter values that ensure that there is no danger to the operator. In the further configuration of the control (e.g. jerk, acceleration), you must ensure that the limit values from the SMPs are observed.

If machine parameters that influence the dynamics of the machine are made available to the end user, the permissible limits must be documented by the machine tool builder. Limits for user parameters cannot be defined through the control!

5.3 Acceptance Test

The acceptance test of a machine must be performed in accordance with the position paper DKE-AK 226.03 by the German Commission of Electrical Engineering (DKE). The safety of the machine is ensured only by the successful acceptance test of the machine tool.

Complete acceptance test

The complete acceptance test must be performed during the commissioning of a machine, and if changes have been made to the software or hardware. During a complete acceptance test, all provided safety functions (such as the compliance with limit values, functions of control units, functions of actuators) are checked. The fault reaction physically takes effect. The correct functioning of the safety functions is tested.

The control prompts you to perform a complete acceptance test by displaying a corresponding warning message. After the acceptance test has been completed successfully, the warning message should be acknowledged by an action (e.g. pressing a special key) that is normally not used for acknowledgment during operation.

The acceptance test must be performed by personnel authorized by the machine tool builder.

Passing of the complete acceptance test and any modifications must be documented in a suitable way.

Acceptance test of series-manufactured machines

The complete acceptance test does not need to be repeated for series-manufactured machines if a complete acceptance test has been conducted on one of these machines, and the hardware and software version as well as the data of the safety-related parameters (protected against editing) match exactly those of the tested machine (see VDE 801/A1 AK4).

However, the basic safety functions, such as emergency stop, the effectiveness of guard door contacts and interlocking devices, etc. must be tested for every machine. Furthermore, the agreement of the actual position in the software with a marked reference position (machine datum) must be checked.

Editing individual SMPs

If changes are made to safety-related machine parameters (SMPs), the partial acceptance test must be performed. Only the safety functions affected by the changes must be checked in this test. The control prompts you to perform the partial acceptance test by displaying a warning message, and requires acknowledgment after the test has been performed.

Procedure

Upon request HEIDENHAIN can provide you with a possible test procedure as a basis for the acceptance test for a machine tool. This is a non-binding proposal, and must be adapted by the machine manufacturer to the requirements of the respective machine. The test also needs to be expanded by OEM-specific functions and modifications. The acceptance test must verify all safety functions and functions of the SPLC program.

5.4 Safety-Related Hardware Signals

The following naming convention applies to the signal names and the watchdog designations:

- 1st position: Description of the function of the signal
- 2nd position: Safety channel to which the signal is assigned
- 3rd position: Origin of the signal, or axis addressed by the signal
- 4th position: Origin of the signal, or axis addressed by the signal

Signal names – Channel A (MC)

Signal names – Cutout channel A			
Old	**New**		**On HSCI participant**
–SH1A	–STO.A.G	Safe torque off global	SPL
–SHS1A	–STOS.A.G	Safe torque off spindle global	SPL
–SH1.x, –SH1.s	–STO.A.x	Safe torque off (axis-specific, PWM)	CC
–AP1.x	–STO.A.P.x	Safe torque off (axis-specific, internal signal)	
–SH1AB	–STOS.A.MC	Safe torque off spindle (axis-specific, internal signal)	
–NE1	–ES.A.SMOP	Emergency stop	SMOP
- - -	–ES.A.SPL	Emergency stop	SPL
- - -	–ES.A.HW	Emergency stop on handwheel	SMOP, HW
ZT.MB.1	PB.A.SMOP	Permissive key	SMOP
ZT.HR.1	PB.A.HW	Permissive button on handwheel	SMOP, HW
ZT.WZM.1	PB.A.TM	Permissive key for tool magazine	SPL, configurable input
–SRG.AS.1, –SRG.T.1	–SD.A.x	Safety door contact	SPL, configurable input
Test.1	–TEST.A.SMOP	Test output on SMOP	SMOP
Test.2	–TEST.B.SMOP	Test output on SMOP (generated by the A channel)	SMOP
	–TEST.A.SPL	Test output on SPL	SPL
	–TEST.B.SPL	Test output on SPL (generated by the A channel)	SPL
–WKZ.SP.1	–TH.A.S1	Tool holder – Spindle 1	SPL, configurable output
–BRK.G.1	–BRK.A.G	Brake global	SPL, configurable output
	–BRK_REL.A.x	Brake port for external relay (axis-specific output for brake control via external relay)	SPL, configurable output

Signal names – Cutout channel A			
Old	**New**		**On HSCI participant**
–PF.PS.ZK	–PF.PS.DC	Power failure – DC power supply	CC, SPL
–PF.PS.AC	–PF.PS.AC	Power failure – AC power supply	CC, SPL
RRK.1	FB_NCC.A	Feedback from chain of normally closed contacts	SPL, configurable input
T.BRK.1	T.BRK.A	Test brake	SPL, configurable input
BAx.1	KSW.A.x	Keylock switch (e.g. selection of operating mode)	SMOP
	CVO.A.SMOP	Control Voltage ON; SMOP	SMOP
	PDO.A.x	Permit drive on; SPL (axis-group-specific drive enabling)	SPL, configurable input
	–STOP.A	NC stop	SMOP
	START.A	NC start	SMOP

Signal names – Channel B (CC)

Signal names – Cutout channel B			
Old	**New**		**On HSCI participant**
–SH2.x, –SH2.s	–STO.B.x	Safe torque off (axis-specific, PWM)	CC
–AP2.x	–STO.B.P.x	Safe torque off (axis-specific, internal signal)	
–SH2.WD	–STO.B.CC.WD.OUT	Safe torque off (axis-specific, internal signal)	
–NE2	–ES.B.SMOP	Emergency stop	SMOP
- - -	–ES.B.SPL	Emergency stop	SPL
- - -	–ES.B.HW	Emergency stop on handwheel	SMOP, HW
ZT.MB.2	PB.B.SMOP	Permissive key	SMOP
–ZT.HR.2	PB.B.HW	Permissive button on handwheel	SMOP, HW
–ZT.WZM.2	PB.B.TM	Permissive key for tool magazine	SPL, configurable input
–SRG.AS.2, –SRG.T.2	–SD.B.x	Safety door contact	SPL, configurable input
–WKZ.SP.2	–TH.B.S1	Tool holder – Spindle 1	SPL, configurable output
–BRK.G.2	–BRK.B.G	Brake global	SPL, configurable output
–BRK.x	-BRK.B.x	Brake (axis-specific, PWM)	CC
	–BRK_REL.B.x	Brake port for external relay (axis-specific output for brake control via external relay)	SPL, configurable output
RRK.2	FB_NCC.B	Feedback from chain of normally closed contacts	SPL, configurable input
- - -	T.BRK.B	Test brake	SPL, configurable input
BAx.2	KSW.B.x	Keylock switch (e.g. selection of operating mode)	SMOP
ME	CVO.B.SMOP	Control Voltage ON; SMOP	SMOP
	PDO.B.x	Permit drive on; SPL (axis-group-specific drive enabling)	SPL, configurable input
	–STOP.B	NC stop	SMOP
	START.B	NC start	SMOP

Signal names – One signal for both channels

Signal names – One signal for both channels			
Old	**New**		**On HSCI participant**
- - -	RDY.x	Power module is ready	CC
- - -	PWM.x	Signals of the PWM interface	CC

5.5 Entries in the OEM.SYS File

The following new key words (TOKEN) appear in the OEM.SYS file of systems with HSCI and functional safety:

IOCCFG = Name and path of the IOC file (e.g. PLC:\IOC\*.ioc). During startup, a control in an HSCI system expects the complete configuration of the HSCI system in the form of an IOC file. This file contains the configuration with all participants, their sequence and the configuration of the inputs and outputs of the PLC and SPLC. The IOconfig software for PCs is used to create the IOC file.

PLCSAFETYCFG = File name and path for conditional compilation of the SPLC program (e.g. PLC:\Splc4\*.cfg).

On the iTNC 530 you select and deselect machine options by making the corresponding entries in machine parameters. Only one PLC program is necessary for all variants of machine options. This PLC or SPLC program is conditionally compiled depending on the machine parameters MP4000.0 to MP4000.15. For this purpose, **PLCCOMPCFG =** followed by the path of the configuration file must be entered in the OEM.SYS file, and the machine options in the MP4000.x machine parameters.

For the SPLC program the entries must be made in the *.CFG file used for this. You can either use the same file as for the PLC program or create a separate file with the same syntax. Then **PLCSAFETYCFG=** must be entered in the OEM.SYS file.

PLCSAFETY = File name and path of the SPLC program (e.g. PLC:\Splc4\*.src).

6 Safety-Related Operating Modes and Interfaces

6.1 Operating Modes (SOM Safe Operating Modes)

The controls offer four safety-related operating modes as per EN 12417 (Machine Tools–Safety–Machining Centers) prepared by the engineering technical committee. The application-oriented operation offered by this promises a high level of acceptance, and therefore safety.
The goal of the standard documented safety measures is that the

- setup,
- manual intervention and
- process monitoring

of automatic production processes is possible on machining centers with open safeguards without endangering the machine operator. Instead of the guards, other safety measures are employed. This becomes necessary on modern machining centers primarily because of the complex movements with varying directions of motion and high acceleration and velocity values.

The SPLC program of the MC and CC decides which of these safety-related operating modes is effective for which axis group. Normally the safety-related operating modes are enabled by one or more keylock switches. On the SMOP, however, the safety-related Key Switch x inputs (KSW.A.x, KSW.B.x) are provided, which are connected with the contacts of the keylock switch and are evaluated by the respective SPLC program. Keylock switches are taken into account only when the guard door is opened. If the guard door is closed, maximum velocities are permissible in all safety-related operating modes. The respectively active operating mode is shown on the screen of the control.

The default values, limitations and the resulting functions possible in the operating modes must be realized by the machine manufacturer in the SPLC program in accordance with EN 12417. The SPLC program must request from the SKERN any safety functions that have to be activated due to the condition of the machine, depending on the active operating mode. Further safety-related functions, such as the control of the motor holding brakes, must likewise be realized via the SPLC program.

The SKERN monitors compliance with the requested safety functions and the safe condition of the machine, and triggers a stop reaction in the event of error in order to safely stop the machine.

The following safety-related operating modes are selectable by keylock switch. The following text lists the most important features of the individual operating modes. Ensure compliance, however, with the other requirements of EN 12417.

6.1.1 Operating mode 1 (SOM_1)

Operating mode 1 (automatic operation, production)
Safe Operating Mode 1 (SOM_1)

- Operation with closed guard door
- No machine motions are possible when the guard doors are open. An error triggers an SS1 reaction.
- Selection, for example, via keylock switch 1 in position 1
- In the safety-related SOM_1 operating mode, the SOS safety function becomes active when the guard door is opened.

If the F_LIMITED soft key is pressed while the guard door is closed, the axes and spindles are decelerated until standstill. In this condition, if the permissive button or key is being pressed, the guard door can be opened without triggering a safe stop reaction for the axes and spindle.

6.1.2 Operating mode 2 (SOM_2)

Operating mode 2 (set-up mode)
Safe Operating Mode 2 (SOM_2)

- Operation with open guard door
- Axis motions of 2 m/min at most (SMP590)
- Spindle stop within 2 revolutions (permissible shaft speed in SMP591)
- Selection, for example, via keylock switch 1 in position 2

Triggering and maintenance of the motion for only **one** axis at a time, with the following measures:

- Axis-direction keys as jog buttons
- NC start key plus permissive key PB.SMOP
- Handwheel keys plus permissive button PB.HW
- Turning wheel on the handwheel plus permissive button PB.HW
- Spindle start or spindle jog buttons plus permissive button or key PB

Maintenance of the spindle run is possible only when the permissive button or key is pressed.

The HEIDENHAIN design makes it possible to continue the programmed movements of axes without the permissive button or key. There is no monitoring here of the permissive buttons or keys by the SKERN. This realization deviates from the requirements of EN 12417. However, various realizations by the machine manufacturer of the SOM_x operating modes are possible if they can be permitted for specific machines. The machine manufacturer must use his machine and risk analysis to decide whether the programmed axis movements can be enabled without the permissive button or key. With the SPLC program you have the possibility of adapting the operating modes at any time so that they completely comply with EN 12417, see page 8–205.

If there are multiple operating units, only one of them is permitted to be functional at a given time (e.g. the handwheel or machine operating panel).

As a protection against unexpected spindle starts, the spindle cannot be started with M03/M04 (Spindle ON clockwise/Spindle ON counterclockwise). If the spindle was switched off via M05 (Spindle STOP), for example, and M03/04 was then programmed, the message "Switch spindle on" is displayed. Spindle Start and the permissive button or key must first be activated before the program continues at SLS.

Dual-channel monitoring of the actual speed of the axes or spindle on SLS. If the monitoring responds, a safe stop (SS1) follows.

The SPLC program in SOM_2 must also safely prevent:

- Automatic pallet changing
- Automatic tool and workpiece changing
- High-pressure coolant
- Tool measurement (e.g. laser)
- Turning operation on drilling and milling centers
- A chip conveyor may be moved only by additionally pressing the permissive key

If the guard door is closed when operating mode 2 is active, operation is possible as in operating mode 1. This happens automatically without any change in the keylock-switch position. This functionality must be realized in the SPLC program, see page 200.
If the F_LIMITED soft key is pressed while the guard door is closed, the axes and spindles are decelerated to the corresponding limit values of operating mode 2. In this condition, if the permissive button or key is being pressed, the guard door can be reopened without triggering a stop reaction for the axis and spindle. The SKERN ensures that opening the guard door while the spindle is running without pressing a permissive button or key triggers a Safe Stop 2 for the axes, followed by an SS1 with transition to STO for the spindle.

6.1.3 Operating mode 3 (SOM_3)

Operating mode 3 (manual intervention, for qualified operators)
Safe Operating Mode 3 (SOM_3)

- Operation with open guard door
- Operation only by a qualified person
- Axis motions of up to 5 m/min (SMP540)
- Spindle stop within 5 revolutions (permissible shaft speed in SMP541)
- Selection, for example, via keylock switch 1 in position 3

Triggering and maintenance of movements for **one or more axes** with the following measures:

- Axis-direction keys as jog buttons
- NC start key plus permissive key PB.SMOP (only triggering)
- Handwheel keys plus permissive button PB.HW
- Turning wheel on the handwheel plus permissive button PB.HW
- Spindle start or spindle jog buttons plus permissive button or key PB

Maintenance of the spindle run is possible only when the permissive button or key is pressed.

The HEIDENHAIN design makes it possible to continue the programmed movements of axes without the permissive button or key. There is no monitoring here of the permissive buttons or keys by the SKERN. This realization deviates from the requirements of EN 12417. However, various realizations by the machine manufacturer of the SOM_x operating modes are possible if they can be permitted for specific machines. The machine manufacturer must use his machine and risk analysis to decide whether the programmed axis movements can be enabled without the permissive button or key. With the SPLC program you have the possibility of adapting the operating modes at any time so that they completely comply with EN 12417, see page 8–205.

If there are multiple operating units, only one of them is permitted to be functional at a given time (e.g. the handwheel or machine operating panel).

As a protection against unexpected spindle starts, the spindle cannot be started with M03/M04 (Spindle ON clockwise/Spindle ON counterclockwise). If the spindle was switched off via M05 (Spindle STOP), for example, and M03/04 was then programmed, the message "Switch spindle on" is displayed. Spindle Start and the permissive button or key must first be activated before the program continues at SLS.

Dual-channel monitoring of the actual speed of the axes or spindle on SLS. If the monitoring responds, a safe stop (SS1) follows.

The SPLC program in SOM_3 must also safely prevent:

- Automatic pallet changing
- Automatic tool and workpiece changing
- High-pressure coolant
- Tool measurement (e.g. laser)
- Turning operation on drilling and milling centers
- A chip conveyor may be moved only by additionally pressing the permissive key

If the guard door is closed when operating mode 3 is active, operation is possible as in operating mode 1. This happens automatically without any change in the keylock-switch position. This functionality must be realized in the SPLC program. This functionality must be realized in the SPLC program, see page 200.
If the F_LIMITED soft key is pressed while the guard door is closed, the axes and spindles are decelerated to the corresponding limit values of operating mode 3. In this condition, if the permissive button or key is being pressed, the guard door can be reopened without triggering a stop reaction for the axes and spindles. The SKERN ensures that opening the guard door while the spindle is running without pressing a permissive button or key triggers a Safe Stop 2 for the axes, followed by an SS1 with transition to STO for the spindle.

6.1.4 Operating mode 4 (SOM_4)

Operating mode 4 (advanced manual intervention, process monitoring)
Safe Operating Mode 4 (SOM_4)

The necessity of operating mode 4 results from the requirements that play a role in particular during single-part manufacturing. Here it is often unavoidable that the safeguards are open even during an automatic process. This is the only way to enable the user to recognize critical collision movements or deviations from the predetermined process and to intervene accordingly.

Danger

There is an increased risk in operating mode 4:

- SOM_4 permits a higher axis speed (SMP552) and spindle speed (SMP551).
- Releasing the permissive button or key for spindle run is permissible.
- You as machine manufacturer must check whether operating mode 4 can be permitted for machine operation.

The following measures apply to operating mode 4:

- Guard door open
- To be used only by qualified operators
- Emergency stop button must be at hand
- The operator must wear protective clothing
- Spindle start only with permissive button or key
- NC start only with permissive button or key
- Wheel on the handwheel operates only with permissive button
- Axis motions of up to 5 m/min (SMP552)
- Spindle stop within 5 revolutions (permissible shaft speed in SMP551)
- Selection via keylock switch 2 or special code word, fingerprint scanner, or USB stick, for example
- Activating the operating mode 4 is permissible only from the operating mode 1
- Display on the control screen that operating mode 4 is active

The SPLC program in SOM_4 must safely prevent:

- Automatic pallet changing
- Automatic tool and workpiece changing
- A chip conveyor may be moved only by additionally pressing the permissive key
- High-pressure coolant
- Tool measurement (e.g. laser)
- Turning operation on drilling and milling centers

During operating through the machine operating panel, the axis and spindle movements are permitted after the start and without further pressing the permissive key. In the Handwheel mode, the permissive button is obligatory for all movements (starting and continuing). If it is entirely necessary for the end user, you can use SMP560 bit 7 to also enable the same behavior for handwheel operation as for operating-panel operation. However, this requires a corresponding risk analysis on your part.

The possibility of selecting operating mode 4 is enabled via a separate parameter (SMP560). If operating mode 4 is selected without having been previously enabled over SMP, the operating mode is not switched, and the **"BA4 not enabled"** error message is displayed.
Dual-channel monitoring of the actual speed of the axes or spindle at SLS. If the monitoring responds, a safe stop (SS1) follows.

SMP560 and the code number for enabling SOM_4 are only accessible to you as the machine manufacturer. You must act on the basis of your assessment of the risk (e.g. safety-related and/or organizational replacement measures / qualified operators).

As a protection against unexpected spindle starts, the spindle cannot be started with M03/M04 (Spindle ON clockwise/Spindle ON counterclockwise). If the spindle was switched off via M05 (Spindle STOP), for example, and M03/04 was then programmed, the message "Switch spindle on" is displayed. Spindle Start and the permissive button or key must first be activated before the program continues at SLS.

The operating mode 4 must remain active until the keylock-switch position changes, the control is switched off, or until the mode is deselected through a soft key. You have to use the SPLC program to ensure that, after leaving the operating mode 4, the user can only change into the operating mode 1.

If the guard door is closed when operating mode 4 is active, operation is possible as in operating mode 1. This happens automatically without any change in the keylock-switch position. This functionality must be realized in the SPLC program. This functionality must be realized in the SPLC program, see page 200.
If the F_LIMITED soft key is pressed while the guard door is closed, the axes and spindles are decelerated to the corresponding limit values of operating mode 4. In this condition, if the permissive button or key is being pressed, the guard door can be reopened without triggering a stop reaction for the axes and spindles. After the guard door has been opened, the permissive button or key can be released again. The SKERN ensures that opening the guard door while the spindle is running without pressing a permissive button or key triggers a Safe Stop 2 for the axes, followed by an SS1 with transition to STO for the spindle.

6.1.5 Operating mode – restricted spindle operation (SOM_S)

Safe Operating Mode S (SOM_S)

Even if the guard door is open, restricted spindle operation permits running a complete cycle (e.g. probing cycle), by pressing spindle start and the permissive button or key once.

Unlike other safety-related operating modes, the operating mode SOM_S cannot be activated by the user, e.g. through the keylock switch. Instead, it must be realized in the PLC program and is usable only in the safety-related operating modes SOM_2, SOM_3 or SOM_4.

If the guard door is open, the restricted spindle operation can be enabled by soft key. After the soft key is pressed, the PLC must set the PLC marker M4058 "restricted spindle operation." If the probing cycle is ended or cancelled, the PLC must reset the marker M4058. The SPLC program can import the marker M4058. If this marker is set, and one of the safety-related operating modes SOM_2 to SOM_4 is activated by the keylock switch, the SPLC program can specify the more restrictive safety-related function SLI with restricted spindle operation for the axis group of the spindle. Now the spindle speed is restricted to <= 50 rpm and path monitoring for two revolutions is active. If the spindle speed or the path is exceeded, an SS1 is triggered.

Even if the SPLC program specifies the safety function SLI, at first the safety function STO applies for the spindle. Even in restricted spindle operation, the spindle must be started with the permissive button or key and spindle start, so that you may specify SLI instead of STO. As soon as that has happened, the spindle may stay in SLI. Not until the end of the probing cycle does the SPLC have to reactivate the safety-related operating mode SOM_2, SOM_3 or SOM_4 selected via the keylock switch. This switches the spindle at standstill back into STO.

6.1.6 Operating mode selection – inputs

The inputs +KSW.A.x (x = operating mode) for the safe operating modes are transmitted by the SMOP to the MC, and the inputs +KSW.B.x are transmitted to the CC.

Through the SPLC you can program as desired the attainment of the various operating modes. Through the SPLC you can also configure the FS inputs for selecting an operating mode. This makes it possible, for example, to attain operating modes through further keylock switches. As an alternative you can use the SPLC program to realize an operating mode change also through the input of various code numbers.

Possible meaning of the inputs (high active):

- **+KSW.A.2**, **+KSW.B.2**: Activation of operating mode 2 – SOM_2
- **+KSW.A.3**, **+KSW.B.3**: Activation of operating mode 3 – SOM_3
- **+KSW.A.4**, **+KSW.B.4**: Activation of operating mode 4 – SOM_4

If more than one input or none of the inputs is active for the operating modes SOM_2, SOM_3 or SOM_4, the SPLC program must ensure that SOM_1 is automatically activated.

In addition, the SPLC program must ensure that the operating mode SOM_4 can only be activated from within SOM_1, and that after SOM_4 is exited, SOM_1 is automatically active.

If when the guard door is open the operating mode SOM_x is changed, for example with the keylock switch, the SPLC program must request an SS2 reaction. The request applies for every change of a safe operating mode:

- If any change of the operating mode SOM_x is made, when the guard door for axes and spindles is open, the SPLC must request from the SKERN the stop reaction SS2 for the axis group of the NC axes or the axis group of the spindles.
- If any change is made between safe operating modes, when the guard door of the tool magazine is open the SPLC must request from the SKERN the stop reaction SS2 for the axis group of the tool magazine.

Normally, the SKERN switches the spindles into STO if the SPLC requests the safety function SOS and the spindle is at a standstill. If necessary, the spindle (like the axes) can be switched at an SS2 reaction to SOS instead of STO, depending on SMP549.x (used for lathes).

If the axes and spindles are moving when the guard door is opened and operating mode SOM_1 is active, an SS1 reaction (emergency stop) by the SKERN results. After attaining standstill, the axes and spindles go into the STO state.

It must be possible to remove the key while it is in the position for operating mode SOM_1. This prevents operation of the machine while the guard is open (= increased danger).

For more information about the inputs of the operating mode selection and the keylock switch to be used, see page 6–153.

The table shows the available safety functions in the various operating modes:

Available safety function	For axes in operating mode				For spindles in operating mode				For auxiliary axes in operating mode			
	1	2	3	4	1	2	3	4	1	2	3	4
Safe torque off (STO)	X	X	X	X	X	X	X	X	X	X	X	X
Safe operating stop (SOS)	X	X	X	X	-[a]	-[a]	-[a]	-[a]	-	X	X	X
Safely limited speed (SLS)	-	X	X	X	-	X	X	X	-	X	X	X
Safely limited increment (SLI)	X	X	X	X	-	-	-	-	X	X	X	X
Safely limited position (SLP)	X	X	X	X	-	-	-	-	-	-	-	-
Safe stop 0 (SS0)	X	X	X	X	X	X	X	X	X	X	X	X
Safe stop 1 (SS1)	X	X	X	X	X	X	X	X	X	X	X	X
Safe stop 1F (SS1F)	X	X	X	X	X	X	X	X	X	X	X	X
Safe stop 2 (SS2)	X	X	X	X	X	X	X	X	X	X	X	X
Safe brake control (SBC)	X	X	X	X	-[b]	-[b]	-[b]	-[b]	X	X	X	X

a. If necessary, the spindle (like the axes) can be switched at an SS2 reaction to SOS instead of STO, depending on SMP549.x (used for lathes).

b. If the spindle has a brake, the safety function SBC is available.

6.1.7 Configuration of axis groups

You can configure by machine parameter whether an axis is an NC axis, a spindle or an auxiliary axis (MP100). The configuration of the axes also affects the behavior of an axis after a safety function is triggered.
Through the additional configuration possibility for working spaces, axes can be secured by different guard doors. To make a model of this behavior, the axes are divided by the axis-specific SMP600.x and the spindles by the axis-specific SMP601.x into up to eight axis groups. All axes of an axis group must be of the same type (NC axis, spindle, or auxiliary axis). The safety kernel software ascertains or checks the type from the entry in MP100.

The SPLC program evaluates the inputs for guard doors, permissive buttons and keys, start /stop keys and keylock switches, and assigns this information to the correct axis groups. For example, a physical door contact can define the guard-door condition of two or more axis groups.

You can use the SPLC program to request from the SKERN the desired safety functions SOS, SLS, SLI, STO or SS0, SS1(F), SS2 for the individual axis groups, depending on the evaluated inputs (see above). The requested safety function is then run by the safety kernel software.

Three axis groups suffice for simple machines:

- Axis group for NC axes
- Axis group for spindle(s)
- Axis group for auxiliary axes

For more complex machines it can be worthwhile to divide the axes into further groups in order to describe individual working spaces that are protected by separate guard doors. For example, one axis group can be used for the auxiliary axes of the tool changer while another is used for auxiliary axes of the pallet changer.
This then makes it possible to ensure that one of the axis groups (e.g. the tool changer) is safely protected by guard doors and can operate normally while the guard doors of another axis group (e.g. pallet changer) are open.

For the safety function Safe Stop 2, the brakes of the axes might have to function in a certain sequence. For example, the spindle is normally not decelerated until the NC axes are stationary. For every axis group, SMP610 can contain a list of other axis groups that have to be stopped before this axis group. If the safety function Safe Stop 2 is triggered for an axis group, all other axis groups listed in this MP are braked first, even if no Safe Stop 2 was triggered for these other axis groups.

Danger

The delays resulting from the braking sequence in SMP610 must be taken into account when complying with the time specifications for axis standstill.

Example of the configuration of MPs for a simple machine tool with three axis groups:
MP600.x: Assignment of axes to axis groups
MP601.x: Assignment of spindles to axis groups

- Axis group 0: NC axes
- Axis group 1: Spindles
- Axis group 2: Tool magazine axis

```
MP600.0: 0    ;1st axis, X
MP600.1: 0    ;2nd axis, Y
MP600.2: 0    ;3rd axis, Z
MP600.3: 2    ;4th axis, b
MP600.4: 0    ;5th axis, C
```

```
MP601.0: 1    ;1st spindle, S
```

```
MP610: Braking sequence of the axis groups
MP610.0: %00000000;For NC axes, wait for no other
                   axis group
MP610.1: %00000001;For spindles, wait for braking of
                   the NC axes
MP610.2: %00000000;For auxiliary axes, wait for no other
                   axis group
```

Example for the configuration of the MPs of a machine tool with two axis groups for NC axes, one spindle and two axis groups for auxiliary axes:
MP600.x: Assignment of axes to axis groups
MP601.x: Assignment of spindles to axis groups

- Axis group 0 and 1: NC axes
- Axis group 2: Spindles
- Axis group 3 and 4: Auxiliary axes

```
MP600.0: 0    ;1st axis, X
MP600.1: 0    ;2nd axis, Y
MP600.2: 0    ;3rd axis, Z
MP600.3: 1    ;4th axis, A
MP600.4: 3    ;5th axis, a
MP600.5: 3    ;6th axis, b
MP600.6: 1    ;7th axis, B
MP600.7: 4    ;8th axis, u
MP600.8: 4    ;9th axis, v
```

```
MP601.0: 2    ;1st spindle, S
```

```
MP610: Braking sequence of the axis groups
MP610.0: %00000000;NC axes of the group 0 do not wait
MP610.1: %00000000;NC axes of the group 1 do not wait
MP610.2: %00000011;NC axes brake before the spindle
MP610.3: %00010000;Auxiliary axes of group 3 can brake only after auxiliary
axes of the group 4
MP610.4: %00000000;Auxiliary axes of group 4 do not wait
```

6.1.8 Magazine axes

As separate safe axes, the additional axes for the tool magazine are defined as PLC axes by machine parameter MP100.

When the magazine door is closed, the automatic positioning and manual traverse of the tool magazine are enabled for a tool change. The positions are specified by the PLC.

The contacts of the magazine door T are to be connected over two channels to FS inputs –SD.A.T (MC) and –SD.B.T (CC) of the SPL. The contacts of the permissive keys TM are connected to the FS inputs PB.A.TM and PB.B.TM.

In order to position the tool magazine while the magazine door is open requires, for example, pressing the dual-channel jog keys TM_R.x or TM_L.x together with the dual-channel permissive key PB.x.TM. This is to be realized in the SPLC program.

If the working spaces for magazine axes and NC axes are separate, the permissive keys TM for the tool magazine must have no influence on the working space of the NC axes and spindles. Vice versa, the permissive keys of the working space for the NC axes and spindles must have no influence on the magazine axes. This SPLC program must ensure this.

When the magazine door T is open (–SD.A.T (MC) and –SD.B.T (CC) are both 0) the tool magazine can only be positioned manually in SLS. The safely limited speed for the magazine axis is specified in SMP590.x (SOM_2).

The following applies for the magazine axes when opening the magazine doors:

- During automatic positioning, the magazine is braked by the SS1 reaction. The ramp gradient can be reduced with MP2590 if problems occur with the tools (see page 4–51).

Automatic tool changing is to be prevented in the operating modes SOM_2, SOM_3 and SOM_4. The axes can be moved manually, whereby the traversing speeds are monitored by the safety function SLS (SMP590.x).

If the permissive key, jog key, or both are released, the SPLC program must trigger an SS2 reaction for the magazine axes. The position feedback control remains active in the subsequent safety function SOS so that the magazine disk cannot be turned while the tool is being inserted. The subsequent reapproach to a grid position must also be realized by the (S)PLC program.

If the guard door is open, a moving magazine axis is braked by an SS1 reaction. The ramp gradient can be reduced with MP2590 if problems occur with the tools.

The magazine axis is allowed to be moved to the next position by pressing the permissive keys and jog keys, whereby the safety function SLS is active.

If the guard doors are closed, it is permitted to move the magazine axes with the jog keys alone. No permissive key is required.

When the magazine door is closed, the magazine axis is referenced together with the axis group of the NC axes in the same working space. The handwheel does not influence the magazine axis.

During an emergency stop or SS0/SS1, the magazine axis is treated just like the group A axes.

6.1.9 Non-safe axes and spindles

With the entry –1 for the respective axis or spindle in MP600.x or MP601.x you define the axis or spindle as non-safe. The following constraints apply to non-safe drives:

- The following applies for non-safe axes:
  - The monitoring of simultaneously moving axes in SOM_2 is performed only for safe axes. Non-safe axes are ignored.
  - When moving non-safe axes in SOM_2, SOM_3 or SOM_4 and with an opened guard door, no limitation to SLS occurs. Even with an opened door, non-safe axes are in the operating mode SOM_1 and can be moved at the maximum feed rate.
  - Safely limited speed (SLS) is inactive
  - Standstill monitoring in the SOS state (SMP545.x) is inactive.
  - Safely limited position SLP (SMP650.x, SMP670.x) is inactive.
  - The maximum permissible position error for referencing or testing the axes (SMP642.x) is inactive.
  - The testing of axes is inactive.
  - Non-safe axes can also be moved if the axis has not yet found its reference.
  - An NC stop always affects all the axes.
  - Nominal-actual value comparison of position values is inactive.
  - Monitoring of the encoder amplitude and frequency is inactive.
  - The safety functions STO, SOS and SBC are not available.
- The following applies for non-safe spindles:
  - Monitoring of the encoder amplitude and frequency is inactive.
  - When switching on a spindle in SOM_2, SOM_3 or SOM_4 and with an open guard door, no limitation to SLS occurs. Even with an open door, non-safe spindles are in the operating mode SOM_1 and can be moved at the maximum shaft speed.
  - A non-safe spindle is not stopped by an SS2 reaction.

6.1.10 Electronic handwheel

The HR 410 FS, HR 420 FS, HR 520 FS and the HR 550 FS wireless handwheel are available to the machine manufacturer.

With the HR 410 FS, the El. Handwheel machine mode of operation is selected by pressing the corresponding key on the MB machine operating panel.
On large machines or machines with work zones that cannot be seen by the operator, switching the machine operating mode on the MB machine operating panel can represent a hazard for the operator. The MB can take over operating sovereignty without permission from the HR or the operator. If this is not permissible due to the risk analysis of the machine, an additional safeguard must be realized through the SPLC program. There must be an additional request in the SPLC program of whether the permissive buttons of the HR are pressed. Only if this is the case can the operating sovereignty be switched, for example. The validity of the signal edge of the pressed permissive buttons must be considered here, which, for example, is valid only for three seconds (permissive button must be let go and pressed again).
Another possibility is the use of an HR 5xx FS. With these handwheels, the operating sovereignty can be switched only from the HR 5xx.

For the HR 420 FS, HR 520 FS and the HR 550 FS wireless handwheel, the El. Handwheel operating mode is activated directly at the handwheel.

An SS2 is triggered by a switch between machine operating modes.

All machine movements that are triggered via the handwheel are monitored regarding the speed limit values specified for SLS (safely limited speed) when the guard door is open.

During the safety self-test, the signal levels that indicate a non-pressed condition must be applied to the inputs of the handwheel permissive buttons.

The direction keys and start keys as well as the wheel on the handwheel unit are active only while the handwheel permissive button is being pressed.
In the El. Handwheel mode, the FS inputs for the handwheel permissive buttons PB.x.HW are selected, and the FS inputs of the permissive keys on the machine operating panel and the magazine axis are deselected so that only the permissive function of the handwheel is effective.
On the HR 410 FS, HR 420 FS and HR 520 FS portable electronic handwheels with cross-circuit safety (two microswitches per permissive button) the normally-open contacts, which are switched in parallel, are routed to the MC through the FS input PB.A.HW of the SMOP, and the normally-closed contacts, which are connected in series, are routed to the CC through the FS input PB.B.HW of the SMOP.
Logic "1" on the MC and logic "0" on the CC signal permission.
The other logic levels do not indicate permission. During a machine movement, they trigger an SS2 reaction for the axes. An SS1 reaction is then activated for the spindle.

As on the other handwheels, in the HR 550 FS with serial data transfer, the permissive buttons are designed with normally open and normally closed contacts. However, the HR 550 FS is not directly connected with the FS inputs of the control. This handwheel is connected with an HRA access point that converts the permissive button information from the HR over relays for the FS inputs of the control. The relays, on the other hand, are designed for both permissive buttons as parallel-circuited normally open contacts. The access point is connected like a cable-bound handwheel to the machine operating panel. The logic "1" states of both relay contacts signalize consent. The other logic levels do not indicate permission. During a machine movement, they trigger an SS2 reaction for the axes. An SS1 with transition to STO is then activated for the spindle.

The handwheels can be used in all four safety-related operating modes SOM_1, SOM_2, SOM_3 and SOM_4. However, SOM_3 and SOM_4 with an active handwheel machine operating mode permit moving only one axis. An error triggers an SS2 reaction. For exceptions, however, the OEM has the capability of using SMP560 bit 9 to allow the simultaneous traverse of two or more axes (e.g. for compensation movements (only relevant in SOM_3 and SOM_4)).

The active safety functions depend on the selected operating mode.

The HR handwheels from HEIDENHAIN do not require both hands for operation, nor is this explicitly required for machine tools.

6.1.11 Use of several operating units

Besides having a machine operating panel, many machines are also equipped with an electronic handwheel or other machine operating units. On such machines, switching between the various operating units must be controlled through the SPLC.

Danger

The SPLC program must ensure that only one of the operating units (handwheel, machine operating panels) is active at any one time so as to prevent danger to the operator.

This can be realized in the SPLC by filtering the input signals (see page 8–219). However, the signals must be filtered so that the keys with stop functions always stay active on all operating units. This applies in particular to all emergency stop buttons on the machine!

In the HEIDENHAIN design, the operating unit is addressed through one channel. The keys' input signals are filtered by the SPLC over two channels. It is ensured with dual channels that no more than one operating unit can be active at any time. The filtering is always done before the PLC scan and the filtered values are set again to the same markers as in the original key conditions. In this way, too, only the filtered markers are available to the PLC program.

In connection with the PLC program it is possible to acknowledge error messages of the control from the additional operating units (e.g. handwheel). The error messages of the control are always shown on the control's BF screen, but they might not appear on the other operating units. If, after a thorough risk analysis, you nevertheless make it possible for the machine operator to acknowledge error messages from such operating units, the operator must expressly be informed of this (e.g. machine tool manual). Acknowledging an error could otherwise lead to an unexpected restart of machine motions.

6.2 Safety-Related Hardware Interfaces

6.2.1 Interfaces of the SPL

Participant	Available interfaces	See page
SPL	FS inputs/outputs — General	6–144
	FS inputs of guard doors SD	6–145
	FS inputs of permissive buttons and keys PB	6–146
	FS inputs of emergency stop	6–147
	FS inputs FB_NCC.A/FB_NCC.B	6–148
	FS inputs PDO.A.x/PDO.B.x	6–148
	FS outputs –TEST.A.SPL/–TEST.B.SPL	6–148
	FS outputs of tool holder TH	6–150
	FS outputs STO.A.G/STOS.A.G	6–149
	FS outputs BRK_REL.A.x/BRK_REL.B.x	6–149

FS inputs/outputs

Safety-related inputs/outputs, FS inputs/outputs

Safety-related (FS) inputs and output signals serve to initiate safety functions or safe operating states through external system components, or to pass on safety-relevant information to external control components.

All requests and acknowledgments for safety functions or safe operating states are to be sent and requested over both safety channels.

Note

The risk analysis you have to make for the safety functions must show the requirements to be fulfilled by the individual safety function (e.g. required performance level d as per EN 13849-1).

All components (e.g. keylock switches, emergency stop button, safety relays, control) that are involved in the individual safety functions must meet the requirements for the respective safety function. The individual safety functions must also be designed according to the determined requirements.

Emergency stop buttons are to be used exclusively for emergency stop purposes. Under normal operating conditions, a machine must not be switched off via the emergency stop buttons. The proper functioning of all emergency stop buttons is to be tested annually by pressing these buttons.

The safety-related inputs/outputs (FS inputs/outputs) lie on the SPL input/output assembly or the SMOP machine operating panel. The corresponding input/output signals must always be routed to the system in two channels, and must be available to both the MC (first safety channel = Index A) as well as the CC (second safety channel = Index B), or be formed by both computer units.

In addition to the respective channel-specific signal (channel A or channel B), the MC (channel A) and the CC (channel B) also receive the signal of the other channel for evaluation.
All FS inputs/outputs have the characteristics of PLC interfaces with logic levels of 0 V and 24 V. They are designed according to the quiescent current principle, i.e. low-level current automatically results in logic "0". This means that the safe state is automatically selected for the operator, control and machine.

The wiring and evaluation of safety-related inputs is to be realized according to the quiescent current principle. A logic level of 0 V at a safe input must result in a safe state for the operator.

The dual-channel inputs/outputs of FS slots make it possible to realize safety functions up to performance level D of the EN 13849. The control of inputs and the transmission of output states also requires components that are approved for use for applications up to PL d. The dual-channel inputs/outputs are not pulsed, but carry static 0 V or 24 V. The inputs/outputs are subjected to forced dynamic sampling in appropriate tests that are part of the safety self-test that must be performed no later than every 168 hours.

AND gating of safe input information

> Note
>
> First, the physical dual channel inputs of the A channel and the B channel are AND gated, and only then is the result of the AND operation forwarded to the SPLC as the input state.

This AND operation means that the SPLCs of the A and B channels will receive the value 0 as input information if two inputs have different states (e.g. A channel = 0, B channel = 1)

If safe inputs are inverted through SMP585.x and SMP586.x, the input information is inverted before the AND operation.

Example:
The physical terminals of a safe PL module have the following states: terminal of A channel = 0, terminal of B channel = 1.
Both inputs are inverted through the setting in SMP585.x and SMP586.x: A-channel information = 1, B-channel information = 0.
The AND gating of the A and B channels therefore results in logic "0".
This logic "0" is transferred as input information to the SPLC input markers.

SMP587.x is used to force the dynamic sampling of safety-related inputs. A prerequisite is that the elements (e.g. the normally open contact of a switch) are supplied by the test outputs –TEST.A or –TEST.B (see page 6–148).

The wiring of safety-related outputs is to be realized according to the quiescent current principle. A logic level of 0 V at a safe output must result in a safe state for the operator.

If there is an external (ES.A, ES.B) or internal emergency stop (crash of the MC's NC software), an SS1 or SS1F will be initiated. The safety-related outputs (FS outputs) are switched off (= 0) if all axes are at a standstill, or no later than after the expiration of the time defined in SMP2172. This means that the FS outputs are usually not switched off until after the actual emergency stop reaction SS1 and the standstill of the axes/spindles.

Guard doors

SD guard door –SD.A.x, –SD.B.x

The contacts of the guard doors must be realized in two channels. They have to be routed in two channels to FS inputs of the SPL.
The SPLC program sees the states of these FS inputs in input markers. From these input markers it recognizes which working space or spaces are no longer secured by closed guard doors and requests from the safety kernel software a corresponding safety function for the axes in this working space.
The configuration divides the axes into axis groups. All axes of an axis group have to be in the same working space.
Various conditions apply for the respective axis groups, depending on the axis operating mode SOM_1 to SOM_4 and the condition of the guard doors (see page 6–125).

Permissive buttons/keys

PB permissive buttons and keys –PB.A.x, –PB.B.x

The contacts of the HEIDENHAIN permissive buttons and keys are arranged in two channels. They are routed over two channels to the corresponding inputs of the SPL or the SMOP.
Permissive buttons and keys always apply for certain axis groups. The SPLC program reports to the SKERN the axis groups for which an effective permissive button or key has been pressed.
A typical milling machine has permissive buttons on the handwheel, and permissive keys on the operating panel and for the tool magazine. Depending on the machine operating mode, the SPLC program decides whether the permissive button on the handwheel is effective, or the permissive key on the operating panel.

Note

The SPLC program must ensure that only one permissive button or key is effective for any specific working space at a given time!

When the guard doors are open, the permissive keys of a machine operating panel (input PB.x.SMOP) must be pressed for spindle motion and NC start. The permissive key integrated on the SMOP consists of two independent sensor elements under one push button (two normally open contacts).

The permissive buttons of the HR 410 FS, HR 420 FS handwheels or a wireless handwheel (PB.x.HW input) must be pressed for axis and spindle movements that are triggered via handwheel keys. On the handwheel a two-step button is used which, however, has a normally open and a normally closed contact.

The permissive keys of the tool magazine (PB.x.TM input) must be pressed for movements of the tool magazine.

The safety functions of the permissive buttons or keys must be ensured by a timer in the SPLC program. The SPLC program detects edges at the physical inputs of the permissive buttons or keys when they are pressed. The permissive buttons or keys are considered pressed only if both contacts are closed. Both contacts of the permissive buttons or keys can be executed as normally open contacts or as antivalent.
After the edges are detected, you have to start a timer in the SPLC program with a time of up to 30 minutes. The permissive button or key retains its validity only for these 30 minutes for triggering or maintaining a movement (determined over machine keys, e.g. NC start, spindle start). Therefore, permission is in effect if the timer's time (max. 30 minutes) has not yet expired and the permissive button or key remains pressed. The permissive button or key is then considered to be pressed (see page 8–187).

Through the risk analysis of your machine you have to define the time for the timer of the permissive buttons' or keys' duration of validity, e.g. on the handwheel. For specific machines, it might be necessary to define the permissive buttons' or keys' duration of validity to be significantly less than the maximum 30 minutes.

The SPLC program must ensure the following prerequisites for the triggering of movements:

- Valid permission is required for:
  - NC start
  - Spindle start
  - Manual axis movement with the handwheel
  - Spindle jog mode
  - Movement of the tool magazine

The SKERN monitors for a valid permission and therefore allows the following movements:

- Manual axis movement with the handwheel
- Spindle jog mode
- Movement of the tool magazine
- Maintenance of movement in handwheel mode
- Maintenance of spindle motion
- Suppression of the protection against unexpected start-up

If the permission is no longer recognized as valid, the stop function SS2 is triggered for the axes and then SS1 for the spindles.

Emergency stop inputs

Emergency stop inputs
Safe dual-channel inputs for the emergency stop are available on the SPL (safe PL), the SMOP (safe machine operating panel) and the HW (handwheel). The corresponding inputs –ES.A.x and –ES.B.x are sent over HSCI to the SPLC of the MC and CC.
If a signal level of logic "0" is available on one of the two –ES.x.x inputs, this already triggers the emergency stop function (SS1). The emergency stop reaction has priority over all other functions and operations and is automatically triggered by the SKERN.
The –ES.A.x/–ES.B.x inputs are stimulated alternately and with a slight delay via the –TEST.A.x and –TEST.B.x test outputs. This makes is possible to detect an emergency stop through the other channel, even during a channel test.

FB_NCC.A / FB_NCC.B

FB_NCC.A/FB_NCC.B "Feedback from chain of normally closed contacts"

The FB_NCC signal must be led to a safe dual-channel input of the SPLC. The feedback inputs are connected with +24 V (PLC) via the serially connected, positively driven, normally closed contacts of all safety-relevant relays and contactors. The normally closed chain is checked during the self-test and cyclically taken into account during operation. The switch-off or functionality of the signal is checked during the self-test after the control is started up.

For better diagnostics it would also be possible to wire inputs on normal PLC inputs from the individual contacts of the chain of normally closed contacts. This would make it possible to determine which contact leads to an error and will issue a corresponding PLC error message.

HEIDENHAIN cannot offer any inspection of whether all safety-related relay contacts are wired into the chain of normally-closed contacts, because this depends on the machine design. All normally-closed contacts of the relays that assume safety-related tasks must be wired into the chain of normally-closed contacts.

Examples for feedback inputs:

- Main contactor
- Relays for Safe Torque Off
- Safety relays for axes/spindle
- Relays for the tool holder
- Contactors for axis-specific switch-off of motor holding brakes by the MC and CC through –BRK_REL.A.x and –BRK_REL.B.x
- Contactor for common switch-off of the motor holding brakes through –STO.A.G

PDO.A.x / PDO.B.x

Axis-group-specific drive enabling

For large machines whose work zone cannot be fully seen, the SPLC program must assign or lock the drive enabling for the individual axis groups depending on the FS inputs (e.g. PDO.A.x/PDO.B.x).

Dynamic test outputs

–TEST.A.SMOP/–TEST.B.SMOP and –TEST.A.SPL/–TEST.B.SPL

In normal machine operation, the same level (logic "1" with closed contacts) can be present for a long period of time at safe inputs (e.g. inputs of the emergency stop switch, door contacts). If during this time, for example, both safe inputs of the emergency switch or the door contacts lose their function, an emergency stop or the opening of the door might not be detected.
In order to ensure that these safe inputs can reliably detect an opening of the contacts (= hazardous condition = logic "0" level), a cyclic dynamic sampling occurs.
The dynamic test outputs –TEST.A.x / –TEST.B.x are used for this.
The function of the inputs is tested in dual channels without triggering the reaction required with actual switching. Due to the alternately delayed dynamic sampling, the functionality is maintained during the test through the other channel.

The automatic tests (forced dynamic sampling) use TEST.A/TEST.B to check whether in the event of switch-off ("0" state) of the supply via TEST.A/TEST.B the corresponding inputs also go to "0" and therefore to the "fail-safe" condition.

STO.A.G / STOS.A.G

STO.A.G "Safe Torque Off," STOS.A.G "Safe Torque Off for Spindle“
As an option, the MC can use the SPL and its FS output –STO.A.G (Safe Torque Off) and –STOS.A.G (Safe Torque Off for Spindle) to control the safety relays in the supply units or compact inverters. This enables the MC with the aid of the SPL to additionally use the safety relays (axes X, Y, Z... and spindle) to lock the power switches (IGBTs). Depending on the wiring, the main contactor can also be circuited (hardware-based separation). This functionality of the MC is not safety-related in the HEIDENHAIN safety strategy and can be deactivated through SMP560 bit 8.

Through the –STO.A.G output it is likewise possible to use a contactor to switch all motor holding brakes together.

The –STO.A.G output is switched off together with the –STOS.A.G output. However, the –STOS.A.G output can be switched by the SKERN independently of –STO.A.G and, if the door is open, is switched off when the spindle is stationary.

Note

The –STO.A.G and –STOS.A.G signals are a single-channel signal in the HEIDENHAIN safety strategy. So do not use this signal for the realization of safety functions that require a dual-channel switch-off (e.g. controlling a tool holder).

SPLC outputs can be defined for the dual-channel switch-off of external assemblies. Functions that require a dual-channel switch-off should be placed on a safe dual-channel output that you must handle from the SPLC depending on the NN_GenOutputEnable interface marker among other things. The SPLC program must ensure the switch-off of these outputs.

Tool holder

TH tool holder

The "open the tool holder" and "close the tool holder" functions must be programmed in the SPLC program. You can use the program of the SPLC to define how the tool holder mode can be achieved. However, this has to be done so that the "open the tool holder" function is possible only through an intentional initiation of this function, e.g. with the "tool holder" key and the permissive key with subsequent "open the tool holder" key.
You must ensure the following in the SPLC program:

For the "open the tool holder" function:

- Set the PLC marker "open the tool holder = logic 1" depending on the SPLC program
- Inquire from the SPL whether the guard door has been opened (SD.A.x, SD.B.x = 0)
- Trigger an SS2 reaction for the spindle
- Inquire from the safety kernel software whether spindle speed is zero (N< 10 rpm)
- Activate the STO safety function (power stage is not ready for operation)
- Inquire from the safety kernel software whether the STO safety function is active

The FS outputs TH.A and TH.B must not be opened unless all above mentioned conditions are fulfilled. Then the tool can be taken from the tool holder.
While the tool holder is opened, the possibility of a spindle start must be ruled out by the SPLC program!

For the "close the tool holder" function:

- Clear the PLC marker "open the tool holder = logic 0" depending on the SPLC program (e.g. by pressing the "tool holder" key).
- The FS outputs TH.A and TH.B close the tool holder.

For the "automatic tool changer" function:

- When the guard door is closed, the PLC marker "open the tool holder" controls the FS outputs TH.A and TH.B,. whereby the SPLC program has to ensure a spindle standstill. Moreover, the SPLC must prevent malfunctions (e.g. lock the "tool holder" key).

BRK_REL.A.x / BRK_REL.B.x

FS outputs BRK_REL.A.x/BRK_REL.B.x

The SPLC MC activates the motor holding brakes through the safety-related outputs –BRK_REL.A.x of the SPL and connected safety relays. If it is desired that the MC be capable of activating the motor holding brakes globally through –BRK.A.G, then the –BRK.A.G signal must be generated by gating the axis-specific signals –BRK_REL.A.x in the SPLC.

The SPLC CC activates the motor holding brakes for specific axes through the safety-related outputs –BRK_REL.B.x of the SPL and connected safety relays. This functionality is safety relevant only if the motor holding brakes are not controlled directly through the axis-specific inverter signals –BRK.B.x.

6.2.2 Interfaces of the SMOP

Participant	Available interfaces	See page
SMOP	FS inputs/outputs – General	6–144
	FS inputs of permissive buttons and keys PB	6–146
	FS input of tool holder TH	6–150
	FS inputs of keylock switch KSW	6–153
	FS inputs of emergency stop	6–147
	FS inputs of machine keys	6–153
	FS inputs CVO.A.SMOP/CVO.B.SMOP	6–154
	FS outputs –TEST.A.SMOP/–TEST.B.SMOP	6–148

Keylock switch

Keylock switch (KS)

The keylock switches serve for selection of a safety-related operating mode. There are two inputs per switch position of the keylock switch on the machine operating panel. The inputs are realized in two channels and can be freely configured through the SPLC program.

The selection of safety operating modes is safety relevant and must therefore be "fail safe." So, in the event of power failure, a missing power supply through TEST.A/TEST.B or wire breakage, the operating mode must be active that provides the greatest protection for the operator. This is SOM_1. Therefore a keylock switch with dual-channel normally-open contacts is to be used, as proposed in the HEIDENHAIN basic circuit diagram. The automatic tests (forced dynamic sampling) use TEST.A/TEST.B to check whether in the event of switch-off ("0" state) of the supply via TEST.A/TEST.B the corresponding inputs also go to "0" and therefore to the "fail-safe" condition.

For machines that offer more than one safety-related operating mode, a dual-channel activation of the various operating modes is required for the HEIDENHAIN system. The keylock switch in the HEIDENHAIN system must be realized as it is shown in the HEIDENHAIN basic circuit diagram. There must be 2 x 2 normally open contacts: two normally-open contacts for SOM_2, and two normally-open contacts for SOM_3. SOM_4 must be activated by an additional keylock switch.

A single-channel selection of the safety-related operating modes for the HEIDENHAIN FS system would mean that the operating modes would no longer meet the required performance level d or category 3.

Machine operating keys

Machine operating keys

The machine operating keys are the keys on the safe machine operating panel (SMOP), as well as all axis-direction keys and the start/stop keys.
Each machine operating key has two switching contacts (two normally-open contacts each) When the machine is switched on and during the cutout channel test, the inputs of the machine operating keys are monitored for logic "0". For this purpose, all machine operating keys in the SPLC program must be combined into a group signal MK.G. This is evaluated by the SKERN in the safety self-test (see page 7–157).

The functions of the machine operating keys only become effective if the MC and CC receive the corresponding signals, i.e. if both contacts have been closed.

Stop keys:
For machine operating keys with a stop function (e.g. spindle stop, NC stop) one normally-open contact each is evaluated by the SPLC of the CC and the other one by the SPLC of the MC.
The stop keys are considered not relevant to safety. The safety is attained through the emergency stop button.

HEIDENHAIN recommends always configuring the logic of stop-key inputs so that the input marker of the SPLC has the value 1 if the stop key is not pressed. You can configure this through SMP585.x and SMP586.x (see page 6–144). This makes these machine operating keys already effective when the MC or CC receives a corresponding signal, i.e. if one of the two contacts was closed.

All braking reactions that are triggered as a result of pressing a stop key must be defined by the machine manufacturer in the SPLC program. These include, e.g.:

- Pressing NC stop
- Pressing spindle stop

HEIDENHAIN recommends triggering an SS2 as the reaction to a stop key. The associated braking process is then monitored by the SKERN.

CVO.A.SMOP / CVO.B.SMOP

Control voltage on; (CVO)
The dual-channel input Control Voltage On (CVO.A.SMOP/CVO.B.SMOP) is transferred by the SMOP through the SPLC to the safety kernel software.

6.2.2.1 Interfaces of the handwheel (HR)

Participant	Interfaces	See page
HR	Permissive buttons PB	6–146
	FS inputs of emergency stop	6–147
	Cable connection to the machine operating panel	6–155
	Radio link to the machine operating panel	6–155

Cable connection

Cable connection of the HR to the machine operating panel

If the connection between the handwheel and X23 on the SMOP is made directly (without access point) by cable, then all lines carrying safety-related data (PB, emergency stop) are dual-channel. The handwheel is connected to the machine operating panel and the data from the machine operating panel is transmitted over HSCI to the other HSCI participants.

Radio link

Radio link or serial data transfer from the HR to the SMOP

The use of an HR 550 FS handwheel necessitates the use of an AP access point (HRA 5xx FS handwheel adapter), which is connected at X23 of the machine operating panel.

For the HR 550 FS wireless handwheel, an unambiguous assignment must be ensured between the handwheel and the access point. For the HR 550 FS wireless handwheel, this mutual assignment of the wireless handwheel and the access point is made through the respective serial numbers, which are unambiguous and not identical. The wireless handwheel must be placed in the AP access point for this. The HR and AP only communicate over the RS 422 serial interface during this assignment.
If you remove the HR from the AP during the serial number exchange process, the process will be canceled and a corresponding error message will be issued. During normal control operation, the control software identifies the wireless handwheel by the serial number of the HR.

During the safety self-test and when the connection to the wireless handwheel is set up, the system ensures that only the HR and the AP that have been assigned unambiguously to each other are addressed. If a difference is found in this comparison of serial numbers, the connection will be terminated. During this entire process the relay contacts in the AP for the emergency stop and the permissive buttons remain open.

During the communication from the wireless handwheel through the access point to the control, the safety-related dual-channel information is transmitted to the AP. This decodes the information and reproduces the information of the permissive buttons and the emergency stop on safety relays in the AP. These are wired to FS inputs at the machine operating panel.

For more detailed information about the wireless handwheel, refer to the Technical Manual for your control.

7 Safety-Related Tests and Forced Dynamic Sampling

7.1 Safety Self-Test

Faultless functional safety is essential for the machine and must therefore be tested at specified intervals (forced dynamic sampling).

When the machine is switched on and at regular intervals during operation, the complete safety self-test and the test of the brakes must be performed to test the functions listed below.

Safety self-test of HEIDENHAIN control components:

- Test of the cut-out channels
- Test of the safety-related outputs
- Test of the chain of normally closed contacts
- Test of the machine control voltage
- Test of the guard doors
- Test of the machine configuration
- Test of the machine keys and permissive buttons/keys
- Test of the emergency-stop circuit
- Test of various internal monitoring functions

Test of the brakes:

- Test of the brake control
- Test of the motor holding brakes (via holding torque)

The guard door must always be closed during the safety self-test and the test of the brakes. However, you can deactivate the closure of the guard doors on your own responsibility for test purposes (by setting SMP560 bit 1 to 1). The default time for the safety self-test of HEIDENHAIN control components is specified in machine parameter SMP511 (it must be performed after no more than 168 hours). As soon as the guard door is opened after this time has expired, the safety self-test must be performed again to ensure the safety of the machine. The default time in SMP511 is monitored by the safety-kernel software.

Note

Please note that the maximum possible time of 168 hours that can be specified for the safety self-test in machine parameter SMP511 applies only to the the control components from HEIDENHAIN. If you are using other components, the respective particular specifications must be complied with!

If, in addition to HEIDENHAIN control components, you are using other components, possibly from other manufacturers, for implementing safety functions, all specifications and any test interval times of the individual components must be complied with. Test intervals even shorter than 168 hours may be required in this context. Appropriate measures must be taken to ensure that these time intervals are maintained.

The operation and testing of motor-holding brakes must be in accordance with Information Sheet No. 005 "Gravity-loaded axes (vertical axes)" issued by the engineering technical committee (BGM (German Employer's Liability Association in the metal industry)). This Information Sheet requires a cyclic brake test to be performed on nonredundant holding systems no later than after the expiration of eight hours or after a working shift is over. For systems that are safely protected from being accessed (e.g. by guard doors with guard locking), the test can be performed right before accessing the systems when the opening of the guard door is requested. This extends the test interval from eight hours to the point in time at which the guard door is to be opened. In this case, the brake test does not need to be performed until the guard door is actually opened. PLC module 9144 enables you to start the brake test and the safety self-test at any time via the PLC program. You can ensure safe monitoring of the test interval by entering the corresponding time in SMP511.

However, the self-test can be started through the SPLC program at shorter intervals than the time entered in SMP511. This makes it possible to prompt the machine operator to perform the safety self-test at shorter intervals. The safety self-test can be started by soft key, for example.
The messages prompting the operator to perform the self-test can be cleared with the CE key, except for the last message (which appears after no more than 168 hours, or after the expiration of the time entered in SMP511).

The safety self-test must be executed for the entire machine within the specified time; an axis-group-specific division is not possible.

If no test is performed within the specified time and the door is open, the machine is brought to a safe stop. If no test is performed and the door is closed, the machine is also brought to a safe stop as soon as the door is opened.
After that, the door must be closed and the test must be performed.
After the test has been completed, the time period specified in SMP511 or the SPLC program is active for a new test prompt.

Danger

After the machine has been switched on, the machine will not be in a safe state until the safety self-test and the test of the brakes have been completed successfully.

Standstill monitoring remains active during the entire self-test.

Note

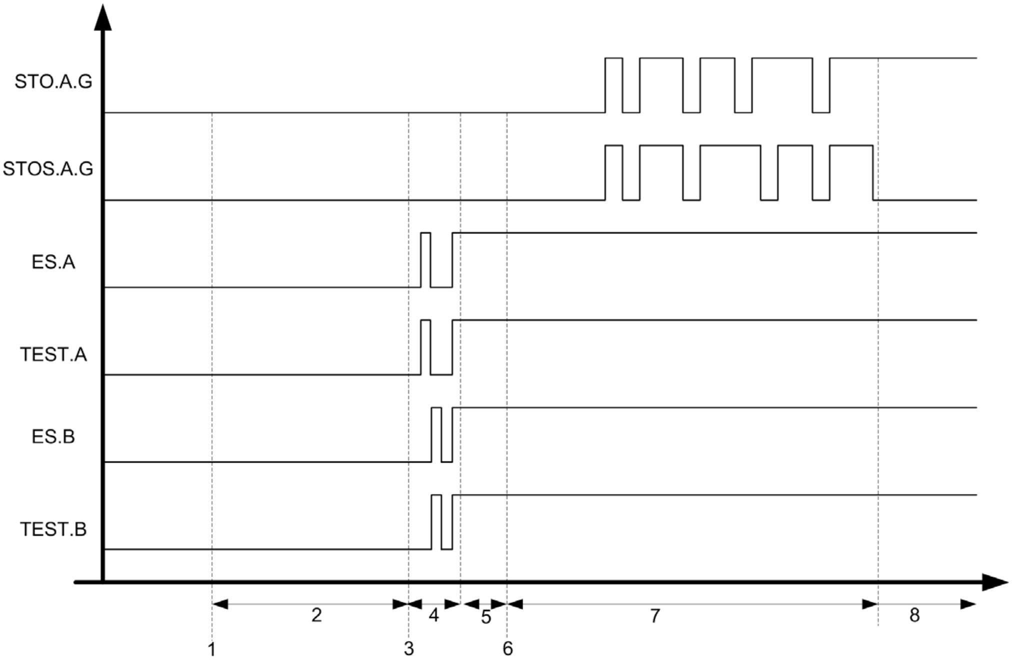
In a system with functional safety, the safety self-test can be performed on the controller units only if at least one axis/spindle is active per controller unit (drive-control motherboard).

7.2 Self-Test Sequence

When the control is started, the safety self-test automatically begins with the first part after the SPLC program has been compiled. In the first part, internal monitoring functions and signals are tested. The machine control voltage must be switched off during the first part. The guard doors of all work envelopes must be closed and the machine control voltage (CVO) must be switched on before the second part begins. The cut-out paths, parts of the external wiring and the test of the brakes are tested during the second part of the self-test. The self-test is performed in the sequence described below. A detailed description of the individual test steps is provided on the following pages.

- Step 1: Start of the self-test
- Step 2: Test of various internal monitoring functions
- Step 3: Test of the chain of normally closed contacts, see page 7–163
- Step 4: Test of the emergency-stop circuit, see page 7–175
- Step 5: Test of the machine control voltage, see page 7–162.
- Step 6: Test of the machine keys and permissive buttons/keys, see page 7–175
- Step 7: Test of the guard doors, see page 7–163.
- Step 8: Test of the brake control, see page 7–164.
- Step 9: Test of the motor holding brakes (via holding torque), see page 7–166
- Step 10: Test of the cut-out channels, see page 7–162

The diagram below shows the basic sequence and the essential signals of the self-test:



Step	Function	Screen display
1	Start of the self test, immediately after compiling of the PLC program	Pop-up window **Self test** **HSCI components are tested**
2	Phase 1 of the self-test: Triggering and detection of essential internal signals are tested.	
3	Test of chain of normally closed contacts via FB_NCC signal	
4	Test of ES.A/ES.B inputs via the TEST.A/ TEST.B test outputs	
5	Waiting for Control Voltage ON (CVO signal)	**RELAY EXTERNAL DC VOLTAGE MISSING**

Step	Function	Screen display
6	Switch-on of machine control voltage is detected, test of chain of normally closed contacts via FB_NCC signal	**EMERGENCY STOP test**
7	Phase 2 of the self-test: - Test of the machine operating keys - Testing the guard doors for being "closed" - Test of the motor brake control - Cut-out channel test, including the triggering and detection of the STO.A.G and STOS.A.G signals On each rising edge of the STO.A.G signal, the chain of normally closed contacts (FB_NCC) and the state of the motor holding brakes (T_BRK) are tested.	
8	Normal control operation Machine control voltage is switched on, STO.A.G output and ES.A/ES.B are at 1. STOS.A.G is at 0.	**TRAVERSE REFERENCE POINTS**

7.3 Test of the Cut-Out Channels

The following cut-out channels are tested:

- –STO.A.G = 0
- –STOS.A.G = 0
- –STO.A.x = 0
- –STO.B.x = 0

To check the effectiveness of the cut-out channel tests, the MC and CC have the following feedback inputs:

- FB_NCC.A and FB_NCC.B: Test of the entire chain of normally closed contacts (e.g. tool holder, motor holding brakes, etc.)
- RDY.x: Test of readiness of the power module

The following function is also tested:

- Switch-off of all safety-related outputs on the SPL and SMOP, and test of the state (= 0).
- Service pack 05 expands the safety selftest as regards the safe outputs. During the test all safe, dual-channel PL outputs are specifically switched off via hardware watchdogs. This state is checked to ensure that all dual-channel outputs assume this state (=0) and remain in it. The PLD-H 04-08-00FS modules with ID 727 219 variant 01 do not fulfill the requirements of this test, and must therefore be replaced by variant 02 modules. Other PL modules already support this test. If the previous PLD version with ID 727 219-01 is in the electrical cabinet when the new test is performed, the test is aborted with the error message "E031 error xxxxxxxx…". The test can be deactivated via SMP560 bit 12 = 1 until the PL modules have been exchanged. The test must be reactivated once the modules have been exchanged!

7.4 Test of Machine Control Voltage

During the safety self-test the operator is prompted to switch on the machine control voltage (CVO). Prior to this, the test has already verified that the machine control voltage is switched off.

7.5 Test of the Chain of Normally Closed Contacts

Interrogation of the complete chain of normally closed contacts (FB_NCC.A, FB_NCC.B inputs) as to whether all safety relays are in the safe state (= relay dropped out). This test is part of the cut-out channel test and is also performed each time the machine is switched back on via Control Voltage ON (all relay contacts must be closed). This means that the chain of normally closed contacts must always be closed before the STO.A.G signal is set. After the test has been initiated, there is a waiting time of max. 200 ms, during which the chain of normally closed contacts must be closed. This waiting time was introduced to give the relays with slower switching times sufficient time to close the normally closed contacts.

The SPLC must transmit the states of the FS inputs FB_NCC.A and FB_NCC.B (feedback from chain of normally closed contacts) to the safety-kernel software to enable the safety-kernel software to check the effectiveness of a cutout during the safety self-test, see page 8–215.
A short circuit to 0 V or 24 V of the FB_NCC signal is detected during the self-test. For this purpose, the K1 relay controlled via –STO.A.G (HEIDENHAIN basic circuit diagram) must be wired to the chain of normally closed contacts.

7.6 Test of the Guard Doors

This test checks whether the guard doors of the work envelope are closed for the safety self-test. If the guard doors are not closed, the self-test will not be continued until the doors are closed. An appropriate message prompts the operator to close the guard doors.

The SPLC must transmit the states of the axis groups to the safety-kernel software to enable the safety-kernel software to check the guard doors during the safety self-test, see page 8–200. The second part of the self-test must not be started until all guard doors are closed so that the operator is not endangered. The SPLC program must inform the SKERN when all axis groups are in the "Automatic mode" safe operating mode (SOM_1).

7.7 Test of the Motor Brake Control

This test checks whether the motor holding brakes can be switched via two channels. The brake control test is performed at the beginning of the safety self-test. If it is unavoidable in exceptional cases (e.g. for test purposes), you can—on your own responsibility—switch off the test collectively for all axes by setting SMP560 bit 3.

Danger

In principle, the test of motor brake control should be active!
If the brake test is deactivated via SMP560 bit 3 for test purposes, a malfunction of the motor holding brakes cannot be detected and the sagging of hanging axes cannot be ruled out.

To perform this test, the test line must be wired to the feedback inputs T.BRK.A and T.BRK.B (see Figure 3.20: block diagram of motor brake control). However, the T.BRK signal is not used to provide feedback information about the state of the brake during operation. The T.BRK signal is used only for the test of motor brake control.

The SPLC must transmit the T.BRK.A and T.BRK.B signals to the safety-kernel software to enable the safety-kernel software to check the motor brake control during the safety self-test, see page 8–217.

The individual tests (see below) of motor brake control are performed by the MC, while the CC monitors the correct test procedure on the MC. If faults occur while the tests of motor brake control are being performed, the MC and the CC each initiate an SS0.

- Depending on how the brakes are controlled during the test, an SS0 is initiated if:
  - one of the transistor contacts in the inverter is not interrupted,
  - one of relays used for controlling the brakes is not switched off via the B channel (= 0),
  - one of the safe SPL outputs used for direct brake control is not switched off (= 0),
  - one of relays used for controlling the brakes is not switched off via the A channel (= 0),
  - there is a short circuit to 24 V,
  - one of the transistor contacts in the inverter does not make a connection,
  - one of the relays used for dual-channel control of the brakes does not switch (= 1),
  - one of the safe SPL outputs used for direct brake control does not switch (= 1), or
  - there is a short circuit to 0 V.

The test does not depend on the state of MP2234.x bit 0. MP2234 bit 0 = 0 is used to output the –BRK.B.x signal to the inverter via the PWM interface. If MP2234 bit 0 = 1, the –BRK.B.x signal is not output. The outputs on the SPL module are used for brake control via the B channel.

For the requirements to be met by the SPLC program for controlling the brakes during the test, see page 199.

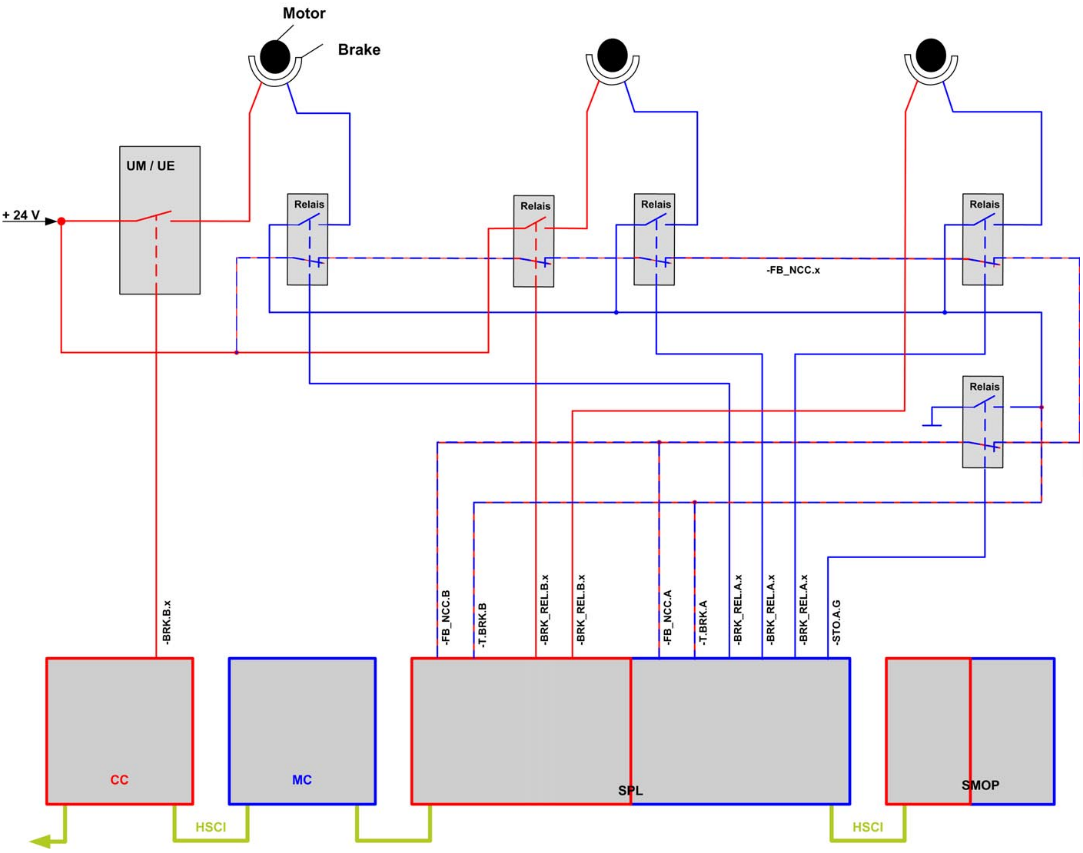


Figure 3.20: Block diagram of motor brake control

A protective circuit in the form of a varistor must be connected in parallel to the inductance (coil of the holding brake) for controlling the motor holding brakes (see basic circuit diagram). Due to the inductance of the motor holding brakes and any relays used, a voltage peak that may exceed 1000 V occurs when the exciting current is switched off. This may destroy other electronics, such as connected PLC inputs/outputs.

Danger

A basic wiring error in the brake control circuit can cause gravity-loaded axes to fall down, in particular during the brake control test. During the first motor brake control test after wiring a machine, a gravity-loaded axis must therefore be secured against falling!

During the brake test, brake control is carried out once by only the B channel, and once by only the A channel. The servo drives are not feedback-controlled during the test. Keep this in mind during the commissioning phase of the machine, and secure the respective axes against falling.

7.8 Motor Brake Test

After the control has been switched on, the test of the motor holding brakes is performed at the end of the self-test. In all other periodically recurring tests, the test of the motor holding brakes is performed at the beginning of the self-test. This prevents the axes from sagging during operation, even if the brakes have become smudged with oil in the meantime, for example.

During the test of the motor holding brakes, a current according to SMP2230.x, is output while the brake is active, thereby applying a torque against the motor holding brake. The control uses the holding torque of the brake to determine in which direction (algebraic sign) the test torque is to be applied, and which amount of test torque is to be applied. As a result, the ratio of the test torque relative to the load on the servo drive always remains the same. The test torque is applied in the direction of the holding torque. In SMP2232.x you define the maximum permissible traverse path. If it is exceeded during the brake test, i.e. a defective motor holding brake is detected, the servo drives are not switched off, but they continue being feedback controlled (the SOS safety function is active) to prevent hanging axes from sagging.
The error message "8300 Motor brake defective x" is generated.

For the setting of machine parameters MP2230.x and MP2232.x, please refer to the Technical Manual of your control.

For hanging and preloaded axes, feedback control applies a certain motor torque while holding the position of the axis (holding torque, holding current). During the test of the motor holding brakes the test torque (test current) is added to the holding torque corresponding to the position. The sign of the test current applied is always the opposite of the sign of the holding current determined. The motor encoder is used for the test of the motor holding brakes. Test procedure:

- Determining the current axis position and the holding torque (the axis is being feedback-controlled)
- Reducing the control parameters, waiting for the activation and the application of the brake
- Switching feedback control off
- Adding the test torque to the holding torque determined. At the same time the position of the axis is monitored, and it is checked whether the test torque is generated (measurement of motor current).

If no increase in current was detected during the test of the motor brakes, the error message "8310 No current in brake test x" is issued. It is not possible to clear the error messages and the message window prompting the operator to move the axes to a safe state.

Danger

Axes with defective motor holding brake must be moved to a safe position before switching off the machine.

The axis/spindle guard doors must be closed while the brake test is being performed; otherwise the error message "MC guard doors are open" or " CC guard door open in brake test" will be issued. The brake test cannot be performed until the axis/spindle guard doors are closed. The SPLC must transmit the status of the guard doors to the SKERN.

If a brake is found to be defective during the test of the motor brakes, the axes remain in closed-loop control. This status is maintained until the control is shut down or the drives are switched off via the PLC. Before switching off the machine or the drives, you must traverse axes with defective motor holding brake to a safe position or somehow else secure them against falling.

For the requirements to be met by the SPLC program for controlling the brakes during the test, see page 199.

You can deactivate the closure of the guard doors on your own responsibility for test purposes (by setting SMP560 bit 1 to 1).

If an axis has more than one motor holding brake, you can only test both brakes together.

The operation and testing of motor-holding brakes must be in accordance with Information Sheet No. 005 "Gravity-loaded axes (vertical axes)" issued by the engineering technical committee (BGM (German Employer's Liability Association in the metal industry)). This Information Sheet requires a cyclic brake test to be performed on nonredundant holding systems no later than after the expiration of eight hours or after a working shift is over. For systems that are safely protected from being accessed (e.g. by guard doors with guard locking), the test can be performed right before accessing the systems when the opening of the guard door is requested. This extends the test interval from eight hours to the point in time at which the guard door is to be opened. In this case, the brake test does not need to be performed until the guard door is actually opened. PLC module 9144 enables you to start the brake test and the safety self-test at any time via the PLC program. You can ensure safe monitoring of the test interval by entering the corresponding time in SMP511.

7.8.1 Brake test for synchronized axes

General information:

The brake test is activated (> 0) or deactivated (= 0) separately for each servo drive via MP2230.x. During the brake test, an additional test torque from MP2230.x, defined via a multiplier, is applied to the motor stall current. This test torque exerts additional load on the holding brake of the servo drive. The axis is prevented from moving during the brake test and the brake test is considered to have been passed only if the brake withstands this load.

The control determines the algebraic sign of the test torque individually for each servo drive depending on the holding torque. If servo drives are not subject to gravitational load, or if the brake is closed and is therefore currently without holding torque, the sign of the test torque cannot be determined exactly.
In software versions up to 606 42x-01 SP02, this caused a problem with the brake test of synchronized axes if different algebraic signs were determined for the master drive and slave drive. In rare cases this could result in the test torques of the master drive and the slave drive counteracting each other so that the synchronized axis is distorted. As a consequence, the result of the brake test could not be attributed to the actual holding force of the brake, which means that the result of the brake test was not meaningful in these cases.
Also, for gravity-loaded axes, the algebraic sign must be opposite to the current holding torque. Otherwise, the power module must generate the holding torque plus the test torque against gravity, and in unfavorable cases this can result in a shut-down through the power modules due to overload.

HEIDENHAIN modified the brake test for synchronized axes as follows:

Behavior during the brake test of synchronized axes:

The function reads the machine configuration to detect which servo drives are operated together as a synchronized axis and which must therefore be handled separately in the brake test. Machine parameter MP850.x is used to configure the servo drives as a synchronized axis. The brakes and servo drives of the synchronized axis are tested simultaneously. It is ensured, however, that the same algebraic sign is used for the test torque of all servo drives. The sign is determined for all servo drives of the synchronized axis based on the entry for the holding torque of the master in MP2630.x. If no value is entered in MP2630.x, the current holding torque of the master is used.

There are two possibilities for starting the brake test. In both cases the function described above is used to test the brakes of synchronized axes simultaneously:

- Automatic brake test
  The brake test takes place automatically during the power-up test of the control, as soon as all servo drives of the respective synchronized axis have been switched on.
- Brake test via PLC module
  Using PLC module 9144, you can start the safety self-test via the PLC. The brake test is then automatically performed at the beginning of the self-test. What is new in the service packs listed below is that the slave drives of a synchronized axis are tested simultaneously with the master. As a prerequisite for the brake test of a synchronized axis, all servo drives of the axis must be switched on and the brakes must be open.

HEIDENHAIN modified the brake test as described above with the following service packs:

- NC software 606 42x-01 SP 02 (December 2010)

Additional possibility as of 606 42x-01 SP02: Testing the brakes of a synchronized axis successively

The above-mentioned service packs 02 and higher will also make it possible to activate a changed brake test sequence via MP860 bit 2. If MP860 bit 2 = 1, the servo drives of a synchronized axis are tested successively rather than simultaneously. As a result, the brake test is performed individually for all servo drives of a synchronized axis.

All brakes and servo drives of the synchronized axis are tested successively, one after the other, at the specified test current. For the brakes and servo drives that are not part of the momentary test, but are configured as connected to the servo drive to be tested, the current is set during the test so that the servo drive is not moved. The brakes of these servo drives must be open for this purpose. This way, each time only the brake of an individual servo drive is tested, without the other servo drives or brakes of the synchronized axis having an effect on the test.

To be able to use this brake test sequence, the individual brakes of the synchronized axis must not be combined. It must be possible to control the brakes individually.

Due to the modified sequence of the brake test, more time is necessary to perform the test for all axes. You may have to consider this in your PLC program if you monitor the times of the power-up test or the brake test.

There are also two possibilities for starting the brake test. In both cases the function described above is used to test the brakes of synchronized axes sequentially:

- Automatic brake test
  The brake test takes place automatically during the power-up test of the control, as soon as all servo drives of the respective synchronized axis have been switched on.
- Brake test via PLC module
  Using PLC module 9144, you can start the safety self-test via the PLC. The brake test is then automatically performed at the beginning of the self-test. What is new in the below-mentioned service packs is that the slave drives of a synchronized axis are tested successively after the master. As a prerequisite for the brake test of a synchronized axis, all servo drives of the axis must be switched on and the brakes must be open.

HEIDENHAIN modified the brake test for synchronized axes as described above with the following service packs:

- NC software 606 42x-01 SP 02 (December 2010)

Constraints for the brake test:

As a prerequisite for the brake test of a synchronized axis, all servo drives of the axis must be switched on and the brakes must be open. The test can only be performed if all relevant servo drives are switched on.

Note

Before performing the brake test, ensure via the PLC program that all servo drives of a synchronized axis are switched on and the holding brakes are open.

For slave drives for which the brake test has been disabled via MP2230.x, the current is adjusted so that the servo drive is not moved while the other servo drives of the synchronized axis are being tested.

Since the algebraic sign of the test torque cannot be determined until the drives are feedback-controlled and the brakes are open, an appropriate waiting time must be specified for the start of the brake test of synchronized axes. The time set in MP2309.x is used for this. The value for MP2309.x must equal the time that passes until the brake is really open after the controller has been switched on. The same time must be entered in MP2309.x for all servo drives of a synchronized axis.

In general, the following applies to the brake control: If the brakes are controlled by the PLC, and not by the inverters, the PLC module 9159 (drive controllers are switched off) transmits the status message to the PLC program regarding the closing of the brakes during the brake test.

HEIDENHAIN recommends:

Note

For all machines on which a brake test for synchronized axes is performed, HEIDENHAIN recommends installing the above-mentioned service packs to be able to use the new behavior of the brake test. If software versions 340 49x-06 and 606 42x-01 are used, the sequential brake test of synchronized axes should also be activated (MP860 bit 2 = 1).

- If required, modify the PLC program with respect to the conditions and the changed behavior of the brake test.
- Test the behavior of the PLC program and the brake test on the machine.
- If required, update the NC software and the PLC program of the affected machines in the field.

If you need assistance in evaluating the situation, also please contact the responsible HEIDENHAIN service agency.

If you also need the modified brake test for synchronized axes for software versions for which no service pack is currently planned, please contact the responsible HEIDENHAIN service agency.

Machine parameters and PLC module:

MP_860.x **Synchronous control**
Input: Bit 2: Brake test for synchronized axes
0 = Test the brakes of a synchronized axis simultaneously
1 = Test the brakes of a synchronized axis successively (new behavior, as of 606 42x-01 SP02)

MP_2230.x **Multiplier for motor current during test of motor brake**
Input: 0.100 to 30.000 [· motor stall current]
0: No test of motor brakes, or motor without brake
Recommended: 1.3 · M_L / M_0

MP_2232.x **Maximum permissible path during test of motor brakes**
Input: 0 to 10.0000 [mm] or [°]

MP_2309.x **Controller parameters adjusted to closed brake**
Input: 0: Not active
0.001 to 5.000 [s]

MP_2630.x **Holding current**
Input: –100.000 to +100.000 [A]

Module 9144 Safety self-test / Emergency stop test
PLC module 9144 is used to activate special functions regarding the safety self-test or emergency-stop test, as well as the functional safety (FS) of a HEIDENHAIN control system.
The test can be started directly through the PLC module. Also, a PLC soft key can be made available through the PLC program if all minimum requirements are fulfilled so that the user can start the self test directly by soft key.

In the self-test performed after the control has been switched on, the test of the motor brakes is performed at the end of the self-test once all cut-out paths have been tested and the servo drives have been switched on. In the repeated self-test via module 9144, the test of the motor brakes is performed right at the beginning of the self-test. The servo drives are not switched off for further tests until the test of the motor brakes has been passed.

The (S)PLC program must ensure that the following minimum requirements are met before the repeated self-test is started:

- All guard doors must be closed and, if possible, locked.
- No active machining operation is allowed.

Further constraints may apply, depending on the control model used:

- **Safety self-test and emergency-stop test for controls with functional safety (FS)**
  The PLC program can determine at what time a test is to be performed or suggested. The PLC program can use PLC module 9037 to inquire how much time is left until the self-test must be performed. The PLC program can use Module 9144 to start the test immediately, taking the minimum requirements (mode 0) into account. The PLC marker 4288 is not supported. If the test is repeated using Module 9144, the brake test is automatically performed at the beginning of the self-test. All servo drives whose brakes are to be tested must be switched on for the brake test. After the brake test, the NC software switches off the servo drives before starting the self-test.
- The marker M4190 is set and the marker M4189 is reset when a test is started.
- The marker M4189 is set and the marker M4190 is reset when the entire test cycle has been completed.
- The marker M4192 is set when there is a request for the control voltage to be switched on. The marker is planned to be supported as of SP 03.

Module 9144 and the PLC markers are used to start the repeated self-test through the PLC and to fully automate the self-test. The test is started via Module 9144 and initiates an external emergency stop through the signals MC.RDY and STO.A.G after the brake test has been completed successfully. Then the test continues up to the point at which the control voltage must be switched back on. This can be done by the user on request by the NC, or the procedure can be automated such that marker 4192 is evaluated and the control voltage is switched on by the PLC. As soon as the control voltage has been switched back on, the self-test is continued up to completion.

Please also note the following when performing the brake test on synchronized axes:
Only if a brake test for the master and an associated slave drive of the synchronized axis is configured via MP2230.x will the slaves automatically be included in the brake test of the master. The brake test of all servo drives of the synchronized axis is based on the settings in the machine parameters.

In order to start the brake test of synchronized axes via PLC module 9144, all drives of a synchronized axis must be switched on via the PLC program before the brake test can be performed. If a servo drive involved is not switched on, the brake test is canceled with the error message **`8330 Brake test was canceled`**.

```
Call:
PS     K/B/W/D  <Mode>
                0: Start self test immediately
                1: Reserved
                10: Define the operating mode for functional safety
                11: Request for testing the axis position
PS     K/B/W/D  <Parameter 1>
                Mode 0: No evaluation, must be programmed
                Mode 1: No evaluation, must be programmed
                Mode 10:
                   0: Operation through machine operating panel
                   1: Operation through manual control unit
                   2: Homing and testing of axes
                Mode 11: Number of axis to be tested
PS     K/B/W/D  <Parameter 2>
                Mode 0: No evaluation, must be programmed
                Mode 1: No evaluation, must be programmed
                Mode 10: No evaluation, must be programmed
                Mode 11: No evaluation, must be programmed
CM     9144
PL     B/W/D    <Status/Error>
                Mode 0:
                   0: Function is executed
                   1: Error according to W1022
```

Error code:

Marker	Value	Meaning
M4203	0	No error
	1	Error code in W1022
W1022	2	Invalid value programmed for mode or parameter
	28	Test already active
	43	This is not an HSCI system or a system with functional safety
	51	Function is not supported by this control
	58	Control without operating-mode group
	61	Function is not supported by this control

Module 9159 Advance status message: Drives will be switched off

```
Call:
CM     9159
PL     W/D      <Drives, in bit code, that are switched off in the time
                defined in MP2308>
```

7.9 Test of the Machine Configuration

The test of the machine configuration takes place right at the beginning of the safety self-test.
In this test, the serial numbers of the HSCI participants, of all EnDat encoders and the inverters are read by the MC. The serial numbers determined are compared with the serial numbers saved. If the list of saved serial numbers does not match the serial numbers determined, a dialog box appears. This dialog box informs the end user about a discrepancy. The user must check the new configuration of the machine at this point and confirm it by entering the OEM password, or he must react to a fault that occurred in the configuration. If the configuration is not confirmed, the safety self-test will be interrupted at this point and will not be continued.

7.10 Test of the Machine Keys and Permissive Buttons/Keys

All machine operating keys (axis-direction keys, handwheel/machine operating panel/tool magazine permissive buttons/keys, tool holder, spindle start, NC start, Control Voltage ON) are checked to verify that they are "not actuated."

The SPLC program determines the keys to be tested. The SPLC program must use a logical OR operation to combine the input markers into the group signal MK.G. It then reports the result to the SKERN, see page 8–217. Also, the SPLC must inform the SKERN about the state of the permissive buttons/keys, see page 8–214.

7.11 Test of the Emergency-Stop Circuit

Test sequence within the safety self-test:
The emergency stop inputs –ES.A.SMOP, –ES.B.SMOP, –ES.A.SPL, –ES.B.SPL, –ES.A.HW and –ES.B.HW are tested using the test outputs –TEST.A.x and –TEST.B.x. –TEST.A.x controls the inputs of the MC, and –TEST.B.x controls the inputs of the CC. A safe stop 1 is initiated if a fault occurs.

During normal control operation the test (forced dynamic sampling) is performed using the dynamic test outputs –TEST.A.x and –TEST.B.x, see page 6–148.

8 SPLC – Safety-Related PLC

8.1 General Information

Note

- HEIDENHAIN reminds its customers that the basic circuit diagram of the control is a non-binding proposal: the OEM must adapt the diagram to the needs of the respective machine.
- HEIDENHAIN reminds its customers that the requirements formulated in this chapter for an SPLC program constitute a non-binding proposal: the OEM must adapt the program to the needs of the respective machine.
- The OEM is responsible for adhering to the relevant standards and safety regulations (EN 12417).
- The OEM is responsible for the safety of a machine. The OEM must ensure the safety of the machine by performing a comprehensive acceptance test. The acceptance test must cover all safety functions of the machine, including all functions that are realized in the SPLC program.
- For general information about the SPLC programming, please refer to the online help of PLCdesignNT, starting from version 2.7. You can download the current version of PLCdesignNT from our FileBase under PC Software.

8.2 Safe Software Structure

Overview of the HSCI participants and the possibility of programming the PLC and SPLC via an external PC:

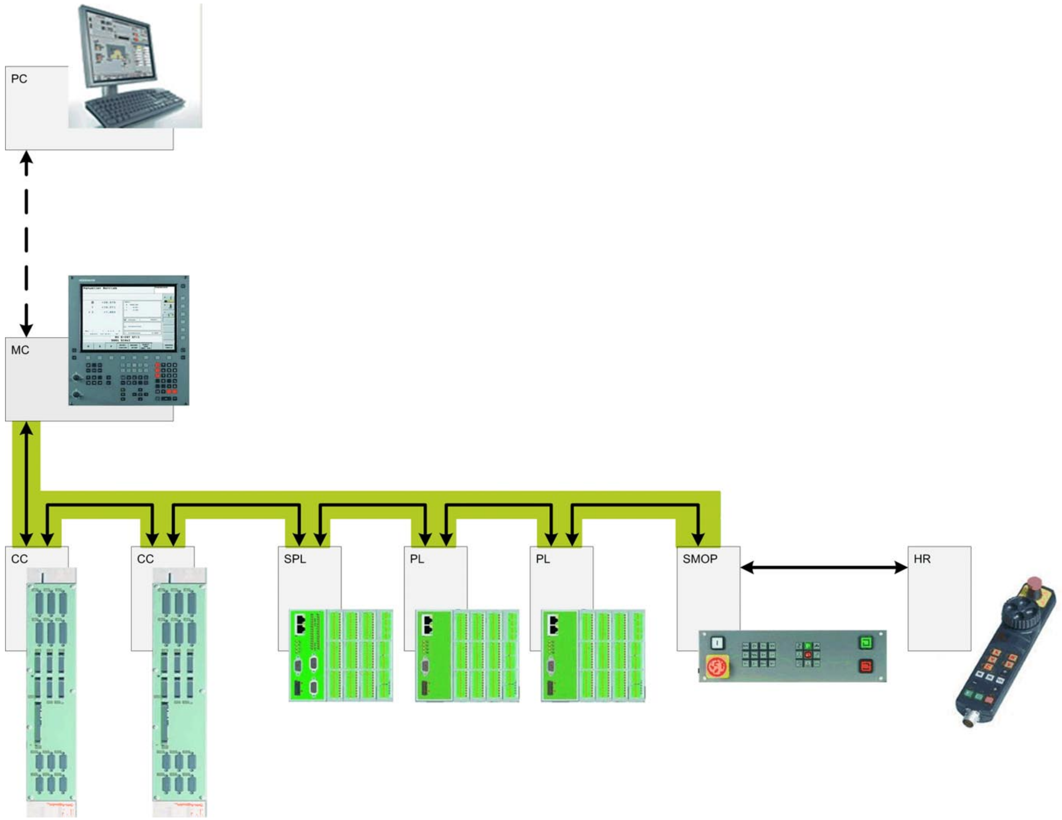


Figure 3.40: Programming

8.3 Software Structure of PLC / SPLC

The HEIDENHAIN Serial Controller Interface (HSCI) is an interface that makes it possible to exchange data via two channels. This is the basis for the safety integrated in the controls from HEIDENHAIN. The relationships between the dual-channel inputs/outputs, the HSCI interface, (S)PLC, SKERN and the development and diagnostic tools affected are described in this chapter.

8.4 Glossary

Software (processes) on the MC, CC and PL:

IPO (MC)	Interpolator of the control (manages the drives). The IPO manages the communication with the CC slaves.
PLC (MC)	Programmable logic control for adapting machine-specific functions by using physical digital and analog inputs and outputs. The term PLC in this case includes both the freely programmable part (PLC program) and the associated run-time environment (PLC run-time system, abbreviated PLC-RTS).
SPLC (MC/CC)	Process on the MC and CC that includes machine-specific functions in the safety functions, using the aid of an SPLC program (running in the respective process) created by the OEM. As with the PLC, the term SPLC includes both the freely programmable part (SPLC program) and the associated run-time environment (SPLC run-time system, abbreviated SPLC-RTS).
SKERN (MC/CC)	SKERN, or safety-kernel software: Processes on the MC or CC in which the basic safety functions of the control are collected. Also, the SKERN triggers the safety functions (such as stop reactions).
CC-FW	Firmware (controller software) on the CC controller unit
PL-FW	Firmware on the PLs and SPLs
Symbol information	Symbolic designations can be used for operands in PLC projects and in SPLC projects (see page 8–181). The system specification understands the term "symbol information" to mean the assignment of symbolic names to operands.
PLCcomp	HEIDENHAIN PLC compiler

Software outside of the control for project setup and diagnostics:

PLCdesignNT	Development tool for creating PLC programs and SPLC programs, see page 8–181. Furthermore, PLCdesignNT can also be used as a diagnostics tool for displaying PLC data and SPLC data, as well as displaying information about the PLC program run.

8.5 SPLC Development Tool

PLCdesignNT integrated software development environment

The PLCdesignNT software development environment provided for you by HEIDENHAIN can now be used for creating SPLC programs as well as PLC programs.

The online help of PLCdesignNT contains comprehensive documentation about the SPLC API to assist your programming:

- Introduction to SPLC programming
- SPLC language content
- SPLC operand addressing
- Data exchange with the PLC

You can download the current version of PLCdesignNT from our FileBase under PC Software.

An integrated setup tool creates a checksum-protected setup of all files belonging to a project. This ensures that when a machine series is put into service, the SPLC program from the acceptance test is installed on the control without the possibility of having been manipulated.

PLC compiler

Compiling on the development system

For developing the program, the compiler of the PLCdesignNT development system from HEIDENHAIN is used to check the syntax of the source files, generate intermediate code from the HEIDENHAIN statement list, and to generate debug information and make it available in a file.

Local compiling

The target system variant of the compiler is located on the control. Each time the control is (re)started, the PLC compiler translates all files belonging to an SPLC project into executable machine code for the SPLC runtime system.

By reading a CRC checksum, the SPLC runtime system makes sure that the code has not been changed since the acceptance testing of the machine.

This ensures that the source code is always stored on the control, and that it is available should service be necessary.

Capabilities of the compiler

The HEIDENHAIN PLC statement language for generating the SPLC program is limited to the commands for data processing (logical/arithmetic gating), memory transfer (load/write to accumulator) and conditional processing (If/Else/Endif).

Compiler functions for SPLC programming

To achieve the dual-channel redundancy, the PLC compiler generates code in two separate runs but from the same source code: once for the SPLC process on the MC hardware and once for the SPLC process on the CC hardware.

During this generation, a CRC sum is determined via the binary data, and is used by the SPLC runtime system to make sure that the code has not been changed since the acceptance testing of the machine.

Operands that serve as an interface to the SPLC runtime system or to the PLC are placed by the compiler on permanently defined address ranges, and information about these ranges is stored in the debug information file.

8.6 PLC and SPLC Programs

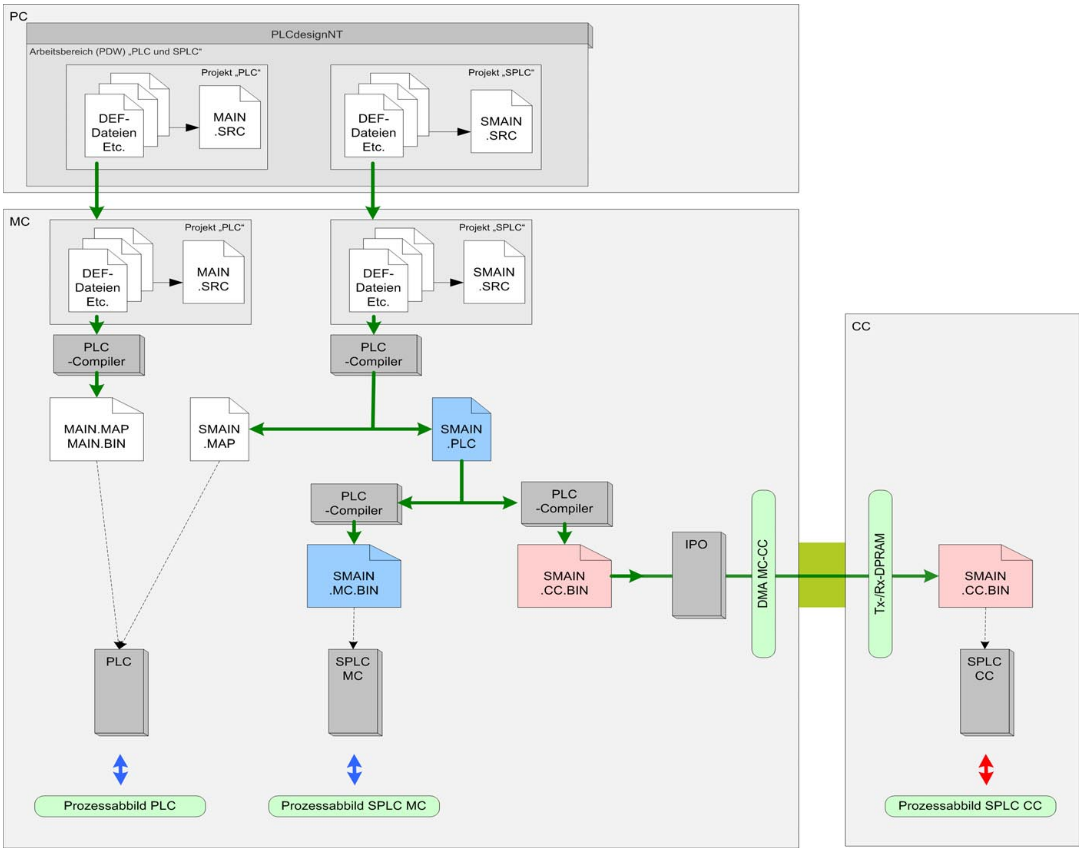


Figure 3.42: Relationship between PLC and SPLC programs

On a safe control, three different PLC programs are run in parallel. Each program saves its operands in a separate process image.

- MAIN.BIN
  The program on the MC, is managed by the PLC runtime system
- SMAIN.MC.BIN
  The program on the MC, is managed by the SPLC-MC runtime system
- SMAIN.CC.BIN
  The program on the CCs, is managed by the SPLC-CC runtime systems

The PLC program and the SPLC-MC program use the I/Os of the A channel. The SPLC program on the master CC uses the I/Os of the B channel.

These programs are developed with the PLCdesignNT development tool in a workspace containing two projects. A project always consists of a main file and any associated files (definition files for process-image data or other source files).

The following cycle times apply:

- PLC cycle time and SPLC-MC cycle time: can be set via MP7602
- SPLC-CC cycle time: permanently 21 ms

Note

Please note that the SPLC-CC does not run at the same clock rate as the PLC.

This means that it is not possible to set a dual-channel output with a PLC pulse. Furthermore, it cannot be guaranteed that the SPLC program will run between two PLC clocks.

Therefore, information from the PLC must be sent to the SPLC as statuses, and not as events.

8.7 Safety of the SPLC Program

The PLCdesignNT programming tool used to create the SPLC project (SMAIN.SRC) and the SPLC programs (SMAIN.MC.BIN and SMAIN.CC.BIN) resulting from the project is not safe. The safety of the SPLC programs is ensured by the successful acceptance testing of the machine tool. The SPLC RTS MC saves the CRCs for the intermediate code (SMAIN.PLC) and the two binary codes (SMAIN.MC.BIN, SMAIN.CC.BIN) in safe machine parameters (SMPs). The SPLC runtime systems check whether each SPLC program is safe in its own channel.

Attention

The safety of the SPLC programs is not ensured until the machine tool has successfully passed the acceptance test. This test must be performed by the machine manufacturer.

Once the machine tool has successfully passed the acceptance test, the respectively valid CRCs are stored in the corresponding SMP691.x, and are used for comparison each time the SPLC programs are translated. If one of the stored CRCs does not match the presently generated CRC, an acceptance test must be performed. The scope of the acceptance test is determined by the changes to the SPLC program. If the control determines that there is a difference between a current CRC checksum and a saved CRC, without the SPLC program having been changed intentionally, then the entire acceptance test must be performed.

An error message appears if the presently generated CRC checksum differs from the corresponding entry in SMP691.x. The error message contains the present checksum, which must then be entered in SMP691.x. The OEM password is needed to confirm this change to the SMP.

8.8 Requirements to Be Met by the SPLC Program

Chapters 8.9 to 8.11 describe the requirements that HEIDENHAIN considers an SPLC program must fulfill for a simple milling machine. HEIDENHAIN reminds its customers that the requirements formulated in this chapter for the SPLC program constitute a non-binding proposal: the OEM must adapt the program to the needs of the respective machine.

Chapter 8.8	Introduction
Chapter 8.9	Interfaces to/from the SPLC (SPLC API), see page 8–185 Description of all data (input and output data) that are available to the SPLC program
Chapter 8.10	Tasks of the SPLC Program, see page 8–196 Specification of the SPLC program and description of all details necessary for implementing the SPLC program
Chapter 8.11	Examples and exceptions, see page 8–221 Description of the functionality of the SPLC program by way of examples and exceptions

8.8.1 Axis groups / working spaces for an example milling machine

A simple milling machine generally has three axis groups:

- Axis group for all NC axes (axis group A)
- Axis group for the spindle (axis group S)
- Axis group of the auxiliary axes for the tool magazine (axis group T)

If there are other auxiliary axes, such as for a pallet changer, then additional axis groups are necessary.

In the HEIDENHAIN safety design, the configuration of axis groups is realized via SMP600.x and SMP610.x, see page 6–136.

Such an example machine has two working spaces:

- Working space for NC axes and spindle. Protected by A/S (axis/spindle) guard door
- Working space for auxiliary axes of the tool magazine. Protected by T (tool) guard door

8.8.2 Moving the axes with open guard doors

If the axis/spindle guard door is open, then movement of the NC axes and the spindle is enabled by selecting a safe operating mode (SOM), see page 6–125.

Any operator can move the tool magazine even if the tool guard door is open by pressing the appropriate keys. For safety reasons, the keys for this operation must be located so that the operator needs both hands to press them. This ensures that he cannot reach into the tool magazine while it is moving.

For more information on guard doors, see page 6–145.

8.9 Interfaces of the SPLC

The safety-related dual-channel inputs and outputs are the interfaces of the SPLC to the safety-relevant hardware of the machine.

8.9.1 The splcapimarker.def definition file

The SPLC-API programming interface is the interface between the SLPC and the SKERN. This programming interface is prescribed by HEIDENHAN, and is described below. The existing interface markers of the SPLC-API are prescribed, and only HEIDENHAIN can change or extend them. The interface markers are specified in the splcapimarker.def definition file. Therefore, an SPLC program is based on the prescriptions of the SPLC-API used.

HEIDENHAIN makes this splcapimarker.def file available to the (S)PLC developer. As soon as the file is included in the SPLC program via the INCLUDE command, the control uses the symbolic SPLC-API. The file consists of all symbolic SPLC operands, which have been gathered in a structure.

HEIDENHAIN releases a revised version of splcapimarker.def at irregular intervals. The most recent version of splcapimarker.def is automatically transferred to the control when the NC software is updated.

After an update of the NC software, you will find the current version of the file in the following directory of the control: PLC:\proto\plc\splcapimarker.def.

This means that if the control's software is updated, the interface description of the SPLC-API and its version can change. In order to ensure that the SPLC-API does not change without being noticed, in SMP693 you must enter the version of the SPLC-API used to create the SPLC program. If the value in SMP693 differs from the version of the SPLC-API of the NC software used, the "Changed NC software version" error message will inform you of this. If the SPLC-API versions differ, then you must check the SPLC program. If necessary, you must adapt it and perform a new acceptance test of the machine. After you have checked the SPLC program you must change the entry in SMP693 for the SPLC-API version.

Proceed as follows:

- Replace the splcapimarker.def file:
  During the update of the NC software, a new version of splcapimarker.def was automatically copied to the PLC partition of the control.

▶ Switch to the Programming and Editing operating mode.

▶ Enter the MOD code number 807667 to switch to the PLC Programming mode of operation.

▶ Press the PGM MGT key to open the file manager.

▶ Switch to the PLC:\proto\plc directory.

▶ Copy splcapimarker.def to the program directory of your SPLC program. Overwrite the existing splcapimarker.def file.

▶ After you have checked the SPLC program and translated it with the new splcapimarker.def file, you must change the entry in SMP693 for the SPLC-API version.

Danger

If the SPLC-API version has changed, you must check the SPLC program. If necessary, you must adapt it and perform a new acceptance test of the machine.

Note

Please also copy the splcapimarker.def file to your PC as well, and add it to the PLCdesignNT project. Otherwise, during the next transfer of SPLC project files to the control, the file might be overwritten by the old version.

The SPLC-API programming interface can also be included in the standard PLC program (INCLUDE). If this is the case, the data from **ApiFromSafety** and **ApiToSafety** are copied to the double-word range of the PLC. This data can then be used for additional interrogations or diagnostic purposes in the PLC program.

8.9.2 Safety-related inputs, FS inputs

The SPLC program for the control of a machine tool can access safety-related inputs (= FS inputs) of the machine operating panel (MB 6xx FS or SMOP) and of dual-channel modules in the SPLs (PL 6xxx FS or SPL). Each safety-oriented input must be wired twice (A and B channels) and the information for the two input terminals must be formed by two independent elements (such as a pushbutton with two normally open contacts), see page 6–144. This rules out the possibility of an individual faulty electrical contact leading to an undesired movement.

Danger

For all physical inputs of the SPLC:
If the input marker of the SPLC program has the value 0, then the assigned safety functions must be activated.

The following safety-related inputs are relevant for a simple milling machine:

- ES: external emergency stop (from operating panel, from handwheel, …)
- CVO: "Control Voltage ON" key (one or more)
- SD: door contacts of the guard doors
- PB: permissive buttons/keys (on the handwheel, operating panel, tool magazine)
- KSW: keylock switches for safe operating modes SOM 2, SOM 3, SOM 4
- T.BRK: test input for motor holding brake
- FB_NCC: feedback from the chain of normally closed contacts
- Axis-direction keys
- Other keys with a Start function (NC start, spindle start, spindle jog)
- Keys with a Stop function (NC stop, spindle stop)

Note

If one of the inputs listed above is missing, then instead of the input marker another marker can be defined whose value is set to 0.

Please see page 6–144 for more information about the safety-related inputs.

Plausibility of the permissive button/key

If a permissive button/key is pressed for longer than 30 minutes without interruption, then the SPLC program is to set the corresponding input marker to 0. If the operator releases the permissive button/key, the input marker must also be set to 0. Furthermore, the SPLC program must set an export marker that tells the PLC program to display a warning. This makes it possible to detect a jammed permissive button/key. In all following considerations, the filtered input marker of the permissive button/key is used. Hereinafter, the permissive button/key is only considered to be pressed if the filtered input marker is set to 1. The 30 minutes are a guideline. The risk analysis of the machine can result in a different, perhaps even shorter value.

8.9.3 Safety-related outputs, FS outputs

The SPLC program for the control of a simple milling machine must handle at least the following physical outputs:

- Control of the tool holder
- Control of the motor holding brakes, either axis-specifically or via a global output

Each safety-related output (= FS output) must be wired twice (A and B channels) and the information for the two output terminals must be acted on by two independent elements (such as two relays connected in series in order to release the brakes), see page 6–144. The SPLC program on the MC controls the A channel, and the SPLC program on the CC controls the B channel. This rules out the possibility of a faulty electrical contact leading to an undesired movement.

Please see page 6–144 for more information about the safety-related outputs.

> Danger
>
> For all physical outputs of the SPLC:
> If the output marker of the SPLC program has the value 0, then the assigned safety functions must be activated, and it must be ensured that connected elements activate a status that is safe for the machine operator.

In software version 606 42x-01 without SP, all safe dual-channel outputs of the control system (system module on PLB, PL expansion modules, PL module of UEC, PL module of UMC) were automatically switched off upon an external emergency stop. This switch-off occurred immediately after a triggered emergency stop (ES.x signals) had been detected by the control system. The SPLC outputs remained switched off until the emergency-stop status was rescinded.

However, the behavior described repeatedly leads to difficulties with complex machines, since safe information must be exchanged and safe outputs set even when in an emergency stop state. This became possible with modifications to the NC software and the firmware of the components affected.

- For outputs of a PL 6xxx (system module on PLB, PL expansion modules) this applies as of 606 42x service pack 01.
- For outputs of a UMC 1xx and UEC 1xx (PL part), this applies as of 606 42x service pack 05.

Safe outputs will then no longer automatically be switched off upon an external emergency stop (ES.x signals). In general, safe, dual-channel outputs will then no longer be switched off via safe status bits (4–75). The machine manufacturer will then be responsible for ensuring that the SPLC program switches them off. The interface marker **`NN_GenOutputEnable`** should be used to make a decision about switching off the safe outputs, see page 8–197.

As of the appropriate service pack, this automatic switch-off only occurs if the control crashes, if an internal fault of the component occurs, or if there is a fault in the HSCI communication.

Please note the following should service be necessary:

- Machine with NC software 606 42x-01 without service pack
  - Installation of the service pack
    The firmware of the components is updated automatically. The SPLC program must handle the switch-off of the safe, dual-channel outputs.
  - Installing a new hardware component
    Even if the firmware of the component is newer, it is overwritten by the firmware from the NC software. The NC software handles the switch-off of the safe, dual-channel outputs.
- Machine with NC software 606 42x-01 and corresponding service pack
  - Installing a new hardware component
    The NC software overwrites the firmware of the component with the firmware from the NC software. The SPLC program must handle the switch-off of the safe, dual-channel outputs.

If you have any questions or need assistance with the implementation of these changes, please contact HEIDENHAIN.

8.9.4 SKERN --> SPLC programming interface

The SPLC program receives the following data from the SKERN safety-kernel software in an **ApiFromSafety** structure of the type **SPlcApiFromSafety**:

Element name	Brief description	See page
NN_AxBrkReleaseReq[<axis>]	Request to release the motor holding brake	8–199
NN_AxGrpInMotion[<axis-group>]	Confirmation that at least one axis of the axis group is in motion	8–198, 8–228
NN_AxPosition[<axis>]	Current position value (actual value) of the axis in the reference system in 0.0001 mm or 0.0001 °	
NN_AxGrpState[<axis-group>]	Confirmation of the safety-related status of the axis group (SLS, SOS, STO, AUTO)	8–198
NN_GenSafe	Confirmation that safe operation is possible with an open guard door	
NN_AxSafe[<axis>]	Confirmation that the position value of the axis is reliable	
NN_BrkActivationTest	Confirmation that the test of the brake control is being performed. For this reason, special rules apply for the control of motor holding brakes.	8–199
NN_GenOutputEnable	Confirmation that safe outputs which trigger or permit a motion may be switched on	8–197

As a rule, the following statuses are possible for **NN_AxBrkReleaseReq**:

Status	Brief description
0 (FALSE)	Request to activate an axis-specific motor holding brake
1 (TRUE)	Request to release an axis-specific motor holding brake

As a rule, the following statuses are possible for **NN_AxGrpInMotion**:

Status	Brief description
0 (FALSE)	All axes of the axis group are at standstill
1 (TRUE)	At least one axis of the axis group is in motion

Please note that SPLC marker **NN_AxGrpInMotion** is not synchronized with PLC marker W1026 Axis in position. Due to differing runtimes, it can happen that axes for PLC and SPLC do not come to a standstill at the same time.

As a rule, the following statuses are possible for **NN_AxGrpState**:

Status	Brief description
S_STATE_STO	Safe Torque Off safety function
S_STATE_SOS	Safe Operating Stop safety function
S_STATE_SLS_2, S_STATE_SLS_3, S_STATE_SLS_4	Safely Limited Speed safety function, specifies the safe operating mode SOM_2, SOM_3 or SOM_4 for activating the respectively permissible speed
S_STATE_SLS_S	Restricted Spindle Operation safe operating mode
S_STATE_AUTO	Automatic Mode safe operating mode (SOM_1)

As a rule, the following statuses are possible for **NN_GenSafe**:

Status	Brief description
0 (FALSE)	The safety self-test must be performed before the guard doors may be opened. Safe operation is not ensured while the guard doors are open.
1 (TRUE)	The safety self-test was performed successfully, and the time until the next required test has not elapsed yet. Safe operation is possible while the guard doors are open.

As a rule, the following statuses are possible for **NN_AxSafe**:

Status	Brief description
0 (FALSE)	The position value supplied for the axis is not reliable, and may not be used for the realization of safety functions.
1 (TRUE)	The axis is a safe axis, the axis has been homed, and the axis position has been verified. The position value supplied for the axis is reliable, and can be used for the realization of safety functions.

As a rule, the following statuses are possible for **`NN_BrkActivationTest`**:

Status	Brief description
0 (FALSE)	Test of the brake control is not currently being performed.
1 (TRUE)	Test of the brake control is currently being performed.

As a rule, the following statuses are possible for **`NN_GenOutputEnable`**:

Status	Brief description
0 (FALSE)	The control is in the "external emergency stop" state. Safe outputs that trigger or permit motions should be switched off via the SPLC program.
1 (TRUE)	The control is in normal operation. Safe outputs that trigger or permit a motion can be set.

8.9.5 SPLC --> SKERN programming interface

The SPLC program supplies the following data to the SKERN safety-kernel software in an **ApiToSafety** structure of the type **SPlcApiToSafety**:

Element name	Brief description	See page
PP_AxGrpStopReq[<axis-group>]	Stop reaction (starting on page 4–50) requested for the axis group	8–210
PP_AxGrpStateReq[<axis-group>]	Safety function (as of 4–60) for the axis group	8–200
PP_AxGrpActivate[<axis-group>]	Report of a permissible motion request for at least one axis of the axis group	8–204
PP_AxFeedEnable[<axis>]	Report of a permissible motion request for the axis	8–208
PP_AxGrpPB	Report of a pressed or valid permissive button/key for the axis group	8–214
PP_GenFB_NCC	Feedback on the status of the chain of normally closed contacts	8–215
PP_GenCVO	Control voltage is switched on or is to be switched on	8–215
PP_AxGrpPermitDrvOn[<axis-group>]	Report of a permissible request to switch on the axes of the axis group (drive enabling)	8–215
PP_GenMKG	Group feedback on the status of the machine operating keys	8–217
PP_GenTBRK	Feedback on the status of the test input of the motor holding brakes	8–217
PP_GenSOM	Feedback on the active safety-related operating mode SOM of the machine	8–218

If the SPLC requests a stop reaction or safety function from the SKERN, then the SPLC program is also responsible for showing the operator any relevant error messages. With correct parameterization of the safe machine parameters and of the SPLC program, all requested stop reactions and safety functions run without error messages from the SKERN or the NC software.

Note

Ensure that all requests (stop reactions, safety functions) by the SPLC program run without errors, and are not unwantedly interrupted by an additional error detection or trigger by the NC software. Should this be the case, then the SPLC program must output error messages or instructions for the operator.

8.9.6 PLC --> SPLC programming interface

The importing of PLC operands (markers, double words) into the SPLC should be declared during the definition of the corresponding SPLC operands. The corresponding SPLC operands are to be considered unsafe, and this should also be reflected in their names. The following naming convention has been proposed:

- **PS_M_Name**: for SPLC operands of type M (marker)
- **PS_D_Name**: for SPLC operands of type D (double word)

The SPLC program needs at least the following data from the PLC program:

- Handwheel keys (input markers for handwheel model HR 410, logical markers for handwheel model HR 420): The keys of these handwheels are not safe inputs, and must therefore be imported from the PLC process image.
- Machine operating mode (the SPLC program must distinguish between "manual operation via operating panel", "automatic operation via operating panel", "manual operation via handwheel" and "automatic operation via handwheel")
- The request for restricted spindle operation
- The request for clamping of individual axes
- The request for opening the tool holder

Example:
Importing the NC start and NC stop keys of an HR 410:

```
#TYPE M
    /sFromPlc:M9900        PS_M_Taste_HR410_NC_Stopp
    /sFromPlc:M9901        PS_M_Taste_HR410_NC_Start
```

The PLC modules 9169 (axes for which I32 does not switch off the drives) and 9143 (activation of the brake test) cannot be used for controls with functional safety.

8.9.7 SPLC --> PLC programming interface

The exporting of SPLC operands (markers, double words) into the PLC should be declared during the definition of the corresponding SPLC operands. The following naming convention has been proposed:

- **`SP_M_Name`**: for SPLC operands of type M (marker)
- **`SP_D_Name`**: for SPLC operands of type D (double word)

The SPLC program must realize at least the following safety-related functions and export the appropriate data to the PLC program:

- Status of the handwheel keys after appropriate filtering
- Status of the tool holder

In addition to the explicitly declared export markers, all input markers of the SPLC program are also exported to the PLC program. Each input marker of the SPLC program is mapped to the PLC program's input marker that belongs to the same physical input. The SPLC program must filter the following SPLC input markers:

- Permissive buttons/keys
- Axis-direction keys
- Keys with a Start function on the machine operating panel
- Keys with a Start function on the tool magazine

The PLC program should never change its input markers!

> Attention
>
> Input markers that are not effective due to safety reasons must be set to 0 by the SPLC program. However, no input markers are to be set to 1.

You can find more information about this filtering in the "Filtering of inputs" chapter.

Example:
Exporting the spindle start and spindle jog keys of an HR 410 FS:

```
#TYPE M
    /sToPlc:M9865       SP_M_Taste_HR410_S_Start
    /sToPlc:M9866       SP_M_Taste_HR410_S_Tipp
```

8.9.8 Diagnosis of the SPLC operands

In the control's integral oscilloscope the following channels are available for the diagnosis of freely definable markers, double words and the interface signals between the SKERN and the SPLC:

- SPLC: SPLC operands of the MC SPLC program
- SPLC CC: SPLC operands of the CC SPLC program

These channels are used to record the SPLC operands. Enter the operand in the input field next to SPLC or SPLC CC.

8.10 Tasks of the SPLC Program

8.10.1 Operation with open guard door

Should the A/S guard door be open, then only either the operating panel or the handwheel can be active. They may never both be active at the same time. The keys for triggering and stopping axis movements of the machine are located on the operating panel and the handwheel:

- In the `El. Handwheel` operating mode, the following keys (if present) on the handwheel may be operable: permissive button, spindle jog key, spindle start key, NC start key, axis-direction keys, and stop keys.
  The permissive key, start keys, spindle jog key, and axis-direction keys on the operating panel must be without function. However, all keys on the operating panel that have a Stop function (NC stop, spindle stop, combined NC and spindle stop), if present, must be effective.
- In all other machine operating modes the permissive key, spindle jog key, NC and spindle start keys, axis-direction keys, and stop keys on the operating panel may be active.
  The permissive button, start key and spindle jog key on the handwheel must be without function. However, all keys on the handwheel that have a Stop function must be effective.
- If the T guard door is also open, then neither the keys on the operating panel nor the keys on the handwheel may be active, aside from those that stop motions.

Machine operating mode:	El. Handwheel	Any but Handwheel	Any
T guard door	Closed	Closed	Open
Keys on the operating panel for:			
Stopping a motion	Active	Active	Active
Starting a motion, permissive key	Inactive	Active	Inactive
Not a machine operating key	No regulation	Active	No regulation
Keys on the handwheel for:			
Stopping a motion	Active	Active	Active
Starting a motion, permissive button	Active	Inactive	Inactive
Not a machine operating key	Active	No regulation	No regulation

8.10.2 Selecting a safety-related operating mode (SOM)

The SPLC program must activate the appropriate safe operating mode based on, for example, the setting of one or more keylock switches. The operating mode SOM_4 may only be selected separately, for example via a second keylock switch. If one keylock switch is in the setting for SOM_4, and the other for SOM_2 or SOM_3, then the machine must switch to operating mode SOM_1. The safety-related operating modes must correspond to EN 12417, and the directives from HEIDENHAIN must be followed, see page6–125 to 6–131.

This includes realization of the following functionality in the SPLC program:

- Switching to another safety-related operating mode
  The SPLC program must not permit direct switching from SOM_2 or SOM_3 to SOM_4, nor from SOM_4 to SOM_2 or SOM_3. If the operator nevertheless tries to switch directly, then the SPLC program must instead switch to the SOM_1 safe operating mode.
- Restricted spindle operation
  The SPLC program must import the requirement for restricted spindle operation from the PLC program. If such a requirement is current, and at least safe operating mode SOM_2 is enabled (via keylock switch, for example), then the SPLC program must prescribe the SLS safety function with restricted spindle operation for the axis group of the spindle, instead of the currently active safe operating mode (see page 6–133).

8.10.3 Requirements to be met by SPLC outputs

Global enabling of the outputs

If the marker **NN_GenOutputEnable** = 0 (meaning that it is not set), the SPLC program is to switch off all SPLC outputs that trigger or permit a motion. Outputs that only serve as status message can always be set, regardless of this marker.

The **NN_GenOutputEnable** marker is set to 0 by the SKERN in the following cases (as a prompt to switch off safe PLC outputs):

- At the end of an SS1 reaction upon an external emergency stop (ES.A, ES.B), when axes/spindles have come to a standstill
- At the end of an SS1F reaction (severe hardware or software fault), when axes/spindles have come to a standstill
- At the beginning of an SS0 reaction

Please note that if there is an SS1 reaction (without external emergency stop), e.g. after speed or position monitoring has triggered, the **NN_GenOutputEnable** marker is not set to 0, in contrast to the STO.A.G signal. Upon an internal emergency stop or a fault from the PET table with emergency stop, the **NN_GenOutputEnable** marker remains set (= 1).

The NC switches off all SPLC outputs, regardless of the status of the output markers, if a fatal error of the control occurs, or if the respective PL module goes in an error state itself.

Note

Upon an emergency stop the SPLC program is responsible for switching off the SPLC outputs. The SKERN simply clears the **NN_GenOutputEnable** marker. The machine manufacturer is responsible for the point at which safe outputs must be switched off.

For more information on safety-related outputs, see page 8–188.

Tool holder

The SPLC program imports the request for opening the tool holder from the PLC program. The PLC program may only place this request if the spindle is at a standstill, and if it has been disconnected from power if the guard door is open. The SPLC program checks whether the PLC program is behaving correctly.

If there is no request from the PLC to open the tool holder, then the SPLC program must close the tool holder, see page 6–150.

If there is a request to open the tool holder, and the guard door is closed, the SPLC program must check whether the spindle is at a standstill (**NN_AxGrpInMotion[S]=FALSE**). Then it can open the tool holder. No further checks are necessary once the tool holder has been opened.

If there is a request to open the tool holder, and the guard door is open, the SPLC program must ensure that the spindle is at a standstill and has been disconnected from power, and that it will remain so. To do so, the SPLC program must set **PP_AxGrpStateReq[S]** to the value **S_STATE_STO_O**. If the spindle is not at a standstill, the SKERN will trigger an emergency stop. In the following SPLC cycle the SPLC program can open the tool holder if the PLC program continues to request it, if the axis group is at a standstill (**NN_AxGrpInMotion[S]=FALSE**), and if the axis group has been disconnected from power (**NN_AxGrpState[S]=S_STATE_STO_O** or **S_STATE_STO**). No further checks are necessary once the tool holder has been opened.

In every cycle in which the tool holder and guard door are open, the SPLC program must set **PP_AxGrpStateReq[S]= S_STATE_STO_O** (especially if the guard door is opened while the tool holder is open).

Motor holding brakes

If the motor holding brake of an axis is controlled via a separate output, then the SPLC program is to copy the value of the marker **NN_AxBrkReleaseReq** to this output, i.e. the SPLC program is to release the brake at just the instant when the marker **NN_AxBrkReleaseReq** is set.

If the motor holding brakes of multiple axes are controlled via a collective output, the SPLC program is to differentiate between normal operation and the brake control test:

- In normal operation (**NN_BrkActivationTest** = FALSE) the SPLC program is to gate the **NN_AxBrkReleaseReq** markers for all drives involved with logical AND, and copy the result to the brake output, i.e. the SPLC program is to release the brakes when the **NN_AxBrkReleaseReq** markers are set for all axes involved.
- During the motor brake control test (**NN_BrkActivationTest** = TRUE), the SPLC program is to gate the **NN_AxBrkReleaseReq** marker for all drives involved with logical OR and copy the result to the brake output.

The SKERN sets **NN_AxBrkReleaseReq** correctly during switch-on/switch-off of the drives: The SKERN also ensures for non-safe axes that **NN_AxBrkReleaseReq** is never set when the drive is switched off. Therefore, it is usually not necessary to consider additional information from the PLC.

During the motor brake control test (**NN_BrkActivationTest** = TRUE) the SPLC program must always observe the value set in **NN_AxBrkReleaseReq**. From a safety point of view, it would not be problematic to activate the motor brake outside of this test, although **NN_AxBrkReleaseReq** is set. If an error occurs during the brake control test, **NN_AxBrkReleaseReq** is set to 0 to activate the brakes.

If the SPLC program releases a motor brake although **NN_AxBrkReleaseReq** is not set, safe brake control cannot be guaranteed anymore. This may be permitted from a safety perspective if according to the machine manufacturer's risk analysis the motor brakes generally do not have a safety function, or do not have a safety function in a special operating situation (e.g. if the guard door is closed). However, it must be noted that temporary single-channel control of the axis brakes, even if permitted from a safety perspective, increases the danger of damage to the machine (especially if there are any hanging axes).

For more information about the SBC safety function and brake control, see page 4–66 and page 7–164 ff.

8.10.4 Requirements on the data of the ApiToSafety structure

The interface data from the SPLC program to the SKERN safety-kernel software are collected in an **SPlcApiToSafety** structure.

From the point of view of the PLC, this structure consists of markers and double words.

PP_AxGrpStateReq

The attribute **PP_AxGrpStateReq** in **SPlcApiToSafety** is an array of double words, where each array index specifies an axis group. The permissible values are defined in the **splcapimarker.def** file as constants:

Status	Brief description
S_STATE_STO	Safe Torque Off safety function
S_STATE_STO_O	Safe Torque Off Operating safety function
S_STATE_SOS	Safe Operating Stop safety function
S_STATE_SLS_2, S_STATE_SLS_3, S_STATE_SLS_4	Safely Limited Speed safety function, specifies the safe operating mode SOM_2, SOM_3 or SOM_4 for activating the respectively permissible speed
S_STATE_SLS_S	Restricted Spindle Operation safe operating mode
S_STATE_AUTO	Automatic Mode safe operating mode (SOM_1)

In **PP_AxGrpStateReq** the SPLC program specifies for each axis group what the minimum level of monitoring for the respective axis group is during the current state of the guard doors and the setting of the keylock switch. **PP_AxGrpStateReq** does not take into account other keys that influence the monitoring (emergency stop, permissive buttons/keys, start keys, stop keys, etc.).

The safety-kernel software might perform even stricter monitoring than prescribed by the SPLC program, but never a less strict monitoring. It reports the monitoring actually in effect to the SPLC program via **NN_AxGrpState**.

NC axes

For each axis group with NC axes, the SPLC program must set the **PP_AxGrpStateReq** marker to one of the following values, depending on the state of the guard door of the associated working space and the active safe operating mode:

Guard door	Safety-related operating mode	**PP_AxGrpStateReq**
Open	SOM_1	**S_STATE_SOS**
Open	SOM_2	**S_STATE_SLS_2**
Open	SOM_3	**S_STATE_SLS_3**
Open	SOM_4	**S_STATE_SLS_4**
Closed	*[a]	**S_STATE_AUTO**

[a] Any value: The value does not influence the decision.

If the control is in safe operating mode SOM_1 and the guard door is open, the SPLC must set the **PP_AxGrpStateReq** marker to the value S_STATE_SOS. However, in this case it is not necessary for the SPLC to additionally request a stop reaction. Setting **PP_AxGrpStateReq = S_STATE_SOS** already ensures that an SS1 reaction will be triggered by the SKERN if an axis should move while the control is in this state.

Spindles

If a tool holder on a spindle is open, then the SPLC program is to set the **PP_AxGrpStateReq** marker for the axis group to which this spindle belongs to the value **S_STATE_STO_0**, so that this spindle is disconnected from power.

If all tool holders on the spindles of an axis group are closed, then the SPLC program is to set the **PP_AxGrpStateReq** marker to one of the following values, depending on:

- the state of the guard door of the associated working space,
- the active safe operating mode and
- the state of the restricted spindle operation (requested / not requested)

Guard door	Safety-related operating mode	Restricted spindle operation SOM_S	**PP_AxGrpStateReq**
Open	SOM_1	Any	**S_STATE_SOS**
Open	SOM_2	No	**S_STATE_SLS_2**
Open	SOM_3	No	**S_STATE_SLS_3**
Open	SOM_4	No	**S_STATE_SLS_4**
Closed	*[a]	Any	**S_STATE_AUTO**

[a] Any value: The value does not influence the decision.

Auxiliary axes of the tool magazine

The tool magazine is typically located in its own working space, with its own guard door. If the working space of the tool magazine is sufficiently separated from the normal working space, then it suffices to consider just the guard door of the tool magazine. In this case the SPLC program should set the **PP_AxGrpStateReq** marker for every axis group with auxiliary axes to one of the following values, depending on the state of the guard door:

Guard door	**PP_AxGrpStateReq**
Open	**S_STATE_SLS_2**
Closed	**S_STATE_AUTO**

In addition, the SPLC program should request suitable stop functions, in order to stop or prevent motions that are not permitted. The setting of the keylock switch is not taken into consideration here, since it is usually located at a greater distance from the guard door of the tool magazine.

If auxiliary axes are accessible from the normal working space, then the SPLC program should specify the requested state of the axis group in a similar manner as for the spindles:
For a closed guard door: **S_STATE_AUTO**; for an open guard door it depends on the setting of the keylock switch: **S_STATE_SOS** or **S_STATE_SLS_***.

Similar rules as for spindles apply to the motions of such auxiliary axes:
A motion must always be started with a permissive key and a specific motion key. The motion may only be maintained as long as the permissive key is pressed.

PP_AxGrpActivate

The attribute **PP_AxGrpActivate** in **SPlcApiToSafety** is an array of logical markers, where each array index specifies an axis group. It can have the following states:

Status	Brief description
0 (FALSE)	Axis group must not be activated
1 (TRUE)	Axis group can be activated

The SPLC program uses the **PP_AxGrpActivate** marker to report to the safety-kernel software that there is a current event permitting a motion of the associated axis group. If the guard door is open, then a key must always be pressed in order to start a motion, so the SPLC program should set the marker at just the instant when a key with which the axis group can be moved is pressed. If the guard door is closed, the machine can start a motion automatically, even without a key being pressed. But no motion may occur as an immediate reaction to the guard door having just been closed. Therefore, the SPLC program should set the **PP_AxGrpActivate** marker if, since the last time the guard door was closed, a key was pressed with which the axis group can be moved. The exact rules vary depending on the type of the axis group.

NC axes

If the working space of an axis group with NC axes is completely protected by guard doors, then the SPLC program is to set the **PP_AxGrpActivate** marker to **FALSE** at first. If an axis-direction key, NC start or permissive button on the handwheel is pressed while the guard door is closed, then the SPLC program is to set the marker to **TRUE**. Once this has happened, the SPLC program should continue setting the marker to **TRUE** as long as the guard door remains closed.

If the working space of an axis group with NC axes is not completely protected by guard doors, and the control is being operated via the operating panel, then the SPLC program is to set the **PP_AxGrpActivate** marker to one of the following values for this axis group, depending on the active safe operating mode and the keys on the machine operating panel:

Safety-related operating mode	Permissive key MB (SMOP)	Axis-direction key	NC start MB (SMOP)	**PP_AxGrpActivate**
SOM_2, SOM_3, SOM_4	[a]	At least one is pressed	*	**TRUE**
SOM_2, SOM_3, SOM_4	Pressed	*	Considered pressed after positive edge detected[b]	**TRUE**
Any other combination				**FALSE**

a. Any value: The value does not influence the decision.

b. The SPLC program sets PP_AxGrpActivate upon the positive edge of the start key if the permissive key is pressed. It clears PP_AxGrpActivate when the start key or permissive key is no longer pressed.

If the working space of an axis group with NC axes is not completely protected by guard doors, and the control is being operated via the handwheel, then the SPLC program is to set the **PP_AxGrpActivate** marker to one of the following values for this axis group, depending on the safe operating mode and the keys on the handwheel:

Safety-related operating mode	Permissive button handwheel (HR)	NC start handwheel	**PP_AxGrpActivate**
SOM_2, SOM_3, SOM_4	Pressed	*[a]	**TRUE**
Any other combination			**FALSE**

[a] Any value: The value does not influence the decision.

If the T guard door is also open, then the SPLC program is to set **PP_AxGrpActivate[A]** to **FALSE** for the NC axes.

MG_Program_ Running marker

In addition to the **PP_AxGrpActivate[A]** marker, the SPLC program is also to handle a marker called **MG_Program_Running**. It should set this marker simultaneously with **PP_AxGrpActivate[A]** if it accepts an NC start as valid, i.e. if it has detected a positive edge for the currently effective start key while a permissive button/key is pressed. Furthermore, the SPLC program is also to set the **MG_Program_Running** marker if it sets the **PP_AxGrpActivate[A]** marker because the guard door is closed. The SPLC program is to clear the **MG_Program_Running** marker if **NN_AxGrpState[A]** is for 1 second in a state that does not permit a motion (**S_STATE_SOS**, **S_STATE_STO_0** or **S_STATE_STO**). The SPLC program needs the **MG_Program_Running** marker in order to control **PP_AxFeedEnable** correctly, see page 8–208.

For the safety-related operating modes SOM_2 and SOM_3 to be in accordance with EN 12417, the permissive button/key must be pressed in order to maintain programmed and automatic motions. For this to function correctly, the SPLC program must clear the **MG_Program_Running** marker if the permissive button/key is not pressed, or if the permissive button/key pressed is not associated with the working space in question. If the **MG_Program_Running** marker was set before deletion, the SPLC program must request an SS2 for an SPLC cycle.

Spindles

If the working space of an axis group with spindles is completely protected by a guard door, then the SPLC program is to set the **PP_AxGrpActivate** marker to **FALSE** for this axis group at first. If the spindle-jog key, spindle start key, NC start or permissive button on the handwheel is pressed while the guard door is closed, then the SPLC program is to set the marker to **TRUE**. Once this has happened, the SPLC program should continue setting the marker to **TRUE** as long as the guard door remains closed.

If the working space of an axis group with spindles is not completely protected by a guard door, and the control is in the **El. Handwheel** operating mode, then the SPLC program is to set the **PP_AxGrpActivate** marker to one of the following values for this axis group, depending on:

- the safe operating mode and
- the keys on the handwheel

Safety-related operating mode	Permissive button handwheel (HR)	Spindle start (single-channel)	Spindle jog (single-channel)	**PP_AxGrpActivate**
SOM_2, SOM_3, SOM_4	Pressed	*[a]	Pressed	**TRUE**
SOM_2, SOM_3, SOM_4	Pressed	Considered pressed after positive edge detected	*	**TRUE**
Any other combination				**FALSE**

a. Any value: The value does not influence the decision.

If the working space of an axis group with spindles is not completely protected by a guard door, and the control is in a "being operated via operating panel" mode, then the SPLC program is to set the **PP_AxGrpActivate** marker to one of the following values for this axis group, depending on:

- the safe operating mode and
- the keys on the machine operating panel

Safety-related operating mode	Permissive key MB (SMOP)	Spindle start	Spindle jog	**PP_AxGrpActivate**
SOM_2, SOM_3, SOM_4	Pressed	*[a]	Pressed	**TRUE**
SOM_2, SOM_3, SOM_4	Pressed	Positive edge	*	**TRUE**
Any other combination				**FALSE**

a. Any value: The value does not influence the decision.

If the T guard door is also open, then the SPLC program is to set **PP_AxGrpActivate[S]** to **FALSE** for the spindle, regardless of the operating mode.

Auxiliary axes of the tool magazine

The SPLC program is to set the **PP_AxGrpActivate** marker for an axis group with auxiliary axes to one of the following values, depending on the state of

- the guard doors of the associated working space,
- the associated permissive key and
- the associated motion keys

Guard door	Permissive key of tool magazine	Motion keys of tool magazine	**PP_AxGrpActivate**
Open	Not pressed	*[a]	**FALSE**
Open	*	No motion key pressed, or more than one at the same time	**FALSE**
Open	Pressed	One motion key pressed	**TRUE**
Closed	*	*	**TRUE**[1]

[a] Any value: The value does not influence the decision.

1) Any pending automatic movements are started by setting the **PP_AxGrpActivate** marker when the guard door is closed. This may mean an unexpected start-up for the operator.
If the tool magazine is designed such that persons can stay inside the tool magazine while the guard door of the tool magazine is closed, additional protective measures must be taken. Under no circumstances may magazine axes move while persons are inside the tool magazine. This can be ensured, for example, by the SPLC program setting the **PP_AxGrpActivate** marker only after the operator has pressed a key to confirm that there is no one left inside the tool magazine. In this way, he confirms that automatic movements may be started.

PP_AxFeedEnable

The attribute **PP_AxFeedEnable** in **SPlcApiToSafety** is an array of logical markers, where each array index specifies an axis. It can have the following states:

Status	Brief description
0 (FALSE)	Axis not enabled
1 (TRUE)	Axis enabled

The SPLC program uses the **PP_AxFeedEnable** marker to report to the safety-kernel software that the associated axis may be moved. This marker is important for when not all of the axes in an axis group may be moved, especially for manual motions using the axis-direction keys.

NC axes

If the working space in which an NC axis is located is completely protected by guard doors (all guard doors of the working space are closed), then the SPLC program is to set the **PP_AxFeedEnable** marker to **TRUE** for this axis.

If the working space in which an NC axis is located is not completely protected by guard doors (not all guard doors of the working space are closed), then the SPLC program is to set the **PP_AxFeedEnable** marker for this axis to one of the following values, depending on the operating mode, the axis-direction keys of this axis, the permissive button on the handwheel and the **MG_Program_Running** marker (see 8–204).

- During operation via the operating panel (manual or automatic), the SPLC program is to set the **PP_AxFeedEnable** marker to **TRUE** for exactly the period that the **MG_Program_Running** marker is set or an axis-direction key for the corresponding axis is pressed.
- During operation via the handwheel, the SPLC program is to set the **PP_AxFeedEnable** marker to **TRUE** for exactly the period that the **MG_Program_Running** marker is set or the permissive button on the handwheel is pressed. The SKERN monitors the maximum number of axes that may be moved simultaneously.

Spindles

For machines with only one spindle, the SPLC program can always set the **PP_AxFeedEnable** marker to **TRUE**. The spindle has the constant 18 in the **PP_AxFeedEnable** marker. **PP_AxGrpActivate** and **PP_AxGrpStopReq** manage the protection against unexpected motions of axes.

There are no generally valid rules for machines with more than one spindle. A risk analysis specific to the situation must be used to decide which spindle or spindles may be moved with which keys if the guard door is open.

Auxiliary axes of the tool magazine

If the working space in which an auxiliary axis is located is completely protected by guard doors, then the SPLC program is to set the **PP_AxFeedEnable** marker to **TRUE** for this axis. If not, then it is to set the marker to **TRUE** for exactly the period that an axis-direction key is pressed for this auxiliary axis.

PP_AxGrpStopReq

The attribute **PP_AxGrpStopReq** in **SPlcApiToSafety** is an array of double words, where each array index specifies an axis group. The permissible values are defined in the **splcapimarker.def** file as constants.

The SPLC program uses **PP_AxGrpStopReq** to request that the safety-kernel software perform a specific deceleration operation.

General information

The SPLC program should set the **PP_AxGrpStopReq** marker for each axis group to one of the following values:

S_STOP_SS1F	Deceleration along the emergency braking ramp, due to emergency stop or fatal error
S_STOP_SS1	Deceleration along the emergency braking ramp
S_STOP_SS1D	Delayed deceleration along the emergency braking ramp
S_STOP_SS2	Deceleration along the contour
S_STOP_NONE	No special deceleration operation

If the SPLC program wants to prevent all axes of an axis group from moving, then it should set the **PP_AxGrpStopReq** marker to the value **S_STOP_SS2** for this axis group. If it wants to prevent motion of a specific axis, then it should set the **PP_AxFeedEnable** marker to **FALSE** for this axis.

Closed guard door

If the working space of an axis group is completely protected by a guard door, then the SPLC program is to set the **PP_AxGrpStopReq** marker to **S_STOP_NONE** for this axis group.

Opened guard door for NC axes

If the working space of an axis group with NC axes is not completely protected by a guard door, then the SPLC program is to set the **PP_AxGrpStopReq** marker for this axis group to one of the following values, depending on operation events:

Event	**PP_AxGrpStopReq**
Stop key is pressed	**S_STOP_SS2**
External stop request (issued by additional external dual-channel devices, for example)	**S_STOP_SS2**
T guard door open	**S_STOP_SS2**[a]
Switchover of safety-related operating mode SOM_x	**S_STOP_SS2**
SOM_2 or SOM_3 is active, A/S guard door is open and the permissive button/key is no longer pressed while an NC program is being run	**S_STOP_SS2**[1]
Other	**S_STOP_NONE**

[a] The risk analysis for the machine must show whether stopping of the NC axes is actually necessary here.

1) You will find more detailed information in the description of **MG_Programm_Running**, see page 8–205. The HEIDENHAIN design generally permits manual axis movements via dual-channel axis-direction keys without additional permissive button/key. However, this results in a complex logic for controlling the **PP_AxFeedEnable** and **PP_AxGrpStopReq** markers.
If you want the operator to also press the permissive button/key for performing manual axis movements with the axis-direction keys, this can be implemented in the SPLC program as simply as follows: Set the **PP_AxFeedEnable** marker permanently to TRUE, and if the guard door is open, set the **PP_AxGrpStopReq** marker always to **S_STOP_SS2** when no permissive button/key is valid or pressed.

Opened guard door for spindle axes

If the working space of an axis group with spindles is not completely protected by a guard door, and one of the safety-related operating modes SOM_2, SOM_3 or SOM_4 is active, then the SPLC program is to set the **PP_AxGrpStopReq** marker for this axis group to one of the following values, depending on operation events:

Event	**PP_AxGrpStopReq**
Stop key is pressed	**S_STOP_SS2**
External stop request	**S_STOP_SS2**
Spindle jog key released	**S_STOP_SS2**
T guard door open	**S_STOP_SS1D**[a]
Switchover of safety-related operating mode SOM_x	**S_STOP_SS2**
Other	**S_STOP_NONE**

[a] The risk analysis for the machine must show whether stopping of the spindle is actually necessary here.

If the operating element is switched, i.e. when changing from handwheel operation to the operating panel, or vice versa, a stop with **S_STOP_SS2** can be useful or even necessary. You, as the OEM, must make this decision separately for each machine, depending on its specific design.

Auxiliary axes of the tool magazine

If the working space of the tool magazine is not completely protected by a guard door, then the SPLC program is to set the **PP_AxGrpStopReq** marker for this axis group to one of the following values, depending on operation events:

Event	**PP_AxGrpStopReq**
T guard door is opened while the tool magazine is in motion	**S_STOP_SS1**
Permissive key and exactly one tilting key are pressed	**S_STOP_NONE**
Switchover of safety-related operating mode SOM_x	**S_STOP_SS2**
Other	**S_STOP_SS2**

There are no stop keys for the auxiliary axes.

Stop event

It suffices for the SPLC program to set a stop request in an SPLC cycle if a stop is necessary. The SKERN is responsible for maintaining the stopped status until the stop has concluded.

PP_AxGrpPB

The attribute **PP_AxGrpPB** in **SPlcApiToSafety** is an array of logical markers, where each array index specifies an axis group. It can have the following states:

Status	Brief description
0 (FALSE)	No valid permissive button/key pressed for the axis group
1 (TRUE)	A valid permissive button/key is pressed for the axis group

The SPLC program uses **PP_AxGrpPB** to report the status of the currently effective permissive button/key to the safety-kernel software.

Permissive buttons/keys

The following rules apply to **PP_AxGrpPB**:

	A/S guard door open AND T guard door open	A/S guard door closed OR T guard door closed	
	Operation via handwheel or operating panel	Operation via handwheel	Operation via operating panel
PP_AxGrpPB[A]	**FALSE**	Permissive button of handwheel	Permissive key of operating panel
PP_AxGrpPB[S]	**FALSE**	Permissive button of handwheel	Permissive key of operating panel
PP_AxGrpPB[T]	Permissive key of tool magazine	Permissive key of tool magazine	Permissive key of tool magazine

For more information on permissive buttons/keys, see page 6–146.

PP_GenFB_NCC

The **PP_GenFB_NCC** attribute in **SPlcApiToSafety** is a marker. It can have the following states:

Status	Brief description
0 (FALSE)	Chain of normally closed contacts is open
1 (TRUE)	Chain of normally closed contacts is closed

Feedback from chain of normally closed contacts

The SPLC program is to copy the value from the SPLC input for the feedback from the chain of normally closed contacts into the **PP_GenFB_NCC** marker.

For more information on the normally closed contacts, see page 6–148.

PP_GenCVO, PP_AxGrpPermitDrvOn

The SPLC uses the **PP_GenCVO** signal to report to the SKERN that the control voltage may be switched on. The **PP_GenCVO** attribute in **SPlcApiToSafety** is a marker. It can have the following states:

Status	Brief description
0 (FALSE)	No valid request for "Control Voltage ON"
1 (TRUE)	Valid request for "Control Voltage ON"

The SPLC uses the **PP_AxGrpPermitDrvOn** signal to report to the SKERN that the drives belonging to an axis group may be switched on. The SPLC program uses the signal to request from the SKERN that the STO safety function be canceled for the axis group, and that the axis group be set to the SOS state.

Theoretically, a separate safe key could be used for this enabling, but in practice the "Control Voltage ON" key is used for this.

The attribute **PP_AxGrpPermitDrvOn** in **SPlcApiToSafety** is an array of logical markers, where each array index specifies an axis group. It can have the following states:

Status	Brief description
0 (FALSE)	No drive enabling
1 (TRUE)	Drive enable

Status "Machine ON"

The SPLC program is to set the **PP_GenCVO** marker when the "Control Voltage ON" key of the machine operating panel is pressed or the latch circuit is set via the corresponding relay (e.g. K1).

Request "Control Voltage ON"

The SPLC program is to set the **PP_GenCVO** marker when the "Control Voltage ON" key of the operating panel is pressed. On simpler machines the "Control Voltage ON" key of the operating panel also switches all axis groups on. In these cases the state of the **PP_GenCVO** marker is to be copied into the markers **PP_AxGrpPermitDrvOn[A]** (for NC axes), **PP_AxGrpPermitDrvOn[S]** (for spindles) and **PP_AxGrpPermitDrvOn[T]** (for auxiliary axes of the tool magazine).

Separate key for "Control Voltage ON" on the tool magazine

If the tool magazine has its own switch-on key, then the SPLC program is to copy the state of this key into the **PP_AxGrpPermitDrvOn[T]** marker. The state of the "Control Voltage ON" key of the operating panel should continue to be copied into the **PP_AxGrpPermitDrvOn[A]** and **PP_AxGrpPermitDrvOn[S]** markers.

For more information on the control voltage, see page 6–154.

PP_GenMKG

The **PP_GenMKG** attribute in **SPlcApiToSafety** is a marker. It can have the following states:

Status	Brief description
0 (FALSE)	No machine operating key pressed
1 (TRUE)	At least one machine operating key is pressed

Group information about machine movement keys

The SPLC program is to set the **PP_GenMKG** marker to **TRUE** for exactly the period that at least one key having no stop function is pressed. Such keys include all permissive buttons/keys, the axis-direction keys on the operating panel and the axis-direction keys for the tool magazine. However, the single-channel axis-direction keys on the handwheel have no influence on this marker.

The **PP_GenMKG** marker should be set appropriately before the signals from the keys are filtered. Only the unfiltered key signals are to be considered for the evaluation of this marker. See the "Filtering of inputs" chapter for more information about the filtering of key signals.

For more information on the machine operating keys, see page 6–153.

PP_GenTBRK

The **PP_GenTBRK** attribute in **SPlcApiToSafety** is a marker. It can have the following states:

Status	Brief description
0 (FALSE)	Test input active
1 (TRUE)	Test input inactive

Test input of the brakes

The SPLC program is to copy the state of the physical test input T.BRK for the motor holding brakes into the **PP_GenTBRK** marker.

For more information on the brake control, see page 7–164.

PP_GenSOM

The **PP_GenSOM** attribute in **SPlcApiToSafety** is a double word. The permissible values are defined in the **splcapimarker.def** file as constants.

Active safe operating mode

The SPLC program is to set **PP_GenSOM** to one of the following values, depending on the active safe operating mode.

Status	Brief description
S_MODE_SOM_1	Safe operating mode SOM_1 active
S_MODE_SOM_2	Safe operating mode SOM_2 active
S_MODE_SOM_3	Safe operating mode SOM_3 active
S_MODE_SOM_4	Safe operating mode SOM_4 active

PP_GenSOM is evaluated at the following locations:

- By the SKERN:
  Allow/Reject the permissive button/key in the "Check axes" mode of operation
- By the NC software:
  Display of active safe operating mode on the screen
- By the NC software:
  Limitation of axis and spindle speed when the F LIMIT soft key is pressed

8.10.5 Filtering of inputs

The most important function involved in exporting operands from the SPLC to the PLC program is the filtering of inputs. The SPLC program must use this filter to always ensure that if a guard door is open, then only **one** operating element may be functional. This filter is a single-channel mechanism.

> Attention
>
> The SPLC program only filters those inputs that trigger a motion, but never the inputs that stop a motion!

For more information about the filtering of inputs of keys, see page 6–142.

Handwheel keys

The SPLC program must read the permissive button on the handwheel as an SPLC input, and import the other handwheel inputs from the PLC program. These inputs must be filtered, and the filtered values then exported to the PLC program.

> Note
>
> This filtering must also be in effect in the SPLC program itself. It should occur after **PP_GenMKG** has been determined, but before the further evaluation of the inputs.

The following filter rule applies here:

```
IF A/S guard door is open
(
      IF T guard door is open OR NOT operation via handwheel
      (
            IF handwheel key without STOP function is pressed
            (
                  set the "handwheel key cleared" export marker
            )
            clear the handwheel permissive button
            clear the handwheel inputs that do not have a STOP
function
      )
)
```

If the A/S guard door is open and the **El. Handwheel** operating mode is not active, then the handwheel must be set inactive. In this situation the SPLC program must clear the permissive button on the handwheel. The PLC program must block the handwheel pulses if it has received the information "not pressed" from the permissive button on the handwheel.

The status of the T guard door only has an influence on the handwheel inputs if the A/S guard door is open.

If the PLC program detects that the handwheel keys have been cleared and the T guard door is open, then it is to display a "T guard door open" message.

Machine operating panel keys

The SPLC program reads the keys on the machine operating panel as SPLC inputs. It must filter the corresponding input markers, and the PLC program then automatically sees the filtered values in its input markers.

> Hinweis
>
> This filtering must also be in effect in the SPLC program itself. It should occur after **PP_GenMKG** has been determined, but before the further evaluation of the inputs.

The following filter rule applies here:

```
IF A/S guard door is open
(
      IF T guard door is open OR NOT operation via MB
      (
            IF MB key without STOP function is pressed
            (
                  set the "MP key cleared" export marker
            )
            clear the MB permissive key
            clear the MB inputs that do not have a STOP function
      )
)
```

The status of the T guard door only has an influence on the inputs of the operating panel if the A/S guard door is open.

If the PLC program detects that the operating panel keys have been cleared and the T guard door is open, then it is to display a "T guard door open" message.

Keys on the tool magazine

The SPLC program reads the permissive key and the tilting keys on the tool magazine as SPLC inputs. It must filter the corresponding inputs, and the PLC program then automatically sees the filtered values in its input markers.

> Hinweis
>
> This filtering must also be in effect in the SPLC program itself. It should occur after **PP_GenMKG** has been determined, but before the further evaluation of the inputs.

The following filter rule applies here:

```
IF T guard door is open
(
      IF NOT T permissive key
      (
            clear tool magazine inputs that do not have a STOP
function
      )
)
```

8.11 Sample Cases

The examples and exceptions described in this chapter are intended to explain and summarize the formal specification of the SPLC program. This section complements the overall chapter, and should serve to improve understanding of the formal specification.

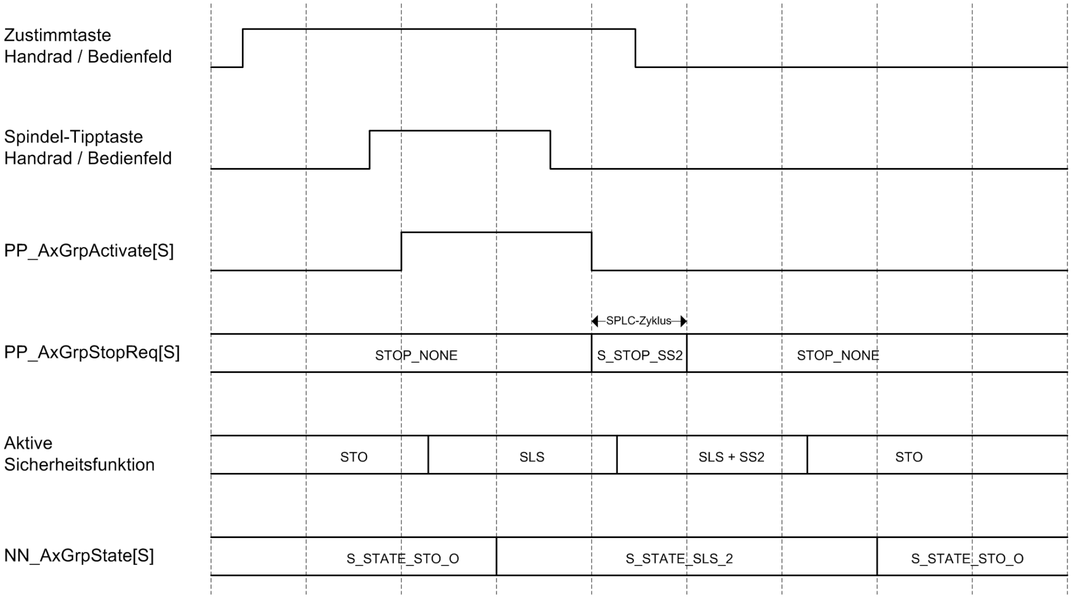
8.11.1 Movement of NC axes and spindle

For the activation of a special operating mode with open A/S guard door, a distinction must be made between keys like NC start and spindle start, where the motion continues even once the key is released, and keys like the axis-direction keys, which only permit a motion as long as the key is pressed. If the motion is to be stopped once the key is released, the SPLC program must set the **PP_AxFeedEnable** marker to **FALSE** upon release of the key. Additionally, it can trigger an SS2 stop for the corresponding axis group.

Spindle jog key

Movement of the axis group S via the spindle jog key

The figure below shows the sequence for motion of the spindle via the spindle jog key either on the operating panel or the handwheel, in the safety-related operating mode SOM_2:



Spindle start key

Movement of the axis group S via the spindle start key

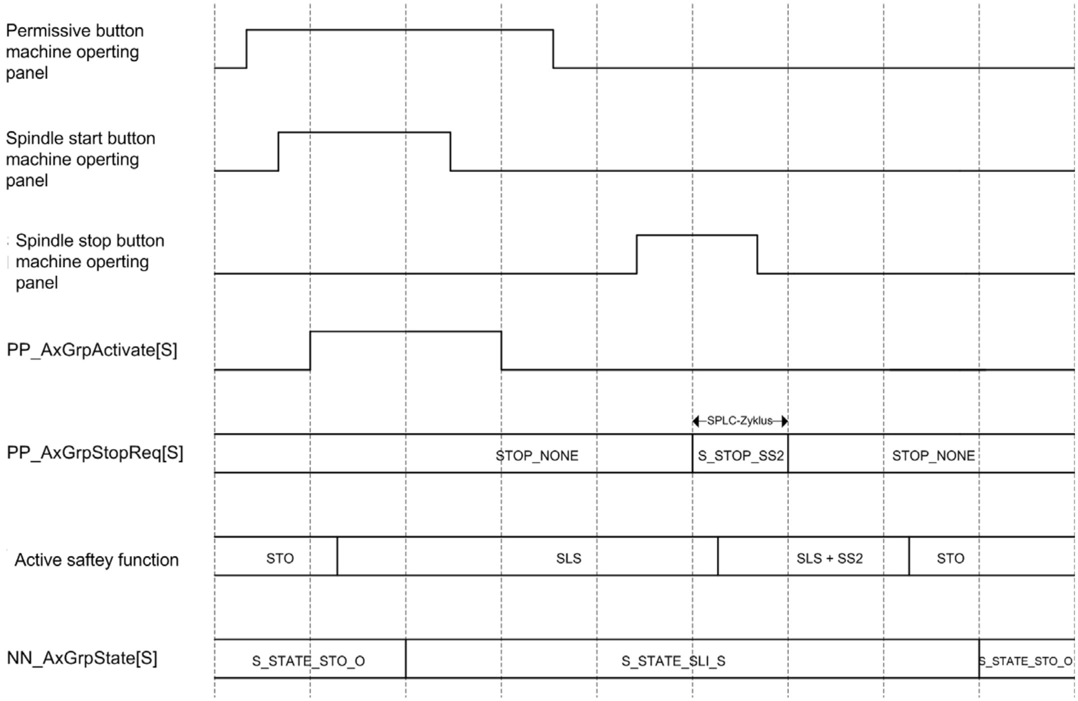
The figure below shows the sequence for starting the spindle via the spindle start key either on the operating panel or the handwheel. The SPLC program detects a valid spindle start upon the positive edge of the spindle start key while the permissive key is pressed.

Here is an example of how this can work:
If the permissive key and spindle start key are pressed, and spindle start was not pressed in the previous cycle, the SPLC program sets the **PP_AxGrpActivate** marker. If either the permissive key or spindle start key are not pressed, it clears the **PP_AxGrpActivate** marker.

After the spindle has been started, it remains in motion until it is explicitly stopped, for example via the spindle stop key or the emergency stop input.

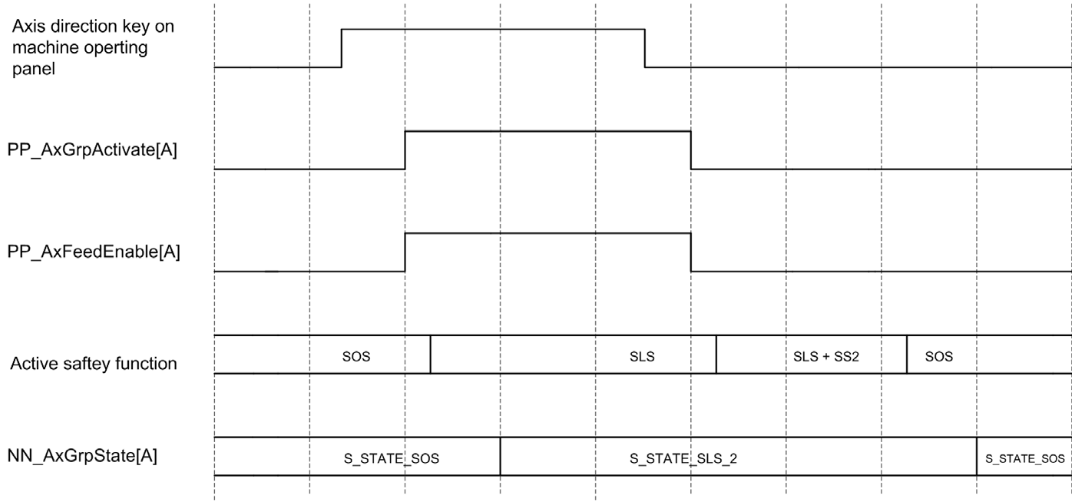
In safe operating modes SOM_2 and SOM_3 without restricted spindle operation, the SKERN also stops the spindle if the permissive key is released. The SKERN receives the status of the permissive key via the **ApiToSafety.PP_AxGrpPB** attribute. The same applies to operation via the handwheel.

Only during operation via the operating panel in safe operating mode SOM_4 or with restricted spindle operation does the spindle continue running upon release of the permissive key, until it is explicitly stopped. This case is shown in the figure below.



Axis group of NC axes

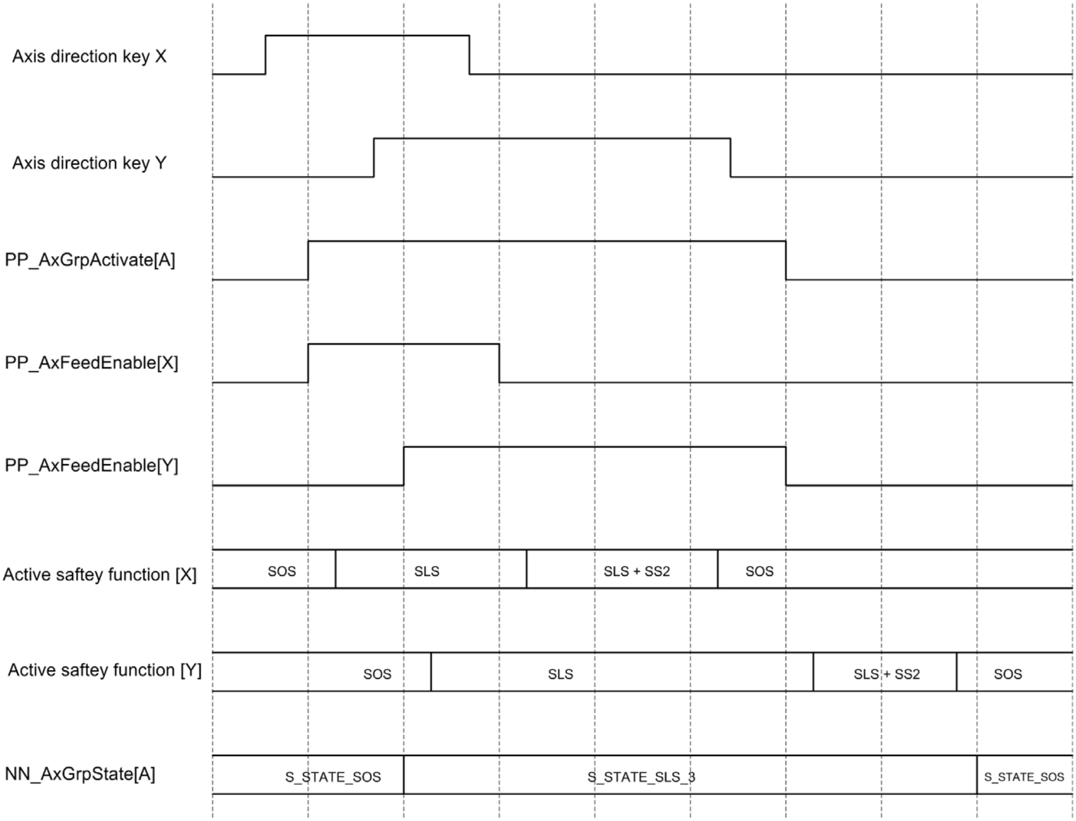
The figure below shows the sequence for a motion of an NC axis (axis group A) via the machine operating panel in SOM_2:



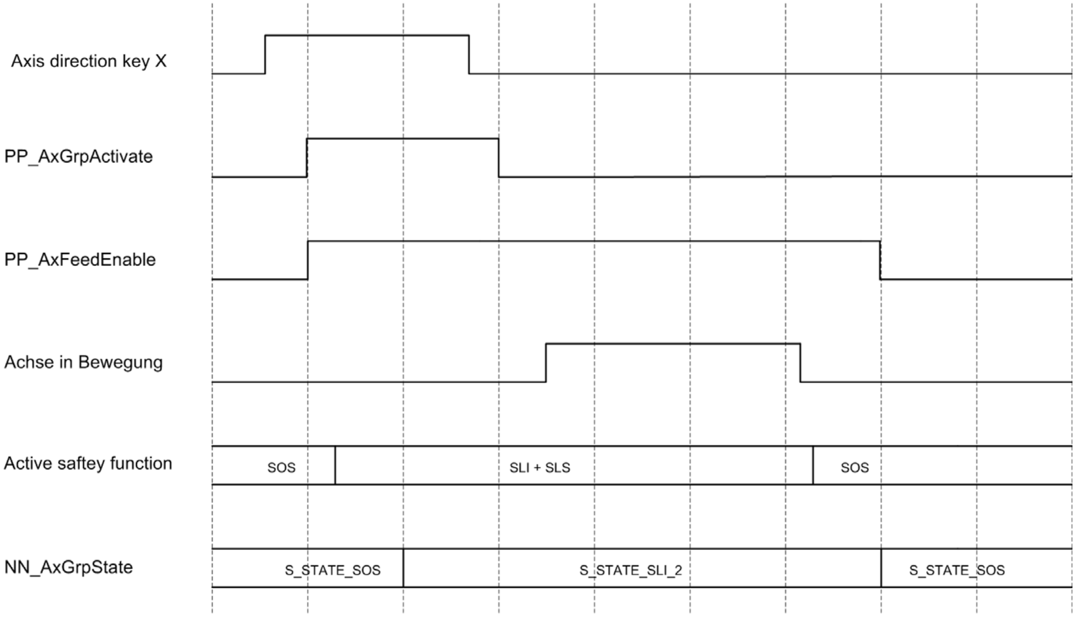
As indicated in the figure, in manual operation the NC axes may be moved with a dual-channel axis direction key via the operating panel, without having to press a permissive key.

On the other hand, the permissive key must be pressed for every axis movement with manual operation of the control in the **El. Handwheel** operating mode, since this is the only dual-channel key on the handwheel. An axis-direction key is not necessary, since the axes can also be moved via the wheel on the handwheel. The SPLC is not aware of any operations using the wheel.

If multiple axes are moved simultaneously, the SPLC program sets the **PP_AxGrpActivate** marker to **TRUE** as long as at least one axis-direction key is pressed. If just one axis-direction key is released, then the SPLC program sets the corresponding **PP_AxFeedEnable** marker to **FALSE**, which triggers a stop of the corresponding axis.

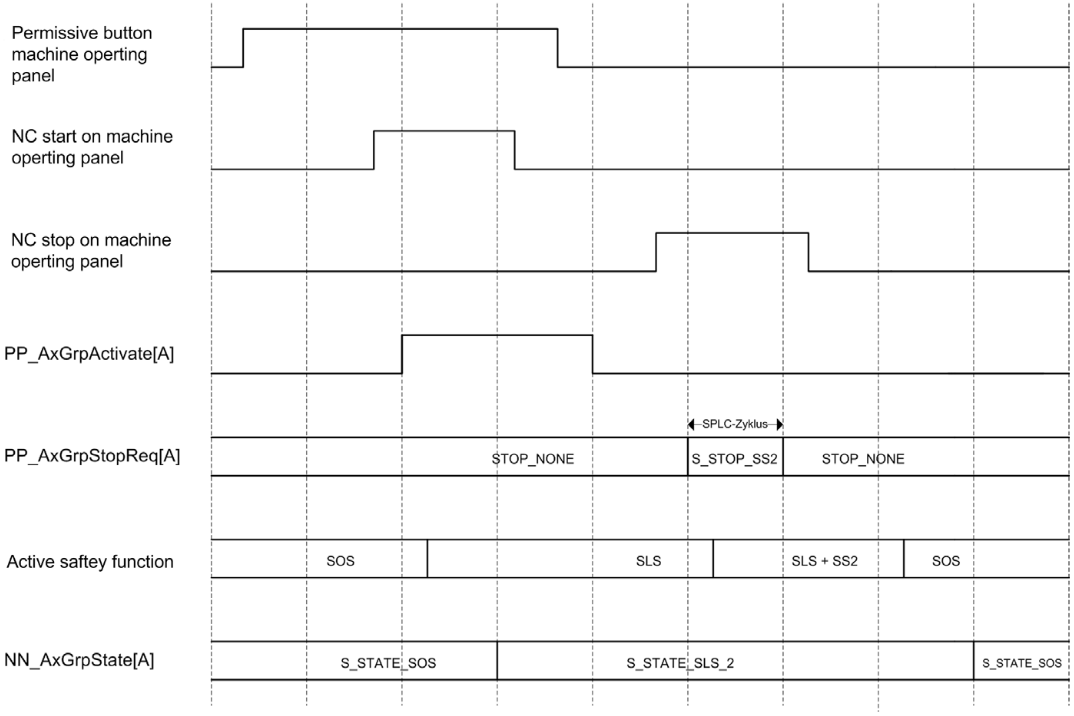


For manual operation with jog increments the SPLC program sets the **PP_AxFeedEnable** marker to **TRUE** when the axis-direction key is pressed, and keeps the **TRUE** status after the axis-direction key is released, until the motion is stopped and the axis-group state switches back to **S_STATE_SOS**. The figure shows the chronological sequence. In some cases the axis motion does not begin until after the user has already released the axis-direction key.



NC start key

The figure below shows the sequence for starting an NC axis via the NC start key on the machine operating panel in SOM_2.



The SPLC program detects a valid NC start upon the positive edge of the NC start key while the permissive key is pressed at the same time. This can be implemented analog to the spindle start. In automatic operation, the SPLC program sets **PP_AxFeedEnable** to **TRUE** for all NC axes.

After an NC start, the NC axis remains in motion until it is explicitly stopped, for example via the NC stop key or the emergency stop input.

The start for automatic operation in the **El. Handwheel** operating mode is identical to automatic operation via the operating panel. When the operator releases the permissive button on the handwheel, the SPLC program sets **PP_AxFeedEnable** to **FALSE**, and the SKERN stops the motion.

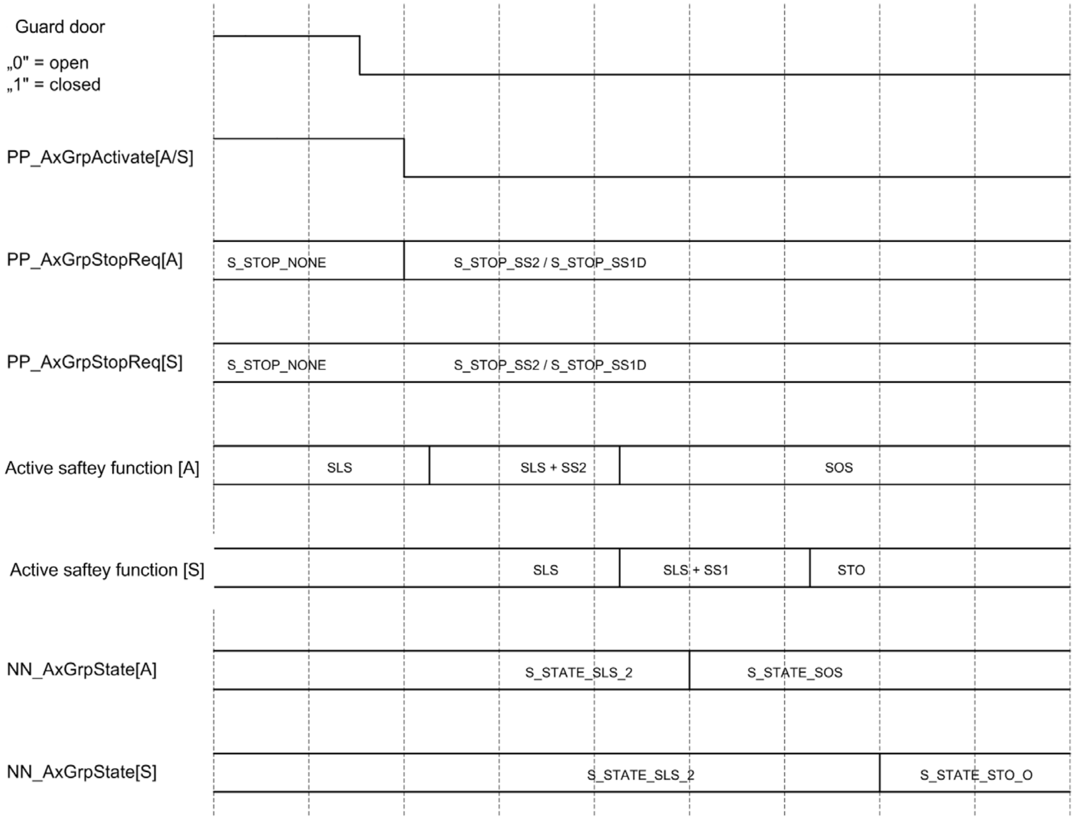
Opening the T guard door

Opening the T guard door during an axis movement while the A/S guard door is open

If the operator opens the T guard door while the A/S guard door is open, the SPLC program sets the following markers to the following values:

- **`PP_AxGrpActivate[A] = PP_AxGrpActivate[S] = FALSE`**
- **`PP_AxGrpStopReq[A] = S_STOP_SS2`**
- **`PP_AxGrpStopReq[S] = S_STOP_SS1D`**

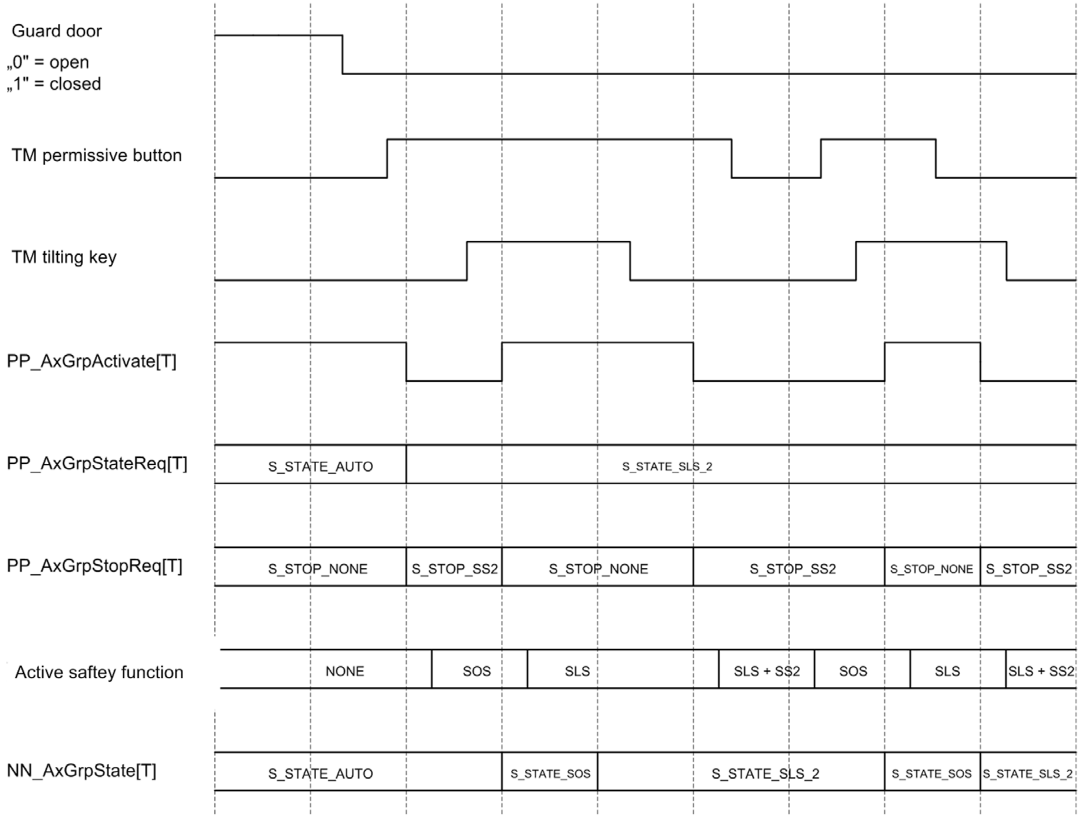
This sequence is shown in the figure below.



8.11.2 Movement of the axes of the tool magazine

If the T guard door is open, the tool magazine can be moved via the T permissive key and the tilting key. These keys are located directly next to the access door of the tool magazine.

The figure shows the sequence for a movement of the tool magazine.



The figure shows a case where the tool magazine is at standstill while the T guard door is being opened (**NN_AxGrpInMotion[T] = FALSE**). Should the tool magazine move while the T guard door is being opened, the SPLC program sets **PP_AxGrpStopReq[T]** to **S_STOP_SS1**, so that the tool magazine is decelerated along the emergency braking ramp, after which the drive is switched off.

HEIDENHAIN

DR. JOHANNES HEIDENHAIN GmbH
Dr.-Johannes-Heidenhain-Straße 5
83301 Traunreut, Germany
☎ +49 8669 31-0
FAX +49 8669 5061
E-mail: info@heidenhain.de

Technical support FAX +49 8669 32-1000
Measuring systems ☎ +49 8669 31-3104
E-mail: service.ms-support@heidenhain.de
TNC support ☎ +49 8669 31-3101
E-mail: service.nc-support@heidenhain.de
NC programming ☎ +49 8669 31-3103
E-mail: service.nc-pgm@heidenhain.de
PLC programming ☎ +49 8669 31-3102
E-mail: service.plc@heidenhain.de
Lathe controls ☎ +49 8669 31-3105
E-mail: service.lathe-support@heidenhain.de

www.heidenhain.de

749 363-21 · Ver01 · 7/2011 · PDF