ZVEI:
Die Elektroindustrie

Whitepaper

Fault tolerance in machine safety

Part I – Basics, Revision 1.0

Devision Automation

Abstract

Fault tolerance in machine safety

In engineering, „fault tolerance“ means the ability of a technical system to maintain its functionality even when failures and fault conditions occur. Fault tolerance increases the availability of a system. This document describes a way to implement fault-tolerant safety functions that allow further operation of a machine or plant in certain fault scenarios without neglecting employee safety.

The term „degraded operation“ is introduced as a synonym for use of safety functions in the degraded condition. In degraded operation, a machine continues to perform a safety function after a fault has been detected. Three different types of degraded operation are defined and the respective limits and restrictions are described. Furthermore, the term „decision-maker“ is introduced, which controls the transition to operation in the degraded condition in the machine when the fault is detected.

It is shown that there are possibilities to maintain the availability of a machine in the event of a fault, for example to end the current machining step in an orderly manner without having to interrupt production.

Editorial staff:

Frank Bauder	Leuze electronic
Thomas Bömer	Institut für Arbeitsschutz (IFA) der DGUV
Helmut Börjes	Wago Kontakttechnik
Dr. Tilmann Bork	Festo
Carsten Gregorius	Phoenix Contact
Joachim Greis	Beckhoff Automation
Richard Holz	Euchner
Florian Rotzinger	Pilz
Frank Schmidt	K.A. Schmersal
Thomas Schulz	BGHM – Berufsgenossenschaft Holz und Metall
Rolf Schumacher	Sick
Klaus Stark	Pilz
Manfred Strobel	ifm electronic

Fault tolerance in machine safety

Published by:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
German Electrical and Electronic Manufacturers’ Association
Devision Automation
Lyoner Straße 9
60528 Frankfurt

Contact:
Dr. Markus Winzenick
Telephone: +49 69 6302-426
E-mail: winzenick@zvei.org

www.zvei.org

November 2019

Content

1 Introduction 5
1.1 Motivation 5
1.2 Scope of application 5
1.3 Standards situation 5
2 Normative references 6
3 Definitions and abbreviations 6
3.1 Definitions 6
3.1.1 Safety 6
3.1.2 Safe state 6
3.1.3 Functional unit 6
3.1.4 Fault 7
3.1.5 Fault tolerance 7
3.1.6 Failure 7
3.1.7 Dangerous failure 7
3.1.8 Safety-related failure reaction (negation) 7
3.2 Abbreviations 7
4 Fault tolerance in systems 8
4.1 Safety-related controls 8
4.1.1 General 8
4.1.2 Fault tolerance 8
4.2 Dangerous failures 10
4.2.1 De-energization principle 10
4.2.2 Safety-related failure reaction 10
4.2.3 Operation in degraded condition 11
5 Risk reduction through safety functions 12
5.1 State transitions 12
5.1.1 Random hardware failures 12
5.1.2 Degradation of safety functions 12
5.1.3 Tolerable faults 13
5.1.4 Decision-maker 14
5.1.5 Safety function in degraded condition 14
5.1.6 Signalling the degraded condition 15
5.2 Variants of operation in degraded condition 16
5.2.1 General 16
5.2.2 Time-limited operation with degraded safety function 17
5.2.3 Operation for an unlimited period of time with complementary measures 19
5.2.4 Operation for an unlimited period of time with additional safety functions 19
6 Conclusion and outlook 19

1 Introduction

1.1 Motivation

Occupational safety in an industrial environment has always been a high priority. Companies have recognised that the protection of employees during work on machines and equipment is necessary for various reasons. On the one hand, legal regulations and rules whose non-compliance is subject to appropriate sanctions have a motivating effect here. On the other hand, the safety technology used on machines and in plants is repeatedly seen as the cause of unwanted machine downtimes, which can lead to manipulation incentives.

Until now, monitoring of protective equipment for machines and plants in industrial environments has been based on the dogma of stopping as quickly as possible in the event of a fault. This means that an expected value is defined for each internal monitoring function and deviations from this expected value lead to a shutdown reaction. Increasing productivity requirements, especially under the aspects of Industry 4.0, demand extended safety concepts for the future.

The aim of this document is to show alternatives to immediate shutdown in case of fault detection. It defines the framework within which machines can continue to operate after detecting faults in safety functions without exposing persons to unacceptable risks.

1.2 Scope of application

Annex I of the Machinery Directive 2006/42/EC lays down the basic health and safety requirements for the design and construction of machinery for the European Economic Area. Accordingly, a manufacturer of a machine must ensure that a risk assessment is carried out in order to determine the safety and health protection requirements applicable to each machine. The machine must then be designed and constructed taking into account the results of the risk assessment.

The ISO 12100 standard establishes guidelines for risk assessment and risk reduction to help suppliers design safe machinery. In addition to the standard, this document describes an approach to the design of safe machinery that also meets new technological requirements as mentioned above.

The scope of this document is limited to the operation of machines/plants under fault conditions in their safety functions. It is aimed at machine builders and system integrators who plan safety functions during the development of the machine and implement them using subsystems. The recommendations in this document are equally applicable to the implementation of safety functions according to ISO 13849-1 and IEC 62061.

This document focuses exclusively on the systems commonly used in machine and plant construction for higher safety requirements, in which the execution of safety functions is still possible even in the event of a fault due to their original dual-channel structure.

Not considered by the application described here are:

- Single-channel safety systems, where safe operation in the event of a fault is generally ruled out,
- Systems with more than two channels (known from the process industry and avionics), regardless of their application.

1.3 Standards situation

This document considers the possible operation of machines/plants in degraded condition and describes additional requirements to be considered during design and integration. This functionality and the resulting requirements are not currently described in any standard.

Operation in a degraded condition complements the principle of energy separation. It designates an additional, time-limited functionality within a safety function. The concept of operation in a degraded condition does not conflict with the protection objectives specified in the Machinery Directive and the requirements specified in standards such as ISO 13849, IEC 62061 and IEC 61508.

The manufacturer/integrator is provided with pertinent information on the considerations for a time-limited safe operation of a machine/plant in the event of a fault in degraded operation. The degraded operation must be described and documented in the technical documentation. The operation of a machine/plant in degraded condition must only be possible in defined fault conditions. This operation is not intended as a regular operating mode in order to serve as a replacement for necessary risk reduction measures. This document covers all the technologies described in the above standards.

2 Normative references

The following documents are helpful for the application of this document.

ISO 12100:2010 Safety of machinery – General principles for design – Risk assessment and risk reduction

ISO 13849-1:2015 Safety of machinery – Safety-related parts of control systems
Part 1: General principles for design

ISO 13849-2:2012 Safety of machinery – Safety-related parts of control systems
Part 2: Validation

IEC 62061:2005 + AMD1:2012 + AMD2:2015
Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

IEC 60073:2002 Basic and safety principles for man-machine interface, marking and identification
Coding principles for indicators and actuators

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document, the following definitions shall apply.

3.1.1 Safety

Freedom from unacceptable risk to the outside from the functional and physical units considered
[IEV 351-57-05]

3.1.2 Safe state

State of a functional unit when safety is achieved
[IEC 61508-4:2010, 3.1.13, modified]

3.1.3 Functional unit

Entity of hardware or software, or both, capable of accomplishing a specified purpose
ISO/IEC 2382:2015

3.1.4 Fault

State of a functional unit, characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources
[ISO 13849-1:2015, 3.1.3, modified]

3.1.5 Fault tolerance

Ability of a functional unit to continue to perform a required function in the presence of faults or errors
[IEC 61508-4:2010, 3.6.3]

3.1.6 Failure

Termination of the ability of a functional unit to perform a required function
Note 1 to entry: After a failure, the item has a fault.
Note 2 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.
[ISO 13849-1:2015, 3.1.4, modified]

3.1.7 Dangerous failure

Failure which has the potential to put a functional unit in a hazardous or fail-to-function state
[ISO 13849-1:2015, 3.1.5, modified]

3.1.8 Safety-related failure reaction (negation)

Enforcement of a safe state following detection of a hazardous fault
[EN 50129:2003, 3.1.33, modified]

3.2 Abbreviations

Abbreviation	Description
CCF	**Common Cause Failure** failure, that is the result of one or more events, causing concurrent failures of two or more seperate channels in a multiple channel system, leading to system failure
MD	**Machinery Directive** Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery
PDS/SR	**Power Drive Systems (Safety Related)** adjustable speed electrical power drive system providing safety sub-functions
SF	**Safety Function** function of a machine whose failure can result in an immediate increase of the risk(s)
SRP/CS	**Safety-Related Part of a Control System** part of a control system that responds to safety-related input signals and generates safety-related output signals
STO	**Safe Torque Off** preventing force-producing power from being provided to the motor

Source: ZVEI

4 Fault tolerance in systems

4.1 Safety-related controls

4.1.1 General

Safety-related control systems for factory automation are currently being designed in such a way that if faults are detected in safety-related components, the safe state is established. This is achieved in almost all situations by switching off the energy. For a single machine, this usually means a machine stop. In complex manufacturing systems, not only a single machine can be stopped, but the entire manufacturing process. Some programmable safety-related systems have functions which, depending on the type of fault, do not switch the entire system to the safe, i.e. energy-free, state, but only individual modules are switched off or rendered inoperable (group switch-off). The selection of these modules depends on the application and must be determined individually during project planning. However, certain machines or machine functions are still switched off when a fault is detected in control architectures that require fault detection.

So far, this has not been problematic, since the degree of automation of machines/plants has increased, but the networking of different production plants has only been successive. However, the dynamics of networking via the Internet have increased in recent years and will form the basis for an "Industry 4.0" in the future. In addition, individual machines and complete production lines are interconnected not only within one production facility, but also between production sites located far apart. The growing number of these connections, the complexity of widely distributed networks and the integration of different technologies increase flexibility. At the same time, however, the shutdown of a complex manufacturing system is not tolerable due to any error in a safety function at a completely different production location. This means that new procedures and methods are needed to ensure safe operation even though a failure in a safety function has been detected. Since this cannot be accepted for every fault, a limitation to certain tolerable faults is necessary. These so-called "fault-tolerant systems" must be clearly specified. This raises the following questions:

- Can dangerous errors be tolerated at all?
- How and/or how long a machine/plant can be operated although a fault has been detected?
- Can a machine/plant in which a fault has been detected be operated without restriction or must processes be changed e.g. operating mode, production speed, etc.?

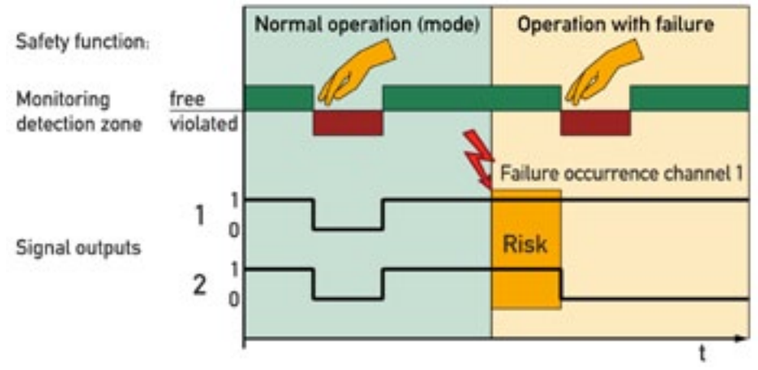
There can be no general answers to these questions, as they will differ depending on the application.

4.1.2 Fault tolerance

Looking at the ISO 13849-1 standard, in its application an undefined "fault tolerance" is already included. In Category 2, fault detection and therefore a fault reaction are only required when the test function is carried out. In a safety function, this means that a fault can exist between two test points. The time between two tests is therefore the time in which a functional unit can continue to operate with a fault.

When Category 3 and Category 4 are applied, fault detection and the resulting fault reaction are required at the latest when the safety function is required (see Figure 1). If no request is made over a longer period of time, a functional unit can possibly be operated with a fault - the fault is tolerated for an indefinite period of time (see Figure 1).

Fig. 1: View of a redundant system according to ISO 13849-1



Source: ZVEI

This kind of tolerance of faults is by no means to be equated with a fault-tolerant system. The difference is as follows: Fault-tolerant systems allow continued operation even though a potentially dangerous failure has already been detected. This is not common for Categories 3 and 4.

In some safety systems and their applications, faults can already be detected via special test routines without a safety function being requested. A fault reaction takes place very quickly, although this is not required under consideration of the above categories. It has to be decided in the respective application whether a fast fault reaction is really required.

In the case of fault-tolerant systems, a fault evaluation is required in addition to fault detection. This makes it possible to decide whether the detected fault can be tolerated or whether it is so serious that immediate shutdown is required. A fault evaluation is not common in currently implemented factory automation safety systems. A possible application and acceptance in practice requires a clear evaluation of faults and their possible effects. The aspect of safety must always be in the foreground, in order not to question the principle of fault tolerance by a careless application. Fault tolerance is not possible without fault evaluation.

As an example from everyday life, we now know car tires with so-called emergency running properties that make it possible to cover the distance to the nearest workshop under certain operating conditions (maximum speed and distance) (see Figure 2).

Fig. 2: Example car tires (Run-flat-technology)

Source: ZVEI

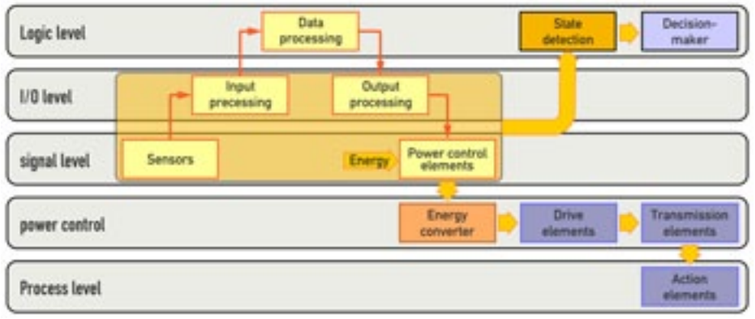
This document describes an adaptation of this principle to applications in functional safety on machines/plants.

4.2 Dangerous failures

4.2.1 De-energization principle

A machine/plant consists of several components that interact and ensure the function of a machine/plant (see Figure 3).

Fig. 3: Schematic representation of a machine control system



Source: ZVEI

Safety-related systems shall at least be designed, constructed, selected, assembled and combined in accordance with the applicable standards and shall use the basic safety principles for the particular application in order to withstand the following:

- the operating stresses to be expected,
- the influence of the material to be machined, and
- other relevant external influences

The application of the principle of de-energization represents a fundamental safety principle that must be particularly observed. The decisive process for stopping or slowing down a mechanism is thereby carried out by removing or reducing the energy. In order to interrupt the energy supply, it may be sufficient to interrupt the energy supply required to generate a torque or force. This can be achieved by disengaging, disconnecting, switching off or by electronic means (e.g. a drive system (PDS/SR)) without electrical disconnection.

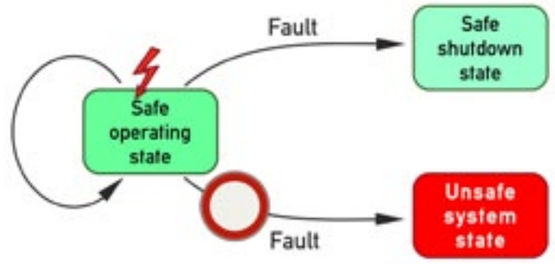
The de-energization principle must not be applied if a hazard would arise due to a loss of energy, for instance release of a tool due to loss of clamping force. If it is to be expected that the restoration or putting into service of the energy supply after an interruption will lead to unexpected movements, the resulting risks must be taken into account accordingly. If a safe shutdown condition is reached due to a dangerous failure, automatic restart of the mechanism must be prevented until the fault has been rectified.

4.2.2 Safety-related failure reaction

The safety-related failure reaction brings about a safe state when a fault is detected. This is achieved by the detection of all dangerous malfunctions and a subsequent safety-related failure reaction (see Figure 4). The following statements apply:

- No fail-to-safe operation without transition to another safe state
- No fail-to-safe operation without the existence of a safe switch-off state

Fig. 4: System with safe monitoring function



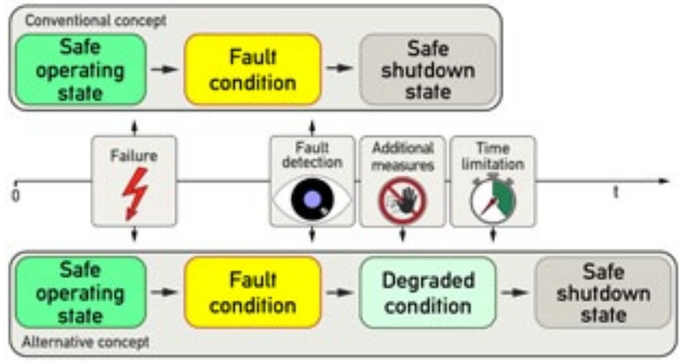
Source: ZVEI

The most elementary safety-related failure reaction is the uncontrolled stopping of the dangerous movement. This is usually achieved by interrupting the power supply. The advantage of uncontrolled shutdown lies in the fact that in most cases safe shutdown can be achieved automatically by adhering to the quiescent current principle even in the event of a power failure. This failure reaction is also referred to as safe torque off (STO).

4.2.3 Operation in degraded condition

Operation in a degraded condition complements the principle of energy separation (see Figure 5). It designates an additional, time-limited functionality within a safety function.

Fig. 5: Comparison of concepts



Source: ZVEI

The aim is to allow the machine functions with sufficient safety within defined limits in the event of defined faults (e.g. condition of a channel outside the permissible tolerance), so that, for example, a cycle is ended and safe operation is maintained or a safe state is reached at the same time.

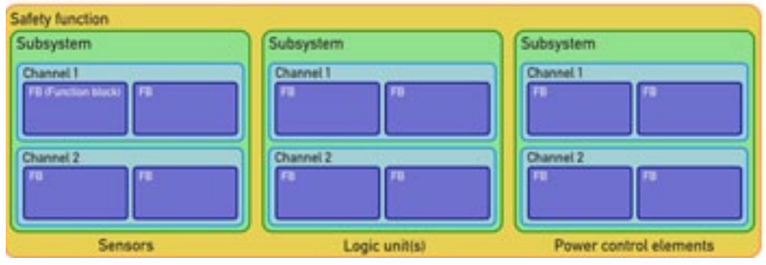
5 Risk reduction through safety functions

5.1 State transitions

5.1.1 Random hardware failures

Failures in functional units are either random (in hardware) or systematic (in hardware or software). A random failure can result from aging of materials that leads to deterioration in the properties of a component. There are several such mechanisms that occur with varying frequency in the different components. As a result, component failures occur after different operating times due to manufacturing tolerances and depending on the respective operating load. Failures of functional units containing many components occur in predictable probabilities, but at uncertain (i.e. random) times. In some cases, failure may also be caused by external events such as lightning or electrostatic discharge. After a failure, the unit has a fault (see Figure 6).

Fig. 6: Failure as opposed to fault



Quelle: ZVEI

Dangerous failures reduce the probability that a safety function will be properly performed when required. This may result in a hazardous condition. Whether or not this potential can be detected depends on the diagnostic means of the system.

5.1.2 Degradation of safety functions

The term "degradation" is used in this document to refer to the temporary or permanent reduction of the contribution of a safety function to the successful reduction of risk during the intended operation of a machine. A distinction can be made between direct and indirect degradation:

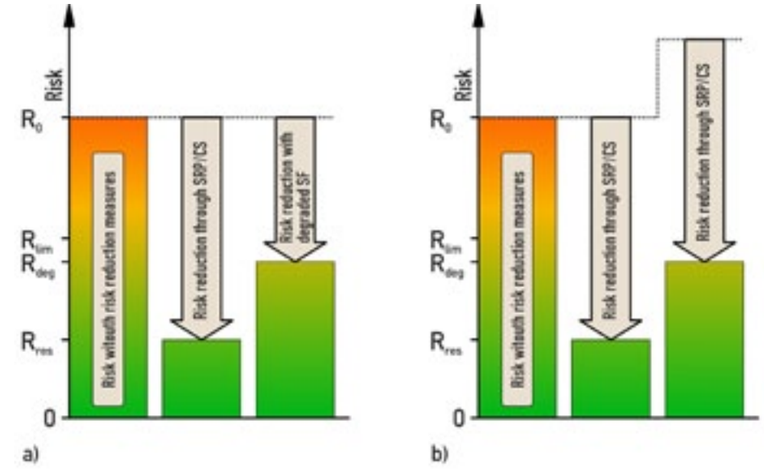
- In the case of direct degradation, the reserve of performance of the safety function is used (see Figure 7 a).
- In indirect degradation, the contribution of the safety function to risk reduction is indirectly reduced by an increase in risk (change in system boundaries) (see Figure 7 b). The original performance of the safety function remains unchanged.

In each of the degradations shown in Figure 7, there is an increase in the residual risk, i.e. there is a gap between the currently achieved residual risk R_{deg} and the original residual risk R_{Rest}. However, the characteristic feature of the degraded condition is that the limit risk R_{Grenz} is not exceeded and the original efficiency of the safety function remains unchanged.

FIG. 7: Darstellung der Degradierungsarten

a) direkt

b) indirekt degradation



Source: ZVEI

Legend

R_0	Risk of a special hazardous situation before protective measures are applied
R_{Grenz}	Required risk reduction through protective measures
R_{deg}	Risk reduction through degraded safety function
R_{Rest}	actual risk reduction achieved by SRP/CS in normal condition (not degraded)

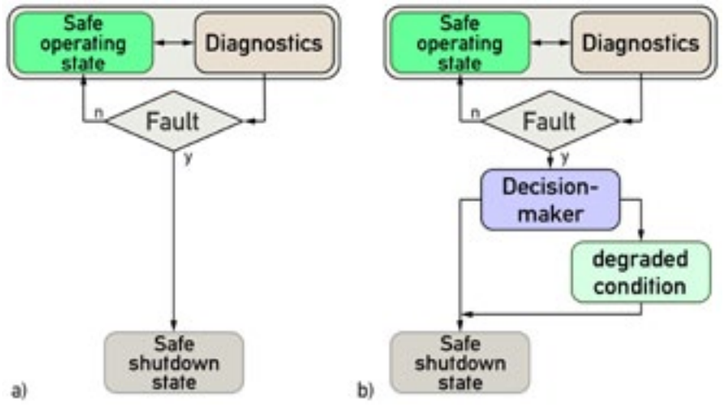
A typical example of indirect degradation may be a driverless transport vehicle in a material flow system. If persons are detected in the guided path of the vehicle, a non-contact protective device triggers a stop. The necessary braking system must be designed so that the vehicle can stop before contact is made between the fixed parts of the vehicle or load and a standing person. Adverse conditions for the influencing factors speed, rated load, friction, ground and gradient must be taken into account by the manufacturer (limits of the machine). If an (unexpected) pipe rupture occurs in an area where the vehicle is travelling, the braking distance can be increased by leaking water to such an extent that the operating range of the device for detecting persons is no longer sufficient.

Indirect degradation is not further considered in this document.

5.1.3 Tolerable faults

The conventional reaction in machine automation to the detection of a fault in a dual-channel structure is the immediate stop. It is the simplest reaction. At the same time, it is undesirable from the point of view of availability and thus susceptible to manipulation (see Figure 8a).

Fig. 8: Diagnostics and decision-maker



Source: ZVEI

New procedures and methods are required if safe continued operation of the machine/plant is to be ensured even though a fault has been detected in a component of the safety function. Since continued operation cannot be accepted for every error, an error estimation and error evaluation must be carried out. A distinction must be made between:

- Non-tolerable faults which, for example, promptly lead to a loss of the functional reserve of the (sub-) system or are caused by systematic failures or common cause failures.
- Tolerable faults that do not immediately endanger the safe function of the (sub-) system.

Depending on the evaluation of the fault, a decision-maker automatically transfers the system to the safe shutdown state or to operation in the degraded condition (see Figure 8b).

5.1.4 Decision-maker

The task of this decision is to branch to the degraded condition or to the safe shutdown state depending on the current system state. For this task, more detailed diagnostics (fault and status detection) is required than usual for the realization of the requirements for individual categories or architectures. The safety level of the decision-maker must be at least equivalent to that of the safety function.

Diagnostics and decision making must be especially conceived on the understanding that faulty states can be caused not only by accidental component failures but also by systematic failures or failures of common cause. Such failures always lead to intolerable faults. In the concrete implementation in a technical system, the realization of a decision-maker therefore requires a high degree of certainty in the decision making process as to whether only a random component failure is definitely the cause of a fault.

5.1.5 Safety function in degraded condition

The opportunities offered by operation in a degraded condition have not yet been consciously exploited. The advantages are obvious:

- The machine availability increases, since the system is able to react more precisely to faults if designed accordingly,
- The continued operation of the machine with degraded safety function avoids an abrupt interruption of production, which reduces incentives for manipulation,
- The implementation of different scenarios supports the design of flexible systems (Industry 4.0).

In order to avoid any misunderstandings, it should again be explicitly stated here that the functionality of the operation in the degraded condition must be implemented by the machine manufacturer/integrator. It is not a functionality whose design can be left to the operator. Like the diagnostics, the described functionality is safety-relevant, but not an independent safety function. For operation in the degraded condition, the safety functions provided for this purpose must be extended to include:

- Detailed diagnostics (fault and status detection),
- Decision logic (fault estimation and evaluation),
- Limits of operation in degraded condition.

The two standards ISO 13849-1 and IEC 62061 do not place any explicit requirements on a diagnostic test interval. In IEC 62061, the diagnostic test interval (referred to there as T2) has little effect on the probability of a dangerous failure per hour (PFHD) to be calculated. A dual-channel system is therefore not immediately unsafe in the event of a fault in a channel due to a random component failure. The remaining channel continues to perform the safety function.

5.1.6 Signalling the degraded condition

If operation is initiated in the degraded condition, there is already a (tolerable) fault in a functional unit of the safety-related control system. The operating personnel must be informed of this status. The signalling can take place via visible and/or audible displays on the machine or at any operating station, up to control rooms with a variety of devices for monitoring processes.

The International Standard IEC 60073:2002 establishes general rules for assigning individual meanings to certain visible, audible and tactile indications in order to:

- Increase the safety of persons, properties and/or the environment by safely monitoring and operating the facilities or processes;
- Achieve precise observation, operation and maintenance of the system;
- Achieve fast recognition of operating states and positions of operating elements.

Color and the temporal change of characteristics (flashing) are the most effective means of attracting attention. The color to be indicated by an awareness system must be selected taking into account the information to be communicated. The degraded condition is an abnormal process state. The color YELLOW is reserved for functions that indicate a warning or an abnormal state (see Figure 9). As a supplementary code to the color, the signaling can take the form of an equilateral triangle to avoid errors that may be caused by persons with color vision impairment.

Fig. 9: General meaning of the colors of indicator lights

Color	Meaning	Explanation
Red	Emergency	Hazardous condition Immediate action to deal with hazardous
Yellow	Abnormal	Abnormal condition Impending critical condition
Green	Normal	Normal condition
Blue	Mandatory	Mandatory action
White	Neutral	May be used whenever doubt exists about application of Red, Yellow, Green, Blue

Source: ZVEI (according to table 4, IEC 60204-1:2016)

Continuous light is used for pure information transfer. A flashing indicator can be used to attract additional attention. This can be used to emphasize in particular that a change of state is imminent.

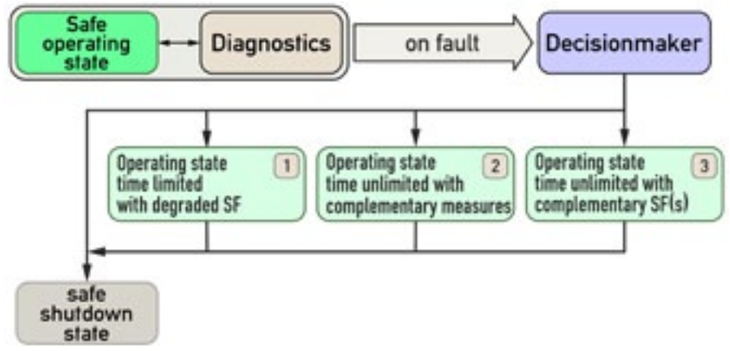
5.2 Variants of operation in degraded condition

5.2.1 General

In principle, up to three variants are available for operating a safety function in the degraded condition (see Figure 10):

1. Time-limited operation with degraded safety function (see Chapter 5.2.2)
2. Operation for an unlimited period of time with complementary measures (see Chapter 5.2.3)
3. Operation for an unlimited period of time with additional safety functions (see Chapter 5.2.4)

Fig. 10: State transitions

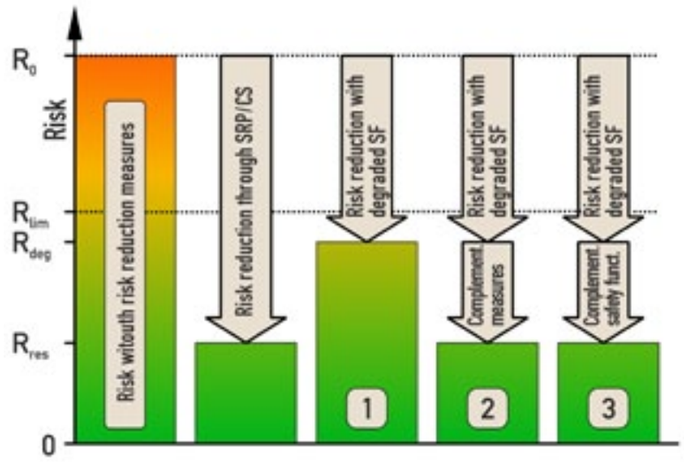


Source: ZVEI

In Figure 10, the transition from the normal state via the decision-maker to the other operating states reflects the view described above. When a first fault occurs, the decision-maker can branch to one of the four states shown. Not all possible operating states need to be provided for in a system. Optionally, a sequence of several degraded operating states can also be run through.

An overview of the contributions to risk reduction achieved by the respective states is shown in Figure 11.

Fig. 11: Variants of risk reduction



Source: ZVEI

5.2.2 Time-limited operation with degraded safety function

The basic idea behind this operating state is the fact that the safety function's contribution to risk reduction was initially unchanged. The probability of failure of the safety function remains almost constant at a low level. The probability of failure of the safety function only increases significantly with further operating time and its ability to reduce risk decreases accordingly (see Figure 12). As a result, with this procedure a machine can only be operated for a limited time (t_{grenz}) until the limit risk R_{grenz} is reached.

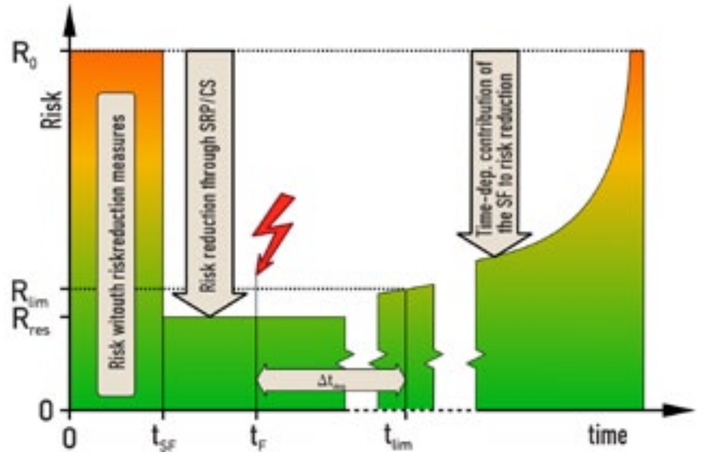
For a dual-channel system in which each channel performs the safety function, the following consideration can be used in the event of failure of a channel: When estimating the probability of failure for such an architecture, it is assumed that a first fault in a channel is detected by a diagnostic test and the fault is displayed, but does not lead to the system being switched off by the decision-maker. Any further fault will increase the risk. By definition, this risk must not exceed the value of R_{grenz}.

Prerequisites for temporary operation with degraded safety function are:

a. The architecture of the system
   Redundant systems (homogeneous or diverse redundancy).
b. The sufficiently low probability of failure
   In the system, a reserve with regard to the probability of failure is provided for constructively. The realized probability of failure for the residual risk to be achieved (R_{Rest}) is lower than the admissible probability of failure for the border risk (R_{grenz}). Currently available systems allow a period Δt_{deg} of up to one week in which the risk reduction is almost completely maintained due to the only slightly increasing probability of failure. Deviating periods (shorter than one week) can be defined by the machine builder based on the risk assessment. If the maximum permissible time Δt_{deg} is reached or if a second fault occurs, the decision-maker of the system immediately initiates the status defined as safe. If the system is repaired within the period Δt_{deg}, the system can continue to be operated. Multiple use of Δt_{deg} without interim repair is not permitted, as the marginal risk may already have been reached. If no safe shutdown state or a repair of the system with degraded safety function has been initiated by the time the maximum permissible time Δt_{deg} has elapsed, the decision-maker of the system must immediately initiate the state defined as safe.
c. Resistance to common cause failure (CCF)
   The general CCF requirements according to ISO 13849-1 must be fulfilled. Proof (verification and validation) that the requirements for CCF ≥ 65 points have been implemented must be carried out with the greatest care.

If all these prerequisites are fulfilled, time-limited operation with degraded safety function is possible.

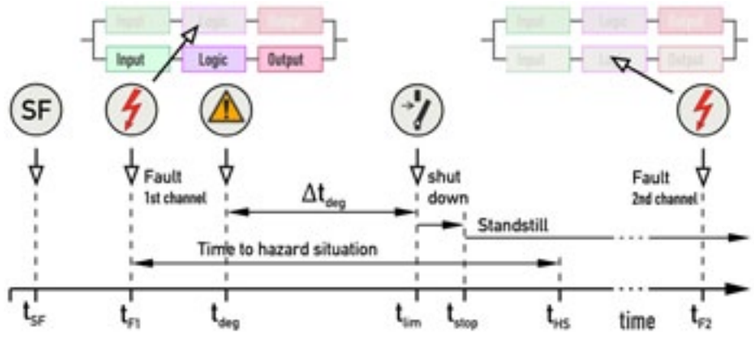
Fig. 12: Qualitative development of the risk



Source: ZVEI

The following diagram (see Figure 13) applies to tolerable first faults. Operation in degraded condition is not permitted for intolerable faults. All factors relevant to the application must be taken into account when determining the time span Δt_{deg}. These are, for example, the required Performance Level or Safety Integrity Level of the considered safety function. Model calculations for dual-channel systems show that a period of one or more days does not result in a significant increase in the probability of failure. The time span must not be extended to values that prove to be uncritical for random hardware failures in purely mathematical terms due to the possibility of common cause-related subsequent failures.

Fig. 13: Time limit for degraded condition



Source: ZVEI

Legende

t_{SF}	Requesting the safety function
t_{F1}	Occurrence of fault in first channel
t_{deg}	Initiation of operation in degraded condition
t_{Grenz}	Achieving the border risk R_{Grenz}
t_{Stop}	Achieving the safe state
t_{HS}	Occurrence of the hazard situation
t_{F2}	Occurrence of fault in second channel

5.2.3 Operation for an unlimited period of time with complementary measures

Since there will be a gap in the required risk reduction after degradation of the safety function (with the initial risk remaining constant), there is a need to close this gap.

The following shall apply to the additional measures to be taken:
- They must be designed by the machine manufacturer/system integrator;
- The status must be signalled (e.g. by warning lamps or acoustic signals).

Appropriate measures to be taken by the operator may include:
- Additional separating guards (e.g. warning tape)
- Manual function limitation
- Use of appropriately trained personnel
- Working and break times adapted to the workload
- Personal protective equipment

The transition reported by the machine to the degraded state must be acknowledged promptly by the operator. If this acknowledgement does not take place within a specified period of time, the decision-maker must put the machine in another safe state. This could be, for example, a standstill.

5.2.4 Operation for an unlimited period of time with additional safety functions

The basic idea of this operating condition is to close the gap in risk reduction caused by degradation by activating other safety functions. If it is possible to reduce the initial risk through this measure in such a way (see Figure 11, Number 3) that the contribution of the degraded safety function to risk reduction is sufficient, this operating condition is not subject to any time limitation, as in the case of time-limited operation (see Chapter 5.2.2)

This operating state offers great potential for maintaining the availability of the machine, as it is only limited in time by further failures. If it is possible to equip the system with several fallback levels, a very flexible reaction to failures is possible.

An example of an internal measure is to install a fallback level in such a way that a failure of one channel of a dual-channel system results in a structural change to a Category 2 according to ISO 13849-1. If this solution is implemented, a time limit can be dispensed with if the required performance level (PLr) is also achieved. As a further example, if a protective device fails, the system could only execute the dangerous movements in slow (creep) mode.

6 Conclusion and outlook

The explanations show that with redundant safety architectures - depending on the level of risk - a dangerous failure in a channel can be tolerated for a certain period of time in order to shut down critical processes in a controlled manner. Especially for machines/plants where a high level of reliability is required, this perspective means an increase in availability compared to the previously customary implementation and ultimately leads to a higher acceptance by the user.

The assessment is in line with the protection objectives of the Machinery Directive and does not conflict with the international standards ISO 13849 and IEC 62061.

Further questions regarding the application implementation are set out in a supplementary document “Fault tolerance in machine safety Part 2 – Requirements”.

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Lyoner Straße 9
60528 Frankfurt am Main
Telephone: +49 69 6302-0
Fax: +49 69 6302-317
E-mail: zvei@zvei.org
www.zvei.org