



Technical Information

Safety-Related Control Technology for Machine Tools

Safety is becoming increasingly important in machine and plant construction. These high requirements mainly serve to protect human beings, but material assets and the environment are also receiving more consideration. The goal of functional safety is to minimize or even eliminate risks that can occur during normal or impaired operation of machines or facilities. This is achieved primarily with redundant systems. For example, axes that are moved in safety-oriented applications require redundant position information and dual-channel safety systems in order to perform the corresponding safety functions.

Various system configurations can be realized in order to capture independent position values. One possibility is the use of two encoders per axis. In many cases, however, a more economical solution requiring only one position encoder is preferred. HEIDENHAIN offers safety-related position encoders as a purely serial, single-encoder solution.

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.

Basic principle

Controls and position encoders from HEIDENHAIN with functional safety meet safety integrity level 2 (SIL 2) as per the EN 61 508 standard, as well as the performance level "d" as per EN ISO 13849-1 (which superseded EN 954-1). These standards describe the assessment of safety-related systems, for example based on the failure probabilities of integrated components and subsystems. This modular approach helps the manufacturers of safety-related systems to implement their complete systems, because they can begin with subsystems that have already been qualified. Safety-related position encoders and the iTNC 530 with HSCI control accommodate this concept.



Functional Safety on Machine Tools

– Safety-Related Controls

With its iTNC 530, HEIDENHAIN is offering the first control with functional safety. Two redundant safety channels that work independently of each other are the foundation for controls with functional safety. All safety-relevant signals are captured, processed and output via two channels. Errors are detected by mutual comparison of the states and data in the two channels. In this way, the occurrence of just one error in the control does not incapacitate the safety functions. The concept described here will also be used for other controls from HEIDENHAIN in the future.

The HEIDENHAIN control system with functional safety consists of the following subsystems:

- HEIDENHAIN control with functional safety
- HSCI system with MC 6xxx main computer and CC 6xxx controller unit
- PL 6000FS for connecting safety-relevant inputs and outputs
- MB 6xxFS machine operating panel
- TE 6xx keyboard unit
- BF 2xx visual display unit
- Power stages and drives for feed axes and spindles
- Position and speed encoders
- HR xxxFS handwheels

Design

The safety-related controls from HEIDENHAIN have a dual-channel design with mutual monitoring. The SPLC (safety-related PLC) and SKERN (safe core software) processes are the basis of the two redundant systems. The two software processes run on the MC main computer (CPU) and CC controller unit (DSP) components.

The basic safety functions are permanently defined in the SKERN software and cannot be changed. The SKERN tasks include:

- Triggering and monitoring stop reactions
- Monitoring of the safe limited speeds in the various safety-related operating modes
- Cross-comparing the data and states of the two safety channels
- Monitoring of system conditions, such as supply voltages, operating temperatures, etc.

The machine manufacturer adapts the SKERN functions to the respective machine tool via the SPLC. The SPLC tasks include:

- Flexible adaptation of the functional safety to the respective machine
- Capture, processing and output of safety-related signals
- Requests for safety functions from the SKERN software

The dual-channel design of the MC and CC is continued in the PL 6000FS and MB 6xxFS input/output systems: all safety-relevant signals (e.g. permissive buttons and keys, door contacts, emergency stop button) are received 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 stages, and to stop the drives in case of an error.

Safety functions

- Safe stop reactions (SS0/SS1/SS2)
- Safe torque off (STO)
- Safe operating stop (SOS)
- Safely limited speed (SLS)
- Safely limited position (SLP)
- Safe brake control (SBC)
- Safe operating modes according to EN 12317

Safety-related operating modes

HEIDENHAIN controls with functional safety offer four safety-related operating modes according to the EN 12417 standard (Machine Tools–Safety–Machining Centers). The application-oriented operation offered by this promises a high level of acceptance, and therefore safety. The goal is to make actions by the machine operator at machining centers possible during

automated production runs, even when protective measures are not in effect (such as guard doors being open), without danger to the operator:

The following safety-related operating modes, as per EN 12417, can be selected, for example by a keylock switch:

Operating mode 1: Automated or production mode

- Operation only with closed guard door
- No machine motion possible if guard door is open

Operating mode 2: Set-up mode

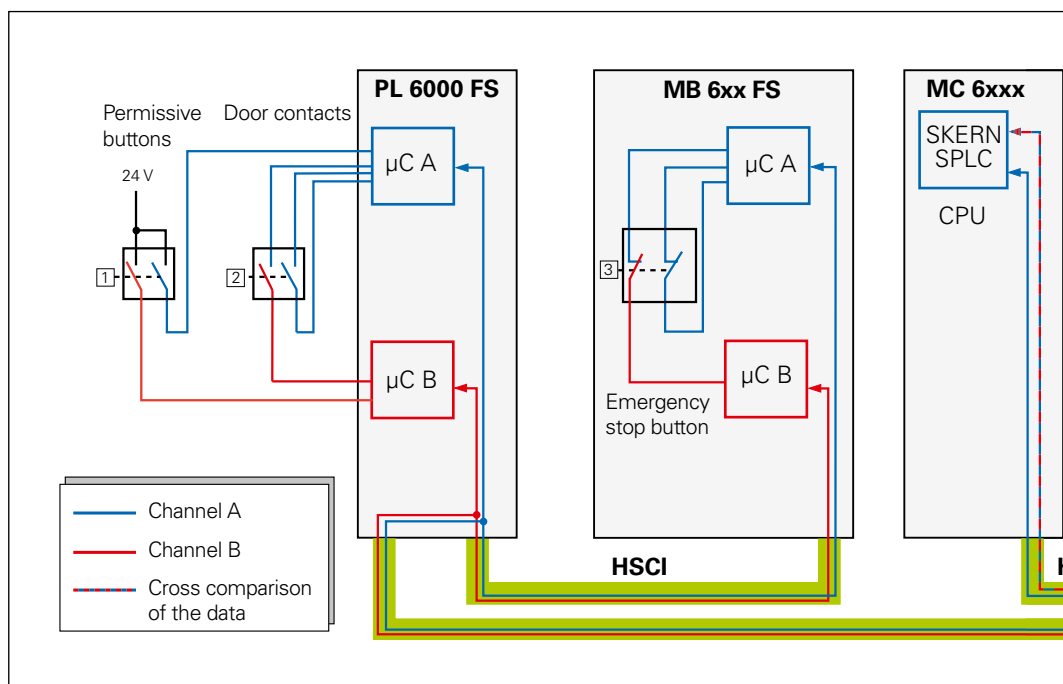
- Operation with open guard doors
- Axis motions of 2 m/min at most
- Spindle stop within 2 revolutions
- Only one axis can be moved at a time (no interpolating motions)
- Spindle rotation only with permissive button

Operating mode 3: Manual intervention

- Operation with open guard door
- Axis motions of 5 m/min at most
- Spindle stop within 5 revolutions
- More than one axis can be moved at a time (interpolating motions)
- Spindle rotation only with permissive button

Operating mode 4: Advanced manual intervention, process monitoring

- Operation with open guard door
- Axis motions of 5 m/min at most
- Spindle stop within 5 revolutions
- More than one axis can be moved at a time (interpolating motions)
- Spindle start only with permissive button



– Safety-Related Position Measuring Systems

The control requires reliable position information for numerous safety functions, including safe reduced velocity, safe absolute position, safe controlled stop, etc. Redundant information is required for this. Diverse techniques sometimes come into use for producing redundant position values. Genuine dual-channel redundancy can be ensured by installing two encoders per axis. Economy, however, makes a solution requiring only one position encoder preferable.

The trend toward purely digital drive concepts will require single-encoder solutions, which permit redundant position value acquisition through purely serial transmission, for safety-related applications.

HEIDENHAIN offers a solution with its safety-related position measuring systems. Single encoder solutions for safety-related applications according to EN ISO 13849 and EN 61508 are supported based on the purely serial EnDat 2.2 interface. All the benefits of serial data transmission are now also available in safety-related applications.

Safety-related position encoders with purely serial data transmission via EnDat 2.2

In a safe drive, the safety-related position measuring system is a subsystem consisting of:

- Encoder with EnDat 2.2 transmission component
- Data transfer line with EnDat 2.2 communication and cable
- EnDat 2.2 receiver component with monitoring function (EnDat master)

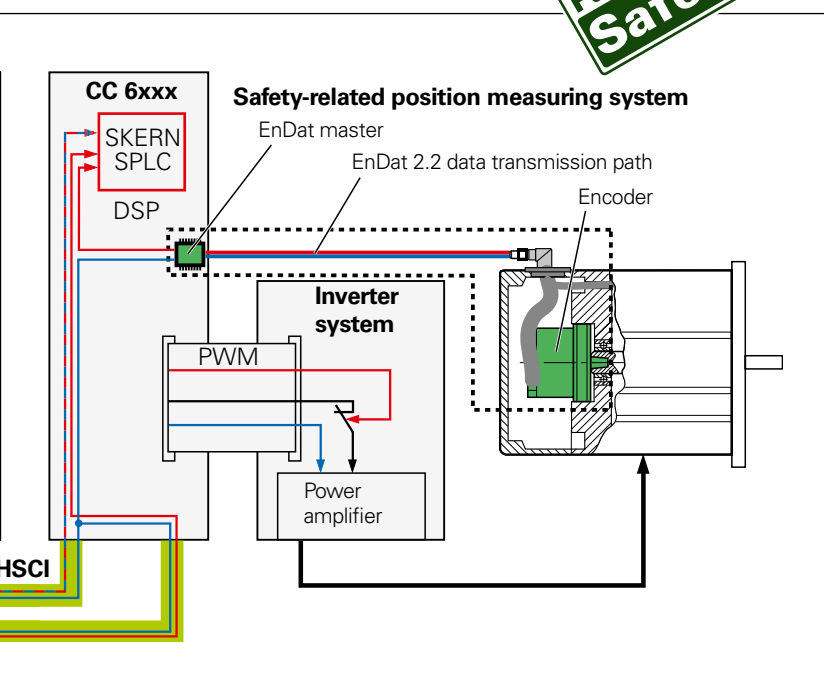
Integration of the position measuring system

The position measuring system is integrated by a mechanical and an electrical interface into the complete system. The encoder is mechanically coupled to the drive through the shaft connection and the coupling, both of which are determined by the geometry of the encoder. Including the EnDat master with monitoring functions in the safe control ensures its electrical integration. The necessary measures have already been defined. The control manufacturer must only implement them. And so the safety-related position measuring system can be incorporated as a subsystem with the corresponding failure probabilities into the safety-related evaluation of the plant's or drive manufacturer's total system.

Function

The safety strategy of the position measuring system is based on two mutually independent position values and additional error bits produced in the encoder and transmitted over the EnDat 2.2 protocol to the EnDat master. The EnDat master assumes various monitoring functions with which errors in the encoder and during transmission can be revealed. The two position values are then compared. The EnDat master then provides the two position values and mutually independent error bits to the safe control over two processor interfaces. In addition, the control monitors the functionality of the safety-related position measuring system and the EnDat master through periodically released tests (forced dynamic sampling).

The architecture of the EnDat 2.2 protocol makes it possible to conduct all safety-relevant information or control mechanisms during unconstrained controller operation. This is possible because the safety-relevant information is saved in the additional information. With every sampling cycle this additional information can be requested by the control in addition to the actual position. According to EN 61508, the architecture of the position measuring system is regarded as a single-channel tested system.



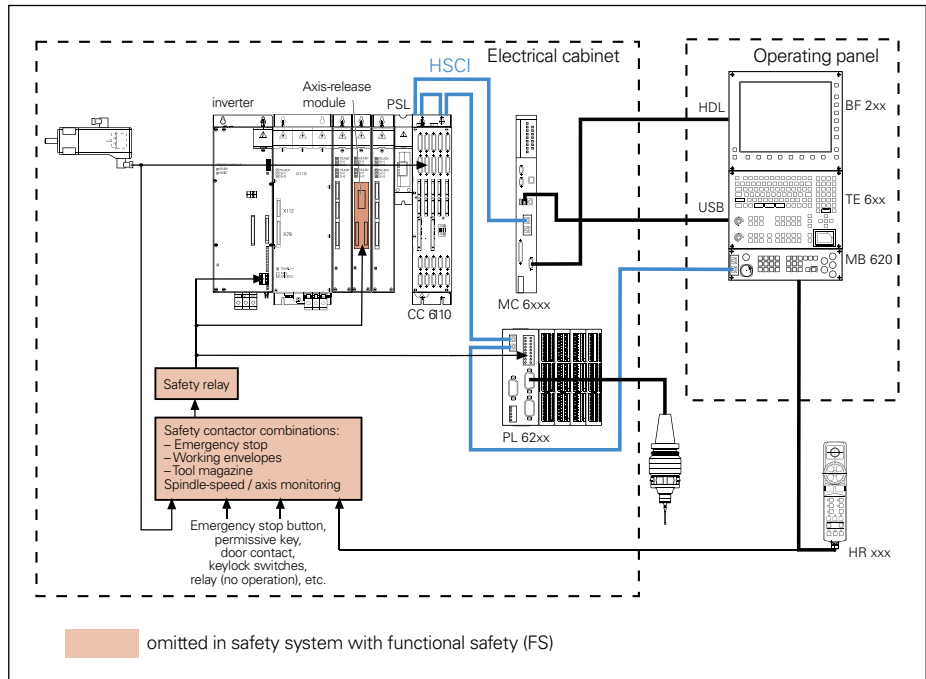
EQN 1337 absolute multiturn encoder
Safety-related position encoder (single-encoder solution)

Comparison of System with/without Functional Safety

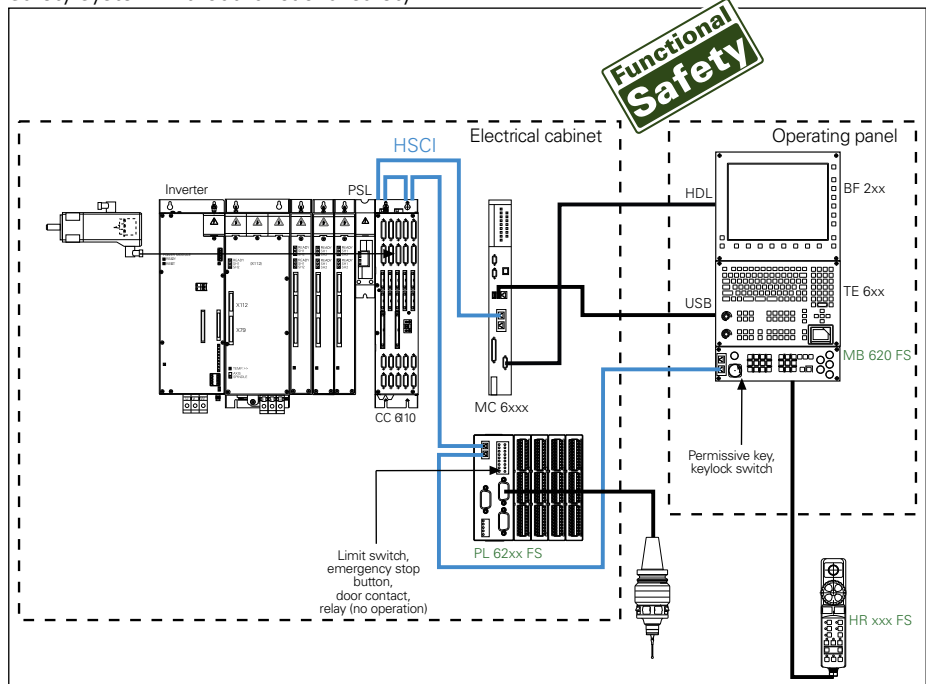
A safety system for controls without integrated functional safety is based on a dual-channel structure.

One of the safety channels is realized through external devices and wiring (e.g. safety contactor combinations, safety relays) for controlling the release of axes and spindles in the inverters and axis-release modules. The second channel features the control consisting of the MC main computer and the CC drive controller modules. It controls the inverters via the PWM interface. The external safety contactor combinations are the central devices for measuring and evaluating all safety-relevant assemblies (e.g. keylock switch, emergency stop button) in this system. Additional external assemblies are needed for monitoring the spindle speed or the axes. Using the input information, the external devices generate output signals that are received as input signals by the two safety channels of the control system.

In the HEIDENHAIN safety system with functional safety (FS), the safety-relevant functions are integrated in the hardware and software. The wiring of the machine is greatly simplified by using the following dual-channel HEIDENHAIN components: PL 6000FS input/output module, MB 620FS machine operating panel and the safe HR xxxFS handwheel. There is no need for the safety contactor combinations, additional devices for spindle-speed and axis monitoring or the wiring of the external safety channel. A safe PLC program permits flexible adaptation of the integrated functional safety to different types of machines by the machine manufacturer.



Safety system without functional safety



Safety system with functional safety (FS)

HEIDENHAIN

333 E. State Parkway
Schaumburg, IL 60173-5337
877-920-2703
www.heidenhain.us

For catalogs, brochures and product information sheets, visit
www.heidenhain.de/docu

For more information:

- Brochure:
iTNC 530 HSCI, Information for the Machine Tool Builder
- Technical Information:
Safety-Related Position Measuring Systems