



5

SINUMERIK Safety Integrated®

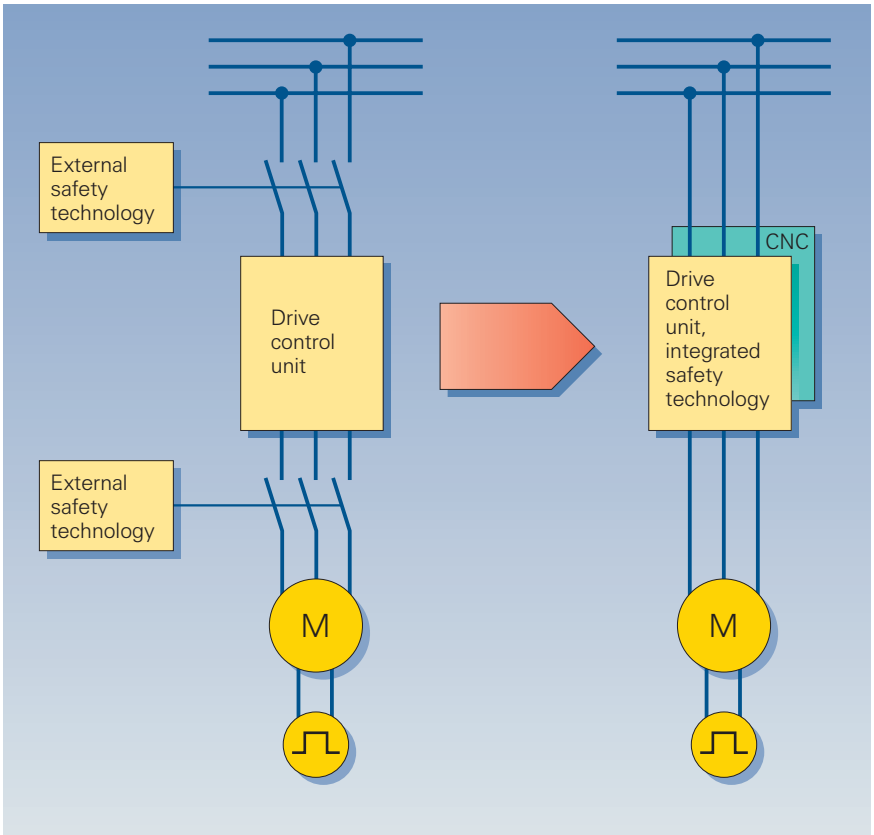
5.1 Drives and CNC Controls with Integrated Safety

(taken from [6], article from the German Trade Association (BG))

Safety measures must be provided on machines to protect personnel against potentially hazardous machine motion. These are mainly used to prevent hazardous machine movements when protective devices are in the open position. These functions include monitoring positions, e.g. end positions, monitoring speeds and stopping or shutdown in hazardous situations.

Up until now, external devices were mainly used to implement these safety measures. These include contactors, switches, cams and monitoring devices. When a hazardous situation is identified, these devices generally result in switching operations using contacts in the power circuit, which stop the potentially hazardous motion, refer to Graphic 5/1.

When integrating safety functions, drive systems and CNC controls are used to realize safety tasks in addition to the actual machine function. Extremely short response times can be achieved due to the short data path from sensing the Safety relevant information, e.g. speed or position, up to evaluation. Generally, systems with integrated safety technology respond extremely quickly when permissible limit values are exceeded or violated, e.g. position or speed limit values.. The integrated safety technology can directly control the power semiconductors in the drive control unit without using electro-mechanical switching operations in the power circuit. This also means that the system is less prone to faults and disturbances. The wiring and cabling costs are reduced as a result of the integration.



Graphic 5/1
External safety technology, integrated safety technology

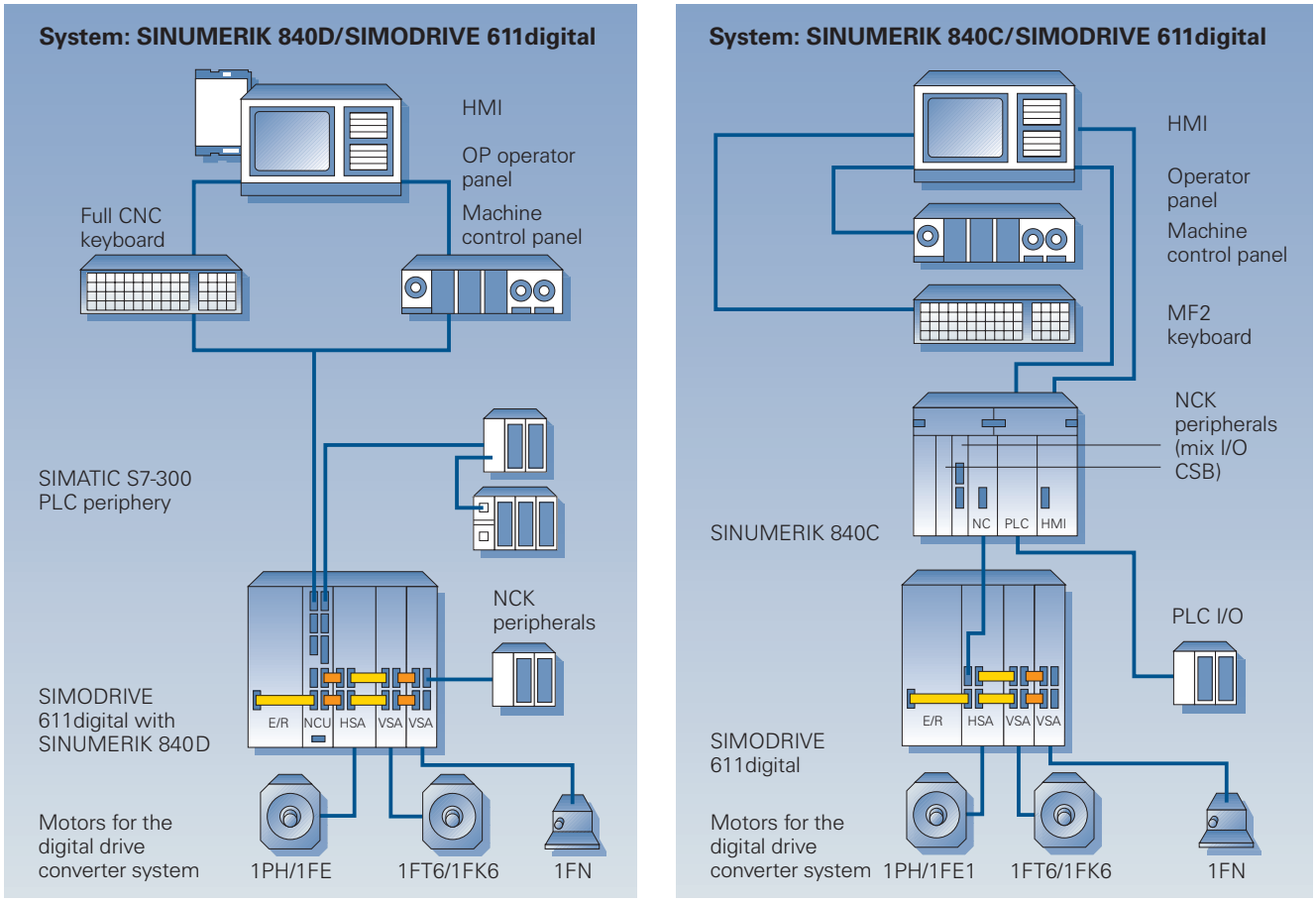
(taken from [6])

5.2 Equipment for NC Machines

Motion Control Systems is part of the A&D Group who develop, manufacture and market numerical controls and drive systems under the SINUMERIK and SIMODRIVE product names. These systems are especially used for complex and high dynamic motion and positioning applications where special demands are placed on precision.



Fig. 5/1
The basic SINUMERIK/SIMODRIVE system



Graphic 5/2
Structure of the SINUMERIK 840D and 840C systems with SIMODRIVE 611digital and motors

5.2.1 SINUMERIK control

SINUMERIK 840D – compact high technology

SINUMERIK 840D is a CNC control for up to 31 axes. It is an integral component of the modular SIMODRIVE 611 drive system. Thus, communications with the drive modules is realized through the shortest path.

Based on the modular SIMODRIVE 611 system, a module has been conceived in the form of SINUMERIK 840D, which provides significant technical advantages over comparable individual solutions.

The highlights include

- Up to 31 axes can be positioned
- Precision better than 1 µm
- Integrated SIMATIC S7-300 CPU with PROFIBUS-DP interface
- Only 50 mm wide in the SIMODRIVE 611 packaging design
- Scalable processor performance
- Integrated, certified safety functions



Fig. 5/2
SINUMERIK 840D – NCU and NCU box

5.2.2 SIMODRIVE drive converters

SIMODRIVE 611digital is a flexible, configurable drive converter system, which is fully aligned to the technical requirements placed on state-of-the-art machines, both economically as well as ecologically. With SIMODRIVE 611digital, Siemens is offering a drive converter system with digital closed-loop control, which is guaranteed to fulfill the highest requirements regarding dynamic performance, speed control range and smooth running characteristics.

As a result of the modular drive converter system design, drive configurations with almost any number of axes or main spindles can be implemented. The axis modules are designed for 1FT6, 1FK6 and 1FN, 1PH main spindle and 1FE built-in synchronous motors.

The SIMODRIVE 611digital drive converter system offers the following advantages:

- It fulfills the requirements for the EMC Directive and EMC compatible supplies
- Low line supply stressing as a result of sinusoidal current operation and regenerative feedback
- Compact design using low-loss power semiconductors
- High level of functionality in the smallest space using highly integrated control electronics

The digital control modules of the SIMODRIVE 611digital are used in conjunction with the 1FT6/1FK6 SIMODRIVE AC servomotors and 1FN linear motors for feed drives and 1FE and 1PH motors for main spindle drives. They evaluate the optical sine-cosine encoders, which are integrated in the 1FT6/1FK6 or 1PH motors.



Fig. 5/3
SIMODRIVE 611digital drive converter system



Fig. 5/4
Digital control module

This means that up to 4.2 million increments/motor revolutions can be achieved as measuring circuit resolution. For 1FN motors, a linear incremental or absolute-coded measuring system with EnDat interface is required to sense the position, speed actual value and pole position. The 1FE motors require a hollow shaft encoder with sinusoidal- cosinusoidal signals for the closed-loop speed and position control. For the control modules with direct position sensing, a direct measuring system can be connected. The certified safety functions are available for all encoder versions.

5.2.3 SIMODRIVE motors

Various drive-related versions can be implemented using the modular SIMODRIVE 611digital drive converter system, and combined as required in a drive group.

1FK6 and 1FT6 servomotors

These represent the optimum solution when highest dynamic performance and precision are demanded. Users hold simple and good controllability, combined with features such as freedom of maintenance and high overload capability, in especially high esteem.

1FK6 and 1FT6 three-phase servomotors are compact permanent-magnet synchronous motors, which have been especially developed for operation with the digital SIMODRIVE 611 digital drive converter system. The fully digital closed-loop control and the new integrated encoder system (motor measuring system) fulfill high demands placed on the dynamic, speed control range, smooth running and positioning accuracy.

Special speed-controlled 1PH induction motors

Based on the transvector control (field-vector control), which was developed and patented by Siemens, an induction motor can be just as simply controlled as a DC motor.

An induction motor controlled by SIMODRIVE 611digital has many advantages over DC motors, such as freedom of maintenance and full availability of the rated torque even at standstill. 1PH motors are equipped with a high-quality encoder system for closed-loop speed control and positioning.

1FN linear motors

1FN three-phase linear motors, together with SIMODRIVE 611digital, form a harmonized linear drive system for the requirements of the machine tool industry. The motors consist of a primary section and a secondary section with rare-earth magnets. When suitable measuring systems are used, the motors can be positioned in the nanometer range. The high traversing velocities and the extremely high dynamic performance, which can be achieved with the motors, are just some of the highlights worth mentioning.

1FE built-in synchronous motors

1FE motors are water-cooled synchronous motors, which are supplied as components. They are mainly used for main-spindle applications. These motors are mainly used together with the SIMODRIVE 611digital drive module where the highest demands are placed on the machining quality, precision, smooth running characteristics and extremely short accelerating times.

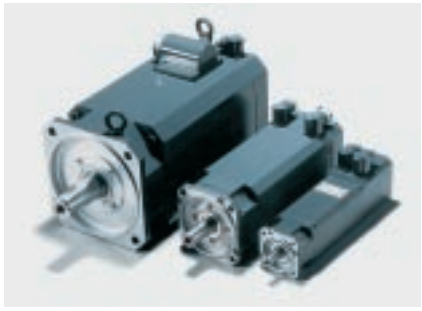


Fig. 5/5
1FT6 servomotors



Fig. 5/6
1PH built-in induction motor



Fig. 5/7
1FN3 linear motor

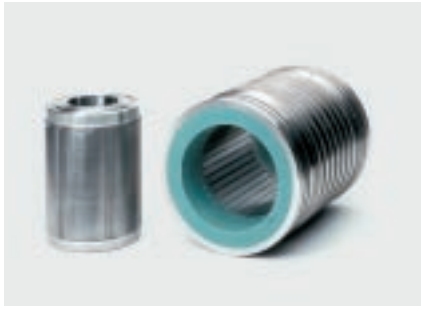


Fig. 5/8
1FE built-in synchronous motor

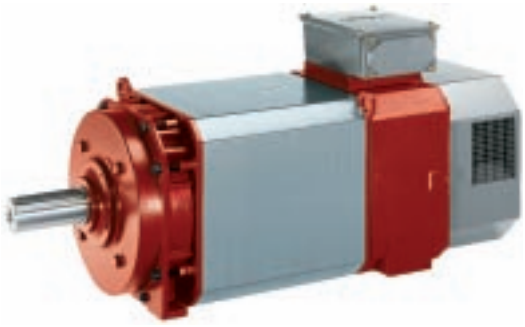


Fig. 5/9
1PH7 induction motor

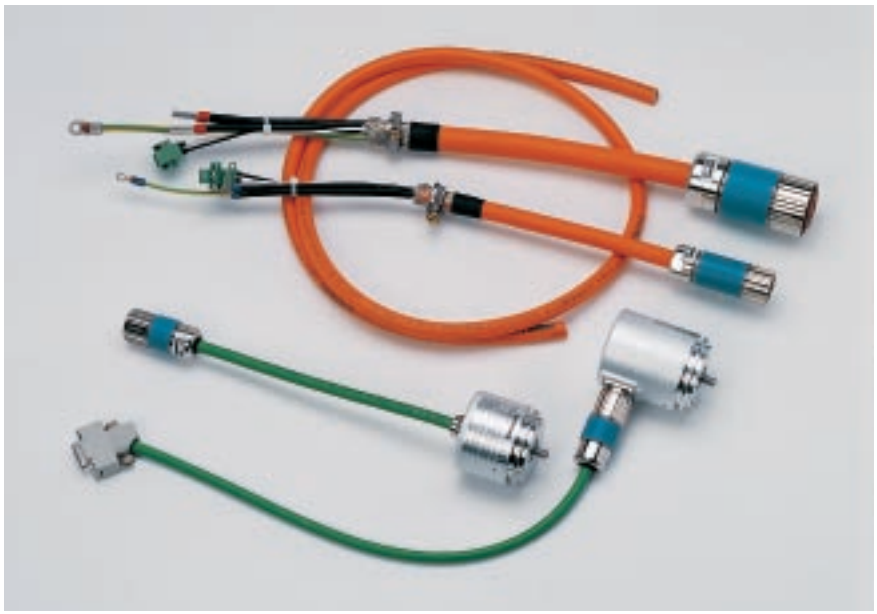


Fig. 5/10
System components and connection systems

5.2.4 Accessories

The Siemens SINUMERIK and SIMODRIVE automation systems are designed for all types of machine tools and processing equipment. With its family of MOTION-CONNECT cables, Siemens is offering the matching pre-assembled cables, cables sold by the meter and connectors which are ideally suited to the particular application. The customer benefits of Siemens pre-assembled cables include:

- System functionality and compatibility are guaranteed
- EC EMC Directives are fulfilled
- In conformance with DESINA
- No mounting problems
- No special tools are required
- MOTION-CONNECT 800, 700, 500 provide a tailored solution for every application
- Perfect functioning of the complete system is guaranteed

The supplementary system components such as encoders, hand wheels, operator control and handheld programming devices are also harmonized with the overall system. The SIMODRIVE sensor measuring systems for measuring distances, angles and velocities are available from Siemens as either incremental encoders or absolute encoders. For the incremental encoders, the interfaces are harmonized with the particular control system. Absolute-value encoders are available in versions with SSI and PROFIBUS-DP. The encoders can be quickly and easily commissioned as they can be parameterized. High machine availability is achieved using system-tested components. The original accessories from Siemens are an essential component of SINUMERIK Safety Integrated applications.

5.3.1 Brief description

Additional up-to-date information is also provided in the SINUMERIK 840D Safety Integrated Function Description.

"SINUMERIK Safety Integrated" offers type-tested safety functions, which allow highly effective personnel and machine protection concepts to be implemented in line with those required in the field. All of the safety functions fulfill the requirements of safety Category 3 in accordance with EN 954-1 and are a fixed component of the basic system. No additional sensors or evaluation units are required.

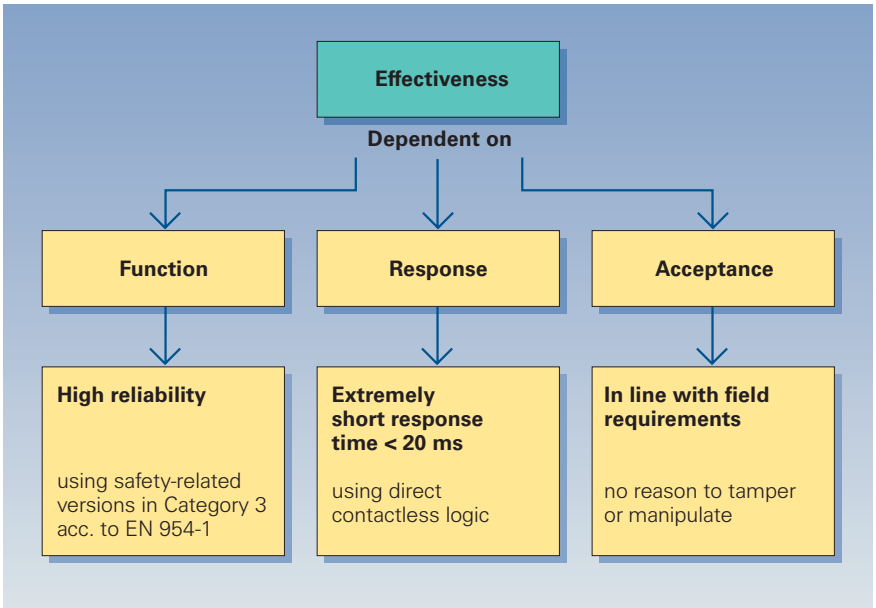
This means:

Lower installation costs on the machine and a smaller electrical cabinet.

The functionality includes, e.g.:

- Functions to safely monitor speed, standstill and position
- Functions to safely logically combine signals

Sensors and actuators, e.g. EMERGENCY STOP button, light curtains, valves or brakes, can be directly connected to the 2-channel periphery. The logical combination and the responses are internally realized using safety-related technology. All safety-relevant faults and errors in the system always result in potentially hazardous motion being stopped or power being quickly disconnected from the motor contactlessly. The drives are always shutdown, in accordance with the operating status of the machine. For example, in the setting-up mode, with the protective door open, the machine can be stopped as quickly as possible (optimum for personnel protection). In the automatic mode, with the protective door closed, it can be shutdown as a function of the machining path (optimum for machine protection).



Graphic 5/3
Highly effective integrated safety technology

This means:

High degree of personnel protection in the setting-up mode with additional protection for machine, tool and workpiece in the automatic mode.

The safety functions offer an intelligent system intervention directly down to the electric drives and measuring systems, which has been unknown up until now. Reliable functioning, fast response and a wide level of acceptance make this approved safety concept highly effective.

A two-channel diverse system structure is formed using the multi-processor topology. The safety functions are embedded redundantly in the NC, drive and internal PLC. The process quantities and the safety-relevant system data are cross-monitored, refer to Graphic 5.4 "Block diagram: Sensing – Evaluation – Response."

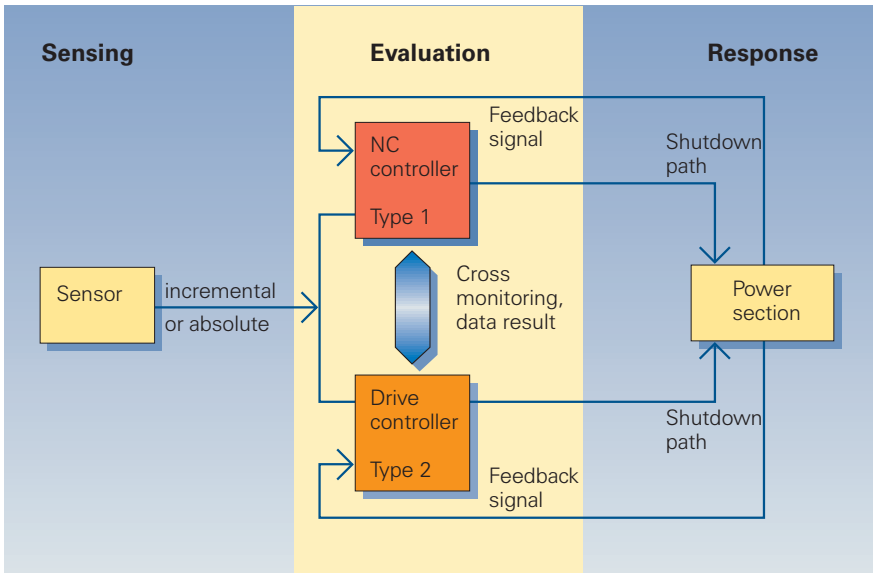
Safety-related software and hardware functions are tested at defined time intervals using an automated forced checking procedure. Refer to Section 5.3.4 "Forced checking procedure."

The special feature of the safety concept is that Category 3 according to EN 954-1 can be implemented with just one measuring system – the standard motor measuring system. A second sensor is not required. However, it can be incorporated as additional direct measuring system (e.g. linear scale).

Additional up-to-date information is also provided in the SINUMERIK 840D Safety Integrated Function Description.

It has been shown that, using this innovative safety technology, new machine operator control concepts can be implemented in line with those required in practice. This means that a new standard of machines has been created, which is safer and more flexible in operation and which increases the plant availability.

The new safety concept is the result of close cooperation with the "Iron and Metal II" Committee of the German Trade Association in Mainz and the "German Statutory Industrial Accident Insurance Association" BIA in St. Augustin and Siemens AG in Erlangen.



Graphic 5/4
Block diagram: Sensing – Evaluation – Response

5.3.2 Function description

The safety functions are available in all operating modes, and can communicate with the process via the safety-related I/O signals. They fulfill the requirements of safety Category 3 (in accordance with EN 954-1). This was proved using a type test corresponding to the EC Directive, which was certified by the BIA in St. Augustin. Refer to Section 5.10 "Type Test Certificate (BG)."



Fig. 5/11
BG test certificate for 840C



Fig. 5/12
BG test certificate for 840D

Safe stopping process

The safe stopping process is not an autonomous function, but describes a procedure which can be implemented using "SINUMERIK Safety Integrated" functions. Safe stopping process safely stops the motion and brings the drive to a safe standstill when a monitoring function or a sensor responds (e.g. light curtain).

All safety-relevant faults and errors in the system or if an appropriate sensor responds, always result in a coordinated, safe shutdown of the hazardous motion. Depending on the system engineering specifications, the power to the motor can be quickly disconnected. This power disconnection between the drive converter and motor, required in special cases (where the drives go into a torque-free condition), is realized contactlessly and can be initiated on an axis-for-axis basis with extremely short response time.

Thus, it is no longer necessary to discharge the DC link in the drive. The drives are always shutdown, according to the operating status of the machine.

The integrated functions are supplemented by activating external braking mechanisms, and, for safety shutdown, results in the shortest possible braking travel. External braking mechanisms can include, for example:

- External mechanical brake, holding or operating brake
- External electrical brake, armature short-circuit or eddy-current brake

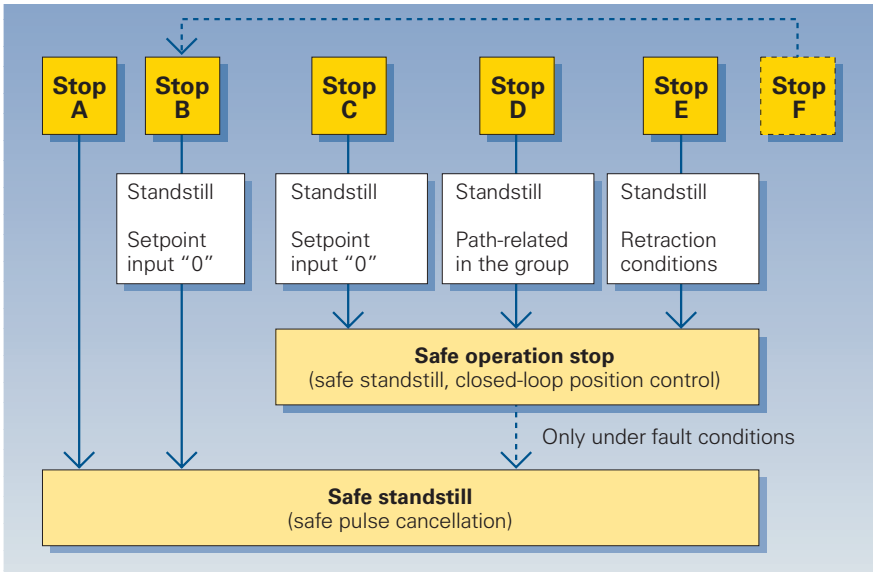
Principally, the line contactor is no longer required if the machine has a main switch, which allows it to be electrically disconnected from the supply.

Example of EMERGENCY STOP

The logical interlocking of safety-related signals and the required responses are realized internally using safety-related technology. The electric drives are safely stopped and are subsequently isolated from the power source via the electronics. Undesirable restart is also safely prevented. External power sources, for example, hydraulic systems or lasers etc. can be shutdown using the safety-related outputs from the integrated EMERGENCY STOP logic and downstream actuators (power contactors, valves, etc.). The coordinated, safe stopping process eliminates or reduces subsequent damage (e.g. crash) when shutting down and permits fast, simple start-up.

Stop responses

A high degree of fail-safety is obtained as a result of the two-channel monitoring structure with its permanent cross monitoring. If differences occur between the two monitoring channels, alarms and stop responses are automatically initiated. The stop responses should safely shutdown the drives corresponding to the particular requirements at the machine. A differentiation is made between stop versions, STOP A, B, C, D, E, F and the test stop.
The system can specify a preset stop response type when a fault/error occurs or the machine OEM can configure the required response. When the limit values, defined using the machine data of the functions, safe operating stop, safe reduced speed, safe software cam, safe software limit switch, are exceeded, the stop responses of the machine OEM can be initiated. Stops A, C and D can also be selected externally, event-related via safety-relevant inputs (SGE). The stop versions are implemented as follows:



Graphic 5/5
Stop versions

- **Stop A**
  Using Stop A, the drive is directly brought into a no-torque condition using the "Safe standstill" function. A drive that is at standstill can no longer undesirably start. A drive that is still moving coasts down. This can be prevented by using external braking mechanisms, such as armature short-circuit, holding and operating brakes. The axis-specific alarm results in a mode stop which means that, as a result of the response in one axis, all of the axes and spindles in a mode group are also shutdown. At the end of Stop A, the axis is at a "safe standstill."
- **Stop B**
  The drive is braked along the current limit in the closed-loop speed-controlled mode and goes into the "safe standstill" status.
- **Stop C**
  The drive is braked along the current limit in the closed-loop speed controlled mode and goes into the "safe operating stop" status.
- **Stop D**
  The drive, as group, including the synchronous axes, is braked path-related, and goes into the "safe operating stop" status.
- **Stop E**
  The drive, as group, including retraction motion, is braked path-related, and goes into the "safe operating stop" status.
- **Stop F**
  The Stop F response is permanently assigned to the cross-monitoring result and data comparison. Thus, faults/errors on the drive and control side are detected. Depending on the configuration, a Stop B or A response is initiated. The "safe standstill" is effective at the end.

When configuring the stop responses, personnel protection has topmost priority. The optimum stop response for machine protection can be configured in the automatic mode with the protective door closed. The goal is always to optimally stop the machine in any particular situation.

Example 1: Grinding machine with open protective door (setting-up operation):

- Feed drive with Stop C: The drives are braked along the current limit axis-specific as quickly as possible and then go into the "safe operating stop". Thus, they remain in the closed-loop position control mode.
- Grinding wheel drive with external Stop A: In this mode, the drive is always kept torque free via the external Stop A with "safe standstill".

Example 2: Grinding machine in the automatic mode:

- Feed drive with Stop E: The drives, as a group, execute a retraction movement (cut themselves free) and are braked along the contour via a ramp and go into the "safe operating stop" status. They remain closed-loop position-controlled.
- Grinding wheel drive with Stop D: The drive is braked along a ramp and is therefore held by the torque load below the sparking limit. The drive goes into the "safe operating stop" status and is kept in the closed-loop position control mode.

Test stop

With the test stop, for each monitoring channel, the complete shutdown path is tested with the external circuitry.

When executing the test, the comparators and stop modules of the two monitoring channels, which are responsible for the stop function, are executed one after the other.

Also refer to Section 5.3.4 on the subject of forced checking procedure.

Safe standstill

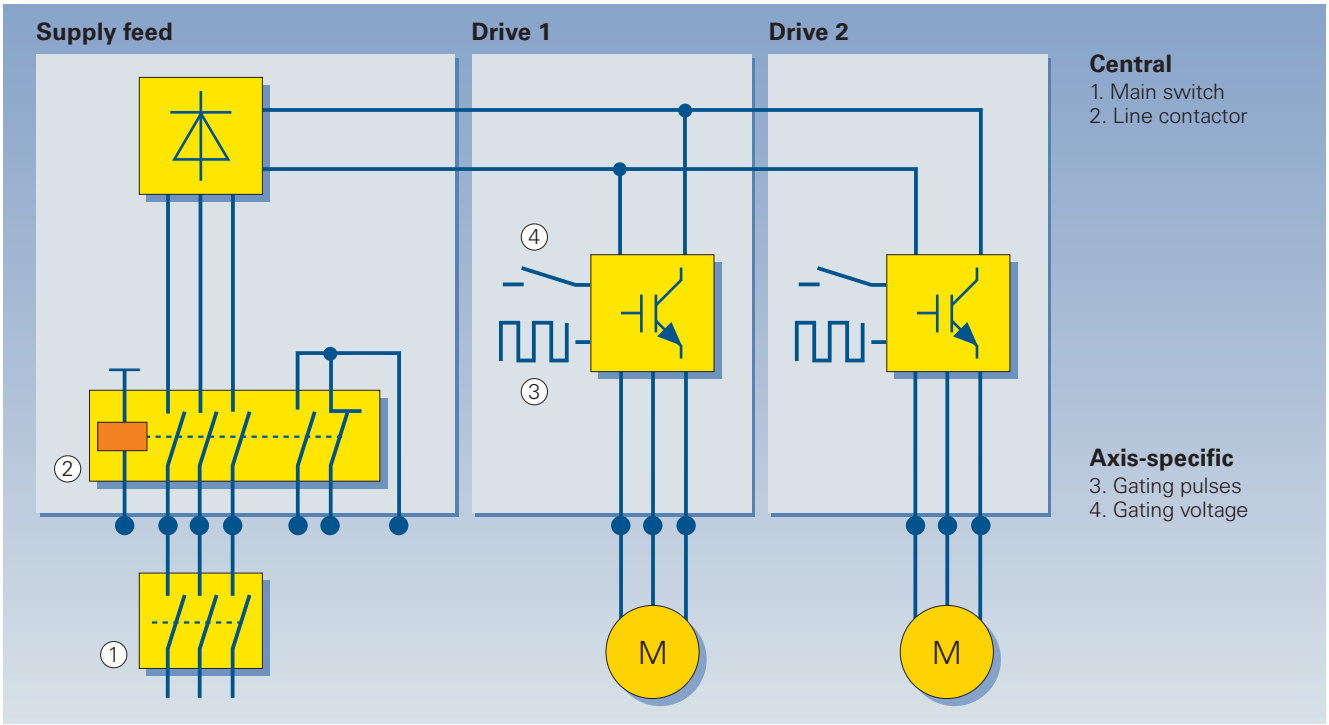
When a fault occurs or in conjunction with a machine function, the "safe standstill" is used to safely disconnect the power feed to the motor. This is realized for each axis. The basis for the "safe standstill" function is the safe pulse cancellation, which is integrated in the SIMODRIVE 611D drive modules.

The machine OEM must take appropriate measures to stop axis movement after the power feed has been disconnected to the motor (e.g. to stop hanging axes dropping).

Features

- The motor cannot accidentally start.
- The power feed to the motor is safely interrupted.
- The motor is neither disconnected from the drive module nor from the drive converter DC link.

Graphic 5/6 shows four basic possibilities of bringing a motor into a no-torque condition. These differ in their principle of operation.



Graphic 5/6
Power disconnection with "safe standstill"

① Main switch:
Mode of operation ⇨ central
Every machine must be equipped with at least one switch that permits the machine to be completely electrically isolated from the line supply (Stop Category 0). This is generally realized with the main switch. This measure protects personnel working on the equipment against electric shock. When open, this switch must be secured so that it cannot be closed.

② Integrated line contactor:
Mode of operation ⇨ central
The complete drive inverter can be electrically isolated from the line supply using the line contactor in the rectifier/feed module. With reference to the drive inverter, this measure represents a Category 0 Stop. In the past, with an integrated line contactor, for EMERGENCY STOP, the drive inverter/motor was brought, in conjunction with a Category 1 Stop, into a no-torque condition. However, electrical isolation is not mandatory for EMERGENCY STOP (refer to the Application Manual, Section 1, Page 1/14).

③ Pulse cancellation in the gating unit
Mode of operation ⇨ axis-specific
The fastest way to bring individual axes into a no-torque condition is to cancel the pulses using the gating unit. However, this measure when applied on its own is not safety-relevant.

④ Control voltage of the opto-coupler
Mode of operation ⇨ axis-specific
When the control voltage of opto-couplers is disconnected, when a fault condition occurs, gating unit pulses which are still present cannot be converted into a torque in the drive power section. However, this measure is, when applied by itself, not safety-relevant. It is not possible to electrically isolate the drive converter DC link (600 V) from the motor. This is also not required for "functional safety".

Conclusion:
Measures ③ and ④ are physically decoupled and together form an effective and safety-relevant method of canceling the drive converter pulses on an axis-for-axis basis. They form the basis for "safe standstill" and can be independently initiated from the drive and the NC. The concept is completed by integrating into cyclic tests (forced checking procedure). This means that a safety-related total concept is created from individual measures, which completely fulfills the requirements for EMERGENCY STOP. It is no longer mandatory to open the line contactor ②.
However, when carrying out work (e.g. service, maintenance….) on live components, the equipment must always be isolated from the line supply.

Safe operating stop
This function is used to safely monitor the standstill position of an axis or spindle. In this case, the drives remain fully functional in the closed-loop position control or closed-loop speed control mode.

Features

- Axis remains in the closed-loop control mode.
- Standstill tolerance window which can be parameterized.
- Configurable stop response when the monitoring function responds (stop B or A).

Safely reduced speed

The safely reduced speed function is used to safely monitor the speed of a drive.

To realize this, the actual speed of the drive is cyclically compared, in the monitoring clock cycle, with the speed limit, selected via safety-related inputs. The speed limits are defined in the machine data.

Various applications and operating statuses at the machine can be monitored using the speed limits for safely reduced speed 1 to 4. Further, the limit values safely reduced speed 2 and safely reduced speed 4 can be graded in 16 steps using "safety-related inputs" (4 bits). The entry is made in % (1 to 100%) and is saved in a table in the machine data. Thus, a total of 34 freely selectable speed limits are available for each drive. This allows personnel and machine protection to be implemented in setting-up mode and also in automatic mode.

Comment: For changeover gearboxes, the correct gearbox ratio must be selected!

Features

- Safe monitoring of the load side speed limits.
- The monitoring limits are adapted to various operating statuses (e.g. test, setting up, automatic mode).
- Configurable safely reduced speed-specific stop responses.

The safely reduced speed-specific set point limiting can provide an important supplement "safely reduced speed".
With this function, for the first time, in addition to the speed actual value, the speed set point is also taken into consideration. The "safely reduced speed-specific set point limiting" automatically limits the set point to the currently effective limit of the "safely reduced speed". If this value changes for a drive, the set point limit is automatically corrected. If the drives operate in a group, then the function acts on all of the coupled drives. This means that the machined contour is always maintained.
Applications:

- When testing programs, e.g. when opening a protective door. This means that no test specific changes have to be made to parameters.
- If, for example, a safety zone is entered using the traversing keys, where lower safely reduced speed limit values are active, the axis is not stopped, but the speed is automatically reduced to the speed set point which is effective there.

Features

- The set point is limited in 1 channel in the NCK as a function of the speed limit values. SG1-SG4, including safely reduced speed override.
- This is effective when traversing the drives using traversing keys or when executing programs.
- The limit value lies X% under the active safely reduced speed limit.
- The axes involved are instantaneously accelerated or braked, interpolating.
- This function is only executed if the programmed set point lies above the active safely reduced speed limit.
- If the programmed set point is less than the active safely reduced speed limit, then the drives traverse as specified in the program.

Safe software limit switch

A working zone/protective zone demarcation or traversing range limiting can be implemented for each axis using the "safe software limit switch". This means that, for example, hardware limit switches are not required on the mechanical system. Two limit switch pairs per axis are available. Each limit switch pair consists of a positive switch (safe limit switch 1+ and safe limit switch 2+) and a negative switch (safe limit switch 1– and safe limit switch 2–). It is possible to toggle between safe limit switch 1 and safe limit switch 2 via the safety-related inputs.

Features

- End positions can be safely defined and evaluated per software.
- Configurable stop responses when end positions are reached.
- Stop response when reaching end positions is realized internally in the software.

Safe software cam

Safe range identification can be implemented for each axis using the "safe software cam" function. This means that today's "hardware solution" can be replaced.

4 cam pairs (safe software cam 1 to safe software cam 4) are available per axis. Each cam pair comprises a positive cam (safe software cam 1+, safe software cam 2+, safe software cam 3+, safe software cam 4+) and a negative cam (safe software cam 1–, safe software cam 2–, safe software cam 3–, safe software cam 4–). Each cam signal can be individually configured via the machine data. The cam signals are output via safety-related outputs.

Features

- Cam positions can be safely defined and evaluated using software.
- Safety ranges are defined.
- Safe cam-dependent changeover of safety functions (e.g. safe position-independent changeover of the safely reduced speed stages).

Safe braking ramp

For this function, there is a requirement that after a stop command, the actual speed must be reduced (the speed characteristic is monitored).

When a stop command is issued, the actual speed plus a speed tolerance, specified using the machine data, is activated as speed limit. This limit is compared with the actual speed (it must remain less than or be the same) and must be cyclically tracked. If the axis was to be re-accelerated while braking, this would be quickly detected and a subsequent response initiated.

Features

- If an axis was to re-accelerate during braking, then this would be quickly detected.
- The safe braking ramp would be automatically activated if a Stop B or C was to be initiated.
- When the safe-braking ramp responds, a direct Stop A is initiated.

Safe programmable logic

The "safe programmable logic" allows, for the first time, safety-related sensors and actuators to be directly connected and logically combined. The logic is redundantly embedded in the NC and in the internal PLC. This means that, for example, EMERGENCY STOP or interlocking concepts for protective doors can be configured using the SINUMERIK Safety Integrated software. The EMERGENCY STOP, in conjunction with the "safe standstill," can now be implemented by the evaluation logic up to power disconnection, contactlessly and using safety-related technology.

Discrete hardware contacts can be eliminated which is reflected in a simplified cabinet design. Only the power contacts (e.g. contactors) are required to directly control the external actuators.

Features

- Universal, programmable logic utilizing safety-related technology.
- The logic is immediately activated after run-up.
- Cyclically executed, independent of the user program.
- Integrated timer for forced checking procedure.
- Effective in all operating modes.

Safety related I/O

The safety-related input and output signals represent the interface to the process. They are digital signals, which are input into the system or come from the system, through two channels and via various peripheral devices (PLCs and NCs). The safety-related inputs and outputs need not to be routed via hardware terminals. In conjunction with the safe programmable logic, when required, they can be internally processed as software signal.

Features

- Safety-related functions can be selected and canceled.
- Limit values can be selected and changed over.
- Status signals can be signaled back.
- Cam signals can be output.
- Sensors can be directly connected.
- Actuators can be directly connected.

5.3.3 System requirements

Also refer to Section 5.9 "Ordering data and documentation".

SIMODRIVE 611digital

- Safety Integrated is only available with digital drives.
- The performance as well as the Standard 2 control of 611digital can be used.
- The control boards must always be ordered with DMS measuring circuit.
- At least one measuring system must always be available.

SINUMERIK

- For SINUMERIK, Safety Integrated is available for the 840C and 840D types in conjunction with SIMODRIVE 611digital. In this case, all of the CPU versions can be used.
- Inputs/outputs for safety-related signals (safety-related I/O). The NC and PLC periphery (I/O) form the two-channel I/O structure.
- SINUMERIK Safety Integrated is a software option, and is formed from a basic and an axis option. In this case, the basic option already has the axis option for 4 drives.
- For the SI functions, CPU system resources (NC, PLC, drive) are required, which are dependent on the scope of the functions used and the number of drives. In borderline cases, it may be necessary to use a higher-performance CPU.

Encoders and measuring circuit

- Generally, every measuring system can be used which fulfills the measuring circuit specifications of SIMODRIVE 611D.
- 1-encoder concept. At least one measuring system is required, which is generally covered using the indirect motor measuring system (IMS) as incremental or absolute encoder.
- 2-encoder concept: A second measuring system is not required; however, it can be integrated as direct measuring system (DMS).
- The measuring-circuit cables must conform to the SIMODRIVE 611 digital specifications, e.g. they must be twisted and screened pairs.

SIMATIC

- All of the standard SIMATIC components can be used.
- I/O for safety-related signals (safety-related I/O). The NC and PLC periphery (I/O) form the two-channel I/O structure.

HMI

- The operator and display units (OPs) are not embedded in the safety concept. They are only used to display safety-relevant data for diagnostics and commissioning.

5.3.4 Basic application information

Basic structure when integrating sensors and actuators

Safety-related signals are processed in an integrated, unified fashion from the sensor, through the evaluation logic (Safety Integrated Platform) up to the actuator, with the demanded performance quality (Control Category according to EN 954-1).

The direct assignment, sensor ⇨ integrated evaluation logic ⇨ actuator, enhances the transparency and avoids mistakes when configuring/engineering and when connecting up. The simpler infrastructure achieved as a result of this increases the machine availability.

A differentiation is made between two connection types:

Connection via the standard I/O periphery of the PLC and NC

This is valid for

- Sensors, for example switches, protective door contacts, EMERGENCY STOP pushbuttons, light curtains, light barriers, and
- Actuators, for example contactors, valves, interlocking solenoids, brakes, signaling lamps.

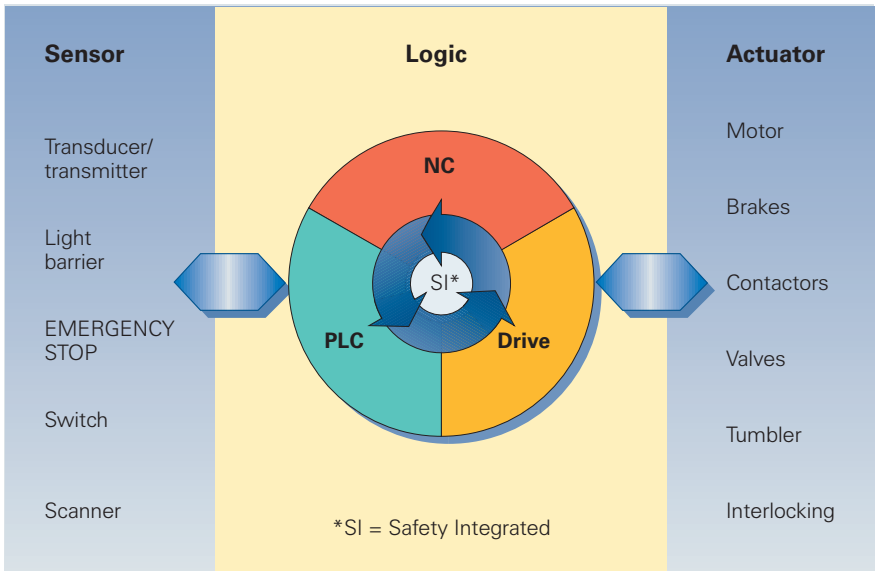
These are directly connected to the standard I/O modules of the PLC and NC (without using evaluation devices). The signals are then transferred to the "SINUMERIK Safety Integrated" platform via separate buses (PROFIBUS and the drive bus).

Connection via specific interfaces and buses

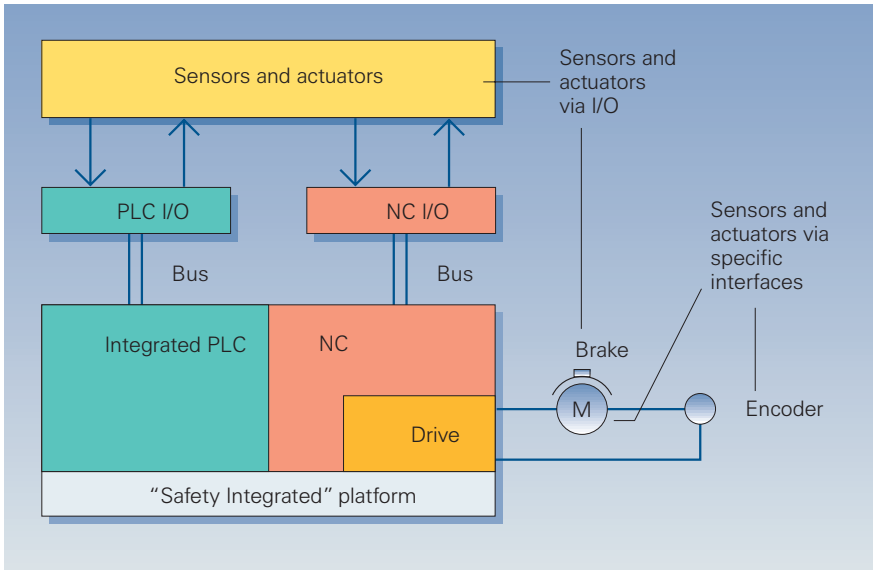
This is valid for

- Sensors, for example motor measuring systems, direct measuring systems as well as for
- Actuators, for example servomotors, spindle motors, linear motors.

These are connected using standard cables via specific interfaces. For measuring encoders and motors, for example, the connection is made directly at the drive (drive converter). The machine infrastructure can be kept extremely simple, as no additional external sensors, e.g. a second measuring system or external evaluation units, are required. Comment: In the future, it is planned to connect the "safety-related inputs" and the "safety-related outputs" exclusively to one 2-channel PLC I/O module; the signals will then be transferred, safety-related, to the "SINUMERIK Safety Integrated" platform via PROFIBUS with PROFISafe.



Graphic 5/7
Block diagram: Sensor – Logic – Actuator



Graphic 5/8
Basic structure of the sensor/actuator integration

Sensor/actuator integration – 3-terminal concept

Integrating sensors

For sensors that are connected via the I/O periphery of the PLC and NC, a 3-terminal concept can be used as basis. If the signals are read from a sensor through two channels, then a single-channel test output for control Category 3 is sufficient. Thus, to integrate the sensor in a safety-related fashion, 3 terminals at the I/O periphery are required.

2 inputs + 1 test output

Integrating actuators

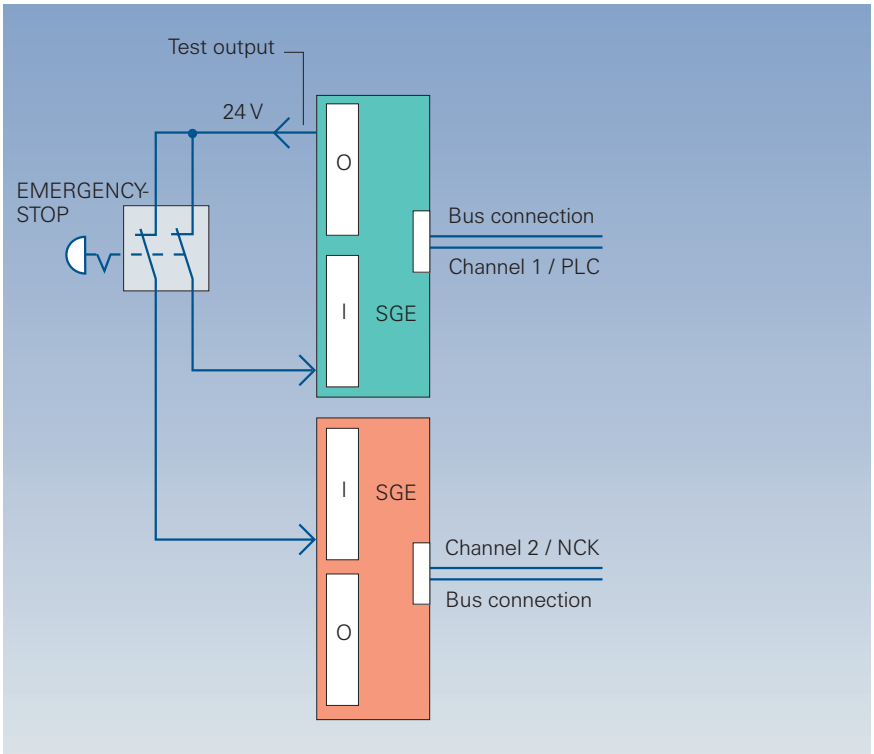
For actuators which are connected through the I/O of the PLC and NC, a 3-terminal concept can also be used as basis. If an actuator is controlled through 2 channels, then it is sufficient to read back the process signal through 1 channel to fulfill control Category 3. This means that to integrate the actuator in a safety-related fashion, 3 terminals are also required at the I/O periphery.

2 outputs + 1 test input

Cross-circuit-fault safety

If the connecting cables are routed, protected in the cabinet or parts of the system, then it can be assumed that faults are extremely improbable (short circuit, cross-circuit ...). As defined in prEN 954-2 Standard, so-called fault exclusion can be assumed for the connecting cable. This means that it is completely adequate if the sensor is designed in accordance with the 3-terminal concept.

The measures applied for cross-circuit fault safety are independent of the control Category 3 or 4.



Graphic 5/9
Safety-related hardware input signals with 3-terminal concept – example of EMERGENCY STOP

Safety related hardware input signals (3-terminal concept)

All safety-related process signals (sensors, e.g. EMERGENCY STOP, protective door, light curtain ...) must be configured redundantly and separately connected as "safety-related inputs" to the 2-channel input periphery of the PLC and NC. In this case, it is not permissible that the input terminals are directly bridged.

Features:

- The sensor is controlled with 24 V from a test output of the PLC through a common connection and fed to the safety-related control via the two input channels 1 and 2.
- In conjunction with the crosswise data comparison and the forced checking procedure, faults (P and G short circuits) can be detected in the connecting cables.
- A pure cross-circuit fault between the two inputs from channel 1 and channel 2 cannot be detected using the 3-terminal concept.

It must be ensured that the signal status of the "safety-related inputs" does not differ. Depending on the tolerance timer (approx. < 1 sec.), if the tolerance time is exceeded, a monitoring function responds and the machine is automatically and safely shutdown.

Comment 1:

For sensors which have pure electronic outputs, i.e. they do not use a contact, which, for instance, is partially possible for light curtains, the circuitry at the PLC and NC inputs remains the same. However, the test output of the PLC is directly connected to the special test input at the sensor. The 3-terminal concept remains essentially the same.

Comment 2:

If a safety component (e.g. EMERGENCY STOP button) is not used as sensor, the two signal-generating elements (e.g. switching contacts for pushbuttons) must be mechanically de-coupled.

Sensor/actuator integration – 4-terminal concept

Integrating sensors

If it cannot be completely guaranteed that the connecting cables are protected against crushing (e.g. cables for BHG/HPU), or if higher requirements are demanded as a result of the particular application, then a pure cross-circuit fault (neither P nor G short circuit) must be assumed in the hazard analysis. This means that the sensor must be connected using the 4-terminal concept. In this case, two separate cables are connected to the two signal-generating elements (e.g. contacts). 4 terminals are required at the I/O periphery to integrate the sensor in a safety-related fashion.

2 inputs + 2 test outputs

Integrating actuators:

Presently, there is no requirement to integrate actuators according to the 4-terminal concept. However, it is possible.

Cross-circuit fault safety:

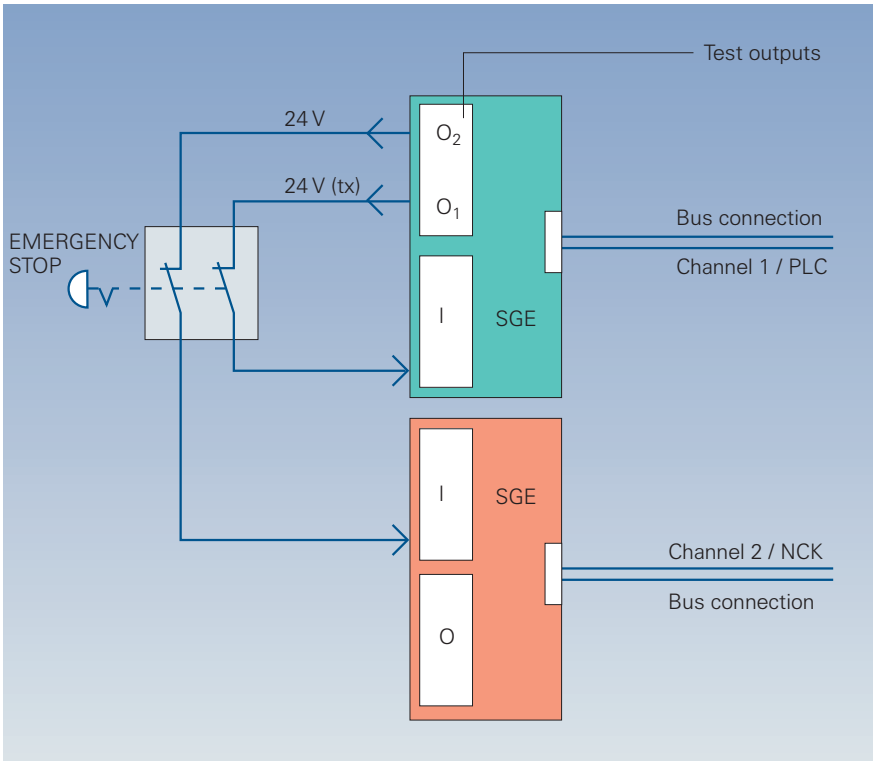
Using this technique, with standard modules, it is possible to implement complete fault detection functionality for the sensor connecting cables. The connecting cables do not have to be routed in any special way.

Safety-related hardware input signals (4-terminal concept)

The basic principle corresponds to that of the 3-terminal concept. The extended measures are intended to detect a cross-circuit fault (i.e. no connection to G or P potential) between two cables.

Features:

- The sensor is directly controlled from two test outputs of the PLC, each with 24 V, and fed to the safety-related control system via the two input channels 1 and 2.
- Test output 1 is delayed by tx with respect to test output 2. This results in a clear signal characteristic at input channels 1/2 as expected response.
- A single-channel test routine in the PLC checks this expected response. The test can be made within the scope of the forced checking procedure.



Graphic 5/10
Safety-related hardware input signals with 4-terminal concept – example EMERGENCY STOP

- In conjunction with a crosswise data comparison and the forced checking procedure, all of the faults (P and G short circuit) including a pure cross-circuit fault in the connecting cables can be detected.

Comment 1:
The concept presented can only be used together with sensors which use contacts with closed circuits (closed-circuit principle). For electronic signals, the sensor must guarantee cable monitoring. If this is the case, a pure cross-circuit fault can also be detected in conjunction with the 3-terminal concept.

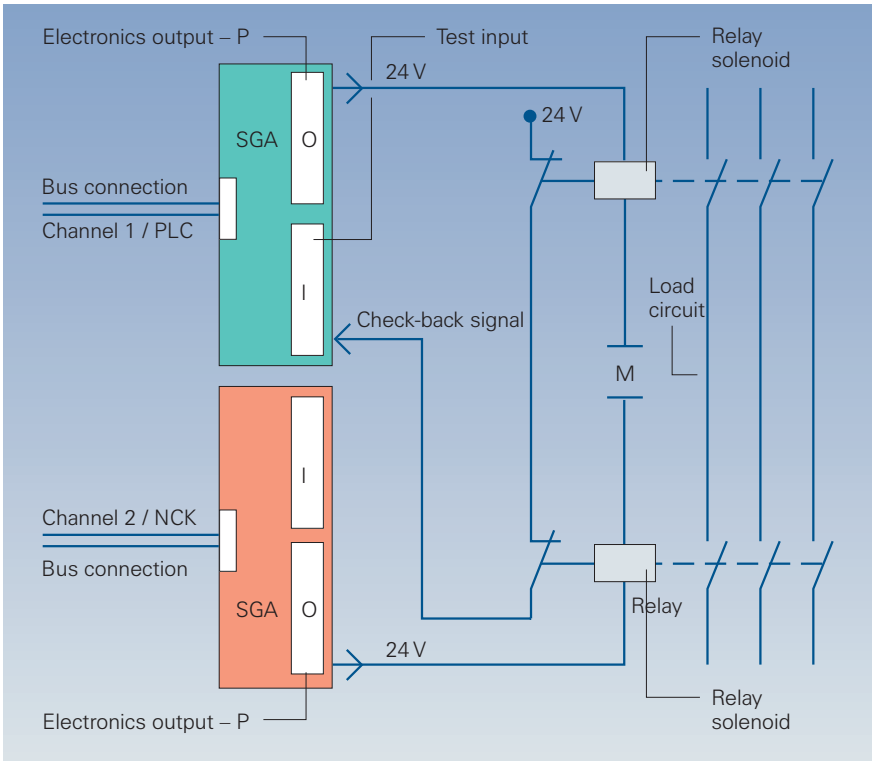
Comment 2:
If a safety component (e.g. EMERGENCY STOP button) is not used as sensor, then the two signal-generating elements (e.g. switching contacts for pushbuttons) must be mechanically de-coupled.

Safety-related hardware output signals – P/P switching

For P/P switching versions, two actuators always switch in series in the load circuit. Both channels (NC and PLC) control the actuators with a positive voltage (24 V) (positive-positive switching). Commercially available contactors can be used as actuators, for example to control motors. If a hydraulic load system is used, then the valves can be directly controlled through two channels. The check-back signal from the load circuit should be derived as directly as possible from the actual process quantity. For example, it is preferable to use a check-back signal from the hydraulic pressure using a sensor instead of using the check-back signal from the hydraulic valve.

Features

- The load circuit is always controlled through two channels.
- The load is always interrupted or switched through 2 channels.
- Commercially available (standard) components can be used as actuators, e.g. contactors, valves, as two devices are always used.
- The check-back signal contacts (NC contacts) of the actuators are permanently connected to 24 V, are switched in series and are read back from the PLC through 1 channel.
- Faults in the control and at both actuators can be detected in conjunction with the forced checking procedure.
- When an actuator fails, the load can still be disconnected through the second channel.
- The actuator can be switched purely via the PLC through 1 channel, dependent on the process.



Graphic 5/11
Safety-related hardware output signals – P/P switching

Safety-related hardware output signals – P/G switching

For P/G switching versions, only a single actuator switches the load circuit. The NC channel controls the actuator with a positive voltage (24 V); the PLC channel controls the actuator with ground potential (0 V) (positive-ground switching). This control version is always required if there is only one solenoid to directly control the load circuit. This is, for example, the case with:

- Tumbler solenoids on protective doors
- Operating brakes hydraulically controlled via valves (e.g. for linear motors)

The load circuit check-back signals should be derived as directly as possible from the process quantity. For example, it is preferable to use a check back signal from the hydraulic pressure using a sensor instead of using the check-back signal from the hydraulic valve.

Features

- The load circuit is always controlled through 2 channels
- However, the load is only interrupted or switched through 1 channel
- Only components which have been proven in operation according to EN 954-2 may be used as actuators, e.g. contactors, valves etc.

The check-back signal contact (NC contact) of the actuator is permanently connected to 24 V and is read back from the PLC through a single channel.

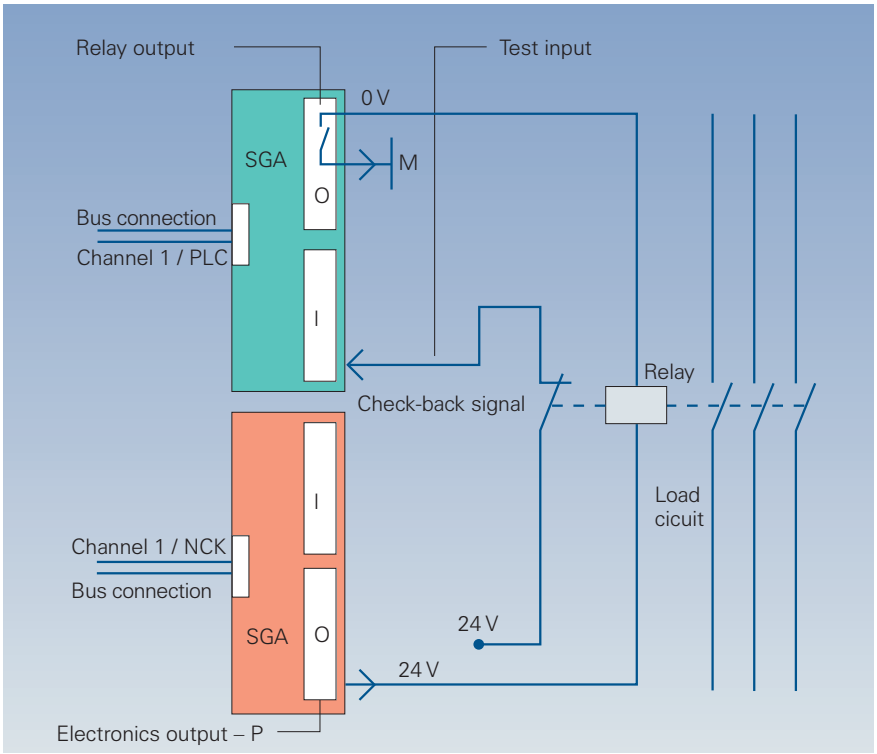
Comment:

If there is no check-back signal contact, then the "safety-related brake control – P/G-switching" can be used as described in Section 5.3.4.

- Faults in the control and at the actuator can be detected in conjunction with the forced checking procedure.
- If the actuator fails, then the load can no longer be safely shutdown via this specific path. In this case, depending on the hazard analysis and the type of actuator, additional measures must be used, e.g. central shutdown and extended test measures.
- The actuator can be solely switched via the PLC through a single channel, dependent on the process.

Application examples

Safety-related actuators could be switched in the load circuit, for example: Contactor interlocking functions, hydraulics directly via valves, pneumatics directly via valves etc.



Graphic 5/12
Safety-related hardware output signals – P/G switching

Safety-related brake control – P/G switching

The basic principle is described in Section 5.3.4 "safety-related hardware output signals – P/G switching."

Axes and mechanical assemblies can, when the drives are powered down, fall downwards due to gravity. For vertical linear axes (hanging axes) or for rotary axes or spindles with non-symmetrical weight distribution, this can result in hazardous motion. This means that these axes and mechanical assemblies must be maintained safely at standstill using appropriate measures. Measures can include e.g.:

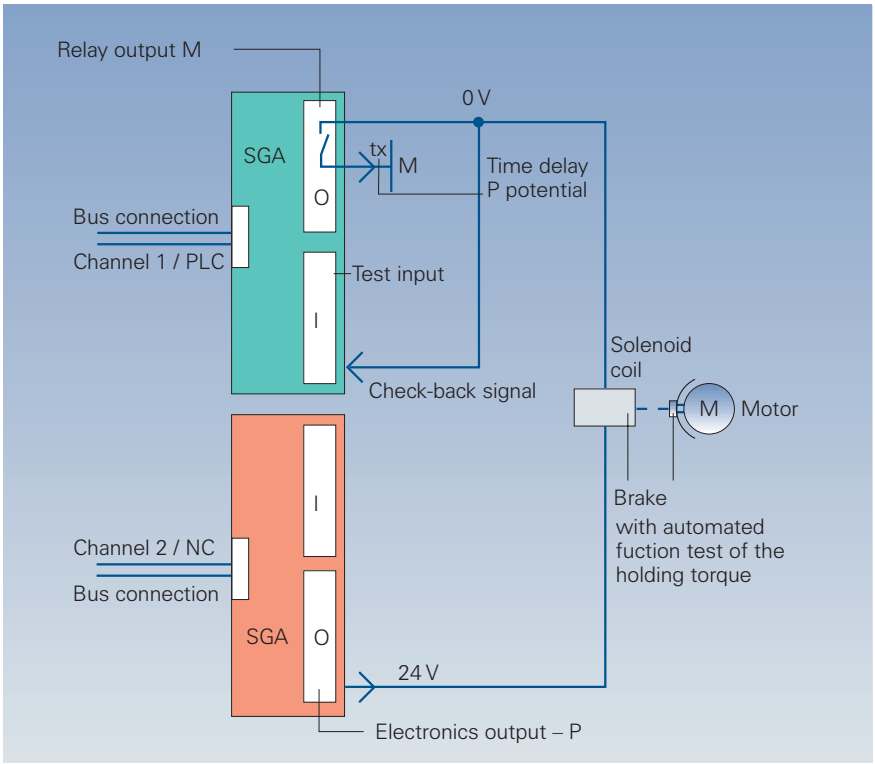
a) Active from time to time
   Holding brake
   Operating brake

b) Continuously active
   Mechanical weight equalization

c) Active in exceptional cases
   Cotter pins
   Support

The measures that are selected depend on the type of work which is to be carried out in the hazardous area. When carrying out work on or with live (under voltage) components (with the exception of safety extra-low voltage), it is always necessary to electrically isolate the equipment from the line supply. The concept must also take into account how long personnel remain in the hazardous area, which may make it necessary to combine several measures. In this case, the basis is always the hazard analysis, which must be carried out for every machine. However, in this particular application, only the safe integration of holding and operating brakes is described. The brakes, which are generally in use today, are not safety-related components.

By integrating the brake into the safety concept, a standard brake (component proven in operation) has a safety-related function. There are no check-back signal contacts on brakes, which means that other test measures are required. Using a safety- related control with forced-checking procedure and cyclic brake test can fulfill these requirements. Using the cyclic brake test, a check is made as to whether the expected holding torque is still available. Faults in the control and at the brake itself can be detected using extended test measures.



Graphic 5/13
Safety-related brake control, P/G switching

Features

- The load circuit is always controlled through 2 channels.
- The load, in this case the braking torque, is only applied through 1 channel.
- The check-back signal is formed from the ground-side connection of the coil. This means that G and P short-circuit faults can be detected. The 3-terminal concept can also be used here.
- The output of channel 1 is switched with delay tx with respect to channel 2. This results in a clear signal characteristic at the check-back signal input as expected response.
- A single-channel test routine in the PLC checks this expected response and this could be executed as part of the forced checking procedure.
- A brake test is provided as extended test measure. This tests the actual available braking torque (the drive deliberately attempts to move against the brake). This is incorporated in the forced checking procedure for the test stop (testing the shutdown/stopping paths).
- During power failures or when cables are interrupted, the brake is mechanically brought into a safe condition as a result of the return springs.
- The wiring to the brake is standard. The connecting cables do not have to be routed in any special way.

- Only components which have been well-proven in operation, in accordance with prEN 954-2, can be used as actuators.

Conclusion:

This application significantly reduces the risk for "hanging axes" as well as "rotary axes or spindles with non-symmetrical weight distribution" for machine tools, handling systems and robots. The brake is integrated, as standard component, into an overall safety-related concept. This means that a second brake is not mandatory.

Depending on the result of the hazard analysis, the following concepts can be, for example, achieved:

1. One brake in the motor
2. One brake at the load
3. One brake in the motor and one brake at the load

This decision is the responsibility of the machine OEM. However, it should be discussed and agreed with the responsible regulatory body.

Comment:

This application can be implemented with SINUMERIK 840D and SIMODRIVE 611D from SW P4.4 (01/99) and in conjunction with the "safe programmable logic."

Additional information is provided in the Function Description for SINUMERIK Safety Integrated.

Safety-related brake control – P/G switching with intermediate relay stage

With this example, contrary to the previously described direct P/G switching version, the brake is controlled through an additional intermediate relay stage to amplify the current. The intermediate relay stage must be used if there is no 2 A output module of the NC I/O and/or no S7 relay module available or if the load current to be switched is > 2 A.

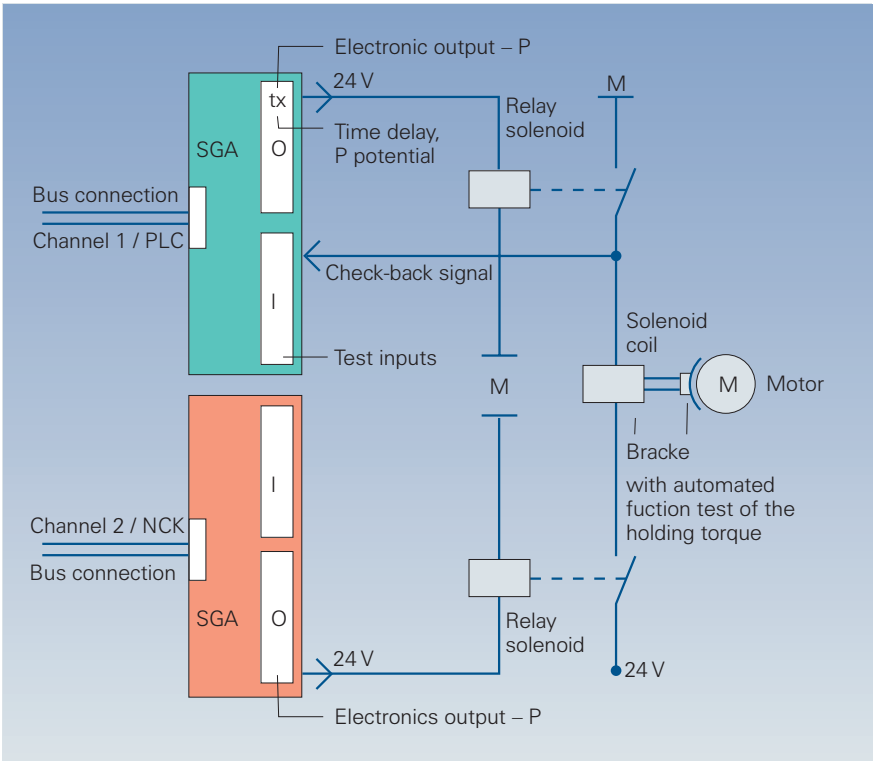
The outputs used in the NC and PLC are standard outputs where the intermediate relay stage is switched P/P.

Caution!

Using the intermediate relay stage, in comparison to the best case (fast, contact-free NC path switching), the response time is extended by the relay switching time. This results in longer sag and therefore a higher residual risk when faults develop.

Features

- Principally, the same features apply as for the direct P/G switching control.
- The control in the 24 V load circuit of the brake remains P/G switching as shown in Graphic 5/14.
- It is not absolutely necessary to integrate positively driven check-back signal contacts of the intermediate relay stage. This means that standard relays can be used without positively driven check-back signal contacts. However, in this case, the prerequisite is that the check-back signal from the G potential of the brake is integrated.
- All of the erroneous functions in the brake control path are detected as a result of the direct check-back signal from the brake G potential, e.g.
  - if the relay does not switch/drop out (e.g. because the relay contacts do not open),
  - short circuits on the 24 V control cables



Graphic 5/14
Safety-related brake control P/G switching with intermediate relay stage

Forced checking procedure, general

(Taken from [6], article of the German Trade Association)

A forced checking procedure must be executed for all steady-state signals and data. Within the required time (8 h), the status must be changed from a logical 1 to a logical 0 or vice versa. If the status has remained static after a fault condition has occurred, then this is detected, at the latest during this forced checking procedure and the subsequent comparison.

A forced checking procedure must be provided, e.g. for all of the components required for shutdown (e.g. contactors and power semiconductors), the so-called shutdown path and for the stopping condition itself. Generally, the shutdown condition, e.g. if a limit value criterion is violated, cannot be tested using another measure, such as cross-comparison, if the machine is in a good condition. This is also true for faults in the complete shutdown path including the associated hardware and software and the power switching elements. By providing a test stop in an 8-hour cycle with comparison, and an appropriate expectation level, faults can be reliably detected, even when the machine is in a good condition (in this case, good condition means that the operator hasn't identified a machine fault).

Forced checking procedure with SINUMERIK Safety Integrated

The forced checking procedure is used to detect faults in the software and hardware of the two monitoring channels. In this case, the safety-relevant components in the two channels must be processed at least once within a defined time period and in all safety-relevant branches. A fault in a monitoring channel results in deviations and is detected by the crosswise data and result comparison.

The user must initiate the forced checking procedure of the shutdown path (test stop) or it must be automatically integrated into the process, and more specifically as an example:

- With the axes stationary after the system or plant has been powered up
- When the protective door is opened
- In a specified frequency (e.g. in an 8-hour cycle)
- In automatic operation, time- and event-dependent.

The forced checking procedure also includes testing safety-relevant sensors and actuators. In this case, the complete signal chain, including the "safe programmable logic" is checked for its correct functioning.

Comment:
For the duration of automatic operation (with the protective door closed), the fixed 8-hour cycle isn't mandatory. In this case, the forced checking procedure can be logically combined, after 8 hours have expired, the next time that the protective door is opened. As a result of the crosswise comparison, errors are detected in the safety-relevant data of the two monitoring channels. For "changing" data, there are tolerance values specified by the machine data. The results of the two channels can deviate within these tolerances, without a response being initiated. An example is the tolerance for crosswise comparison of the actual positions. Faults and errors, which are detected as a result of the forced checking procedure and crosswise comparison, result in a Stop F response and initiate additional stop responses (refer to Section 5.3.2 "Stop responses").

Application examples

By combining "SINUMERIK Safety Integrated" safety functions, completely new operator control concepts can be implemented at machines with different requirements.

- **Setting-up operation with the protective door open**

  With the protective door open, feed or spindle drives can be operated with safely reduced speed or are safely monitored at standstill. The drives are always monitored by the electronics and do not have to be disconnected from the power source. Working and protective zones can be implemented using safety-related technology with functions to identify ranges and limit traversing ranges. An enabling switch in conjunction with SINUMERIK Safety Integrated is not mandatory. However, depending on the requirement, it can be used, e.g., to changeover safety functions. In the standard case, the drives may only be moved using jog keys in dead man operation*.

- **Test operation with the protective door open**

  For the first time, program test operation is possible where the complete program or program parts are executed with safely reduced speed in a so-called "dry run". In this case, the operator ensures that the program is continually executed by pressing a button, generally the start button. If a program error is identified when testing, then the operator can hold the program by releasing the start button or by pressing the EMERGENCY STOP button. During this test phase, the safety functions are active. They respond when limit values are violated, and automatically shutdown the drives.

- **Integrated, contact-free EMERGENCY STOP**

  The EMERGENCY STOP button can be connected directly to the redundant input periphery of the PLC and NC through its two contacts without having to use additional evaluation logic. The logical combination and the required responses are realized internally using safety-related technology. The electric drives are safely shutdown and are then contactlessly isolated from the power via the electronics. A restart is safely prevented. External power sources, for example hydraulic systems or lasers etc., can be shutdown using safety-related technology via the redundant output periphery from the integrated EMERGENCY STOP logic and down, stream actuators (power contactors, valves, ...).

  Comment regarding EN 60204:

  The new national foreword of EN 60204 now principally allows EMERGENCY STOP to be implemented using software and electronics. However, it must be proven that the new specific standards, such as e.g. EN 954-1 or IEC 61508, are maintained. This means that the national foreword of EN 60204 now makes it possible to use innovative safety technology bypassing the Section 9 of EN 60204, which is in some instances no longer up to date.

* **Dead man operation**
This term originally comes from the railways. Significance: The function is only maintained as long as the actuation elements (jog button) are pressed. If the actuation element is released, the function is interrupted, and measures are initiated to stop the hazardous motion.

5.4 Standards and Directives

- **Protective door interlocking, light curtains etc.**

  Protective door interlocking, light curtains or other safety-relevant sensors and actuators can also be directly connected according to the same basic principle as for EMERGENCY STOP.

- **De-coupled safety areas and mode groups**

  Various safety zones and mode groups are possible using integrated safety technology. These can include, for example, the working zone, re-equipping area or magazine, de-coupled from the automation system. EMERGENCY STOP functions, protective door interlocking functions etc. are then configured on a cell-for-cell basis. When shutting down, they are firstly effective for the drives and units associated with this particular cell or safety zone. This means that, while the machine is working in the automatic mode in the actual working zone, the necessary setting-up and service work can be carried out in parallel in the other safety zones. In this case, the drives can be operated with the protective door open, with, for example, "safely reduced speed". At the same time, at the re-equipping station, also with the protective door open, a new workpiece can be set up. The EMERGENCY STOP pushbuttons, assigned to the safety areas, are only accessible if the appropriate protective door is opened, and therefore function as a cell EMERGENCY STOP. The cell EMERGENCY STOP only acts on the drives or units located in the safety zone (mode group). The central EMERGENCY STOP, located outside, acts on the complete machine.

The integrated safety technology allows the previous mode groups, whose mode of operation today is still significantly influenced by hardware-related solutions, to be re-allocated. A re-allocation of the modes could look like this:

	pr EN 12417 Machining centers	pr EN 12415 Automatic lathes	EN 775 Industrial robots	pr EN 1921 Automatic production systems
Enabling switch device	Category 3	Category 3	Category 3*	Category 3*
Reduce speed incl. protection against unexpected starting (n = 0)	Category 3	Category 3	Category 3*	Category 3*
	Category B and enabling circuit			Category B* and enabling circuit
Interlocking protective devices	Category 3	Category 3	Category 3*	Category 3*
				Category 1* (service doors/flaps)
Limiting end stops	–	–	Category 3*	Category 3*
EMERGENCY STOP	Acc. to EN 60204	Category 3	Category 3*	acc. to EN 60204-1

* EN 775 and pr EN 1921 have been derived from the International Standards ISO 10218 and ISO 11161. However, there is no direct reference to these standards in EN 954. However, the technical requirements are comparable.

Graphic 5/15
Overview of safety-related controls in C Standards
(Taken from [6], Specialist article from the German Trade Association)

- Test: Traversing manually, setting up and testing program parts (cyclic dry run), held via the jog button (in dead man operation) with reduced process parameters.
- Automatic test: Cyclic program execution using the jog button (dead man operation) with partially reduced process parameters (e.g. reduced rapid traverse speed).
- Automatic: Cyclic program sequence with full process parameters.

Innovative machines require new operating mode concepts where integrated safety technology forms the basis. This means more flexibility with increased safety.

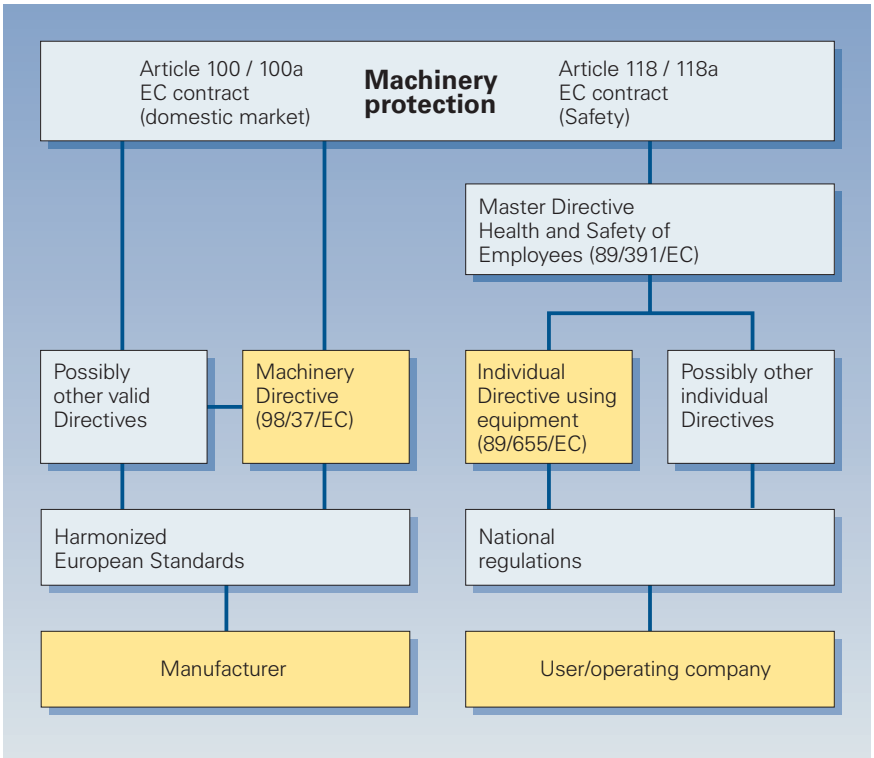
5.4.1 Requirements from EC Directives

The "EC Machinery Directive" and the "EC Individual Directive – Using equipment" define the basic protective goals. They make the manufacturer as well as the user of machines responsible in fulfilling and maintaining these protective goals. All EC Directives are anchored in the national legislation of the EC Member States. If the EC Directives are not fulfilled, this constitutes an offence.

With the CE Mark and the Declaration of Conformance, the machinery OEM must indicate that he maintains all of the EC Directives, valid up to this date.

Standards provide support and are pathfinders when it comes to implementation, but, contrary to the EC Directives, they are not binding. This fact opens up a certain degree of flexibility for innovative safety concepts when this potential is consequentially used. Generally, standards reflect the state-of-the-art technology. On the other hand, new innovative technical concepts represent the state of science, which is taken into account in updated standards.

When implementing EC Directives, deviations can be made from the Standards, if the same level of safety is achieved in another way. However, it is important to be able to prove that this level has been achieved. This can be realized, for instance, using a type test. If this is certified by a notified body, authorized in the EC (e.g. BIA), then this is valid throughout the EC.



Graphic 5/16
Requirements of the EC Directives
Source: "Machinery in Europe" from Alfred Johannknecht and Hans-Jürgen Warlich

5.5 Testing and Approval

(taken from [6], article from the German Trade Association [Berufsgenossenschaft])

There is no mandatory testing specified for drive systems with integrated safety. This applies for applications in the area of machine tools, robots, automated production systems, food making machinery etc. For machines, which are specified in Attachment IV of the Machinery Directive (e.g. presses, woodworking machines), machine testing may be mandatory, which possibly means that the drive system must also be checked and tested.

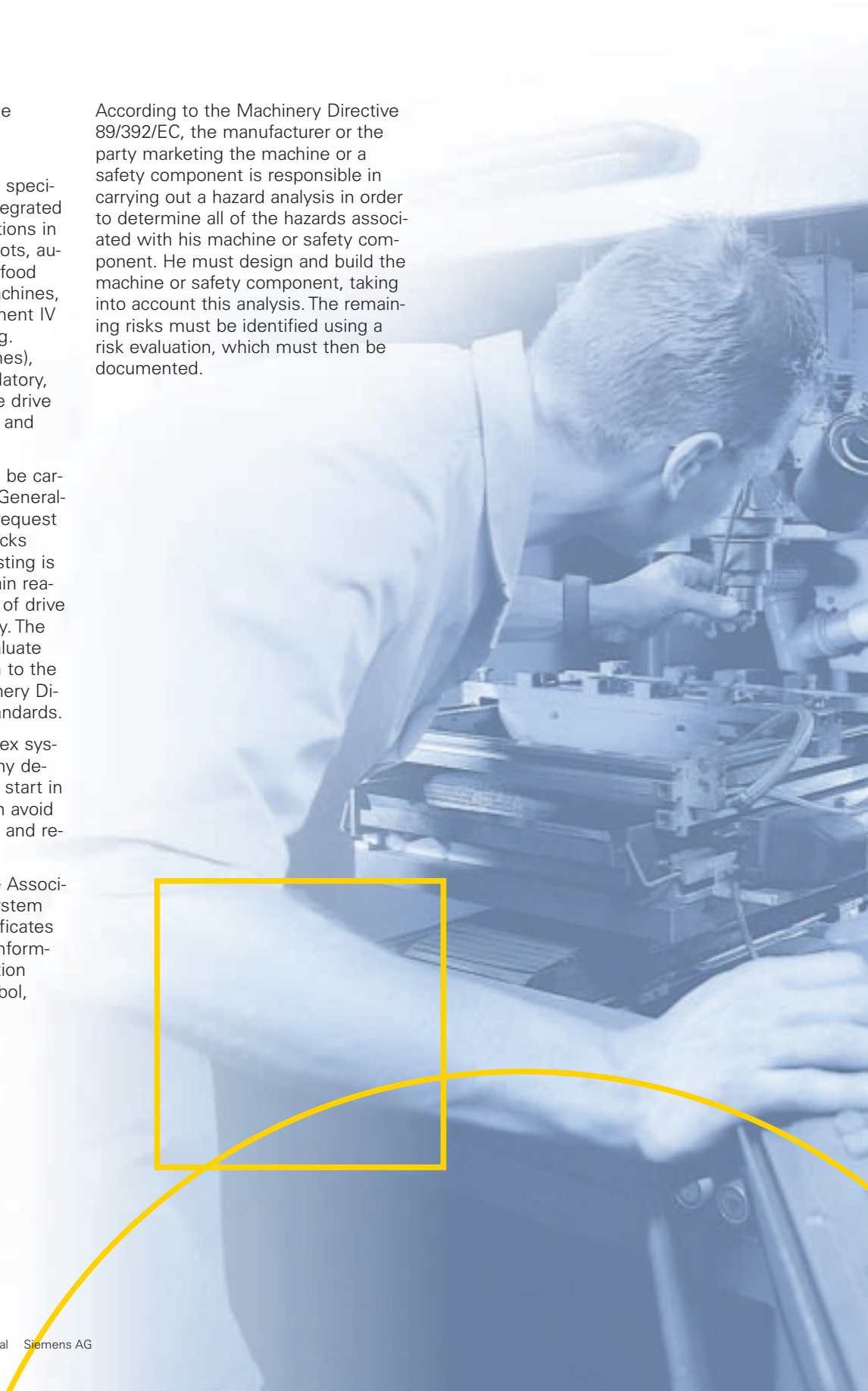
Independent of this, tests can be carried out on a voluntary basis. Generally, users and machine OEMs request that an independent body checks these components, even if testing is not mandatory. One of the main reasons is due to the complexity of drive systems with integrated safety. The user himself cannot easily evaluate whether the systems conform to the protective goals of the Machinery Directive and the associated Standards.

Tests of these types of complex systems should always accompany development, i.e. should already start in the conceptual phase. This can avoid problems during development and reduce testing costs.

For tests by the German Trade Association, Test and Certification System "BG-Prüfzert" , type test certificates according to EC Directives conforming to ZH1/419 [5], in conjunction with the appropriate test symbol, can be issued.

5.6 Hazard Analysis and Risk Evaluation

According to the Machinery Directive 89/392/EC, the manufacturer or the party marketing the machine or a safety component is responsible in carrying out a hazard analysis in order to determine all of the hazards associated with his machine or safety component. He must design and build the machine or safety component, taking into account this analysis. The remaining risks must be identified using a risk evaluation, which must then be documented.



5.7 Enhanced Availability Using Integrated Safety Technology



Completely new operator control concepts for machines with various requirements can be implemented by combining the safety functions listed under Section 5.3.2 "Function description". The operator can intervene, for example, in the magazine or re-equipping station (setting-up) while the machine is running.

However, optimum protection of the operator has topmost priority. The correct use and operation of the machine, specified as a result of the process, must be maintained at all times.

Machine protection (machine, workpiece, tool ...) can benefit from these new possibilities.

With integrated safety technology, there is a clear trend away from pure hardware and electromechanical solutions to software and electronics, therefore successively replacing technology which is subject to wear and tear.

Further, integrated safety technology provides an intelligent intervention in the system, directly down to the sensors and actuators. Completely new diagnostic capabilities are created, which are especially effective in providing preventive faultfinding. Even for faults and errors that suddenly occur during production, fast trouble-shooting and coordinated, safe shutdown can significantly reduce risk of personnel injury and/or machine damage.

Integrated safety technology permits:

- Optimized process operations
- Partial processes can run in parallel
- Simpler machine infrastructures
- Machine operator control concepts in line with those required in practice.

Impact on the availability:

- Reduced potential for faults
- Longer production uptimes
- Shorter downtimes

Integrated safety technology represents a significant potential to enhance the availability.

5.8 Customer Support

Spectrum of systems, products and services (for machine OEMs and end customers)

Service	Description
Concept generation	Starting from the hazard analysis and the required customer operator control philosophy, the safety functions are adapted to the machine. This involves, for example: • Mode types • Safety functions with the protective doors closed • Safety functions with the protective doors open • EMERGENCY STOP concept • Investigation of safety-relevant, external signals and elements
Standard configuring/ engineering	Starting from the concept generation, the following standard functions are integrated in the machine circuit diagrams: • Safe standstill, safe operating stops • Safely reduced speed • Safe software limit switches, safe software cams In this case, external safety elements (e.g. door interlocking functions, EMERGENCY STOP push buttons,) are either conventionally configured or they are logically combined using "Safe programmable logic".
Configuring safe programmable logic	Starting from the standard software, the following objects are generated for the safe programmable logic: • Function chart • Logic program for the PLC area • Logic program for the NC area • Required data blocks (e.g. DB18) These objects are embedded in the overall system.
Commissioning	Starting from the configured software which was generated, safety functions are commissioned. The customer provides the machine so that the drives can be traversed (moved), and the cabinet is wired up according to the engineering documentation.

Service	Description
Acceptance certificate	Starting from the existing engineering documentation and completed commissioning, an acceptance certificate is generated for the safety functions. These include: • Description of the machine (name, type ...) • Description of the safety and operator control concepts • Description of the axis-specific safety functions • Testing all of the safety functions including the safe programmable logic • Documenting the test results The customer receives the acceptance certificate as hardcopy and electronically on a data medium.
Approval procedure	Support when administering and backing up an approval procedure from approved bodies (e.g. BG/BIA) or large customers.
Workshop	Workshops on the subject of machine safety are modified in line with individual customer requirements and, when required, are held at the customer's facility. Possible contents can include: • Machinery Directives, general Standards • C Standards (machine-specific) • Hazard analysis, risk evaluation • Control categories (according to EN 954-1) • SINUMERIK Safety Integrated – function and system description • Configuring, machine data • Commissioning • Acceptance certificate
Hotline	For acute problems during commissioning, experts on "SINUMERIK Safety Integrated" can be reached under the SINUMERIK Hotline No. (refer to Section 8.7).
Local service	Experts analyze faults and problems locally. The causes are removed and a solution concept is drawn up and implemented.

5.9 Ordering Data and Documentation

5.9.1 Software

Software 840D	Order No.	Comments
Basic option	6FC5250-0AC10-0AA0	Including 4 drives
Axis option	6FC5250-0AC11-0AA0	From the 5th drive
Multi access option	6FC5250-0AC12-0AA0	13 additional axes/spindles

Software 840C	Order No.	Comments
Basic option	6FC5150-0AC10-0AA0	Including 4 drives
Axis option	6FC5150-0AC11-0AA0	From the 5th drive
Multi access option	6FC5250-0AC12-0AA0	13 additional axes/spindles

Comment: For SINUMERIK 840C, only the basic functions are available – no SPL

5.9.2 Hardware

SIMODRIVE Performance control	Order No.	Comments
1-axis version	6SN1118-0DG22-0AA1	Measuring circuit for current signals
1-axis version	6SN1118-0DG23-0AA1	Measuring circuit for voltage signals
2-axis version	6SN1118-0DH22-0AA1	Measuring circuit for current signals
2-axis version	6SN1118-0DH23-0AA1	Measuring circuit for voltage signals

Comment: We recommend the input for voltage signals.
The control boards must always be ordered with a DMS measuring circuit.

SIMODRIVE Standard 2 control	Order No.	Comments
2-axis version	6SN1118-0DM23-0AA0	Measuring circuit for voltage signals

Comment: The control boards must always be ordered with a DMS measuring circuit.

SINUMERIK 840C NCK periphery	Order No.	Comments
Mixed I/O modules	6FC5111-0CB02-0AA0	16 inputs, 16 outputs, 0.4 A
Terminal strip converter, 37-pole	6FC9302-2BD01	With LED's (green)
Pre-assembled cable	6FC9344-3XY00-1AF0	Module → converter, 5 m

SINUMERIK 840D NCK I/O	Order No.	Comments
NCU terminal block	6FC5211-0AA00-0AA0	For 8 DMP compact modules
Digital inputs	6FC5111-0CA01-0AA0	DMP compact, 16 inputs
Digital outputs, 24 V DC/0.5 A	6FC5111-0CA02-0AA2	DMP compact, 16 outputs
Digital outputs, 24 V DC/2 A	6FC5111-0CA03-0AA2	DMP compact, 8 outputs
Pre-assembled cable	6FX2002-1CA01-1AB0	Drive bus → terminal block, 1 m

5.9.3 Documentation

SINUMERIK 840C Safety Integrated Function Description	Order No.	Comments
German	6FC5197-0AC50-0AP0	Manufacturers Documentation
English	6FC5197-0AC50-0BP0	Manufacturers Documentation

SINUMERIK 840D Safety Integrated Function Description	Order No.	Comments
German	6FC5297-6AB80-0AP0	Manufacturers Documentation
English	6FC5297-0AB80-0BP1	Manufacturers Documentation
French	6FC5297-0AB80-0DP1	Manufacturers Documentation

Brief Description Safety Integrated	Order No.	Comments
German	6ZB5411-0AG01-0BA0	E20001-A0030-M103
English	6ZB5411-0AG02-0BA0	E20001-A0030-M103-Y-7600