Metodyki projektowania i modelowania systemów

Metodyka zgodna z IEC 61508
<u>Zagadnienia</u>

- *Project Development Process Overview*
- *Documentation*
- *Configuration Management*
- *Function Safety Management*
- *Safety Requirements*
- *Safety Validation Test Planning*
- **System Architecture Design**
- **Hardware Design**
- **Software Design**
- *Implementation*
- *Integration and Safety Validation Test Execution*
- *Modification Procedure*
- *Vertification*

Functional Safety

An IEC 61508 SIL 3
Compliant Development Process
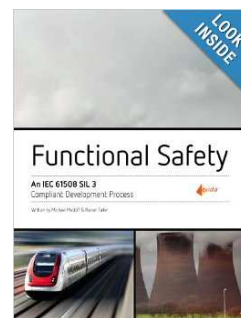
Functional Safety - An IEC 61508 SIL 3 Compliant Development Process
November 20, 2010
by Michael Medoff & Rainer Faller

1

Metodyka zgodna z IEC 61508
System Architecture Design

Functional Safety

8.1 Requirements of IEC 61508

- Decompose the system design into subsystems and elements each with specific defined functionality
- User hierarchical design to manage complexity
- Use semi-formal methods to document the design
- Achieve independence between safety and non-safety functions or functions of different safety integrity levels
- Create test cases for integrating subsystems and elements together
- Analyze potential failure modes of the product and plan safety measures to prevent the failure modes from causing hazardous situations
- Identify any data communications that are used in the implementation of safety functions.

Schemat architektury systemu
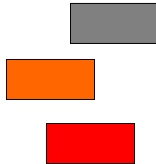
Gray – C1 = Interference Free component, interface or component. A component that is neither safety critical nor safety relevant, but interfaces with such subsystems.

Orange – C2 = Safety relevant subsystem, interface, or component. A single failure in safety relevant areas cannot cause an unsafe situation to occur, but in combination with a second failure of any hardware or software unit, an unsafe situation may occur.

Red – C3 = Safety critical subsystem, interface component. A single failure in safety critical areas could cause an unsafe situation to occur.

Metodyka zgodna z IEC 61508
System Architecture Design

Functional Safety

Table 8.1 System Architecture Checklist

	Item	Comment / Initials
☐	Design has been partitioned into subsystems and interfaces between subsystems are clearly defined.	
☐	A notation is used to represent the architecture that is unambiguously defined	
☐	Computer Aided Specification Tools are used	
☐	Consider whether the architecture design description fulfils the specified safety requirements.	
☐	The design is clear and easily understood by the development and verification team;	
☐	The required safety performance is feasible based on this design;	
☐	The design is testable for further verification	
☐	The design will support safe modification to permit further evolution	

Table 8.2 Integration Test Plan Checklist

	Item	Comment / Initials
☐	All test procedures include pass/fail criteria	
☐	The integration plan shall consider details of those who shall carry out the integration.	
☐	Tests include input data which adequately characterizes normally expected operation	
☐	Input value ranges (equivalence classes) are created from the inputs to be tested. Values from all ranges are included in the tests (including both permissible and inadmissible ranges). Values from the range limits are included and extreme values are included.	
☐	Performance Testing is included including avalanche/stress testing.	
☐	If a requirements model was developed, then test cases based on this model are included.	

Metodyka zgodna z IEC 61508
System Failure Modes and Effect Analysis (FMEA)

Functional Safety

8.11.4 System FMEA Documentation

Once the design has been broken down into the appropriate number of design functions, the following should be described for each design function:

Specyfikacja wszystkich funkcji

- Function – Summarizes the function

- Description – Describes the function in detail

- Protective Measures – Describes any planned or actual measures in the design to protect against dangerous failures. This should include both protective measures and diagnostics.

- Safety Criticality Level – A categorization of the worst case impact of a failure to this function. As defined in previously in this chapter the categorizations are Safety Critical (C3), Safety Relevant (C2) or interference free (C1).

- Failure Modes of Function – A list of ways that the function can fail. These are not the causes of the failure, just a description of the actual failure. In addition, the following information should be defined for each failure mode:

Metodyka zgodna z IEC 61508
System Failure Modes and Effect Analysis (FMEA)

Functional Safety

- Effect of failure – what is the effect of the failure in terms of functional safety without any detection or mitigation. Possible values are dangerous (safety function will not work properly), safe (false trip), no effect (safety function will continue to work properly, loss of diagnostics (safety function will continue to work, but some diagnostics will not), annunciation failure (safety function will continue to work, but if diagnostics detect problem they may not be annunciated properly), fail high (output will be stuck at the high end of its range; whether this is dangerous or not depends on the application), or fail low (output will be stuck at the low end of its range; whether this is dangerous or not depends on the application).

- Safety Measure / Diagnostic – Describes any planned or actual measures in the design that will protect against this failure mode along with the actions taken by each measure.

- Update Rate of Diagnostic

- Level of Effectiveness of safety measure – For diagnostics, this field documents how likely the diagnostic is to detect the failure mode as defined in section 8.11.2.

Metodyka zgodna z IEC 61508
System FMEA Example
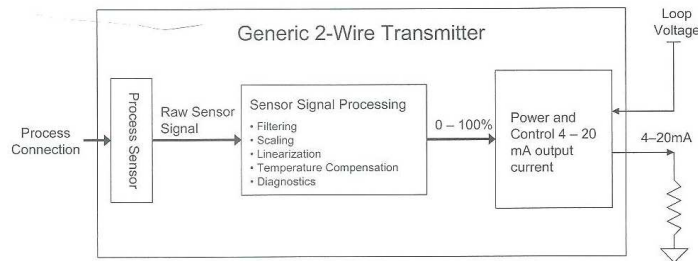
Generic 2-Wire Transmitter

Figure 8.3 High Level Block Diagram for Generic Two Wire Transmitter

The function of a two wire transmitter is to provide a scaled representation of the monitored process measurement as a 4-20mA current within specified worse case accuracy and response time. The worst case accuracy is called the "safety accuracy" which is different from the specified product accuracy. The safety accuracy is a value chosen in order to determine if an accuracy error is significant enough to be considered a dangerous error by the FMEA. For a typical product, the safety accuracy is 2% of scale which may be significantly worse than the product's specified accuracy. The user of the transmitter for a safety application must take the safety accuracy into account when setting the trip threshold for a SIF.

Metodyka zgodna z IEC 61508
System FMEA Example

Function: The process sensor will measure the desired process parameter.

Description: The desired process parameter is measured by a sensor which outputs a voltage signal representative of the process parameter.

Protective Measures: The sensor output is expected to be within a particular valid voltage range which is less than the actual physical range possible for the output.

Criticality Level: Safety Critical (C3)

Failure Modes of Function	Failure Effect (without mitigation)	Safety Measure / Diagnostic	Level of Effectiveness
Sensor outputs inaccurate signal with error greater than safety accuracy (typically 2%)	Dangerous	None	None
Sensor outputs inaccurate signal with error less than safety accuracy (typically 2%)	No effect on safety operation		
Sensor fails high (constant output greater than maximum value)	Safe or Dangerous depending on application	Outside of reasonable range detection (within 3 sample update periods)	High
Sensor fails low (constant output lower than minimum value)	Safe or Dangerous depending on application	Outside of reasonable range detection (within 3 sample update periods)	High
Increased noise (variation in output greater than safety accuracy with fixed input)	Dangerous	None	None
Slower than specified response to change in input value	Dangerous	None	None
Loss of process material containment (leak in process to sensor interface)	Safe or Dangerous depending on application	None	None
Stuck at one output value within normal range	Dangerous	Outside of reasonable range detection	Low

4

Metodyka zgodna z IEC 61508
System FMEA Example

Function: The Signal Processing subsystem measures the sensor output signal and provides the output to control the 4-20mA Output (performs linearization and sensor compensation corrections according to factory calibration settings and performs filtering and scaling of the process variable according to user configuration) and also performs product diagnostics.

Description: The microprocessor is assumed to include the following sub functions:
- Nonvolatile storage for calibration and user configuration
- Analog to Digital converter for sensor output voltage
- CPU with integrated RAM, program ROM, and hardware interface ports
- CPU clock oscillator
- Scaled output interface

Protective Measures: A/D monitoring of independent reference voltage levels above and below expected min and max sensor range outputs (2 point calibration verification), use logical and temporal monitoring of program execution to trigger independent low side watchdog timer, background walking 1/0 testing of RAM, background CRC16 testing of program RAM, CRC16 testing of static parameters based on factory calibration and user configured settings, reasonability range checks on sensor input and scaled output parameters.

Criticality Level: Safety Critical (C3)

Failure Modes of Function	Failure Effect (without mitigation)	Safety Measure / Diagnostic	Level of Effectiveness
Analog to Digital Accuracy Faults	Potentially Dangerous	• 2 Point verification of known reference voltage • Sensor input reasonability check	Medium level of effectiveness

---

Metodyka zgodna z IEC 61508
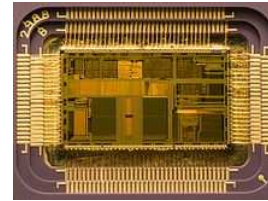### *System FMEA Example*

Criticality Level: Safety Critical (C3)

Failure Modes of Function	Failure Effect (without mitigation)	Safety Measure / Diagnostic	Level of Effectiveness
Analog to Digital Input Multiplexer Failures	Potentially Dangerous	• 2 Point verification of known reference voltage (outside senor reasonable range) • Sensor input reasonability check	Medium level of effectiveness (limited to low if other inputs are within valid sensor range)
(CPU) Register Faults	Potentially Dangerous	• Cross coverage from CRC16 tests, RAM walking 1/0 tests, and program execution monitoring	Medium level of effectiveness
(CPU) Incorrect ALU calculations	Potentially Dangerous	• Reasonable range tests for sensor and scaled output data • Watchdog timer and program flow monitoring • Cross coverage of CRC16 diagnostics	Low level of effectiveness
(CPU) Faults that impact program Flow	Potentially Dangerous	• Independent low side watchdog timer triggered from logical and temporal program execution monitoring with default override on 4-20mA output	Medium level of effectiveness

(CPU) Faults to internal RAM	Potentially Dangerous	• Walking 1/0 RAM test • Reasonable range tests for sensor related data • Watchdog timer and program flow monitoring	Medium level of effectiveness (for Hard Faults) Low level of effectiveness (for Soft Faults)
(CPU) Faults to internal program ROM	Potentially Dangerous	• CRC16 of ROM contents	High level of effectiveness
Corruption or loss of data in nonvolatile storage	Potentially Dangerous	• CRC16 of critical content	High level of effectiveness
Loss of Main CPU clock	Dangerous	• Independent low side watchdog timer with default override on 4-20mA output	High level of effectiveness
Loss of Main CPU clock	Dangerous	• Independent low side watchdog timer with default override on 4-20mA output	High level of effectiveness
Main CPU clock oscillate at sub harmonic	Potentially Dangerous	• Independent low side watchdog timer with default override on 4-20mA output	Low level of effectiveness
Main CPU clock oscillate at super harmonic	Potentially Dangerous	• None	None
High or Low Failures of scaled output signal	Potentially Dangerous	• Reasonability range check by Logic Solver	High level of effectiveness for properly configured logic solver
Drift failures of scaled output signal	Potentially Dangerous	None	None

Function: 4-20mA output current portion of Power and control 4-20mA output

Description: Receives signal representing desired output current and controls output current to the desired level by a closed loop analog voltage to current converter

Protective Measures: No internal diagnostic but out of normal range (OOR) output (either below 3.3mA or above 24 mA) that can be detected by a properly configured safety transmitter.

Criticality Level: Safety Critical (C3)

Failure Modes of Function	Failure Effect (without mitigation)	Safety Measure / Diagnostic	Level of Effectiveness
mA Output OOR High	Potentially Safe or Dangerous depending on application	• Properly configured safety PLC can detect > 21.6 mA as out of normal range (OOR)	High level of effectiveness if safety PLC configured to detect and properly handle High output conditions
mA Output OOR Low	Potentially Safe or Dangerous depending on application	• Properly configured safety PLC can detect output < 3.6 as out of normal range (OOR)	High level of effectiveness if safety PLC configured to detect and properly handle Low output conditions
Output drift	Safe or Dangerous depending on application and direction of drift	None	None
Output fault that may prevent response to changes such as stuck at valid in range analog level or slow drift	Dangerous	None	None

6

Metodyka zgodna z IEC 61508
Analiza wyników *FMEA*

Functional Safety

FMEA (FAILURE MODE AND EFFECT ANALYSIS)
- *Identify critical or hazardous conditions.*
- *Identify potential failure modes*
- *Identify need for fault detection.*
- *Identify effects of the failures.*

IEC 61508
- nie wymaga aby 100% uszkodzeń niebezpiecznych (*dangerous*) było wykrywane
- wymaga obliczenia/oszacowania współczynnika uszkodzeń niebezpiecznych
- wymaga obliczenia/oszacowania współczynnika uszkodzeń niebezpiecznych wykrywalnych i niewykrywalnych (*dangerous detected / dangerous undetected*) -> prowadzi to do analizy FMEDA

Metodyka zgodna z IEC 61508
Analiza wyników *FMEA*
http://fmea-fmeca.com/

Functional Safety

FMEA - FMECA
Your Guide for FMEA Information and Resources

Failure Mode and Effects Analysis

What is a FMEA?
Learn what a FMEA is and some of the lingo, along with some good background and history on FMECA.

How to Perform a FMEA?
Covers the FMEA methodology and includes a nice infographic to help you visualize the process.

Design FMEAs
Learn how to apply FMEA to evaluate your design and identify potential flaws or safety hazards.

Types of FMEA
Learn about the different types and approaches to FMEA.

Key Benefits of FMECA
Many companies are already reaping the benefits. Use FMECA to ensure safety, quality, and safeguard your reputation.

Process FMEAs
FMEA can also be used to analyze a process, such as manufacturing, assembly or hospital patient care.

FMEA Software and Tools
Don't skimp when it comes to FMEA software. Consider the long term costs and invest wisely.

FMEA Examples, Standards
Quickly come up to speed with this large selection of examples, templates, presentations and standards.

Functional FMEAs
Especially on large systems, a functional approach can save time and money with good results.

RPN
S x O x D
Risk Priority Number(RPN)
Used heavily in many industries to assess risk. Learn how to properly use it and avoid the pitfalls.

Criticality Analysis
Mil-Std-1629A approach for determining the criticality of failure effects.
$C_m = \beta \alpha \lambda_p t$

Best Place for FMEA
Find out the best place to focus your limited time and resources.

Metodyka zgodna z IEC 61508
Hardware Design

9.1 Requirements of IEC 61508

- Design and develop the hardware in the safety related system to meet the hardware safety requirements specification.

- The design shall meet the requirements for architectural constraints on hardware safety integrity.

- The design shall meet the requirements for quantifying the effect of random failures (Probability of failure on demand and probability of failure per hour).

- The design shall meet the requirements for systematic safety integrity.

- The design shall meet the requirements for system behavior on detection of a fault.

- The design shall meet the requirements for data communications processes if there are any safety critical communications in the design.

Metodyka zgodna z IEC 61508
Hardware Design

- Design mechanical parts / structures
- Design hardware circuits
- Select hardware components and ensure that they are de-rated so that they will not be overstressed
- Include measures in the design to protect against environmental stresses
- Inspect the hardware
- Design ASICs and programmable devices such as FPGAs using a hardware description language (HDL)
- Inspect the HDL code created for the ASIC/Programmable logic design
- Perform Module Testing on HDL modules
- Perform component FMEDA (Failure Modes Effects and Diagnostics Analysis)
- Perform Fault Injection Testing
- Perform qualitative and quantitative analysis on any safety critical data communications

Metodyka zgodna z IEC 61508
Components Selection/De-rating

De-rating is defined as 'a policy of deliberately under stressing components in order to provide increased reliability'. The selection of components of higher stress capability than is required for normal operation is an empirical but effective and well established method of reducing their failure rate;

Component Type	Parameter Derated	Derating Factor (%)
Resistor	Power	80%
Resistor Variable	Power	75%
Transistor	Power	75%
Diode	Voltage	50%
Diode Signal	Voltage	85%
IC Linear	Current	85%
IC Digital	Fan-out	80%
Thermistor	Power	50%
Capacitor	Voltage	75%
Transformer	Power	80%
Relays	Contact Current	50%
Switches	Contact Current	50%

Applied R&M Manual for Defence Systems Part C - R&M Related Techniques

IEC 61508
– typowy czynnik 67%

Metodyka zgodna z IEC 61508
Hardware ASIC PLD

Functional Safety

Device Validation Test Plan and Procedures
Device Architecture Definition
Detailed Device Design
- source code standard
- Defensive Programming Techniques
  (self check to find problems during run time)
- Modularisation
- Code inspection
- Module testing
- Functional testing
Design for Testability (SIL3 ASIC 99% stuck at faults must be detectable)

Metodyka zgodna z IEC 61508
Component FMEDA Failure Modes Effect and Diagnostics Analysis

1. BOM(Bill of Materials)
2. Schematics
3. Failure Rate Database

Metodyka zgodna z IEC 61508
Component FMEDA - definicje

- Failure Rate of the component (λ) – This information is provided by sources mentioned above or by the tool.

- Failure Modes of the component – This information is provided by the sources mentioned above or by the tool.

- Distribution of Failure Modes – This information categorizes the individual failure modes for a component by a percentage of all failures. The percentages must add up to 100% for all failure modes. This information is provided by sources mentioned above or by the tool.

- Effect of Failure – For each failure mode of a component, the effect on the overall product or assembly without taking into consideration any diagnostics or redundancy should be described.

- Diagnostics – Document the diagnostics that are planned or implemented that would detect this failure.

- Diagnostic Coverage (DC) – For each failure mode of a component, list the percentage of failures that should be detected by diagnostics. In many cases, the diagnostic coverage can be determined by tables A.1 through A.15 of IEC 61508 part 2. These tables state which failure modes must be detected for a given level of diagnostic coverage and the maximum diagnostic coverage achievable based on diagnostic technique. From these tables you can determine what level of diagnostic coverage is achieved by your diagnostics. The coverage is expressed in the standard as low, medium, or high which translates into 60%, 90% and 99% when filling out the DC value in the spreadsheet.

- Behavior – For each failure mode of a component, categorize the effect of the failure into one of the following categories:

  - Safe – (S) failure of an element / system that plays a part in implementing the safety function that:

    a. results in the spurious operation of the safety function to put the EUC into a safe state or maintain a safe state; or,

    b. increases the probability of the spurious operation of the safety function to put the EUC into a safe state or maintain a safe state.

  - Dangerous – (D) failure of an element / system that plays a part in implementing the safety function that:

    a. prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,

    b. decreases the probability that the safety function operates when required.

  - High – (H) failure that causes the output signal to go to the maximum output current (> 20mA for 4-20mA output) or output voltage. This may be considered safe or dangerous depending upon the application.

- Low – (L) a failure that causes the output signal to go to the minimum output current (< 4mA for 4-20mA output) or output voltage. This may be considered safe or dangerous depending on the application.

- Annunciation – (A) a failure that does not directly impact functional safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). This is considered a subset of the no effect failure.

- No effect – (#) a failure of a component that is part of the safety function but has no effect on the safety function or causes the output current or voltage to deviate by less than x% of the actual value (where x is the safety accuracy of the product).

- Not Part – (-) means that this component is not part of the safety function but is part of the circuit diagram and is listed for completeness.
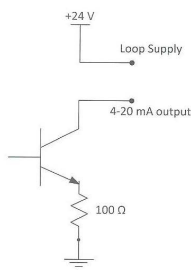
Metodyka zgodna z IEC 61508
Component FMEDA - definicje

Identyfikacja i klasyfikacja uszkodzeń SAFETYLON

Uszkodzenia niebezpieczne wykrywalne (Dangerous Detected - DD)

Uszkodzenia niebezpieczne niewykrywalne (Dangerous Undetected- DU)

Uszkodzenia nie powodujące zagrożenia (Safe - S)

Uszkodzenia niebezpieczne (Dangerous - D)

Uszkodzenia nie powodujące zagrożenia wykrywalne (Safe Detected - SD)

Wszystkie możliwe uszkodzenia

Uszkodzenia nie powodujące zagrożenia niewykrywalne (Safe Undetected - SU)

SafetyLon Training Workshop Moduł 3 – Podstawy bezpieczeństwa funkcjonalnego   © LMD&LUS&PLUG   Slajd nr 23

„Metodyki projektowania i modelowania systemów" Cyganek & Kasperek & Rajda © 2018 Katedra Elektroniki AGH

Metodyka zgodna z IEC 61508
Component FMEDA

Functional Safety

Trying is the first step towards failure.

+24 V

Loop Supply

4-20 mA output

100 Ω

Resistor general low power resistor 0.7 FITS (failures per 10^9 hours)

Figure 9.3 Simple 4-20 mA Output Circuit

Comp. Name	Component Description	λ	Failure Mode	Failure Mode Distribution	Effect of Failure	Diagnostic	DC	Behavior	λ_{DD}	λ_{DU}	λ_S	λ_H	λ_L	λ_A	λ_{NE}
R1	General Purpose Resistor, Low Power	0.7	Short	10%	Current > 20mA	None	0	High	0	0	0	0.07	0	0	0
			Open	60%	Current = 0mA	None	0	Low	0	0	0	0	0.42	0	0
			Reduced Resistance	15%	Increased Current	None	0	High	0	0	0	0.11		0	0
			Increased Resistance	15%	Decreased Current	None	0	Low	0	0	0	0	0.11	0	0
								Total	0	0	0	0.18	0.53	0	0

„Metodyki projektowania i modelowania systemów" Cyganek & Kasperek & Rajda © 2018 Katedra Elektroniki AGH

Metodyka zgodna z IEC 61508
Component FMEDA

Przykład dla mikrokontrolera

Component	Name	Qty	Failure Mode	Effect	λ	%λ	Distri bution	Funct. Failure Mode	DC	Beh avior
Microcontroller-Microprocessor	U100	1	Register, Internal RAM	Bad Output	1.0E-07	50%	15%	CPU	0.90	D
			ALU	Bad Output	1.0E-07	50%	60%	CPU	0.90	D
			Address Calculation	Bad Output	1.0E-07	50%	15%	CPU	0.90	D
			Program Counter, Stack Pointer	Bad Output	1.0E-07	50%	5%	CPU	0.90	D
			Interrupt Handling	Bad Output	1.0E-07	50%	5%	CPU	0.90	D
Microcontroller – On board RAM	U100	1	Safe Failures	None	1.0E-07	20%	50%	RAM	0.90	S
			Dangerous Failures	Bad Output	1.0E-07	20%	50%	RAM	0.90	D
Microcontroller – On board ROM	U100	1	Safe Failures	None	1.0E-07	20%	50%	ROM	0.99	S
			Dangerous Failures	Bad Output	1.0E-07	20%	50%	ROM	0.99	D
I/O	U100	1	"Stuck at" faults	Bad Output	1.0E-07	10%	15%	I/O	0.90	D
			Short Circuit between any 2 connections	Bad Output	1.0E-07	10%	15%	I/O	0.90	D
			Open circuit of any connection	Bad Output	1.0E-07	10%	15%	I/O	0.90	D
			Parasitic oscillation of outputs	Bad Output	1.0E-07	10%	15%	I/O	0.90	D
			Changing values (e.g. I/O voltage of analog device)	Bad Output	1.0E-07	10%	15%	I/O	0.90	D
			Functional Faults	Bad Output	1.0E-07	10%	25%	I/O	0.90	D

Metodyka zgodna z IEC 61508
Component FMEDA – przykłady baz danych

System Reliability Center
201 Mill Street
Rome, NY 13440-6916
888.722.8737
or 315.337.0900
Fax: 315.337.9932

Part Failure Mode Distributions

The following table summarizes a sampling of failure mode information collected by RAC.

Device Type	Failure Mode	α	Device Type	Failure Mode	α
Accumulator, Tank	Leaking	0.47	**Antenna**	No Transmission	0.54
	Seized	0.23		Signal Leakage	0.21
	Worn	0.20		Spurious Transmission	0.25
	Contaminated	0.10			
Actuator	Spurious Position Change	0.36	**Battery, Lithium**	Degraded Output	0.78
	Binding	0.27		Startup Delay	0.14
	Leaking	0.22		Short	0.06
	Seized	0.15		Open	0.02
Alarm, Annunciator	False Indication	0.48	**Battery, Lead Acid**	Degraded Output	0.70
	Failure to Operate on Demand	0.29		Short	0.20
	Spurious Operation	0.18		Intermittent Output	0.10
	Degraded Alarm	0.05			
Battery, Rechargeable, Ni-Cd	Degraded Output	0.72	**Capacitor, Tantalum**	Short	0.57
	No Output	0.28		Open	0.32
				Change in Value	0.11
Bearing	Binding/Sticking	0.50	**Capacitor, Tantalum, Electrolytic**	Short	0.69
	Excessive Play	0.43		Open	0.17
	Contaminated	0.07		Change in Value	0.14

Metodyka zgodna z IEC 61508
Component FMEDA – przykłady baz danych

SIEMENS

SIEMENS NORM
SN
29500-9

Ausgabe / Edition 2005-11

ICS 31.020
Deskriptoren: Ausfallrate, Bauelement, Erwartungswert, Schalter — Ersatz für Ausgabe 1992-04
Descriptors: Failure rate, component, expected value, switch — Supersedes Edition 1992-04

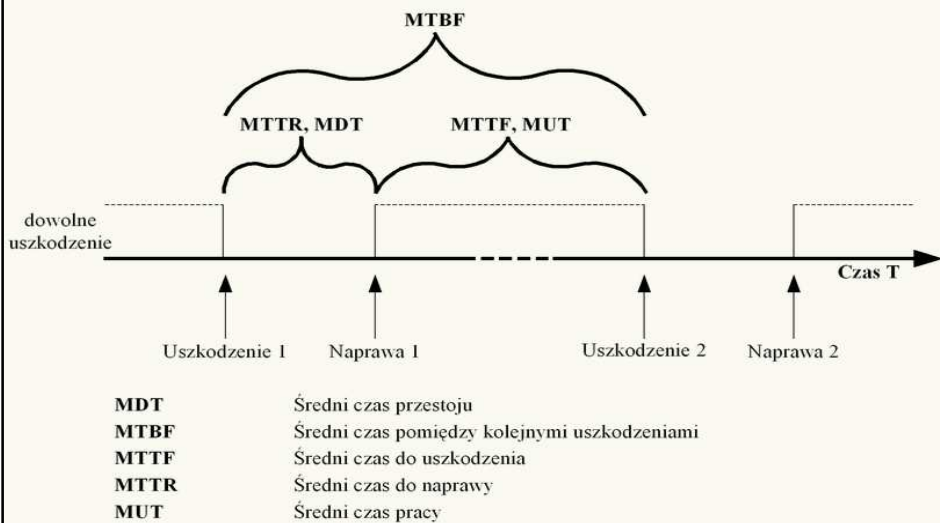...onents

Part 9: Expected values for switches and buttons

	Ausfallrate pro beschaltetem Durchgang / *Failure rate per connected continuity* λ_{rel} in FIT [1] [2]
Dipfix-Schalter/ *Dipfix switch*	0,3
Codierschalter/ *Encoding switch*	1
Folientaste/ *Membrane key*	20
Schalter und Tasten für Schwachstromanwendungen Kontaktkraft: > 20 cN Kontaktwerkstoff: Edelmetalle und deren Legierungen (ausgenommen reines ungeschütztes Ag) *Switches and buttons for light-current applications* *Contact force: < 20 cN* *Contact material: noble metals and their alloys* *(except pure unprotected Ag)*	2
Schalter und Tasten für höhere elektrische Belastbarkeit Kontaktkraft: > 20 cN *Switches und buttons for higher electrical load* *Contact force > 20 cN*	4

1) FIT = 1×10⁻⁹ h⁻¹; (Anzahl der Ausfälle pro 10⁹ Bauelementestunden) / *1 FIT equals one failure in 10⁹ components hours*
2) Bei Schaltern und Tasten mit Leuchtelementen ist die Ausfallrate für diese Leuchtelemente getrennt zu berücksichtigen./ *For switches and buttons with illuminating elements, the failure rate for the illuminating elements has to be taken into account*

Metodyka zgodna z IEC 61508
Wyniki *FMEA*

MDT	Średni czas przestoju
MTBF	Średni czas pomiędzy kolejnymi uszkodzeniami
MTTF	Średni czas do uszkodzenia
MTTR	Średni czas do naprawy
MUT	Średni czas pracy

Metodyka zgodna z IEC 61508
Wyniki *FMEA*

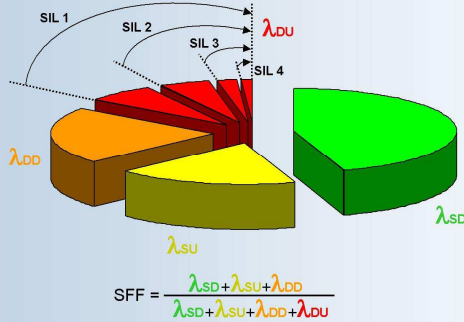*The Mean Time Between Failures (MTBF) is a statistical mean value for error-free operation of an electronic device*

Metodyka zgodna z IEC 61508
Wyniki *FMEA*
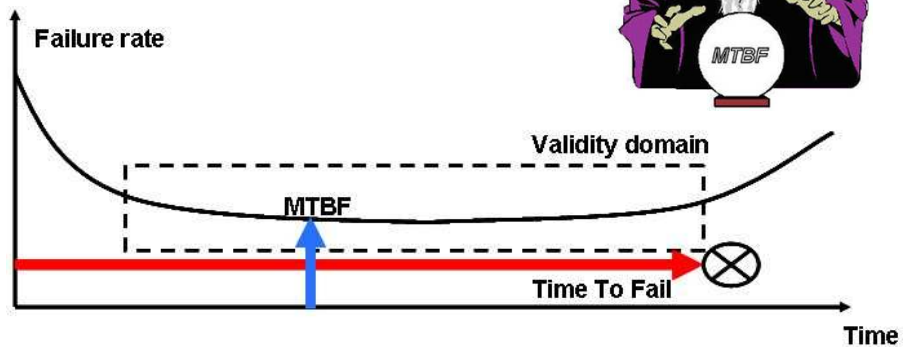
$$MTBF = \frac{1}{\sum_{i=1}^{n} \lambda_n}$$

MTBF= T/R where T = total time and R = number of failures

Metodyka zgodna z IEC 61508
### Wyniki *FMEA*

Safe Failure Fraction: Safe failure fraction (SFF) is a relatively new term resulting from the IEC 61508 and IEC 61511 committees' work to quantify fault tolerance and establish the minimum level of redundancy required in a safety instrumented function. Per IEC, "Safe failure fraction is the ratio of the (total safe failure rate of a subsystem plus the dangerous detected failure rate of the subsystem) to the total failure rate of the subsystem."

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

Types of random hardware failures:
- *Safe undetected (SU);*
- *Safe detected (SD);*
- *Dangerous detected (DU);*
- *Dangerous undetected (DD).*

Metodyka zgodna z IEC 61508
Hardware – data communication

Transmission Error	Definition	Detection Method
Repetition	Due to an error of a bus participant, old, non-up-to-date messages are repeated at an incorrect point in time. This may cause a dangerous situation in a receiver (e.g. access door closed although it is already open).	Sequence Number and Timestamp
Deletion	Due to an error of a bus participant, a message is deleted (e.g. request for safe stop).	Sequence Number
Insertion	Due to an error of a bus participant, a message is inserted. (e.g. release of a safe stop)	Sequence Number, Source and Destination Identifier, Feedback Message, and Identification Procedure.
Re-sequencing	Due to an error of a bus participant, the sequence of messages is changed. Example: Before going to a safe stop, a safe reduced speed is to be selected. If the messages are swapped, the machine is running instead of going to a safe stop.	Sequence Number and Timestamp
Corruption	Due to an error of a bus participant, or due to errors on the transmission medium, messages are corrupted.	Safety Code (CRC) and Cryptographic Techniques
Delay	1. The transmission line is overloaded by the data exchange that occurs during normal operation. 2. A bus participant causes overload by sending incorrect messages so that a service associated with a message is delayed or impeded.	Timestamp and Timeout
Masquerade	Due to an error of a bus participant, safety relevant and non-safety relevant messages get mixed up.	Feedback Message, Identification Procedure, and Cryptographic Techniques
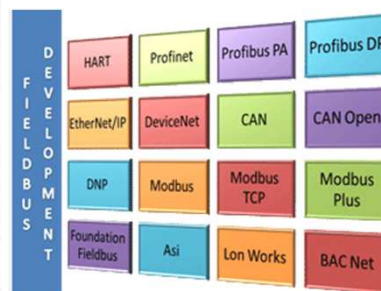
Metodyka zgodna z IEC 61508
Software

10.1 Requirements from IEC 61508

- Create a software architecture that fulfills the software safety requirements

- Select a suitable set of tools to be used in the development, verification and validation

- Design software such that it is verifiable and can be safely modified

- The design methodology shall address static and dynamic aspects of the design

- Design shall be documented using an unambiguous notation

- The design shall meet the requirements for systematic safety integrity.

- The design shall meet the requirements for system behavior on detection of a fault.

- The design shall meet the requirements for data communications processes if there are any safety critical communications in the design.

Metodyka zgodna z IEC 61508
Software Architecture

- Software Architecture Design
- Control Flow Strategy
  - Cyclic means that tasks are periodically executed in a set order. The tasks can be executed as fast as possible, or they can be executed at a constant rate (e.g. all tasks run every 100ms). A worst case cycle time should be defined and should be tied into the program flow control so that if it is ever exceeded the device annunciates an error or a watchdog reset occurs.
  - Time triggered means using a time triggered architecture [4]. In such an architecture, all ". . . activities are initiated based on the progression of a globally synchronized time base. Each application is assigned a fixed time slot on the time-triggered bus, which contains the messages exchanged between the jobs of each application which can therefore only be exchanged according to a defined schedule" [1], part 7, section C.3.11.
  - Event driven means that tasks are driven by arbitrary events at unpredictable points in time. If event driven triggering is used, a maximum response time to events must be established and either guaranteed by design, or diagnostics shall exist to annunciate an error or take action to move the system into a safe state.

- Safety integrity of all safety related data
- Memory allocation strategy
- Traceability

Metodyka zgodna z IEC 61508
Software Architecture Checklist

Functional Safety

Item	Comment / Initials
☐ Design has been partitioned into components and components are documented as to whether they are new, existing, or proprietary. For existing components, documentation is included as to whether they have been previously verified or not, and if so under what conditions.	
☐ Software/Hardware Interactions are specified	
☐ A notation is used to represent the architecture that is unambiguously defined	
☐ The design features for maintaining the safety integrity of data are documented	
☐ Control flow triggering is specified. One of following methods must be used: cyclic behavior with guaranteed maximum cycle time, time triggered architecture, or event driven with guaranteed maximum cycle time.	
☐ Memory allocation strategy is documented	
☐ Integration Tests are Documented	
☐ The design of software diagnostics is described. At a minimum there should be diagnostics on hardware, and on software control flow and data flow.	
☐ Structured Methods or semi-formal methods are used to create the design. Examples include Structured Analysis and Design, Data Flow Diagrams, State Transition Diagrams, Decision/Truth Tables, or Time Petri nets.	

„Metodyki projektowania i modelowania systemów" Cyganek & Kasperek & Rajda © 2018 Katedra Elektroniki AGH

Metodyka zgodna z IEC 61508
Software Architecture Checklist

Functional Safety

		Comment
☐	Computer Aided Specification Tools are used	
☐	The design of all software modules is included or referenced.	
☐	Consider whether the software architecture design description fulfills the specified software safety requirements.	
☐	The design is clear and easily understood by the development and verification team;	
☐	The required safety performance is feasible based on this design;	
☐	The design is testable for further verification	
☐	The design will support safe modification to permit further evolution	
☐	The detailed design fulfills the software architecture design (if detailed design is included in this document).	
☐	Data structures are verified for: • -completeness • -self consistency • -consistency with functional requirements	
☐	Verify all plant interfaces and associated software for detection of anticipated interface failures and tolerance to these failures.	

„Metodyki projektowania i modelowania systemów" Cyganek & Kasperek & Rajda © 2018 Katedra Elektroniki AGH

18

Metodyka zgodna z IEC 61508
Software Criticality and HAZOP

Zaawansowana inżynieria oprogramowania

Wprowadzenie do metody HAZOP

Jakie **odchylenia** mogą powstać?

Jak mogą wpłynąć na **bezpieczeństwo i operacyjność**?

Jakie **akcje** są konieczne?

Opis procesu

Systemy krytyczne i HAZOP (32)

Przypadek Therac-25

https://pl.wikipedia.org/wiki/Therac-25

Eksperci analizujący system zadają sobie następujące pytania:

1. Jakie odchylenia mogą powstać?
2. Jak mogą wpłynąć na bezpieczeństwo i operacyjność?
3. Jakie akcje są konieczne, aby temu zapobiec?

Koncepcja wykładu: **Jerzy Nawrocki**
Slajdy/Lektor/Montaż: **Łukasz Olek**

http://wazniak.mimuw.edu.pl/images/e/e9/Zio-11-wyk-bw.pdf

„Metodyki projektowania i modelowania systemów" Cyganek & Kasperek & Rajda © 2018 Katedra Elektroniki AGH

Metodyka zgodna z IEC 61508

Functional Safety

Pozostało:
- *Implementation*
- *Integration and Safety Validation Test Execution*
- *Modification Procedure*
- *Verification*

„Metodyki projektowania i modelowania systemów" Cyganek & Kasperek & Rajda © 2018 Katedra Elektroniki AGH