ZVEI:
Die Elektroindustrie

Whitepaper

# Fault tolerance in machine safety

## Part II - Requirements, Revision 1.0


Automation Division


## Imprint

**Fault tolerance in machine safety**

Publisher:
ZVEI e. V.
Electro and Digital Industry Association

Automation Division
Lyoner Straße 9
60528 Frankfurt am Main, Germany

Contact:
Dr. Markus Winzenick
Phone: +49 69 6302-426
E-Mail: markus.winzenick@zvei.org

www.zvei.org

January 2022

# Abstract


## Fault tolerance in machine safety

In engineering, fault tolerance means the property 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 continued operation of a machine or system in the event of certain fault scenarios without neglecting the requirements for personal protection.

Part I of the white paper describes the theoretical basis for operation in a degraded condition. Part II (this document) describes the necessary prerequisites for operation in a degraded condition. The prerequisite for the application of Part II is the consideration of Part I.

Requirements are defined for the subsystems that are suitable for degraded operation. A procedure is described for how the integrator of a safety function can design degraded operation and implement it in the machine using subsystems suitable for this purpose. In addition, it provides the manufacturer of safety components with guidance on this.

Part III of the white paper describes further requirements for an overall system suitable for operation in a degraded condition, such as the control of systematic failures while taking into account common cause failures, etc.



**List of Authors:**

| | |
|---|---|
| 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 |
| Jens Mehnert | K.A. Schmersal |
| Michael Niehaus | Lenze |
| 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 |

# Table of Contents

# 1 Introduction

## 1.1 Motivation

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

Up to now, monitoring of protective devices and controls for machines and systems in the industrial environment has been based on the dogma of the fastest possible shutdown 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 safety-related reaction to a failure.

Increasing productivity requirements, especially under the aspects of Industry 4.0, demand expanded safety engineering concepts for the future.

The aim of this document is to show alternatives to immediate shutdown in the event of fault detection. It defines the concepts under which machines can continue to operate when faults are detected in safety functions without exposing people to unacceptable risks.

## 1.2 Area of application

The scope of the document is limited to the operation of machines and systems under fault condi-tions in their safety functions. It is aimed at machine builders and system integrators who plan the safety functions during the development of the machine and implement them using subsystems. The recommendations from this document are equally applicable when implementing the safety functions in accordance with the ISO 13849-1 and IEC 62061 standards.

The necessity of implementing safety functions is always one of the results of the risk reduction measures for a machine or system resulting from the risk assessment. The basis for the risk assessment is ISO 12100, which describes all the requirements for the iterative process. Procedures for estimating the safety level required for a safety function are described in the ISO 13849-1 and IEC 62061 standards. In this way, with the results of the risk assessment - before risk-reduction measures are implemented - it can be demonstrated in detail in a further step that the residual risk in fault-tolerant operation does not exceed the previously defined limit risk at any time and in any operating state of the machine or system.

The focus of this document is exclusively on systems commonly used in mechanical and plant engineering for higher safety requirements, in which the execution of the safety function is still possible even in the event of a fault due to its originally two-channel structure.

Not considered by the application described here are in particular:

- Single-channel safety systems in which safe operation in the event of a fault is excluded,
- Systems with more than two channels (known e.g. from the process industry and avionics),
- Systems with voters, in which a faulty channel can be detected and switched off, for example, by a majority vote.
- Hot standby systems in which, in the event of a failure, a running backup system takes over the tasks of the failed system.
- Cold standby systems in which, in the event of a failure, a backup system is booted up sufficiently quickly to take over the tasks of the failed system.

# 2 Terms and abbreviations

## 2.1 Terms

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

### 2.1.1 Failure

Termination of the ability of a functional unit to perform a required function.

Note 1 to term: After a failure, the unit has a fault.

Note 2 to concept: The “failure“ is an event, in contrast to the “fault“, this is a state.

[ISO 13849-1:2015, 3.1.4, modified.]

### 2.1.2 Dangerous failure

Failure that has the potential to place a functional unit in a hazardous condition or malfunction.

[ISO 13849-1:2015, 3.1.5, modified.]

### 2.1.3 Fault

Condition of a functional unit characterized by the inability to perform a required function, except for the inability during preventive maintenance or other planned actions or due to the absence of external means.

[ISO 13849-1:2015, 3.1.3, modified].

### 2.1.4 Tolerable fault

A tolerable fault in a two-channel system is a fault that can be unambiguously located in one channel of the system so that an effect on the second channel can be excluded.

Note 1: Clearly locating the fault in a channel requires diagnostic measures in the system that may go beyond diagnostics for general detection of a fault in the system.

Note 2: If the detection of a fault does not lead to the immediate deactivation of the safety function, special care must be taken during development to avoid and control possible subsequent faults in order to prevent the fault from spreading to the second channel at a later stage (e.g. as a result of faulty communication or heating).

### 2.1.5 Fault tolerance

Ability of a functional unit to continue to perform a required function in the presence of faults or deviations.

[IEC 61508-4:2010, 3.6.3].

### 2.1.6 Functional unit

Unit of hardware or software, or both, capable of performing a specified task.

[ISO/IEC 2382-1, 01-01-40].

Note: Functional units can be not only logic units, but also sensors and power drive systems.

### 2.1.7 Interface-type

The interface-type describes a standardized interface between transmitters of signals (sources) and receivers of signals (sinks) with specifications on the generation and evaluation of test pulses.

- Type A for floating contacts as information source;
- Type B for discrete semiconductor outputs with external clocking;
- Type C for discrete semiconductor outputs with integrated diagnostics;
- Type D for plus-minus switching semiconductor outputs with integrated diagnostics.

[Source: ZVEI Position Paper CB24I]

### 2.1.8 Link-Typ

The link-type describes a standardized interface for the transmission of safety-related information as well as diagnostic information between logic units and field devices.

### 2.1.9 Logic-type

The logic-type describes a standardized structure of the logic of safety-related functional units for linking inputs and outputs:

- Type E An SSF realized from discrete components;
- Type 1 a fixed SSF in the device;
- Type 2 one of n SSF selectable;
- Type 3 a parameterizable SSF;
- Type 4 multiple SSF with communication.

[Source: ZVEI Whitepaper "Safety Aspects for Software in Industrial Applications"]

### 2.1.10 Safe condition

State of a functional unit in which safety is achieved
[IEC 61508-4:2010, modified].

### 2.1.11 Safety

Freedom from unacceptable risk of harm arising from and external to the safety-related systems under consideration.
[IEV 351-57-05, modified.]

### 2.1.12 Safety sub-function (SSF)

Part of a safety function whose failure can lead to a failure of the safety function.
[ISO/CD 13849-1:2019, 3.1.52]

### 2.1.13 Safety-related reaction to a failure (Negation)

Enforcement of a safe state following detection of a hazardous fault.
[IEV 821-12-38]

# 3 Abbreviations

| Abbreviation | Description |
|---|---|
| CCF | **Common Cause Failure**<br>Failure of different items resulting from a single event |
| EDM | **External Device Monitoring**<br>Monitoring the state of external control devices |
| EUC | **Euqipment Under Control**<br>Equipment used for manufacturing, transportation or other activities |
| FSCP | **Functional Safety Communication Profile**<br>Technology specification for the implementation of a safety communication layer |
| FS-DI | **Functional Safety Digital Input**<br>Safety-related device which converts an essentially two-state signal to a single-bit binary number |
| FS-DO | **Functional Safety Digital Output**<br>Safety-related device which converts a single-bit binary number to a two-state signal |
| IGBT | **Insulated-gate bipolar transistor**<br>Bipolar transistor with insulated gate electrode |
| MooN (D) | **M out of N**<br>Architecture with M out of N channels (with diagnostics) |
| MSF | **Mechanic Subfunction**<br>Assembly consisting of functionally interconnected individual elements that perform a sub-function of the mechanical transmission system |
| OSSD | **Output Signal Switching Device**<br>Component of the machine's safety-related control system that interrupts the circuit to the machine primary control element |
| PDS (SR) | **Power Drive Systems (Safety Related)**<br>Adjustable speed electric power drive systems providing safety sub-functions |
| SDCI | **Single Drop Communication Interface**<br>Point-to-point communication interface for small sensors and actuators |
| SF | **Safety Function**<br>Function of a machine, where a failure of the function can lead to an immediate increase in risk |
| SRASW | **Safety-Related Application Software**<br>Software that is used to implement control functions in a safety-related system |
| SRP/CS | **Safety-Related Part of a Control System**<br>System safety-related part of a control system |
| SSF | **Safety Sub-function**<br>Part of a safety function |
| STO | **Safe Torque Off**<br>Function that prevents force-producing power from being provided to the motor |

Quelle: ZVEI

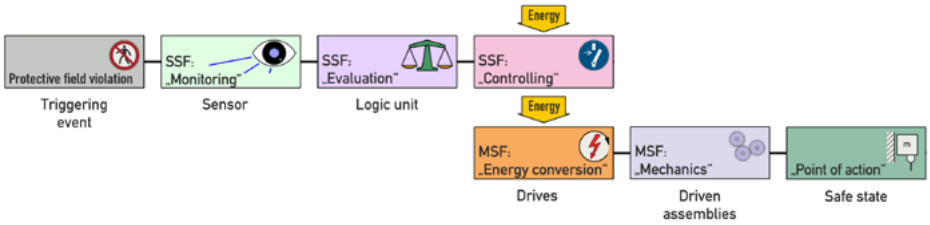
# 4 Operation in degraded condition

## 4.1 Diagnostics and decision maker

### 4.1.1 Safety sub-functions

Part of the risk reduction process[1] is to define the required safety functions for the machine, for example "Safe stop of a hazardous movement". A safety function is generally implemented by several subsystems (see Figure 4.1). These subsystems then perform corresponding safety sub-functions [e.g. a power drive system the SSF "Safe stop 1" (SS1)]. Several safety functions can be shared by an individual subsystem, often at least by the logic unit. Conversely, several safety sub-functions can also be performed by a single subsystem (e.g. sensor: SSF "monitoring & SSF "evaluation"). The function of a mechanical transmission system can also be divided into mechanical sub-functions.

**Figure 4.1: Subsystems and their functionalities**




### 4.1.2 Fault tolerance in machine safety

The usual reaction in machine automation up to now when an fault is detected in a two-channel structure is the immediate stop. This is the simplest reaction. At the same time, it is undesirable from the point of view of availability and therefore susceptible to manipulation.

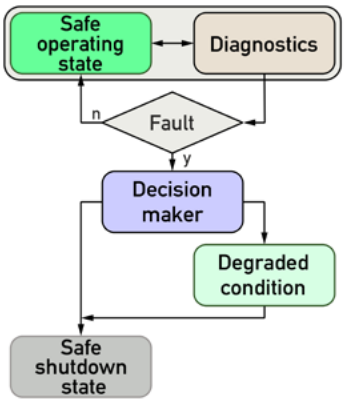
If safe continued operation of the machine/plant is to be ensured even though a fault has been detected in a component of the safety function, new procedures and methods are required. Since continued operation cannot be accepted for every fault, a fault assessment and fault evaluation must be carried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

- intolerable failures which lead, for example, to a loss of the functional reserve of the sub-system in a timely manner or which result from systematic failures or failures due to common cause;
- tolerable faults, these do not directly endanger the safe functioning of the subsystem.

Depending on the evaluation of a fault, a decision maker (see Figure 4.2) automatically transfers the system to the safe shutdown state or to operation in the degraded condition.

Note: Functional units can be not only logic units, but also sensors and power drive systems.

**Figure 4.2: Diagnostics and decision maker**




[1] In this document only mechanical hazards due to moving parts are considered.

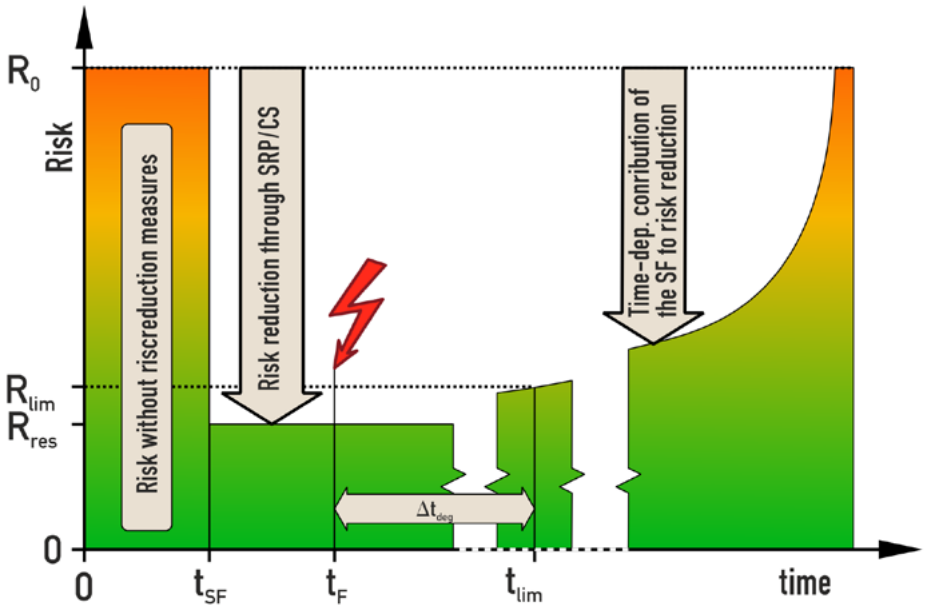
The task of this decision is to branch to the degraded condition or to the safe shutdown state depending on the current system state. This task requires a more detailed diagnostics (fault and state detection) than is usually required to realize the requirements for individual categories or architectures. The decision maker must be at least equivalent in level to that of the safety sub-function.

Diagnostics and decision-making must be designed especially against the background that faulty states can be caused not only by random component failures but also by systematic failures or failures due to a 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.

### 4.1.3 Time-limited operation with degraded safety sub-function

The basic idea of this operating state is the fact of the initially unchanged contribution of the safety sub-function to risk reduction. The failure probability of the safety sub-function remains almost constant at a low level (see Figure 4.3). Only with further operating time does the failure probability of the safety sub-function increase significantly and its ability to reduce risk decreases accordingly. Consequently, with this approach a machine can only be operated for a limited time ($t_{lim}$) until the limit risk $R_{lim}$ is reached.

## Figure 4.3: Qualitative progression of risk




Prerequisites for time-limited operation with degraded safety sub-function are:

a. The architecture of the system

Redundant subsystems (homogeneous or diverse redundancy).

b. A sufficiently low probability of failure

In the subsystem, a reserve with respect to probability of failure is provided by design. The realized failure probability for the residual risk to be achieved ($R_{res}$) is lower than the permissible failure probability for the marginal risk ($R_{lim}$). Currently available subsystems allow a period $\Delta t_{deg}$ of up to one week, in which the risk reduction is almost completely preserved by the only slightly increasing probability of a fault. Deviating periods (shorter than one week) can be defined by the machine builder based on the risk assessment. When the maximum permissible time $\Delta t_{deg}$ or the second failure occurrence is reached, the state defined as safe is immediately initiated by the decision maker of the subsystem. If the subsystem is repaired within the time period $\Delta t_{deg}$, the subsystem can continue to operate. Multiple use of $\Delta t_{deg}$ without intermediate repair is not permissible, since the risk $R_{lim}$ may already have been reached. If no safe shutdown state or no repair of the subsystem with degraded safety subfunction has been initiated by the time the maximum permissible time $\Delta t_{deg}$ occurs, the decision maker of the subsystem must immediately bring about the state defined as safe.

c. Resistance against common cause failures (CCF)

The general CCF requirements according to ISO 13849-1 shall be met. The proof (verific-tion and validation) that the requirements for CCF ≥ 65 points have been implemented must be carried out with the utmost care.

If all these conditions are met, temporary operation with a degraded safety sub-function is possible.

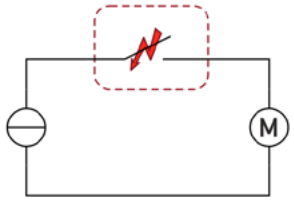
## 4.2 Qualified diagnostics

### 4.2.1 Failure behaviour of systems

A simple circuit will serve as an example to illustrate the failure behaviour of systems (see Figure 4.4). A single fault in the switch leads to the following behaviour:

- failure to open the switch prevents the load from being switched off
- failure to close the switch prevents the load from being switched on.

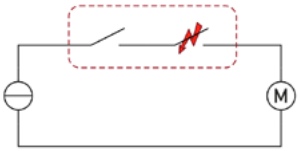
**Figure 4.4: Single-channel circuit (1oo1)**




If the load is to be switched off in the event of a fault, a two-channel system can be used (see Figure 4.5). A fault in one of the two switches leads to the following behaviour:

- failure to open a switch does NOT prevent the load from being switched off
- failure to close a switch prevents the load from being switched on.

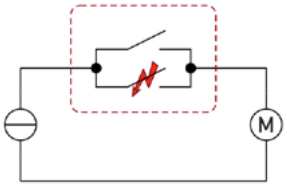
**Figure 4.5: Dual channel shutdown (1oo2)**




If it is necessary to ensure that the load is switched on, a two-channel system can also be used (see Figure 4.6). This system must be designed differently from the previous one. A fault in one of the two switches leads to the following behaviour.

- failure to open a switch prevents the load from being switched off
- failure to close a switch does NOT prevent the load from being switched on.

**Figure 4.6: Dual channel availability (2oo2)**

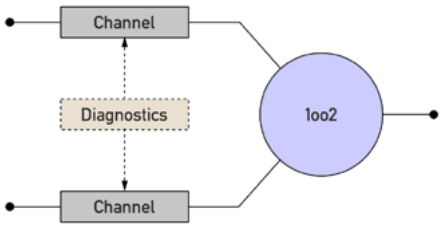



Generally, these systems are referred to as MooN (‚M out of N'). Here, N denotes the number of available channels. M is the number of channels that must be functional for the architecture to perform its (partial) safety function correctly

### 4.2.2 1oo2-architecture

This architecture consists of two parallel channels so that each of the channels can perform the safety sub-function (see Figure 4.7). Therefore, a dangerous failure must exist in both channels before the safety sub-function would fail on demand. It is assumed that any fault detected by diagnostics is only reported and does not change any output states or the output comparison [see Annex B. 3.2.2.2., IEC 61508-6:2010].

## Figure 4.7: Block diagram for 1oo2

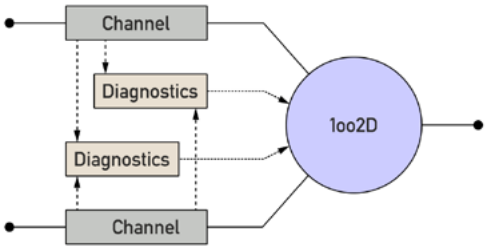



In the machine sector, it is not usual to only output an fault message without changing the output state. Rather, when an fault is detected, the output or outputs are set to the safe state. This is the architecture commonly used so far for the outputs of safety-related devices with a two-channel structure. In the event of a single fault, switch-off of the load is ensured.

### 4.2.3 1oo2D architecture

This architecture consists of two parallel channels. Each of the channels can perform the safety sub-function. If the diagnostics detect a fault in one channel, the output comparison is adjusted so that the overall output state follows the other channel (see Figure 4.8). If the diagnostics detect faults in both channels or a deviation that cannot be assigned to either channel, the output is set to the safe state. To detect a deviation between the two channels, each channel can determine the state of the other by means independent of itself [see Annex B.3.2.2.4., IEC 61508-6:2010].

## Figure 4.8: Block diagram for 1oo2D



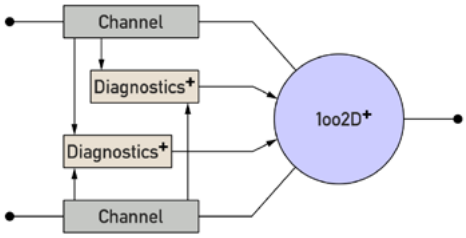

This architecture would allow fault-tolerant continued operation in the event of a single fault in a channel, regardless of the nature of the fault.

### 4.2.4 1oo2D+ architecture

This architecture is equivalent to 1002D, but additionally includes an extended diagnostics. This so-called "Qualified Diagnostics" evaluates:

- What is the fault?
- Where is this fault located? (e.g. which channel)
- Can the safety sub-function continue to be executed?

## Figure 4.9: Block diagram for 1oo2D+



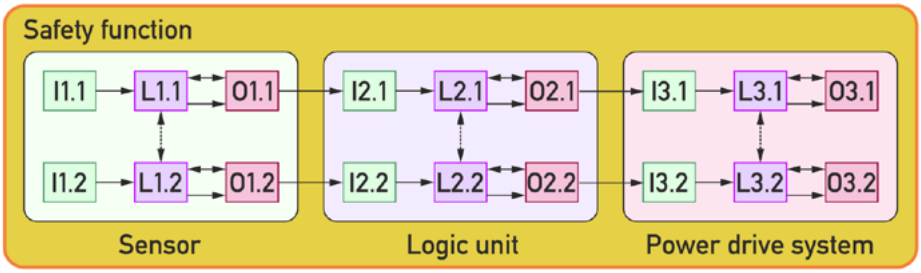

The result of the qualified diagnostics can additionally be made available as a diagnostic status (following Namur NE 131) via status signals:

- Failure:
  Due to a malfunction in the safety device or its periphery, the output signal is invalid.
- Function check:
  Work is being carried out on the safety device, the output signal is therefore temporarily invalid (e.g. frozen).
- Out of specification:
  Deviations from the permissible ambient or process conditions determined by the device through self-monitoring, or faults in the device itself, indicate that the measurement uncertainty for sensors or the setpoint deviation for actuators is probably greater than would be expected under operating conditions.
- Maintenance requirement:
  The output signal is still valid, but the function reserve will soon be exhausted or a function will soon be restricted due to operating conditions (e.g. operation in degraded condition).
- If no status signals are set, it can be assumed that the safety device is functioning as intended.

## 4.3 Safety-related systems

The following sections consider a typical system of sensors, a logic unit, and power drive systems performing safety functions together (see Figure 4.10).

## Figure 4.10: Safety-related block diagram




This document is limited to electrical power drive systems [PDS(SR)]. In principle, the procedure can also be transferred to fluid power drive control systems.

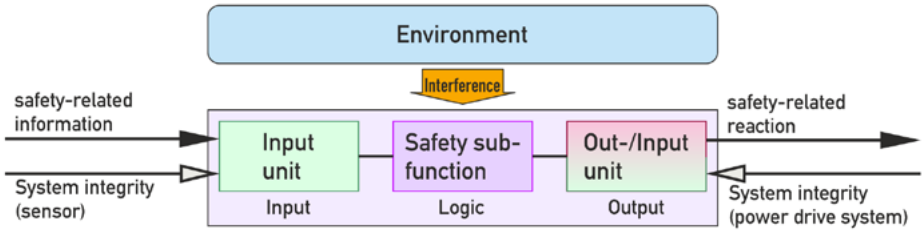
# 5 Safety-related logic units

## 5.1 Structure

A safety-related logic unit (see Figure 5.1) consists at least of:

- an input unit,
  status information (system integrity) and safety-related information from the machine or process is transmitted to the input/output system of the logic unit by binary, digital, incremental or analog signals;
- a processing unit (safety sub-function),
  according to the application program, the processing unit processes signals supplied by the sensors and the internal data memory, and it generates signals that are sent to both the actuators and the internal memory;
- an output unit
  the decisions and results determined by the safety sub-function are transmitted to the machine or process by the use of appropriate binary, digital, incremental or analogue signals.

### Figure 5.1: Safety-related logic unit




Logic units have to perform the following tasks as the "final decision maker":

- Detection and evaluation of sensor or power control faults at inputs and outputs.
- Evaluation of the diagnostic information of the field devices.
- Maintain operation in a degraded condition using diagnostic information.
- Shutdown of operation in degraded condition after a defined maximum time.
- Shutdown of operation in the degraded condition after the conditions for degraded operation have ceased to exist.

A suitable logic unit must have the following characteristics:

- Ability to classify fault patterns with associated behaviors (degraded operation, shutdown).
- Possibility to maintain degraded operation in case of fault detection.
- Possibility to set basic conditions for degraded operation (e.g. maximum degraded operation time).
- It must be a qualified SRP/CS with architecture 1oo2.

## 5.2 Realization forms of logic units

### 5.2.1 General

Characteristic features of the processing unit functionalities described here are logic-types (see ZVEI white paper “Safety aspects for software in industrial applications“).

A processing unit must be able to maintain operation of the safety function in the degraded condition at all times using the diagnostic information. In this document, it is initially assumed that a logic unit does not allow operation in the degraded condition. Any fault detected should immediately cause the safe state. In general, operation in the degraded condition is possible for logic units.

Three basic forms of logic units are presented below. Mixed forms of these are possible.

### 5.2.2 Safety switchgear

A safety switching device consists of:

- a processing unit,
  logic-type 1 or type 2 (an active SSF in the device);
- one input/output unit,
  integrated, not expandable;
- optional:
  manual reset function,
  monitoring of external control devices (EDM).

### 5.2.3 Modular safety controls

A modular safety controller consists of:

- a processing unit,
  logic-type 4 (several active SSF, with communication);
- one or more input/output unit(s),
  locally (communication via backplane bus), and/or
  externally (communication via fieldbus).

### 5.2.4 Embedded systems

An embedded system consists of:

- a processing unit,
  logic-type 4 (several active SSF, with communication);
- no input/output unit, but with
  a communication interface for a direct communication between the processing unit, other logic units and the field devices (fieldbus).

## 5.3 Input/output units of logic units

### 5.3.1 Properties of input/output units

Input/output units generally use a modular functionality, which allows a configuration of the logic unit according to the requirements of the machine or production process and also a later extension (up to the maximum configuration).
An input/output unit may be located locally in close proximity to the processing unit, or it may be installed near the sensors or actuators of the machine or manufacturing process, i.e. remote (external) from the processing unit.

### 5.3.2 Local input/output units

The interface function to sensors and actuators converts the following:

- the input signals and/or data supplied by the machine or manufacturing process into suitable signal levels for further processing;
- the output signals and/or data provided by the signal processing function into appropriate signal levels to control the actuators and/or indicators.

Communication between the processing unit and the local input/output systems generally takes place via a communication interface with a proprietary protocol (backplane bus).

### 5.3.3 External input/output units

The interface function to sensors and actuators is identical to the local systems. Communication to the processing unit is via a communication interface with open protocol (fieldbus).

## 5.4 Requirements for interface function

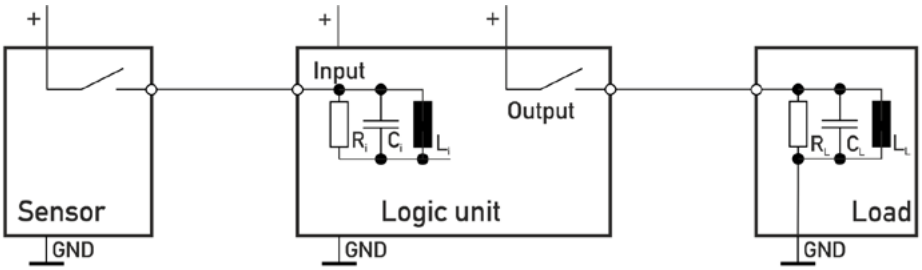
The functions of the inputs and outputs described below apply equally to input/output units of sensors and power drive systems

### 5.4.1 Non-safety-related digital inputs/outputs

Positive logic (current drawing inputs/current supplying outputs, see Figure 5.2):

- Digital inputs comply with the requirements of IEC 61131-2:2017, chapter 6.4.4.2.
- Digital outputs comply with the requirements of IEC 61131-2:2017, chapter 6.4.6.1.

## Abb. 5.2: Positive Logic



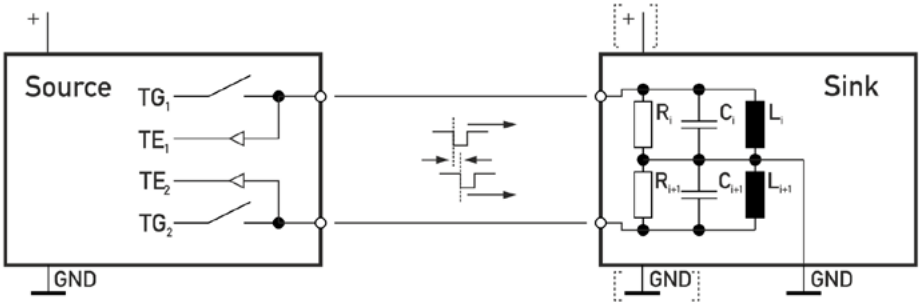

### 5.4.2 Safety-related digital inputs/outputs

Binary 24 V interfaces with dynamic testing in the area of functional safety. Characteristic features of these interfaces are interface-types (see ZVEI position paper CB24I):

- Interface-type C (two-channel output with self-monitoring, see Figure 5.3)

A source switches the supply voltage to the output when switched on. In the off state, the output is disconnected from the supply voltage. When switched on, the source sends test pulses to the output. The correct function of the output is monitored in the source itself.

## Figure 5.3: Interface-type C (two-channel)

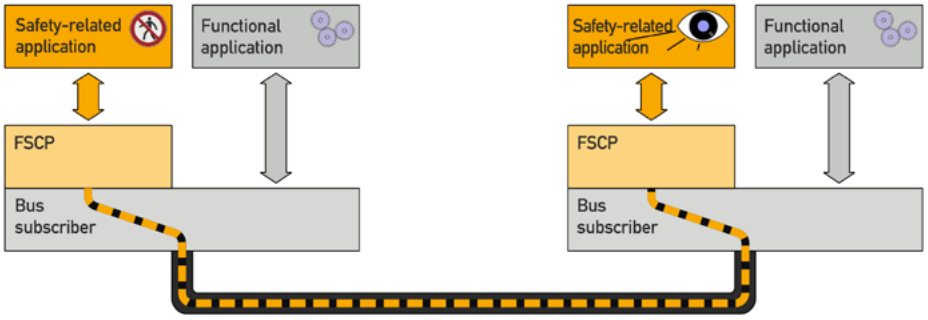



Interface-type C is often used for “OSSD” outputs (Output Signal Switching Device) - e.g. for safety outputs of light curtains.

### 5.4.3 Functionally safe communication interface

Most safety-related communication functions follow the “Black Channel“ principle. An existing fieldbus is used as a transmission channel for a special type of messages consisting of safety data and additional safety measures (see Figure 5.4). The purpose of these measures is to limit the residual fault probability for data transmission during operation to the level required by relevant safety standards or better.

## Figure 5.4: Black Channel




The communication function is generally performed by serial data transmission via a fieldbus (FSCP) or via a point-to-point connection (SDCI). For functionally safe communication via fieldbuses, several profiles have been standardized in the IEC 61784-3-x series.

# 6 Interfaces to sensors

## 6.1 Self-designed subsystems

Qualified subsystems are often used as sensors and power drive systems, for example:

- Safety light curtains
- Safety laser scanners
- Servo drives with integrated safety sub-functions [PDS(SR)]

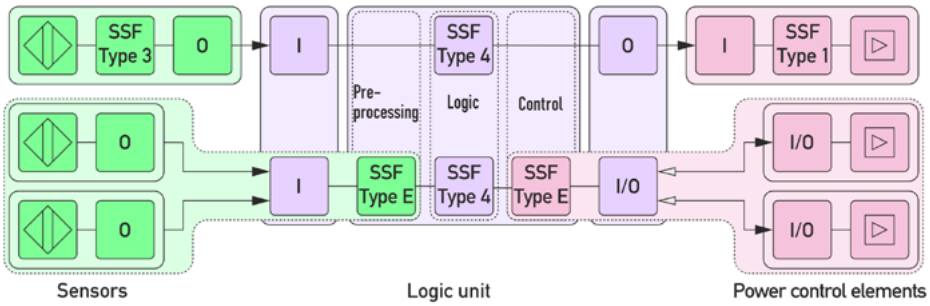
Qualified subsystems perform their diagnostics within the respective subsystem. On the other hand, subsystems can be built as combinations of discrete (non-safety-related) components such as position switches, contactors or valves (see Figure 6.1). In the case of such self-designed subsystems, diagnostics is not performed within the subsystem itself, but must be implemented in the logic unit by the application software (SRASW).

Ideally, the safety-related application software follows the general architecture model for software (see Figure 7, ISO 13849-1:2015):

- Preprocessing
  Evaluating signals from safety-related sensors,
- Logic
  Realization of the specified safety sub-functions (logic type 4),
- Control
  Control and monitor the drive elements according to the results of the logic.

For sensors, a diagnosis can only use information from the comparison or the time sequence of the input signals (preprocessing). On the output side, additional signals such as position monitoring, are required for a diagnosis (control).

### Figure 6.1: Realization of subsystems




Such self-designed subsystems have logic-type “E”. The integrator implements a safety sub-function by interconnecting non-safety-related components. The integrator is responsible for determining the achieved safety level.

Self-designed subsystems consisting of discrete components typically do not have their own logic. Therefore, diagnostics and a decision maker cannot be integrated into such subsystems themselves. These functionalities can only be implemented in the logic of the processing unit. The determination of the maximum permissible time $\Delta t_{deg}$ for an operation in the degraded condition must be performed by the integrator in these cases.

## 6.2 Safety-related sensors

### 6.2.1 Overview

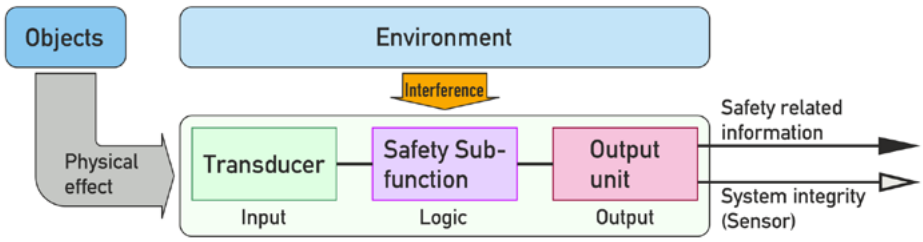
A safety-related sensor (see Figure 6.2) consists at least of:

- a sensor unit (transducer)
  it collects information about the physical properties of the objects and/or environmental influences and provides it as input for the processing unit;
- a processing unit (safety sub-function)
  it processes the information generated by the sensor unit to produce safety-related information;
- an output unit
  it provides safety-related information.

The output unit may provide one or more of the following types of electrical signal (see 5.4):

- safety-related digital outputs
- non-safety related digital outputs
- functionally safe communication interface

**Figure 6.2: Safety-related sensor**




### 6.2.2 Features of the transducer

The sensor unit is not within the scope of this document.

### 6.2.3 Functionalities of the safety sub-function

Characteristic features of the functionalities described here are logic-types (see ZVEI white paper "Safety aspects for software in industrial applications").

**Logic-type 1 (one fixed SSF in the device):**

- Safety-related sensor (e.g. proximity switch, light curtain),
  internal structure fixed, without possibilities to change the SSF.

**Logic-type 2 (one of n SSF selectable):**

- Safety-related sensor with several SSF, one of which must be selected by switches before commissioning or the selection is made by means of coding through wiring (e.g. for the detection capability of the sensor).

**Logic-type 3 (parameterizable SSF):**

Variant 1: Selection of the safety sub-function:

- Safety-related sensor with several SSF, one of which must be selected and transferred to the sensor by means of an (external) "programming device" before commissioning.

Variant 2: Selection of parameters:

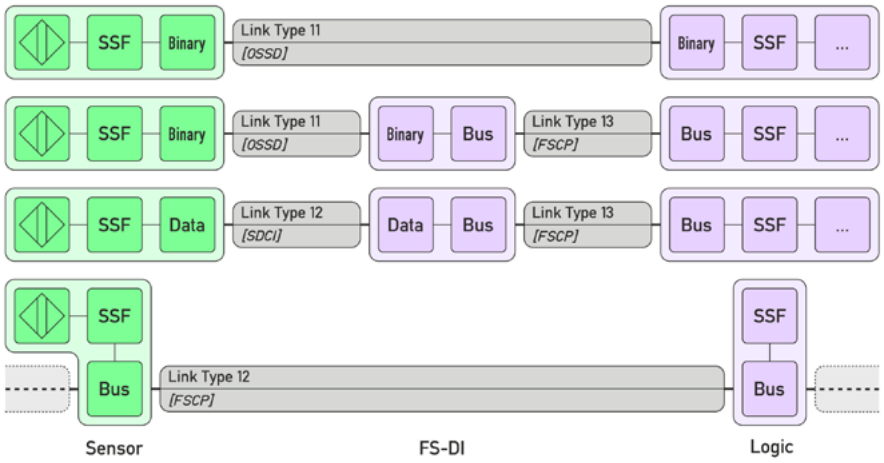
- Safety-related sensor with one or more SSFs (only one SSF active at a time), which must be parameterized by means of an (external) "programming device" before startup and the parameters transferred to the sensor (e.g. protective fields of the safety laser scanner).

## 6.3 Classification of interfaces to sensors

### 6.3.1 Overview

The subsystem "Sensor" contains a qualified diagnostics and a decision maker. Interface requirements do not depend on the logic-type of the sensor. Characteristic features of the required functionalities are the link-types defined below.
The following interfaces are considered (see Figure 6.3):

**Figure 6.3: Link-types for sensor interfaces**




### 6.3.2 Link-type 11

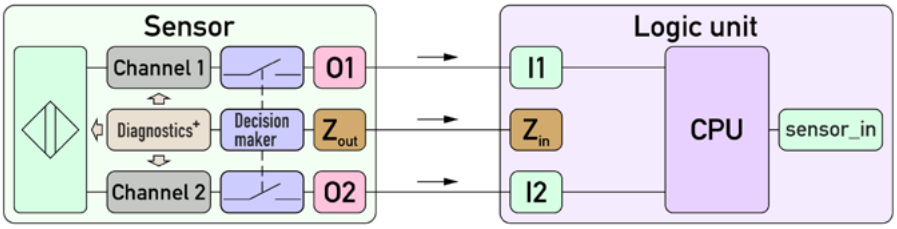
**Usage**

- Connection of safety-related sensor with logic unit:

**Structure (see Figure 6.4):**

- Two-channel output of the sensor (interface-type C),
- Digital output (not safety-related) from the sensor to the controller,
- Sensor contains qualified diagnostics and decision maker.

**Figure 6.4: Link-type 11**




**Behavior:**

- Sensor detects faults (and conditions that could lead to faults)
- If the decision maker in the sensor can clearly assign the fault and assesses it as tolerable, the outputs are not switched off.
- The status signal "Operation in degraded condition" is provided via the signal output.
- After the sensor-specific maximum permissible time $\Delta t_{deg}$ has elapsed, the outputs are switched off.

### 6.3.3 Link-type 12

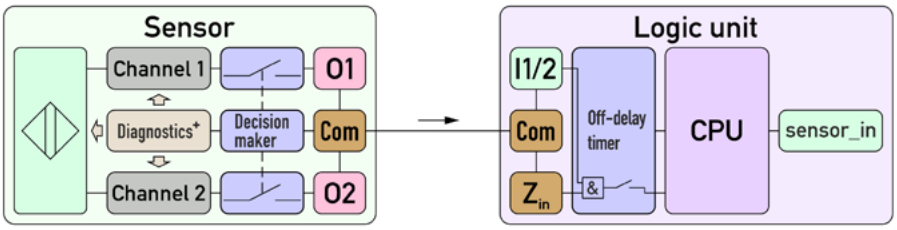
**Usage:**

- Connection of safety-related sensor with logic unit
- Connection of safety-related sensor with FS-DI

**Structure (see Figure 6.5):**

- Communication of the sensor with the controller via
  - a safety-related serial point-to-point connection (SDCI), or
  - a safety-related fieldbus protocol (FSCP)
- Safety-related output information via at least one data bit
- Safety-related status signal "Operation in degraded condition" via a further data bit (qualifier bit).
  - Qualifier bit HIGH: Operation in degraded condition (tolerance time running)
- In addition, fault numbers, long texts, etc. can be transferred in a functional part of the log.
- Sensor contains qualified diagnostics and decision maker

## Figure 6.5: Link-type 12




**Behavior:**

- Sensor detects faults (and conditions that could lead to faults).
- If the decision maker in the sensor can clearly assign the fault and assesses it as tolerable, the output information is not reset.
- The status signal "Operation in degraded condition" is reported to the controller / FS-DI.
- After the sensor-specific maximum permissible time $\Delta t_{deg}$ has elapsed, the output information is reset.
- The logic unit can use a parameterizable function block (off-delay timer, see Appendix A) to provide a shorter limitation for operation in the degraded condition specific to the application.

### 6.3.4 Link-type 13

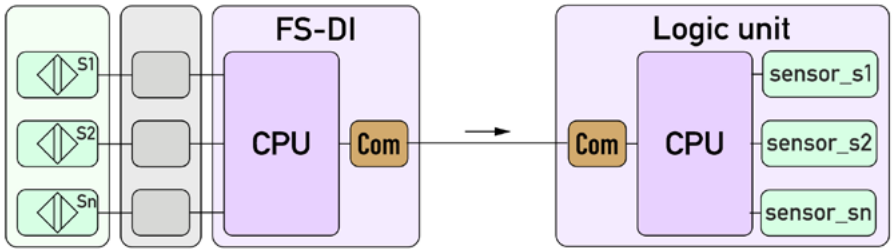
**Usage:**

- Connection FS-DI with logic unit

**Structure (see Figure 6.6):**

- Communication of the FS-DI with the controller via
  - a safety-related backplane bus, or
  - a safety-related fieldbus protocol
- "Concentrator" for output and diagnostic information of all connected sensors (link-type 11, 12)
- FS-DI can optionally contain qualified diagnostics and decision maker for itself.

## Figure 6.6: Link-type 13



# 7 Interfaces to power drive systems

## 7.1 Safety-related power drive systems [PDS(SR)]

### 7.1.1 Overview

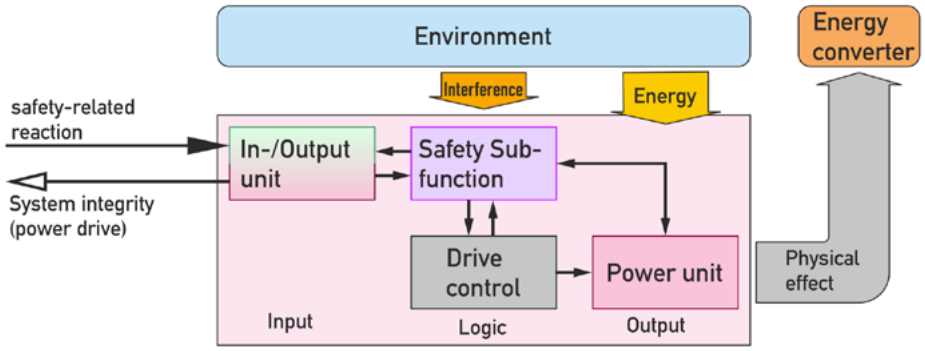
A safety-related power drive system (see Figure 7.1) consists at least of:

- an input/output unit
  provides safety-related information.
- a processing unit (safety sub-function)
  processes the information received from the controller to enable power control;
- a power unit (basic drive module)
  controls the power transmitted to the energy converter;

The input/output unit can process three types of electrical signal:

- analog electrical signals (e.g. current, voltage),
- hybrid analog and digital electrical signals (e.g. digital switches and I/O link)
- purely digital signals (e.g. via a fieldbus protocol).

**Figure 7.1: Safety-related power drive system**




### 7.1.2 Features of the power section

The power section is not within the scope of this document. Certain power drive systems, such as robot controllers, require several power units to control the different axes in parallel. Externally, such a control behaves identically to a power drive system with a single basic drive module.

### 7.1.3 Functionalities of the safety sub-function

Characteristic features of the functionalities described here are logic-types (see ZVEI white paper "Safety aspects for software in industrial applications").

**Logic-type 1 (one fixed SSF in the device):**

- Safety-related power drive system (e.g. Safe Torque Off (STO))
  internal structure fixed, without possibilities to change the SSF.

**Logic-type 2 (one selectable from n SSF):**

- Safety-related power drive system with several SSF, one of which must be selected by switches before commissioning or the selection is made by means of coding through wiring (e.g. for the stop category).

**Logic-type 3 (parameterizable SSF):**

Variant 1: Selection of the safety sub-function:

- Safety-related power drive system with several SSF, one of which must be selected and transferred to the sensor by means of an (external) "programming device" before commissioning.

Variant 2: Selection of parameters:

- Safety-related power drive system with one or more SSF (only one SSF active at a time), which must be parameterized by means of an (external) "programming device" before commissioning and the parameters must be transferred to the sensor (e.g. braking ramp).

**Logic-type 4 (multiple SSF with communication):**

- Safety-related power drive system with several (active) SSFs which must be selected by means of an (external) "programming device" prior to commissioning, input/output configured (software wiring) and parameterised if necessary, and the configuration must be transferred to the switching device.

### 7.1.4 Safety sub-functions of power drive systems

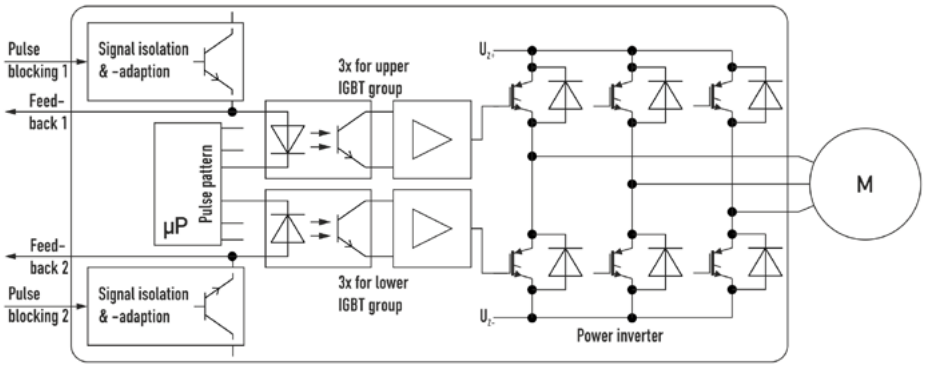
Usually, safety-related sensors (see chapter 5.2) perform only a single safety sub-function at a time. In contrast, power drive systems can perform different SSFs simultaneously (for more details see IEC 61800-5-2). These can be divided into two groups:

- Stop functions,
  Function for stopping drives:
  - Safe torque off (STO),
  - Safe stop 1 (SS1),
  - Safe stop 2 (SS2).

- Monitoring functions,
  Function for monitoring drive parameters:
  - to prevent the exceeding/falling below of a single limit value, or
  - to maintain a range within specified limits.
  - The response of a monitoring function usually triggers a stop function.

The SSF "STO" has a special role in a power drive system. This SSF is generally designed as a pulse inhibit (see Figure7.2). It is the common safety-related reaction to a failure for all other sub-functions integrated in the drive. Usually, STO is implemented with two channels (further details chapter 4.2.2, IFA Report 4/2018). Each channel blocks half of the pulse signals to the power transistors (IGBT).

## Figure 7.2: Pulse inhibit (Source: IFA Report 4/2018)



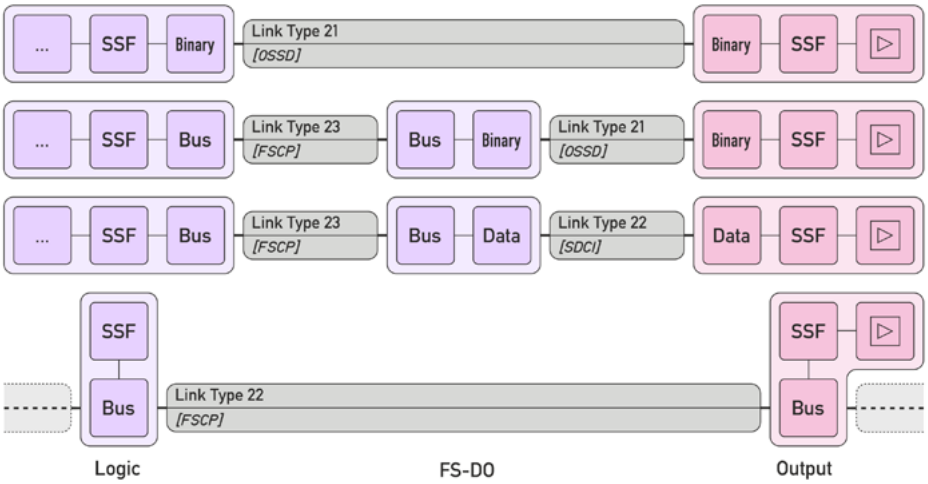

It is possible to integrate operation in the degraded condition for the SSF "STO" as well. However, any fault here should immediately lead to shutdown..

## 7.2 Classification of interfaces to power drive systems

### 7.2.1 Overview

The "power drive system" subsystem includes a qualified diagnostic and a decision maker. Interface requirements do not depend on the logic-type of the power drive system. Characteristic features of the required functionalities are the link-types defined below. The following interfaces are considered (see Figure 7.3):

**Figure 7.3: Link-types for power drive systems**




### 7.2.2 Link-type 21

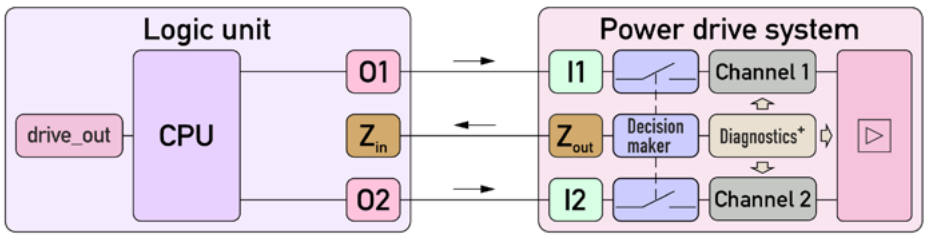
**Usage:**

- Connection logic unit with power drive system:

**Structure (see Figure 7.4:)**

- Two-channel output of the controller (interface-type C).
- Digital output (not safety-related) from the power drive system to the control system.
- Power drive system contains qualified diagnostics and decision makers.

**Figure 7.4: Link-type 21**




**Behavior:**

- Power drive system detects faults (and conditions that could lead to faults).
- If the decision maker in the power drive system can clearly assign the fault and assesses it as tolerable, the power section is not switched off.
- The status signal "Operation in degraded condition" is provided via the signal output.
- After the device-specific maximum permissible time $\Delta t_{deg}$ has elapsed, the power section is switched off.

### 7.2.3 Link-type 22

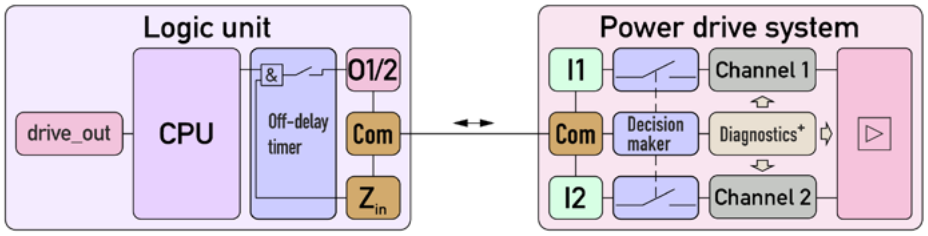
**Usage:**

- Connection logic unit with power drive system
- Connection FS-DO with power drive system

**Structure (see Figure 7.5):**

- Communication Control with power drive system via:
  - a safety-related serial point-to-point connection (SDCI),
  - a safety-related fieldbus protocol (FSCP).
- Safety-related output information about at least one data bit.
- Safety-related status signal "Operation in degraded condition" via a further data bit (qualifier bit)
  - Qualifier Bit HIGH: Operation in degraded condition (tolerance time running).
- In addition, fault numbers, long texts, etc. can be transferred in a functional part of the log.
- Power drive system contains qualified diagnostics and decision makers.

## Figure 7.5: Link-type 22




**Behavior:**

- Power drive system detects faults (and conditions that could lead to faults).
- If the decision maker in the power drive system can clearly assign the fault and assesses it as tolerable, the power section is not switched off.
- The status signal "Operation in degraded condition" is reported to the controller / FS-DO.
- After the device-specific maximum permissible time $\Delta t_{deg}$ has elapsed, the power section is switched off.
- The logic unit can use a parameterizable function block (off-delay timer, see Appendix A) to provide a shorter limitation for operation in the degraded condition specific to the application

### 7.2.4 Link-type 23

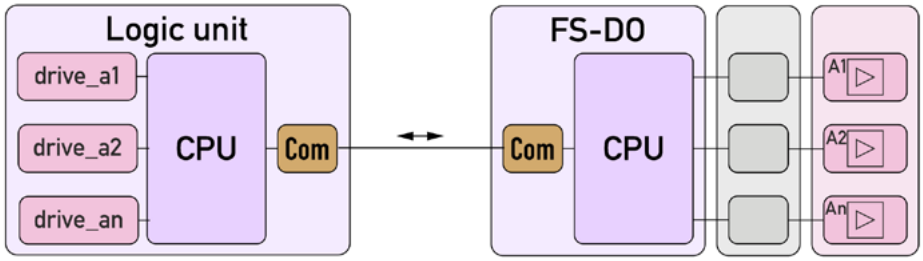
**Usage:**

- Connection logic unit with FS-DO

**Structure (see Figure 7.6:)**

- Communication of the controller with the FS-DO via:
  - a safety-related backplane bus,
  - a safety-related fieldbus protocol.
- "Concentrator" for output and diagnostic information of all connected power drive systems (link-type 21, 22)
- FS-DO can optionally contain qualified diagnostics and decision makers for itself.

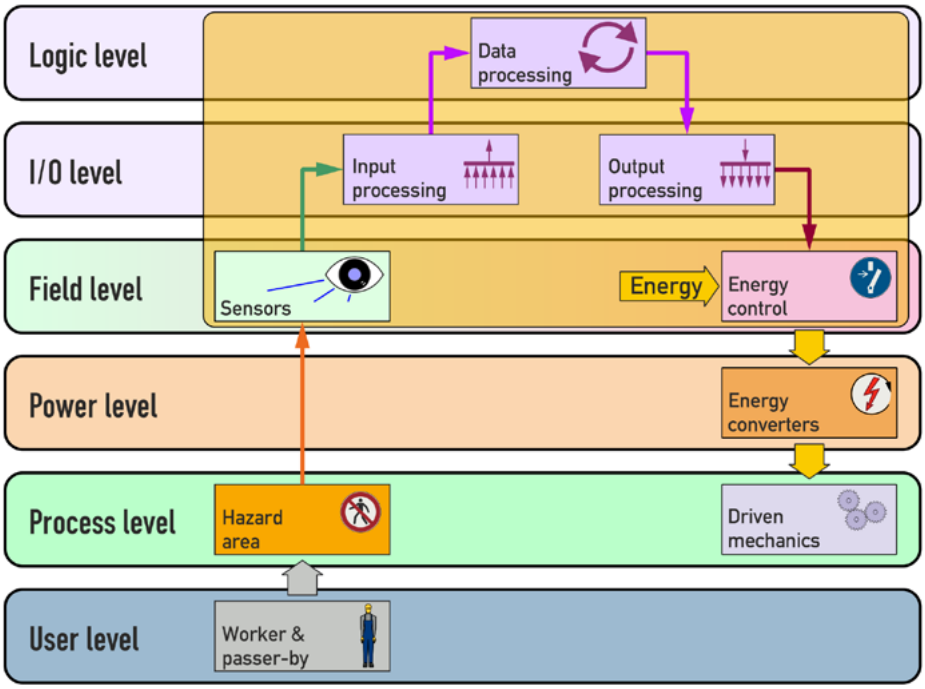
## Figure 7.6: Link-type 23



# 8 Conclusion and outlook

A machine is a complex piece of technical equipment (EUC) with one main function, for example preparation, treatment or processing of work objects by means of active movements. It is characterized by a functional concatenation of mechanisms for the conversion of energy types (see Figure 8.1).
The work equipment is controlled and monitored by an EUC control system, which responds to input signals and/or an operator, and generates output signals that cause the equipment to operate in the desired manner.

### Figure 8.1: EUC control system




The processing unit of a safety-related logic unit may also include a qualified diagnostics and a decision maker for itself. It must be ensured that it can guarantee operation of the entire safety function in a degraded state for a limited time at any time.

In the case of self-created subsystems made of non-safety-related components, safety-related logic units perform qualified diagnostics and include the decision maker, if they themselves carry out the preprocessing of sensor signals or the control of power drive systems.

The status signal “Operation in degraded state“ is transmitted as a message signal or as a safety-related signal depending on the interface used (link type).

Further issues relating to integration in products are dealt with in a supplementary document “Fault tolerance in machine safety Part 3 - Integration“

The explanations show that the implementation of time-limited operation with degraded safety subfunction in safety-related sensors and power drive systems is possible in accordance with the protection objectives of the Machinery Directive and does not contradict the harmonized standards ISO 13849 or IEC 62061.

Operation in the degraded state breaks - in compliance with the standard - with the dogma of immediate energy separation in the event of a fault. This increases the safety and availability of machines and systems:

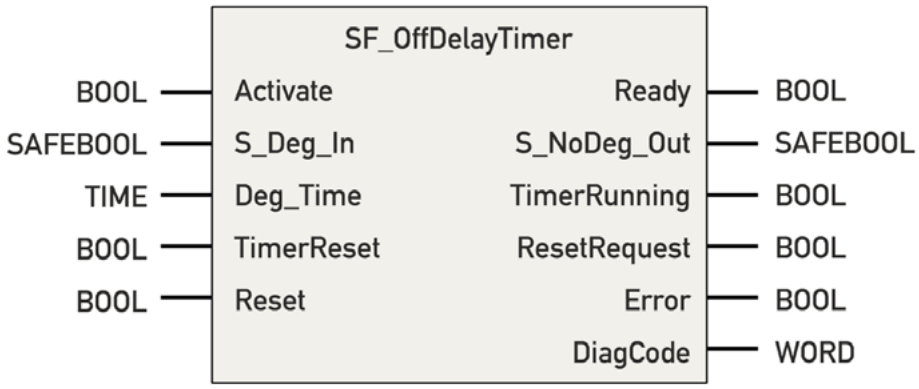
- Reduction of manipulation incentives.
- No consequential damage due to shutdown at inopportune times.
- Increase in productivity.
- Occasion-based maintenance without downtime.

This document describes the basis for the implementation of a qualified diagnostics and a decision maker in safety-related products to enable the operation of a machine/plant in a degraded state. Users and manufacturers are called upon to implement these advantages in machines.

# Annex A "Off-Delay Timer" function block

## A.1 Function block (FB)

### Figure A.1: Function block "Off-delay Timer



## A. 2 Interface description

### Tabelle A.1: Interfacebeschreibung

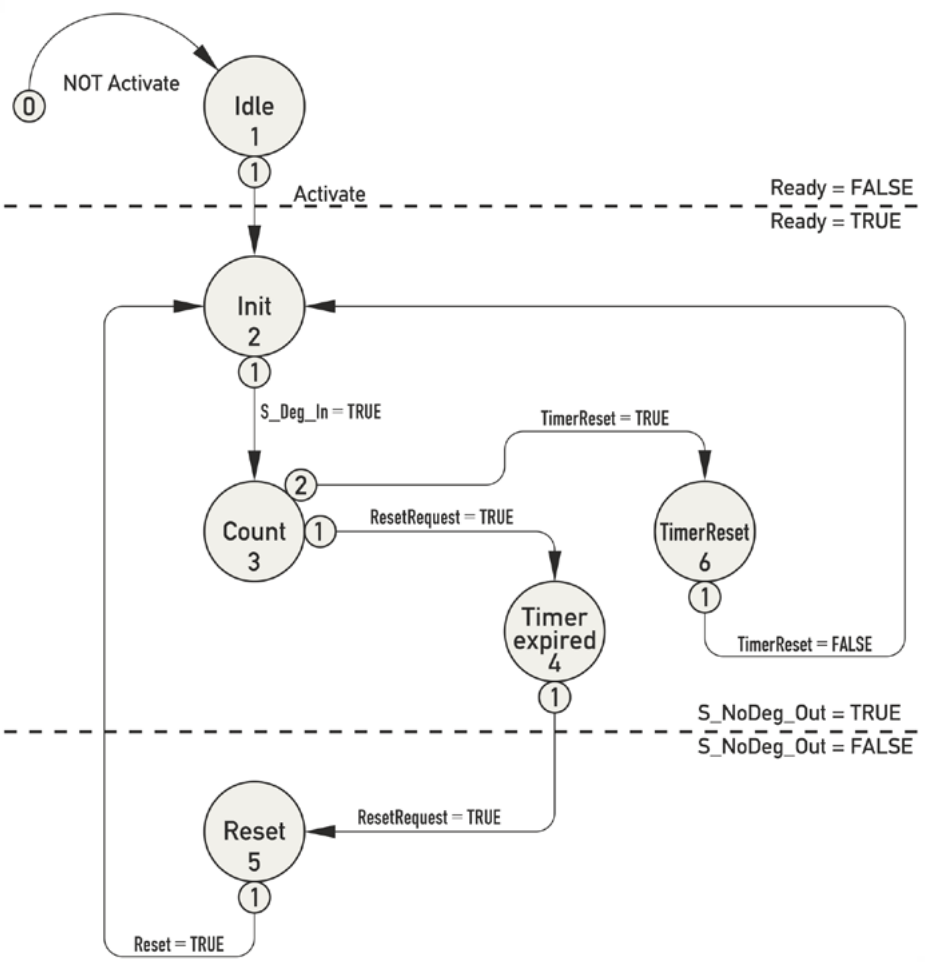
| FB Name | SF_OffDelayTimer | | |
|---|---|---|---|
| An FB SF_OffDelayTimer makes it possible to realize application-related shorter times than $\Delta T_{max}$ for degraded operation The output signal of the FB is switched off after the parameterized time has elapsed. The time $\Delta T_{max}$ is fixed at 48h | | | |
| **VAR_INPUT** | | | |
| **Name** | **Data Type** | **Initial Value** | **Description, Parameter Values** |
| Activate | BOOL | FALSE | See PLCopen[2] documentation |
| S_Deg_In | SAFE-BOOL | FALSE | Variable.<br>Receipt of the decision maker<br>FALSE: Degraded operation is not selected.<br>TRUE: Degraded operation is selected, Timer expires |
| Reset | BOOL | FALSE | See PLCopen documentation |
| TimerReset | BOOL | FALSE | Input for resetting the timer from the evaluation logic (optional) |
| DegTime | TIME | T#0h | Value range: 0 ... 48h (2880min)<br>Countdown degraded operating time. |
| **VAR_OUTPUT** | | | |
| Ready | BOOL | FALSE | See PLCopen documentation |
| S_NoDeg_Out | SAFE-BOOL | TRUE | Safety-related output signal.<br>TRUE: Timer has expired, maximum operating time has been reached.<br>FALSE: Timer has not started or is running. |
| TimerRunning | BOOL | FALSE | FALSE: Timer has not started<br>TRUE: Timer running |
| ResetRequest | BOOL | FALSE | Optional. See PLCopen documentation |
| Error | BOOL | FALSE | See PLCopen documentation |
| DiagCode | WORD | #0000 | See PLCopen documentation |
| Notes:<br>1. Reset input since the device can optionally be reset via software<br>2. TimerRunning output as a message output for the user, in order to be able to initiate corrective measures in good time. | | | |

Quelle: ZVEI

[2] PLCopen is an independent worldwide organization providing efficiency in industrial automation based on the needs of users. PLCopen and its members have concentrated on technical specifications around the IEC 61131-3 standard in order to reduce costs in industrial engineering.

## A.3 State transition diagram

### Figure A.2: State transition diagram



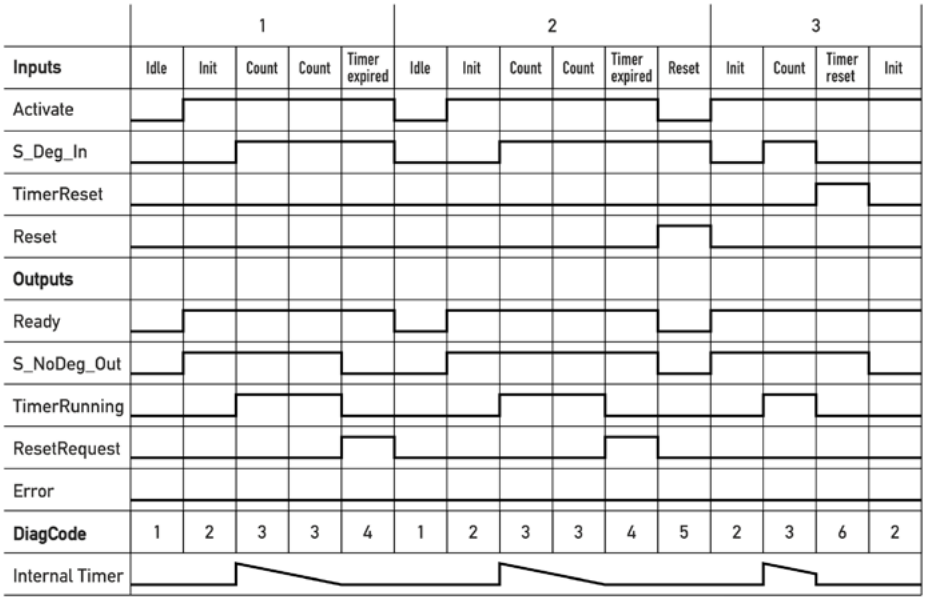
## A.4 Specific error codes

### Table A.2: Specific error codes

| DiagCode | State name | State description and initial state |
|---|---|---|
| 1 | Idle | The function block is inactive (initial state)<br>Ready = FALSE<br>S_NoDeg_Out = FALSE<br>TimerRunning = FALSE<br>ResetRequest = FALSE |
| 2 | Init | The decision maker is ready, degraded operation is not activated<br>Ready = TRUE<br>S_NoDeg_Out = TRUE<br>TimerRunning = FALSE<br>ResetRequest = FALSE |
| 3 | Count | Degraded operation has been activated, time expires<br>Ready = TRUE<br>S_NoDeg_Out = TRUE<br>TimerRunning = TRUE<br>ResetRequest = FALSE |
| 4 | Timer expired | The time has expired, shutdown request<br>Ready = TRUE<br>S_NoDeg_Out = FALSE<br>TimerRunning = FALSE<br>ResetRequest = TRUE |
| 5 | Reset | Resetting the block after the countdown has expired<br>Ready = FALSE<br>S_NoDeg_Out = FALSE<br>TimerRunning = FALSE<br>ResetRequest = FALSE |
| 6 | Timer reset | Countdown is reset and can be restarted<br>Ready = TRUE<br>S_NoDeg_Out = FALSE<br>TimerRunning = FALSE<br>ResetRequest = FALSE |

## A.4 Typical Timing Diagram

### Figure A.3: Timing diagram




Key:
1: Expiration of the timer after activation S_Deg_In and reset of the controller
2: Expiration of the timer after activation S_Deg_In and reset of the function block
3: Resetting the timer before expiration


ZVEI e.V.
Lyoner Straße 9
60528 Frankfurt am Main, Germany
Phone: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org