IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

The SISTEMA Cookbook 6

Definition of safety functions:
what is important?

Version 1.0 (EN)

Authors: Ralf Apfeld, Michael Hauke, Stefan Otto
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Alte Heerstrasse 111
53757 Sankt Augustin
Germany
Tel.: +49 2241 231-02
Fax: +49 2241 231-2234
Internet: www.dguv.de/ifa

Published by: Deutsche Gesetzliche Unfallversicherung e. V. (DGUV)
Glinkastrasse 40, 10117 Berlin, Germany

– June 2015 –

Contents

Introduction

In the context of EN ISO 13849-1 [1] and EN ISO 12100 [2], a safety function is a safety-related control function of a machine that reduces the risk presented by the machine to an acceptable level. The correct definition of the safety function is therefore of essential importance to machine safety. Unfortunately, after almost two decades of safety functions being applied in practice, incomplete, incorrect or misleading definitions are still encountered, even in generic safety standards.

This SISTEMA cookbook describes the essential points to be considered during the definition of safety functions in the field, and illustrates them with repeated reference to a progressively developed example (blue background). Summarizing key questions between individual passages (red background) assist the reader in detailing his own safety functions. Where a machine-specific product standard containing defined safety functions is available, this cookbook can be used as a supplement to it.

The cookbook thus facilitates communication at the interface between definition and implementation of safety functions. It is intended on the one hand for persons tasked with defining safety functions for the purpose of reducing risks in the context of the risk analysis of a machine; on the other, it addresses the perspective of control design by explaining all relevant parameters.

1 Safety functions for risk reduction

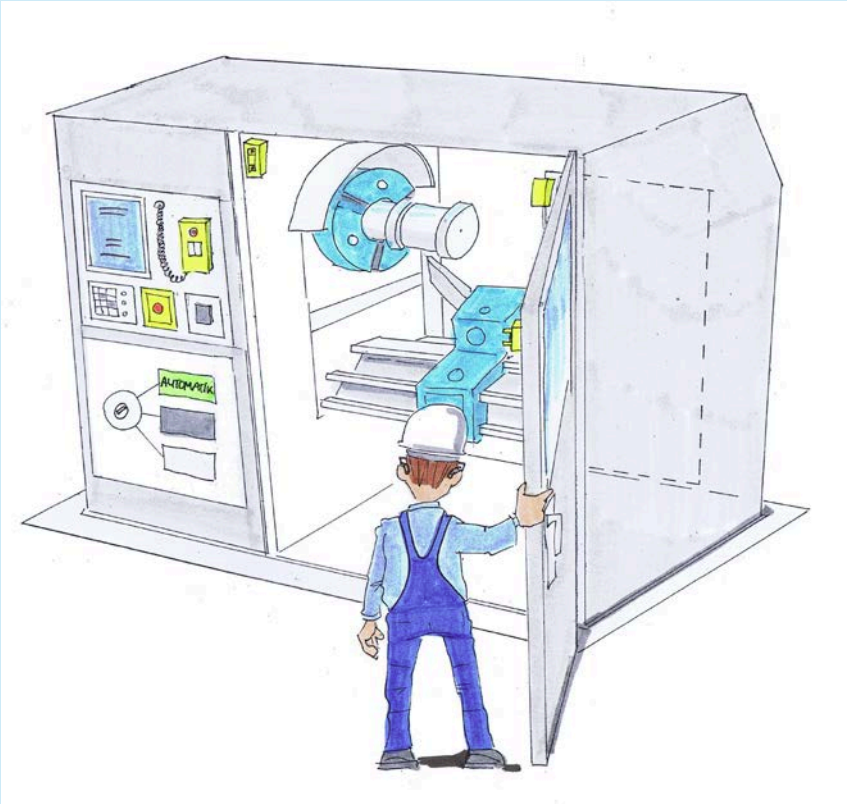
Safety functions constitute an important element of the risk-reduction procedure described in EN ISO 12100. Accordingly, the standard defines the safety function as a function of a machine whose failure can result in an immediate increase of the risk. Whether and to what extent the risk on a machine must be reduced is determined from the risk assessment. In this assessment, the risk presented by a machine at the different stages of its life cycle is analysed and evaluated.

Risk reduction is described in EN ISO 12100 as a three-stage process. This standard requires each risk considered in the risk assessment process to be minimized in the first instance by inherently safe design of the machine. Only where this is not possible should safeguarding and complementary protective measures be implemented. Such measures include guards and protective devices.

Should, despite all safeguarding measures, residual risks remain, the risk reduction may be attained in the third and final step only by user information and organizational measures.

The role of the safety function in the process of risk reduction is illustrated with reference to the example of a lathe (see Figure 1 and Table 1). The stated safety function will then be described in further detail in the subsequent chapters.

Figure 1: Opening the safety door in automatic mode



The lathe features a front and a rear safety door providing access to the machining area. Rotation of the spindle and workpiece and movement of the axis for displacement of the tool constitute dangerous movements. The safety doors are not equipped with guard locking: they can therefore be opened even whilst the machine is running. Machining of the workpiece is permissible only in automatic mode and with the safety doors closed.

Table 1: Excerpt from the risk assessment

Hazard	Inherently safe design	Safeguarding	User information
Fire resulting from ignition of the cooling lubricant	Use of non-flammable cooling lubricants	Not applicable	The use of flammable cooling lubricants is not permitted.
Pinching/shearing caused by movement of the axes (automatic mode)	Not possible	Safety function: "Opening of a safety door results in all machine movements being stopped"	Not applicable
Setup by untrained personnel (setup mode)	Not possible	Not possible	Only trained personnel have access to the key for the operating mode selector switch

2 Basic definition of safety functions

2.1 Limits of safety functions

Risk assessment to EN ISO 12100 begins with definition of the limits of the machinery. Parallel to this procedure, the limits of the safety functions must also be considered:

- **Use limits**

  Definition of the use limits of a safety function includes analysis of the machine's operating modes. The tasks of the machine operatives differ, in some cases considerably, in terms of the exposure to hazards in the various operating modes. Whereas in automatic mode, the danger zone is often safeguarded by guards, setup of a machine often entails the performance of tasks in immediate proximity to the danger zone. Depending upon the operating mode, different requirements therefore apply to the necessary degree of risk reduction, or the risks to be considered take different forms. Accordingly, different safety functions may be used in different operating modes. It is advantageous for the selection of the operating mode to be treated as a safety function in its own right (see Section 5.1).

- **Space limits**

  Where several spatially separated danger zones exist on a machine, the operative may be at only one danger zone at any one time. In this case, it is advisable for a dedicated safety function to be defined for each danger point. If, for functional reasons, triggering of a safety function must nevertheless stop multiple machine movements, it is still sufficient for definition of the safety function to consider only the movements that actually give rise to a hazard in the situation or location concerned (see Chapter 5.3 of BGIA Report 2/2008e, "Functional safety of machine controls" [3]).

  Even where several danger points overlap within a danger zone, separate safety functions can be defined for the hazards presented by individual machine parts, even when identical components are in some cases used for execution of the safety functions. A description of the method to be followed in this case can be found in the Expert Committee Information Sheet concerning safety functions to EN ISO 13849-1 in the case of overlapping hazards [4].

  Note:

  The need for safety functions to be divided up further is a result of the influence of the number of components upon their probability of failure (PFH_D) (see Chapter 3).

  The situation for the guards the operation of which is to trigger the safety function is similar to that for the dangerous machine parts: a person accesses the danger zone only through one of several safety doors, for example. It is therefore perfectly legitimate in the cases described to consider only one safety guard per safety function. Each of the other (identical) safety guards has its own (identical) safety function (see Section 5.3 of [3]).

  Note:

  The cascading of safety doors may have negative consequences for the diagnostic coverage. This must be taken into account when safety functions are analysed separately for multiple safety doors (refer in this context to ISO/TR 24119 [5] and to [6]).

- **Time limits**

  The machine limits considered by EN ISO 12100 also include the time limits of the machine. Among these are its mission time and the lifespan of the components. The intended mission time of the machine is relevant to the safety functions because it has an influence upon subsequent calculation of the probability of failure (PFH_D) of the safety function (see Chapter 3). In turn, a limited lifespan of the components involved in the safety function may result in them having to be renewed before completion of the mission time. In the context of EN ISO 13849-1, a mission time of 20 years is assumed.

2.2 Basic elements of safety functions

As is already evident from the example stated, namely "Opening of a safety door results in all machine movements being stopped", the formulation of a safety function generally includes three items of information:

1. Triggering event
2. Safety-related reaction
3. Dangerous part of the machine

Once the limits of the safety function as presented in the previous section have been defined, these three aspects can now be specified in greater detail:

- **Triggering event**

  The triggering event is generally operation of a safety guard – in the example stated, opening of a safety door. In consideration of the space limits of the safety function however, only the safety door opened by the operator should be considered.

  Where, as in the example, the machine under analysis has several safety doors, a dedicated safety function can be defined for each safety door when the danger zone is identical. Apart from the safety doors themselves, the safety functions are identical:

  "Opening of the (front) safety door **ST1** results in all machine movements being stopped."
  "Opening of the (rear) safety door **ST2** results in all machine movements being stopped."

  In the discussion below, only the safety function for the front safety door will be considered in greater detail.

- **Safety-related reaction**

  The safety-related reaction brings about the safe state. The most elementary safety-related reaction is uncontrolled stopping (STO, safe torque off) of the dangerous movement (see Section 3.1 of [7]). This is generally achieved by interruption of the power supply. The benefit of uncontrolled stopping is that in the majority of cases, the safe state can be brought about automatically even in the event of a power failure, owing to observance of the fail-safe principle. Conversely, if the dangerous movement is to be stopped as quickly as possible following a demand upon the safety function and if this is not possible by STO alone owing to running-on of the machine part under analysis, a controlled stop (SS1, safe stop 1) of the motor may be advantageous. A controlled stop followed by a safe stop (SS2, safe stop 2) is used when owing to the requirements of the machining process, the motor must be maintained in a controlled position once it has stopped.

In the example of the lathe considered here, it is assumed that in the machining process, the workpiece must also continue to be held in a controlled position even after stopping, in order to prevent loss of the position. Accordingly, with reference to the example of opening of the front safety door, the following formulation is required for the safety function under consideration here:

"Opening of the safety door ST1 results in **a controlled stop (SS2)** of all machine movements."

The safety-related reactions described above are usual for electric drives. They can however also be transferred to other technologies, such as hydraulic and pneumatic cylinders.

Once a safe state has been reached by a safety-related reaction, it may not generally be left until the triggering event has been cancelled (in order to provide protection against unexpected start-up). In the safety function considered here, for example, the stationary drive must not be able to restart unexpectedly whilst the safety door is still open. In some cases, conscious acknowledgement of the safety function by manual resetting of the safety guard may also be necessary, as for example when the operative is able to step behind the safety door.

- **Dangerous part of the machine**

  Since the safety function is defined based upon the risk assessment and the hazards identified by it, the machine part that gives rise to a hazard for the operative in the situation concerned, for example as a result of movement, radiation or heat, is always to be considered dangerous. Should several hazards overlap in a danger zone on the machine under analysis, it may be advantageous for them to be assessed separatelyfor each machine part.

  In the example under consideration here, it is advantageous for the safety functions to be broken down as follows:

  "Opening of the safety door ST1 leads to a controlled stop (SS2) of **the axis A1**."
  "Opening of the safety door ST1 leads to a controlled stop (SS2) of **the spindle S1**."

  In the discussion below, only the safety function for stopping the axis A1 will be considered further.

With definition of the triggering event, the safety-related reaction and the dangerous machine part, the three most important aspects of the safety function are defined. During formulation of a safety function, it is therefore advantageous to begin by asking the following three questions:

What event triggers the safety function?

What is the safety-related reaction?

Which machine part presents the hazard?

2.3 Operating mode

In addition, in consideration of the use limits (Section 2.1), the operating modes must be determined in which the safety function is to be available:

In what operating mode is the safety function to be active?

Stopping of a dangerous movement when a safety guard is operated is a typical safety function for automatic mode. By contrast, in setup mode, in which the axis may be moved even when the safety door is open, this safety function is not relevant.

"**Automatic mode**: opening of the safety door ST1 leads to a controlled stop (SS2) of the axis A1."

2.4 Required Performance Level (PL_r)

As part of the risk assessment, the level of the risk associated with the hazard under analysis must be estimated. If the risk is to be reduced by a safety function, EN ISO 13849-1 proposes the use of the risk graph for this purpose. By estimation of the anticipated injury severity, the frequency and duration of exposure to the hazard and the facility for avoidance of the hazard or limitation of the harm, the risk graph produces a direct estimation of the required Performance Level PL_r of the safety function.

With what Performance Level PL_r is the safety function to be implemented?

For the safety function stated above, risk assessment in accordance with the product standard yields a required Performance Level PL_r of c.

2.5 Demand rate

The demand upon a safety function is made when the triggering event occurs (see Section 2.2). When the safety function is executed correctly, the demand leads to the safety-related reaction. Conversely, activation of a safety function refers to the safety function generally being made available, for example by selection of an operating mode.

Safety functions are executed by the safety-related parts of the control system (SRP/CS, see also Chapter 3). Where parts subject to wear are used for this purpose, such as position switches, relays, contactors or valves, the nature, duration and frequency of their use is reflected directly in their lifespan. The attained Performance Level of the safety function is also related directly to these parameters through a component's probability of failure. A further case for which the demand rate is relevant is the use of Category 2 architectures for implementation of safety functions. For Category 2, application of the simplified method for estimation of a Performance Level to EN ISO 13849-1 may necessitate a test rate at least one hundred times greater than the demand rate. The demand rate must therefore be known in order for the required test rate to be determined. Estimation of the demand rate on the safe side is required even when it is not known precisely.

Protection against unexpected start-up is an element of safety functions that is relevant not only as a consequence of the process of stopping, but also once the dangerous machine

movements have been stopped (see Section 2.2, "Dangerous part of the machine"). A demand is generally also made upon the safety function when a safety device is operated whilst the machine is at rest, for example when the safety door of a machine must be opened in automatic mode for the purpose of a workpiece change. The consequence of this for the demand rate is that the demand when the dangerous machine movements are at rest must also be considered. The control chain that is triggered is identical in the two cases.

How frequently must the demand upon the safety function be anticipated?

"Automatic mode: opening of the safety door ST1 leads to controlled stopping (SS2) of the axis A1. **The demand is made on average 6 times per hour.**"

Activation of the safety function occurs by selection of the "automatic mode". The **demand** is made upon the safety function when the safety door is opened.

2.6 Running-on

Certain time limits within which the safe state must be brought about before a person is able to reach the danger point apply to each safety-related reaction. This particularly applies when electro-sensitive protective equipment (such as a light curtain) is used for safeguarding. Running-on of the system as a whole, i.e. the reaction time of the safety device plus the time required for the dangerous part of the machine to come to a halt, is mutually dependent upon the safety distance to the danger zone in this context (see [8]).

Note:

Should the power supply fail (see also Section 4.1) or a component develop a fault, the running-on time may increase (see Section 6.4 of [7]).

How soon after the demand is made upon the safety function must the safe state of the part of the machine be reached?

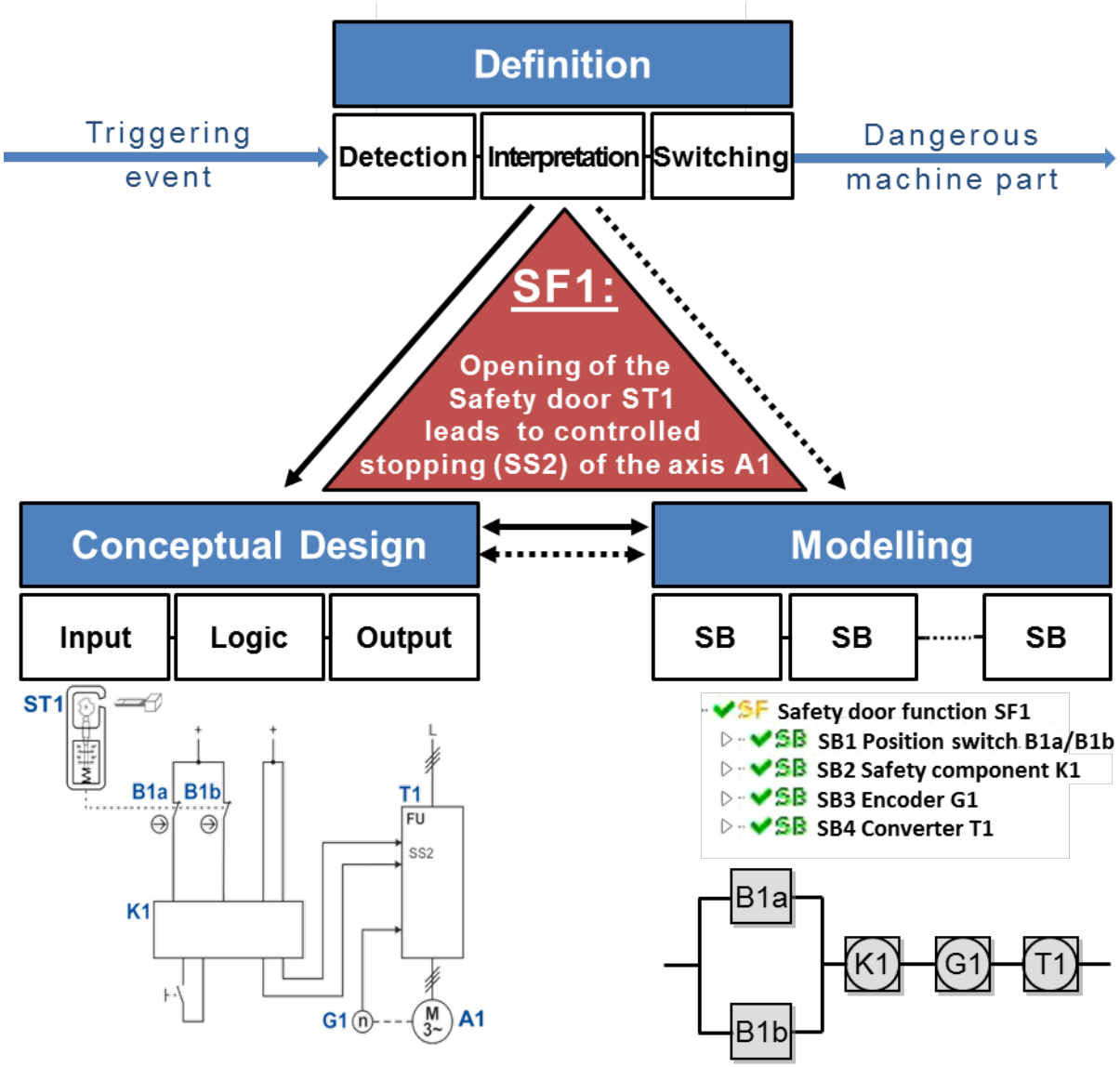
"Automatic mode: opening of the safety door ST1 leads to controlled stopping (SS2) of the axis A1 **within a maximum of 800 ms**. The demand is made on average 6 times per hour."

3 From definition to implementation of the safety function

A safety function is executed by the control system. EN ISO 13849, "Safety of machinery – Safety-related parts of control systems" [1], addresses the relevant safety-related parts of the control system (SRP/CS). The analysis of the safety functions was extended to include calculation of their probability of dangerous failure (PFH_D) during revision of this standard in 2006. This analysis is based in part upon the failure values of the components involved in execution of the safety functions. Unfavourable definition of a safety function – such as when the definition encompasses too many components – can now rapidly lead to the required Performance Level, which is the measure of the function's overall probability of failure, not being attained. Estimation of the PFH, for example with the aid of SISTEMA [9], is used to determine whether implementation of the safety function by the SRP/CS satisfies the required Performance Level.

The relationship between formal definition, conceptual design of the control system and modelling in SISTEMA will be discussed in greater detail below (see Figure 2).

Figure 2: From definition to implementation



- **Definition**

  In accordance with the basic elements of a safety function described in Section 2.2, this function can be broken down into three sub-functions: detection of the triggering event, interpretation of the detected signal, and the safety-related response of switching of the dangerous part of the machine into the safe state.

- **Conceptual design**

  During conceptual design of the safety-related parts of the control system (SRP/CS), for example in a schematic circuit diagram, suitable components connected together by interfaces are assigned to the three sub-functions. The input is responsible for detection of the triggering event. In the example, the position switch B1 represents the input of the safety function, which detects the triggering event, i.e. opening of the safety door. Interpretation of the input signals is performed by the logic, which in this case is implemented by the safety switching device K1. The logic links the input to the output of the safety function. At the output, "switching" of the outputs of the power control elements executes the safety-related reaction: in the case of the example, by tripping the safety sub-function SS2 in the frequency converter T1. The encoder G1 is also required at this point for safe monitoring of the axis movement.

  Note:

  Sensor – logic – actuator is often used rather than input – logic – output to describe the group. However, the term ”actuator” at least may be misleading in this context, since it could be understood to mean the motor (or cylinder) to be stopped on the machine under analysis. The motor itself is however not generally considered a part of the SRP/CS, provided a dangerous movement is no longer possible in the absence of drive energy. An exception are axes subject to gravitational force, on which, depending upon the implemented safety function and operating mode, the motor associated with the axis – and holding devices, where present – must also be included in the analysis. (For vertical axes subject to gravitational force, see Section 4.1.)

- **Modelling**

  For estimation of the PFH_D of a safety function, the safety-related parts of the control system are modelled in SISTEMA on a chain of sub-systems (SB1, SB2, etc.). This can be described logically by a safety-related block diagram (dangerous failure of each sub-system leads to failure of the safety function.) The number of sub-systems is not defined from the outset, but is dependent upon the hardware used and the choice of architecture. It is possible for the complete safety function to be implemented in the form of a single sub-system (such as a programmable laser scanner with integrated cutoff relay) or as a chain of sub-systems of any desired length. In the example considered here, the position switch B1 and its two positively opening contacts B1a and B1b form a (two-channel) sub-system representing the input of the safety function. For this application, a fault exclusion can be reasoned for the (single-channel) mechanism of the position switch, as a result of which it is not considered in the safety-related block diagram. Besides the safety switching device (the logic component of the safety function), the frequency converter T1 (with integral stop function) and the encoder G1, which are both part of the output of the safety function, constitute encapsulated sub-systems. For further details, refer to SISTEMA Cookbook 1 [10].

- **Sequence of implementation**

  In practice, a safety function is generally modelled in SISTEMA following conceptual design of the safety-related parts of the control system. This design procedure is shown in Figure 2 by unbroken arrows.

Several cycles of conceptual design and modelling must often be iterated before a suitable implementation of the control solution is reached. It may be necessary to divide a sub-function into multiple sub-systems or to group multiple sub-systems into a single sub-system, for example when a frequency converter with integral safety functions encompasses the sub-systems of logic and output.

Note:

Alternatively, the sub-systems may be determined directly from the sub-functions derived from definition of the safety function, and the safety-related parts of the control implemented only afterwards. This procedure is shown in Figure 2 by dotted arrows, since it is followed only rarely in practice. It is useful at this point for the safety function to be divided into sub-functions based upon the formal definition (detection – interpretation – switching). Once each sub-function has been mapped to a sub-system, a suitable separate technical control implementation is sought for each sub-system.

4 Special aspects

4.1 Failure of the power supply and availability on gravity loaded axes

A power failure is generally not to be treated as a fault, but as a foreseeable operating state. The response to this state must assure the bringing about of a safe state. In the majority of cases, the de-energized state itself constitutes a safe state, provided a hazardous movement cannot arise.

Machine parts subject to gravitational force may give rise to hazards even in the de-energized state, as a result of unintended dropping. Where the intended use of a machine permits the presence of a person beneath a gravity loaded axis, stricter requirements apply to the machine's fail-safe behaviour. For more information on this subject, please consult the information sheet ”Gravity loaded axes – vertical axes” [11].

In particular cases it may be advantageous for safety functions that are to be performed where power (electrical, pneumatic, hydraulic, etc.) is present to be separated from safety functions for the event of power failure. Following detection of a power failure, different means may then be used to bring about a safe state (such as stopping of a workpiece spindle in the event of failure of the hydraulic power used for workpiece clamping; see SF3 in [12]). The reaction time is once again an important factor.

What safety-related reaction is required in the event of power failure?

The safety function on the lathe described in the example is active when power is present. In the event of power loss, a separate safety function ensures that the dangerous movements are stopped. The function can be implemented for example by means of pneumatically released brakes that are applied in the event of power failure (refer to Example 14 in [7]).

4.2 Prioritization of safety functions

Where two competing safety functions can be triggered in parallel, priorities must be defined in order to ensure which of the two is to be executed. This may also be important when a second safety function is to be triggered before the safety-related reaction of a safety function has been completed. Whether triggering of the second function is to be ignored and the reaction of the first function is to be completed, or the first function is to be interrupted by the second, must be determined by appropriate assignment of priorities.

In most cases, it will be advantageous to prioritize safety functions based upon their safety-related reactions, i.e. to assign priority to the safety function that most strongly reduces the risk of injury. Here too, it must be considered that safety functions can fail in the event of failure of the power supply or incidence of a fault.

Is the safety function assigned a greater or lower priority compared to other safety functions?

On the lathe, the safety function for monitoring the safety door is assigned a lower priority than the safety function for stopping the drive when the emergency-stop device is actuated (see Table 2).

Table 2: Automatic mode

Priority	Safety function (brief description)	Safety-related reaction
1	Emergency stop	STO
2	Safety door monitoring	SS2

4.3 Combining of safety functions

Safety functions may be dependent upon other safety functions. On the majority of machines for example, an enabling function may be executed only at a safely limited speed (SLS) of the motor axes when a safeguard is open (see also Sections 5.2 and 5.3). Consequently, when it is ascertained that a safety function (in this case, SLS) is already active when a demand is made upon a second safety function (in this case, the enabling function), the first safety function can be considered as a basis for risk assessment for the second (see BGIA Report 2/2008e, Annex A, Example 4 [3]).

Note:

This is also reflected in the fact that the process of risk reduction to EN ISO 12100 is an iterative process: following each definition of a safety function, a check is performed once again of whether the risk for the hazard under analysis has been adequately reduced or whether further measures based upon those already defined are required. This influence of one safety function upon the risk reduction to be attained by a second is therefore permitted in one direction only. The PL_r values of the two functions must not mutually reduce each other, as the overall risk reduction attained would otherwise be inadequate.

Are further active safety functions a condition for use of the safety function?

5 Special safety functions

In this chapter, three further safety functions will be discussed with reference to the example of the lathe.

Figure 3: Working with the safety door open in setup mode

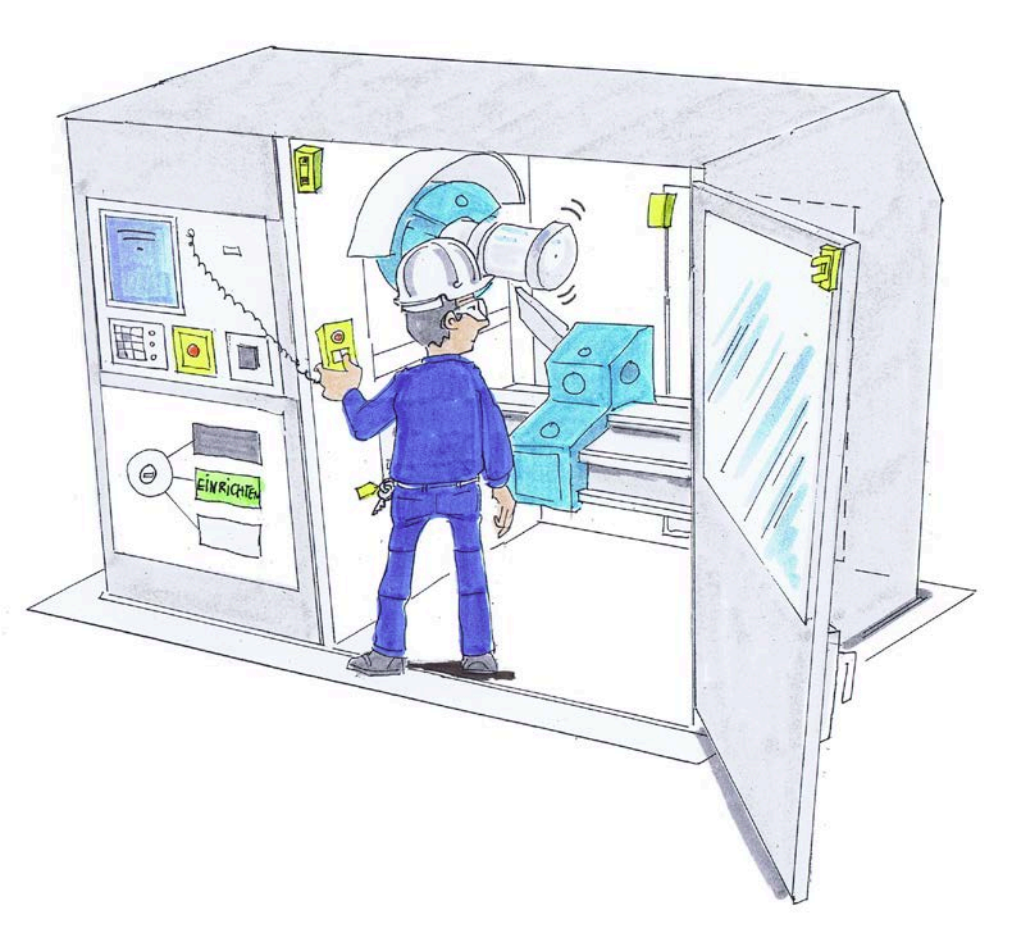


Figure 3 shows the lathe in Figure 1 in setup mode. An operator authorized to change the operating mode (by means of the lockable operating mode selector switch) uses an enabling device to control an axis of the machine whilst the safety door is open.

5.1 Operating mode selection

The change in operating mode may cause safety functions (such as monitoring of the safety door) to be deactivated and other safety functions (such as the enabling function) to be activated. Owing to the operating mode's influence upon the risk reduction by the provision of safety functions, it must therefore be assured that no more and no less than one operating mode is selected at any one time. A change to a different operating mode may occur only deliberately, and not as a result of failure of the control system. The question arises whether the control aspect of operating mode selection (such as the operating mode selector switch) is part of each safety function implemented on the machine, or whether operating mode selection can be regarded as a safety function in its own right. Analogous to the procedure with overlapping hazards (see Section 2.1 and [4]), in which discrete hazards are separated, selection of the operating mode is regarded as a safety function in its own right. This also

prevents the components for operating mode selection from further increasing the average probability of a dangerous failure per hour (PFH_D) in each individual safety function. In the normal case, the safety function of selection of the operating mode can be defined as follows:

"The safety functions required for the selected operating mode are activated according to the position of the operating mode selector switch."

5.2 Enabling function

In some operating modes, it may be necessary for work to be performed with the safeguard open, for example in troubleshooting or setup mode. Special control modes are generally used for this purpose. These ensure that at any instant, machine movements can be performed only where explicitly instigated by the operative. This can be achieved for example by means of an inching switch and/or enabling facility.

Operation by means of an enabling facility involves two-stage or three-stage enabling switches that must bring the affected part of the machine to a halt when released and (only on three-stage enabling switches) when fully depressed. The associated "enabling function" safety function must be defined accordingly in this case (see also Section 6, Table 2):

"Setup mode: release of the two-stage enabling switch leads to controlled stopping (SS2) of the feed axis."

The "inching mode" safety function must be defined in the same way. Here too, releasing of the inching switch must result in the machine stopping.

Note:

In general, the risk when a guard is open cannot be adequately reduced by an enabling function or inching mode alone. Only by simultaneous execution of a safety function for limitation of the movement can the required risk reduction be attained (see Sections 4.3 and 5.3).

5.3 Control of movements

For variable-speed electric power drive systems, safety sub-functions for limiting the movement are defined in the standard (see Chapter 3 of [7]). These include the SLS (safely limited speed) safety function already referred to. The standard defines this function as follows: "The SLS function prevents the motor from exceeding the specified speed limit." Whereas this definition of the safety function already appears adequate from the perspective of risk reduction to EN ISO 12100, further provisions are required for the control equipment and for determining the attained Performance Level in accordance with EN ISO 13849. As described in Chapter 2.2, the triggering event (exceeding of the specified maximum speed) and the safety-related reaction (stopping of the monitored axis, for example by SS1) must be stated, with reference to the specific dangerous movement/dangerous part of the machine. Further limiting functions may relate for example to the position, acceleration and torque.

Supplementary to the safety function referred to in Section 5.2, the following safety function can be formulated for implementation of the safely limited speed (SLS) (see also Section 6, Table 2):

"Setup mode: violation of the speed limit of the axis A1 leads to a controlled stop (SS1) of the axis A1."

The frequency of the demand upon the safety-related reaction (see Chapter 2.5) is not always easily estimated for these limit functions. Ultimately, the frequency with which the monitoring function must react to violation of a speed limit is dependent upon the reliability of the functional (not safety-related) control responsible for controlling the speed. For estimation of the demand rate, it is however worth considering that a machine that must be stopped, acknowledged and restarted continually (e.g. several times a day) owing to triggering of a limit function will not generally be accepted in the application.

"Setup mode: violation of the speed limit for axis A1 leads to a controlled stop (SS1) of the axis A1. **The demand is made on average once per day (estimation on the safe side).**"

6 Complete definition of safety functions

Based upon the key questions stated, it will be possible to describe the particular safety function in full in accordance with Table 3:

Table 3: Definition of a safety function in table form

Brief description	What is the brief description of the safety function?
Triggering event	What event triggers the safety function?
Safety-related reaction	What is the safety-related reaction?
Dangerous part of the machine	Which machine part presents the hazard?
Operating mode	In what operating mode is the safety function to be active?
PL_r	With what Performance Level PL_r is the safety function to be implemented?
Demand rate	How frequently must the demand upon the safety function be anticipated?
Running-on	How quickly after the demand is made upon the safety function is the safe state to be reached?
Behaviour in the event of a power failure	What safety-related reaction is required in the event of power failure?
Priority	Is the safety function assigned a greater or lower priority compared to other safety functions?
Supplementary safety function	Are further active safety functions a condition for use of the safety function?
Additional parameters	What additional parameters must be considered?

Table 4 lists the examples used in this SISTEMA cookbook in full, and supplements them with further examples where necessary.

Table 4: Examples of full definition of the safety functions

	SF1	SF2	SF3
Brief description	Safety door function	Enabling function	Safely limited speed (SLS)
Triggering event	Opening of the front safety door	Release of the two-stage enabling button	Violation of the speed limit
Safety-related reaction	Controlled stop (SS2)	Controlled stop (SS2)	Controlled stop (SS1)
Dangerous part of the machine	Forward feed axis	Forward feed axis	Forward feed axis
Operating mode	Automatic mode	Setup mode	Setup mode
PL_r	c	d	c
Demand rate	6x per hour	10x per day	1x per day
Reaction time	800 ms	200 ms	200 ms
Behaviour in the event of a power failure	Uncontrolled stopping (STO) of the forward feed axis	Uncontrolled stopping (STO) of the forward feed axis	Uncontrolled stopping (STO) of the forward feed axis
Priority	2 (with lower priority than the emergency-stop function)	3 (with lower priority than the safely limited speed (SLS) function)	2 (with higher priority than the enabling function)
Supplementary SF	-	Safely limited speed (SLS)	-
Additional parameters	-	-	-
Remarks	-	-	-

7 Literature

[1] EN ISO 13849-1: Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (12/08). Beuth, Berlin 2008

[2] EN ISO 12100: Safety of machinery – General principles for design – Risk assessment and risk reduction (03/11). Beuth, Berlin 2011

[3] Hauke, M.; Schaefer, M.; Apfeld, R.; Bömer, T.; Huelke, M.; Borowski, T.; Büllesbach, K.-H.; Dorra, M.; Foermer-Schaefer, H.-G.; Grigulewitsch, W.; Heimann, K.D.; Köhler, B.; Krauss, M.; Kühlem, W.; Lohmaier, O.; Meffert, K.; Pilger, J.; Reuss, G.; Schuster, U.; Zilligen, H.: Functional safety of machine controls – Application of EN ISO 13849. BGIA Report 2/2008e. Published by: Deutsche Gesetzliche Unfallversicherung, Berlin 2009. www.dguv.de/webcode/e91335

[4] Sicherheitsfunktionen nach DIN EN ISO 13849-1 bei überlagerten Gefährdungen. Fachausschuss-Informationsblatt No 047. Issue 05/2010. Published by: Fachausschuss Maschinenbau, Fertigungssysteme, Stahlbau, Mainz 2010. www.bghm.de, Webcode 626

[5] ISO/TR 24119: Safety of machinery – Evaluation of fault masking in serial connections of guard interlocking devices with potential-free contacts (anticipated 2015)

[6] Apfeld, R.: Überwachung von Schutztüren an Maschinen – Hilfestellung durch die neue DIN EN ISO 14119. Technische Sicherheit 4 (2014) No 4, pp. 45-49 www.dguv.de/webcode/m621988

[7] Apfeld, R.; Zilligen, H.; Köhler, B.: Safe drive controls with frequency converters. IFA Report 7/2013e. Published by: Deutsche Gesetzliche Unfallversicherung, Berlin 2014. www.dguv.de/webcode/e635980

[8] EN ISO 13855: Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body (10/10). Beuth, Berlin 2010

[9] Software-Assistent SISTEMA: Safety Integrity Software Tool for the Evaluation of Machine Applications. A Tool for the Easy Application of the Control Standard EN ISO 13849-1. www.dguv.de/webcode/e34183

[10] Apfeld, R.; Hauke, M.; Schaefer, M.; Rempel, P.; Ostermann, B.: The SISTEMA Cookbook 1. From the schematic circuit diagram to the Performance Level – quantification of safety functions with SISTEMA. Published by: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA), Sankt Augustin 2010. www.dguv.de/webcode/e109249

[11] Gravity loaded axes – vertical axes. Division information sheet No 005. Edition 09/2012. Published by: Fachbereich Holz und Metall der DGUV, Mainz 2012. www.bghm.de, Webcode 627

[12] Drehmaschinen – „Werkstückspannen“ – Beispielrechnung einer Sicherheitsfunktion nach DIN EN ISO 13849. DGUV Information FB-HM-039. Issue 10/2014. Published by: Fachbereich Holz und Metall der DGUV, Mainz 2014. www.bghm.de, Webcode 626