Safety Systems

Prof. Dr.-Ing. habil. Josef Börcsök,

HIMA Paul Hildebrandt GmbH + Co KG, Germany

Introduction

Our society is based on a modern industry. Within a modern industrial society, automation technology is definitely a key factor for success. No industrial processing plants and manufacturing companies could exist any longer without automation technology. As a result, the market for industrial automation technology is one of the strongest growing markets.

A long time very conservative environment, namely safe automation technology, has been strongly changing over the last two decades towards fully electronic control and automation systems.

The processing and manufacturing industries are challenged more than ever because of many, rapidly changing requirements. In the last 10 years, nearly no technical area has been innovating as strongly as safe automation technology. Due to rapid improvements in microelectronics, new fields opened in this area.

Also society is forcing new requirements for safe products and manufacturing procedures. Ecological requirements and laws for production security (product liability, machine guideline, safety guideline e.g. IEC61508) are important examples of it.

The globalization of Industry leads to an increasingly hard competitiveness. From this and the fact that economic success of industrial companies is more and more important, results the imperative to increase the plant safety and to product more efficiently. This, in turn, affects considerably the whole automation technology, safe and not.

Further, the global distribution of production locations requires that homogeneous products are manufactured with equivalent quality and consistent safety standards independently of the production location.

Pursuing the objectives mentioned above, requires an increased automation level leading simultaneously to a high innovation pressure on the technology.

If 100 years ago a mechanical governor was sufficient to peform controlling tasks, nearly all components of a modern production plant have now a sophisticated automation equipement whose functions can be overloaded, coordinated and optimized. The world-wide information exchange among distributed production locations, as well as the integration of automation technology with the MSR world are two further factors contributing to the state of technology.

Sensors, actors and bus networks should also be considered in this connection. Safely automating means to collect information, to process it and, according to the results, to affect the process such that it can performe the intended tasks correctly while ensuring a maximum of safety.

The more precise and effective, efficient and accessible, flexible and safer production plants and flows must be, the more information about the plant state is required. As a result, ann expanding number of measuring and monitoring points for processing data is essential. This incresingly higher information quantity would usually restrict the capacity of I/O units. An I/O unit contains generally hundreds to tens of thousands I/O ports. The number of required processing I/O ports alone, would go beyond the scope of the geometrical requirements.

Due to this requirements, the manufacturer of safety-related automation systems must develop innovative approaches which take the requirements demanded by the operators into consideration.

Ancillary conditions to such automation systems are easily operability, simple handling, high reliability and safety for the controlling process.

The requirements for safety-related automation system are as essential as the normative requirements and those given by law. These last consider not only the hardware, but the operating system, programming languages for processing applcations and diagnosic devices. The overall life cycle of such a system is therefore taken into consideration.

1 Basics of Functional Safety

1.1 History of Development

For nearly 20 years, great effort has been made in developing National, European und International standards for control engineering. In the early 1980s the International Electrotechnical Commission (IEC) and the German Institute of Standardization (DIN) investigated the fundamental requirements for protective systems using measurement and control techniques.

The IEC was mainly concerned with computer technology. DIN was concerned with risk assessment (DIN V 19250), the general requirements for protective devices (DIN V 19251) and computers in systems with safety tasks (DIN V VDE 0801). In 1989, these German standards were integrated into the European standards, e. g. the EN 1050 for risk assessment and the EN 954-1 in scalable requirements for safety-relevant controller components. Later in 1991, the IEC developed a holistic standard encapsulating full life cycle concepts and titled "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems" (IEC 61508). This is now an Australian Standard.

1.2 Fundamental Considerations

In safety-related, microprocessor based systems, random component faults are not the main factors leading to a failure. The most important contributor is the specification of how the system should operate, implemented by the engineer or the programmer. The next major factor is modifications after commissioning, operation and maintenance, as the end user often does not understand the intent of the original design and safety engineering. Measures must be taken to prevent or minimise such errors in a a safety system's development and/or design phase.

For the original manufacturer of safety related systems, the standards DIN V VDE 0801 and IEC 61508 differentiate between measures for **fault avoidance** during the development stage and **fault control** of the final product. Fault avoidance procedures in designing electronics are implemented by the manufacturer and verified by a test organisation such as the German test institute "Technischer Überwachungsverein" (TÜV). These measures are applied during planning, development and manufacturing such that errors can be detected and corrected. The measures for fault control are part of the system hardware and software functionality and result in an appropriate safety-related action.

1.3 Fault Avoidance Basis and Measurement

In complex systems, errors can only be managed effectively with rigorous procedures for the design, development and maintenance phases. The aim is to avoid errors from the very beginning using constructive and analytical processes along with testing and verification procedures throughout the overall safety life cycle.

IEC 61508 describes the individual phases of the safety life cycle prescribing fundamental requirements for each phase. Parts 2 and 3 of the standard contain guidelines for the implementation of electrical, electronic and programmable electronic (PES) systems. By following these guidelines, a complex safety system can be realized and an acceptable degree of fault avoidance achieved. These measures are contained in the annex A and B of Parts 2 and 3, ordered according to their effectiveness and detailed in Part 7.

The concept of the safety life cycle is based on the fact that in complex systems, functional safety can be ensured using verification procedures over the whole system life cycle. German test institutes such as the TÜV have applied this approach for many years when certifying microprocessor based systems for safety related applications. The so-called "development-accompanying examination" in the product requirement specification/concept phase is the first step for being accepted by such a test institute. The examination continues with the system design, operation, modification and maintenance phases.

The safety-related reliability of complex safety systems can be only achieved by implementing rigorous and analytic processes which incorporate continual verification and testing procedures. The extent of these measures varies depending on the necessary risk minimisation required by the safety function. Figure 1 shows the concept of risk reduction. Required risk reduction may be achieved by combining technical and non technical methods, with the result that the remaining (residual) risk of the hazardous plant or equipment is reduced to an acceptable level.
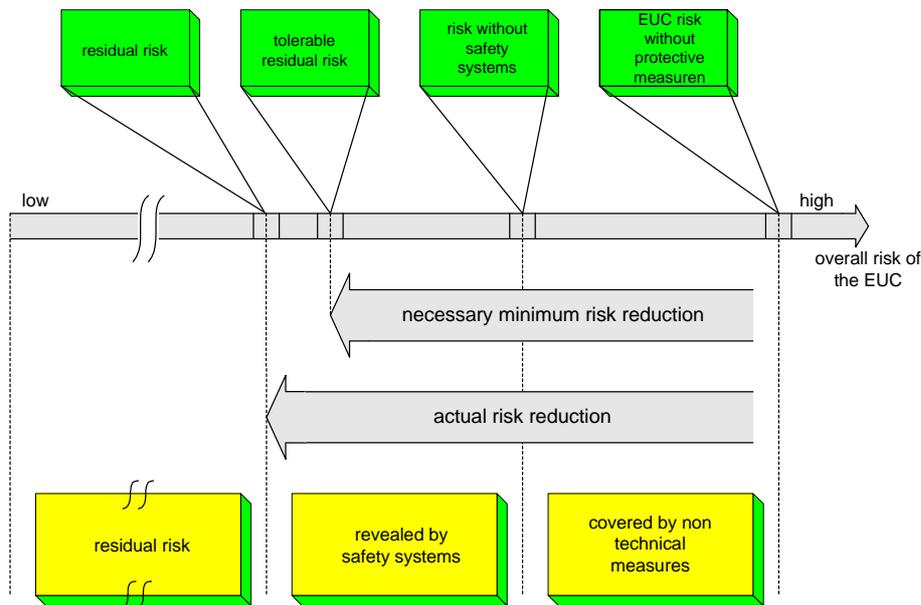

Figure 1: Risk Minimisation Model for Plant and Equipment

This question remains unanswered: "How is this acceptable residual risk defined?" In Germany, it is generally accepted that the tolerable residual risk cannot be absolutely specified. The necessary risk reduction of technical equipment can only be determined based on analogy against experience. Plants and equipment located near human being and which could potentially cause the loss of human life or damages, require substantial fault avoidance and fault control. Figure 2 and Figure 3 demonstrate the processes used by manufacturers and test institutes for avoiding faults. A measurement for the degree of risk reduction is the so-called Safety Integrity Level (SIL), as defined in the standard AS 61508. The SIL identified in AS 61508 can be approximately compared with the categories specified in EN 954, Part of 1 and the requirement classes (AK) defined in DIN V VDE 0801 and DIN V 19521, as shown in Table 1.
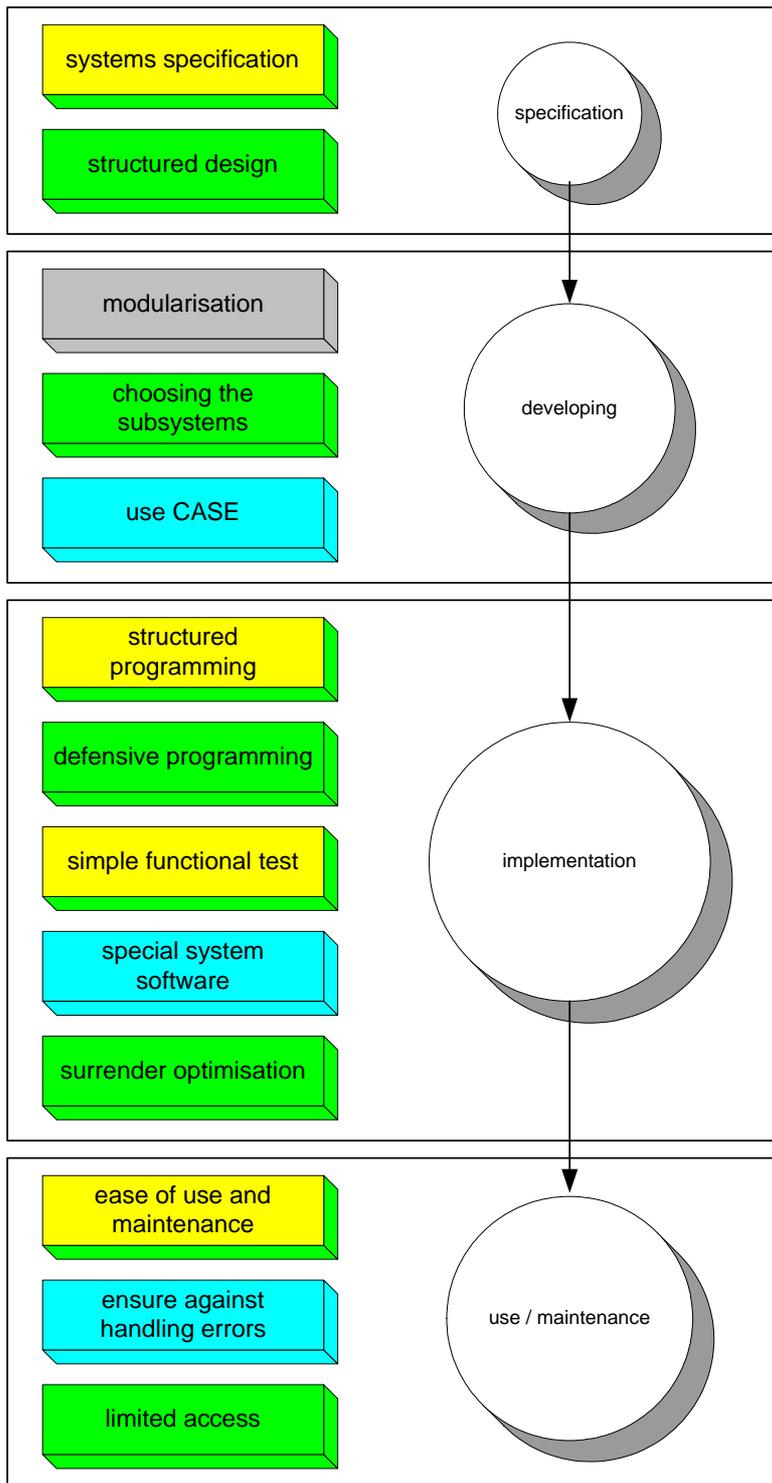
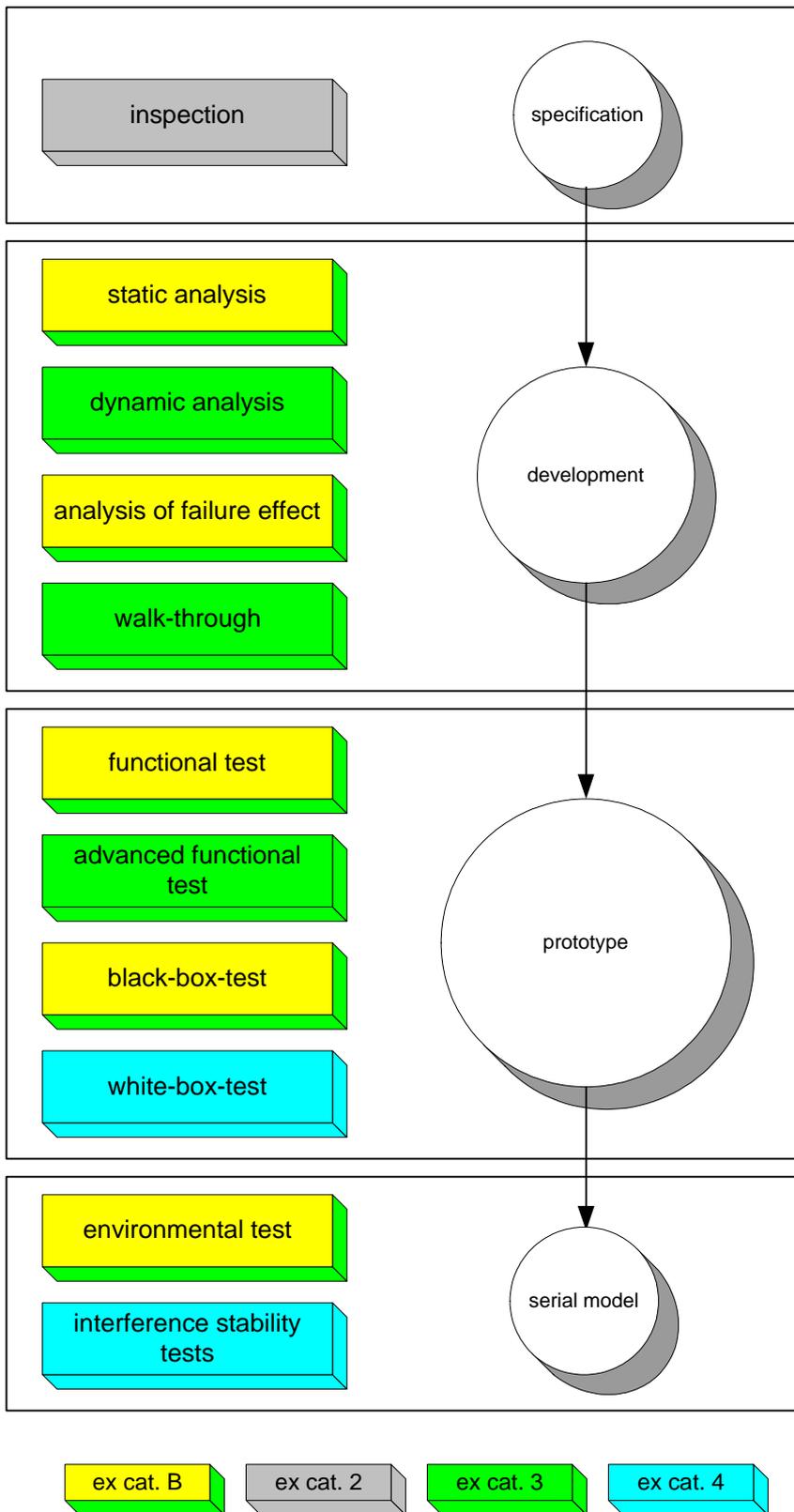**Figure 2: Fault Avoidance Measures for Manufacturers**

Figure 3: Fault Avoidance Measures for Test Institutes

Table 1: Qualitative Relationship between Fault Avoidance Measures, According to the Separate Standards

Category (EN 954-1)	Requirement class (DIN V 19250)	SIL (IEC 61508)	description
B	1	-	Control Systems according the state of the art/proven in use
2	2/3	1	Test
3	4	2	Single fault tolerance with partial fault detection
4	5/6	3	Self monitoring
-	7/8	4	Not relevant for machine protection

1.4 Fault Control Basis

Comparing the three schematics above, one can see that risk reduction is a function of the architecture and that the methods used for avoiding faults vary accordingly. All standards for functional safety identify a complex system's safety-related reliability as a function of redundancy as well as technical or non technical measures for detecting faults in its subsystems.

However, it is not possible to develop a complex system which does not contain any faults. The system's risk reduction can be affected by single components' random failures. These cannot be avoided and consequentially they must be controlled. To put "the control of faults" into context means (1) using redundancy, the fault does not lead to the failure of the safety equipments ability to function; or (2) the fault is diagnosed sufficiently early to repair the safety equipment in a satisfactory time period. In addition to redundancy and fault detection, a further important factor for evaluating a safety system is the component's reliability.

The necessary risk reduction for a safety function based on reliability data of electronic components can be expressed mathematically. According to IEC 61508, the Safety Integrity Level (SIL) is the probability of failure to perform the safety function on demand or the probability of failure per hour, as shown in Table 2.

Table 2: Definition of Safety Integrity Level According to IEC 61508

SIL	Low demand mode of operation (Average probability of failure to perform its design function on demand)	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

It is important, that the components' reliability is not predefined. That is why requirement classes, categories and SILs cannot directly compared with one another for the aspect to fault control. A correlation can only be established if the relevant structures are described more precisely and the single-channel subsystems have assigned failure rates.

Table 3 showes the relationship for structures of electronic safety systems, used as protective system for machinery in category B, category 2, category 3 and category 4.

Table 3: Context between Controller Architectures and SILs

SIL	System architecture (Controller structure)	Mean Time To Failure MTTF (Years) In/Processing/Out	CCF β (%)	Diagnostic coverage per Channel (%) In/Processing/Out	Category
-	Single channel PE, single channel PE I/O	15/15/30	-	0/0/0	B
	Single channel PE, single channel I, Ext. WD (t / nt)	15/15/30	-	0/60/0	B
	Dual channel PE, dual channel I/O, 1oo2	15/15/30	5	0/0/0	inapplicable
1	Single channel PE, single channel I, Ext. WD (t / nt)	15/15/30	-	100/60/100	2
	Single channel PE, single channel I, Ext. WD (t / nt)	7,5/15/10	-	100/60/100	2
	Dual channel PE, IPC, dual channel I/O 1oo2	15/15/30	5	100/60/100	3
	Dual channel PE, IPC, dual channel I/O 1oo2	15/15/30	10	100/90/100	3
	Dual channel PE, IPC, dual channel I/O 1oo2	45/15/60	10	100/90/100	3
2	Dual channel PE, single channel I, Ext. WD (t)	15/15/30	-	100/90/100	2
	Dual channel PE, IPC, dual channel I/O 1oo2	15/15/30	1	100/90/100	3
	Dual channel PE, IPC, dual channel I/O 1oo2	30/30/60	5	100/90/100	3
	Dual channel PE, IPC, dual channel I/O 1oo2	7,5/15/10	1	100/99/100	4
3	Single channel PE, single channel I, Ext. WD (t)	30/30/60	-	100/99/100	2
	Dual channel PE, IPC, dual channel I/O 1oo2	45/45/90	1	100/99/100	4

Caption:

WD(t/nt: Watchdog timer and associated switch-off path tested/untested
WD(t):   Watchdog timer and associated switch-off path tested
I/O: Input/Output
PE: Programmable electronics
Cat.:   Category
1oo2:   Dual channel safety-related structure
CCF: Common cause failure
IPC: Comparison between the channels

Conditions for single-channel systems:

- All test rates: 1/ (15 minutes)
- The demand rates: 1/ (24 hours)
- The repair rates: 1/ (8 hours)
- The life span: 10 years
- The MTTF of the watchdog timer: 100 years
- The MTTF of the switching of paths is as a normal switching of paths

Conditions for two-canal systems:

- All test rates: 1/ (24 hours)
- The demand rates: 10/ hour
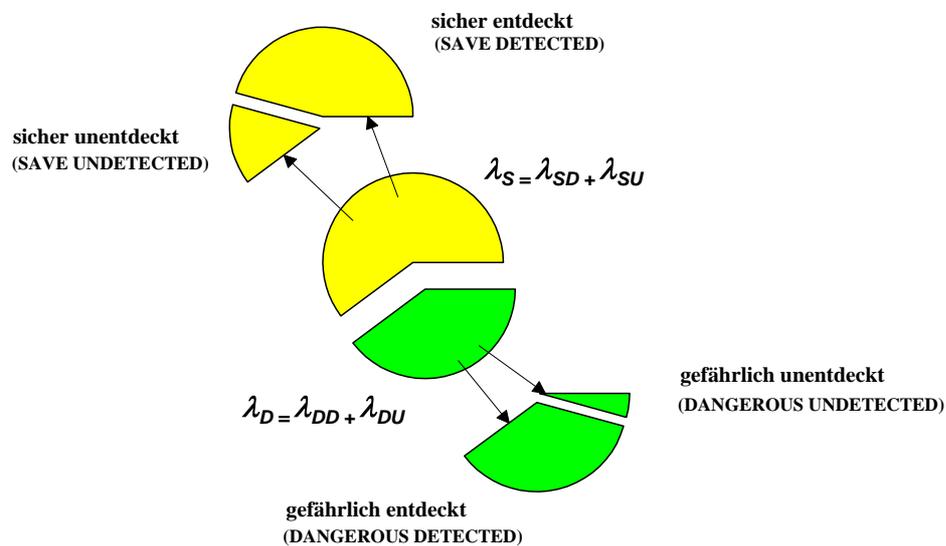- The repair rates: 1/ (8 hours)
- The life span: 10 years

sicher entdeckt
(SAVE DETECTED)

sicher unentdeckt
(SAVE UNDETECTED)

$$\lambda_S = \lambda_{SD} + \lambda_{SU}$$

gefährlich unentdeckt
(DANGEROUS UNDETECTED)

$$\lambda_D = \lambda_{DD} + \lambda_{DU}$$

gefährlich entdeckt
(DANGEROUS DETECTED)

Figure 4: Failure Distributions in a Safety System (Qualitativ)

Table 4: Input Parameters for Calculating Typical Controller Structures

| Description of the input parameters	Parameter
MTTF of sensors, PE-devices and PLC	15 years
MTTF of a shut down path of actuators	30 years
MTTF of Watchdogs	100 years
Lifetime operating	10 years
Repair rate (after a fault detection or a dangerous event)	1/(8 hours)
All test rates of single channel systems	1/(15 minutes)
All test rates of multi channel systems	1/(10 seconds)
All demand mode of single channel systems	1/(24 hours)
All demand mode of multi channel systems	1/(10 seconds)

The SIL calculation is based on the architectures shown in Figure and the initial parameters specified in Table 4. Given an operating lifetime of 10 years, an average probability of failure can be calculated. For the individual structures in machine protection, common conditions are accepted.

category B or 1 of EN 954-1

$$\lambda_{SCS} = \lambda_S + \lambda_{PE} + \lambda_A \qquad\qquad p_{dang} = 1 - e^{-\lambda_{SCS} \cdot t}$$
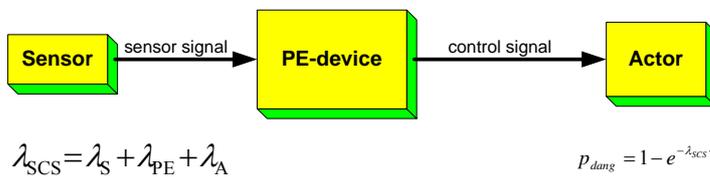
category 2 depending of EN 954-1
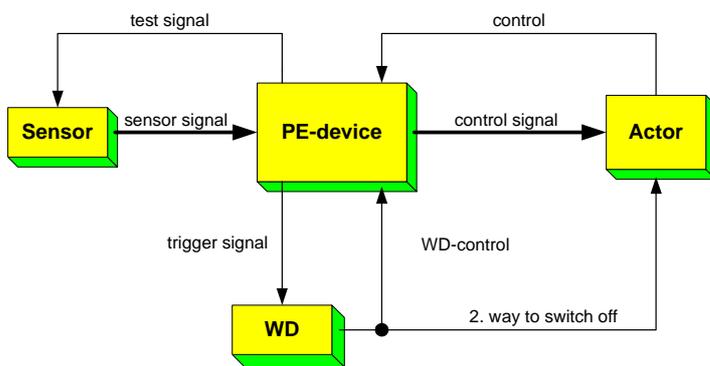
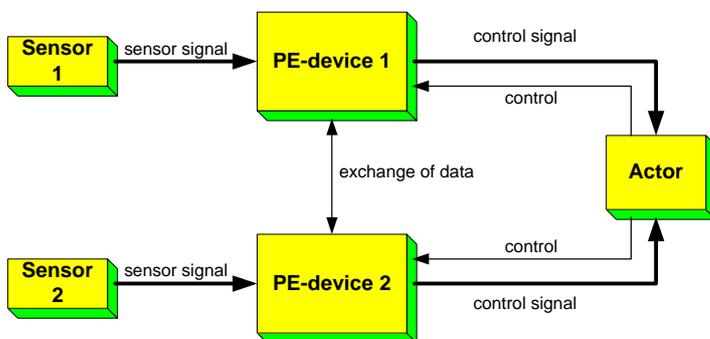**category 3 or 4 depending of EN 954-1**

Figure 5: Overview of System Architectures as shown in table 1.3

Requisites for relevant system structures:

General requisites:

- Due to the switch-off of the drive, the machine takes over the safe state.
- The safety system itself does not initiate a dangerous/hazardous situation. In the worst case, a dangerous failure prevents the safety system from performing the safety functions.
- When faults are detected, the safety system will be repaired. After repair, the system is considered 100 % safe.

The necessity of automatic tests for detecting failures is shown in Table 5. Examples of self-test with estimation of the effectiveness can be found in the appendix A of IEC 61508, Part 2. The following tables (Table 5 and Table 6) show in context the relative effectiveness in relation to diagnostic coverage.

Table 5: Faults or Failures to be Detected During Operation or to be Analyzed in the Derivation of Safe Sailure Fraction

Component	Requirements for diagnostic coverage or safe failure fraction claimed		
	low (60 %)	medium (90 %)	high (99 %)
Electromechanical devices	Does not energize or de-energize welded contacts	Does not energize or de-energize Individual contacts welded	Does not energize or deenergize Individual contacts welded No positive guidance of contacts (for relays this failure is not assumed if they are built and tested according to EN 50205 or equivalent) No positive opening (for position switches this failure not assumed if they are built and tested according to EN 60947-5-1, or equivalent)
Discrete Hardware Digital I/O	Stuck-at	DC-fault model	DC-fault model, drift, oscillation
Analogue I/O	Stuck-at	DC-fault model, drift, oscillation	DC-fault model, drift, oscillation
Power supply	Stuck-at	DC-fault model, drift, oscillation	DC-fault model, drift, oscillation
Bus General	Stuck-at of the addresses	Violation of timing conditions / time out	Violation of timing conditions / time out
Memory management unit (MMU)	Stuck-at of data or addresses	Wrong address decoding	Wrong address decoding
Direct memory access (DMA)	No or continuous access	DC fault model for data and addresses Wrong access time	All faults which affect data in the memory Wrong data or addresses Wrong access time
Bus-arbitration	Stuck-at of arbitration signals	No or continuous arbitration	No or continuous or wrong arbitration
CPU Register, internal	Stuck-at for data and	DC fault model for data and addresses	DC fault model for data and addresses

RAM	Addresses		Dynamic cross-over for memory cells No, wrong or multiple addressing
Coding and execution including flag register	Wrong coding or no execution	Wrong coding or wrong execution	No definite failure assumption
Address calculation	Stuck-at	DC fault model	No definite failure assumption
Program counter, stack pointer	Stuck-at	DC fault model	DC fault model
Interrupt handling	No or continuous interrupts	No or continuous interrupts Cross-over of interrupts	No or continuous interrupts Cross-over of interrupts
Invariable memory	Stuck-at for data and addresses	DC fault model for data and addresses	All faults which affect data in the memory
Variable memory	Stuck-at for data and addresses	DC fault model for data and addresses Change of information caused by soft-errors for DRAM with integration 1 Mbits and higher	DC fault model for data and addresses Dynamic cross-over for memory cells No, wrong or multiple addressing Change of information caused by soft-errors for DRAM with integration 1 Mbits and higher
Clock (quartz)	Sub- or super harmonic	Sub- or super harmonic	Sub- or super harmonic
Communication and mass storage	Wrong data or addresses No transmission	All faults which affect data in the memory Wrong data or addresses Wrong transmission time Wrong transmission sequence	All faults which affect data in the memory Wrong data or addresses Wrong transmission time Wrong transmission sequence
Sensors	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation
Final elements	Stuck-at	DC fault model Drift and oscillation	DC fault model Drift and oscillation

Remark:

Bus arbitration is the mechanism to determine, which device controls the bus.

Stuck-at is a failure category, which shows a constant "0" or "1" on the pins of the component.

The DC-fault model incorporates the following modes:

Stuck-at

Line break

High impedance outputs

Short circuit between signal lines.

Table 6: Diagnostic coverage and effectiveness for different subsystems

Component	Low diagnostic coverage	Medium diagnostic coverage	High diagnostic coverage
CPU	total less than 70 %	total less than 90 %	
register, internal RAM	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
coding and execution including flag register	50 % - 60 %	75 % - 95 %	-
address calculation	50 % - 70 %	85 % - 98 %	-
program counter, stack pointer	40 % - 60 %	60 % - 90 %	85 % - 98 %
Bus			
memory management unit	50 %	70 %	90 % - 99 %
bus-arbitration	50 %	70 %	90 % - 99 %
Interrupt handling	40 % - 60 %	60 % - 90 %	85 % - 98 %
Clock (quartz)	50 %	-	95 % - 99 %
Program flow monitoring			
temporal	40 % - 60 %	60 % - 80 %	-
logical	40 % - 60 %	60 % - 90 %	-
temporal and logical	-	65 % - 90 %	90 % - 98 %
Invariable memory	50 % - 70 %	99 %	99,99 %
Variable memory	50 % - 70 %	85 % - 90 %	99 % - 99,99 %
Discrete hardware			
digital I/O	70 %	90 %	99 %
analogue I/O	50 % - 60 %	70 % - 85 %	99 %
power supply	50 % - 60 %	70 % - 85 %	99 %
Communication and mass storage	90 %	99,9 %	99,99 %
Electromechanical devices	90 %	99 %	99,9 %
Sensors	50 % - 70 %	70 % - 85 %	99 %
Final elements	50 % - 70 %	70 % - 85 %	99 %

In addition to the measures mentioned for controlling random faults, the German and International standards describe measures for controlling systematic failures. These are supplementary to the measures for fault avoidance. Examples are plausibility testing and program monitoring by an external watchdog. These two measures can be helpful to detect disturbances in the functional software in time, which are caused either by programming failures or by unexpectedly strong electromagnetic influences on the systems memory.

1.5 External Influences

Obviousely, like all safety-related controllers, bus systems must withstand the expected operating and environmental demands. Less emphasis is required by safety systems for the maintaining operation (high availability). The principal purpose is that a safety-relevant controller never fails to danger under the influence of usual disturbances and environmental conditions.

Criteria are specified for environmental checks, which demand a fixed behaviour of a bus system under disturbances (vibration, EMC).

Table 7: Environmental Demands Performance Criteria for the Behaviour of Safety - Related Bus Systems

Performance criteria	Description
A	The bus system must work intended during and after the disturbing influence.
B	The bus system must work after the disturbing influence intended. With exceeding of the time Out time because of disturbing influence the safety-relevant participants must introduce the safe condition. Restarting is to be realized application-dependently automatic or by explicit release. Bus communication is automatically again taken up after disturbing influence.
C	The safety related introduce participant the safe condition. Communication failed. All safety-relevant participants remain in the safe condition. The re-establishment of the correct enterprise takes place via setters.

1.5.1 Electromagnetic Influences

IEC 61000-6-2 shows only a minimum of requirement for electromagnetic compatibility (EMC) immunity. The standard requires further performance criteria, which are adapted for bus systems.

We differentiate between conducted disturbances, electromagnetic interference and electrostatic influence. In field bus systems, all three factors influence the transmission reliability. Bit or burst errors are caused, for example, by single disturbances pulses.

Fieldbus systems can tolerate electromagnetic disturbances or react safely. In this aspect, they differ from other modern controllers. The first solution is passive screening e. g. by EMC filtering and special wiring. The second is active tolerance e. g. by detection of disturbed messages, block replications and retransmissions. If this measure is possible within the demanded reaction time, the system availability is not affected. In the case of strong and longer persisting EMC, the bus system takes over its safe state. Normally, very good protection from EMC influences is ensured by a combination of these two measures providing both safety and availability.

Apart from the direct influence of the transmission of messages, further disturbances can impair the electronics devices' safe functioning. The destruction of the entire bus protocol circuit or of other important components, such as the safe guarding mechanism (in redundant system, a common cause failure), for example, should be taken into cosideration. These influences must also be considered with field bus systems.

1.5.2 Mechanical and Climatic Influences

Ín addtion to EMC, further influences in field operation should be considered, such as shock, vibration, temperature and humidity. Bus systems are not different from other safety-relevant systems, in this aspect. The following table shows four different application areas with different severity levels for mechanical examinations.

Table 8: Range of different applications

Range of application I: None increased demands
Range of application II: Average environmental technical or operating conditioned influences are to be expected, the assembly place protect the installation against strong influence.   Note: It is to be noted that cabinets are set up also at exposed places and so they can exist also in the range of application III or IV.
Range of application III: One proceeds from hard environmental technical or operating conditioned influences. That is particularly for process near installations of sensors and actuators the case. Electrical fitting spaces also exposed and fall under this range of application.
Range of application IV: It concerns the external area. In addition to range of application III are considering harder requirements (e. g. lightning protection).

It is recommended that safety related bus systems are only installed within the specified environment. Further, existing relevant standards should be observed.

2 Literature

[1] IEC/EN 61508: International Standard 61508 Functional safety: Safety-related System. Geneva, International Electrotechnical Commission

[2] Börcsök, J.: International and EU Standard 61508, Presentation within the VD Conference of HIMA GmbH + CO KG, 2002

[3] Börcsök, J.: Elektronische Sicherheitssysteme, Hüthig publishing company.

[4] Börcsök, J.: Sicherheits-Rechnerarchitektur Teil 1 und 2, lecture of University of Kassel, 2000/2001.

[5] Börcsök, J.: Echtzeitbetriebsysteme für sicherheitsgerichtete Realzeitrechner, lecture of University of Kassel, 2000/2001.

[6] DIN VDE 0801: Funktionale Sicherheit, sicherheitsbezogenener elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES), (IEC 65A/255/CDV: 1998), Page: 27f, August 1998

[7] DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen. Beuth publishing company, Berlin 1998

[8] DIN VDE 0801/A1: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben, Beuth publishing company

[9] IEC 60880-2: Software für Rechner mit sicherheitskritischer Bedeutung, 12/2001

Prof. Dr.-Ing. habil. Josef Börcsök is executive vice president for research and development of the company HIMA + CO KG industry automation. He has been operating in the field of safety-related computer technology for several years and is member of several DKE committees. He lectures at universities, as well as at universities of applied sciences with lectures of automation systems, computer technology, realtime systems and safety-related computer technology.

Address:
HIMA GmbH + Co KG, Albert Bassermann-Str. 28, D-68782 Bruehl in Mannheim,
Tel.: 06202-709-270, email: j.boercsoek@hima.com