Kierunek Elektronika i Telekomunikacja,
Studia II stopnia
Specjalność: Systemy wbudowane

Metodyki projektowania i modelowania systemów

No to zaczynamy….

Wprowadzenie do systemów wbudowanych

- Analiza wymogów
- Założenia projektowe
- Przegląd architektur systemowych
- Podział projektu na część sprzętową i programową
- Implementacja / Integracja
- Zagadnienia bezpieczeństwa funkcjonalnego/ Klasyfikacje SIL.

Dokumentacja projektowa i produkcyjna systemów

- Analiza specyfikacji projektowej
- Dokumentacja przedprojektowa
- Dokumentacja ścieżki sprzętowej (edytor schematów, vault, zarządzanie listą komponentów)
- Dokumentacja ścieżki programowej (Doxygen, SVN)
- Dokumentacja produkcyjna i serwisowa;

Bezpieczeństwo funkcjonalne

http://www.iec.ch/functionalsafety/

Definicja z witryny UDT

„Bezpieczeństwo funkcjonalne rozumiane jako ogólne podejście do wszystkich działań w cyklu życia bezpieczeństwa systemów zawierających elektryczne i/lub elektroniczne i/lub programowalne elektroniczne elementy składowe”

Bezpieczeństwo funkcjonalne jest tylko częścią polityki bezpieczeństwa dla systemów

Bezpieczeństwo funkcjonalne dotyczy systemów aktywnych!

Bezpieczeństwo funkcjonalne[PN-EN 61508-4] to część bezpieczeństwa całkowitego odnosząca się do EUC (ang. *Equipment Under Control*) i systemu sterowania EUC, która zależy od prawidłowego działania systemów E/E/PE (system elektryczny/ elektroniczny/ programowalny elektroniczny) związanych z bezpieczeństwem, systemów związanych z bezpieczeństwem wykonanych w innych technikach i zewnętrznych środków do zmniejszania ryzyka.

IEC 61508 Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

EC 61508 is intended to be a basic functional safety standard applicable to all kinds of industry. It defines functional safety as: "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities."

Functional Safety and IEC 61508

http://www.iec.ch/functionalsafety/

IEC International Electrotechnical Commission

myIEC | Subscribe | Sitemap | FAQs | Contact us | Feedback

International Standards and Conformity Assessment for all electrical, electronic and related technologies

You & the IEC | About the IEC | News & views | Standards development | Conformity assessment | Members & experts | Developing countries | Webstore | Search... | Advanced search

About the IEC > What we do > Technology sectors > Functional Safety

IEC 61508

Functional Safety

IEC 61508 Explained

FAQ - Edition 2.0

FAQ - Edition 1.0

S+ IEC 61508 | IEC 61508 ed2.0 | IEC 61508 ed1.0

S+ IEC 61508

S+ IEC 61508 edition 2.0 Commented version (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

The CD contains parts 1 to 7 of IEC 61508 edition 2.0 published in April 2010, along with the S+ IEC 61508 Commented version of the entire series. All files are in PDF format.

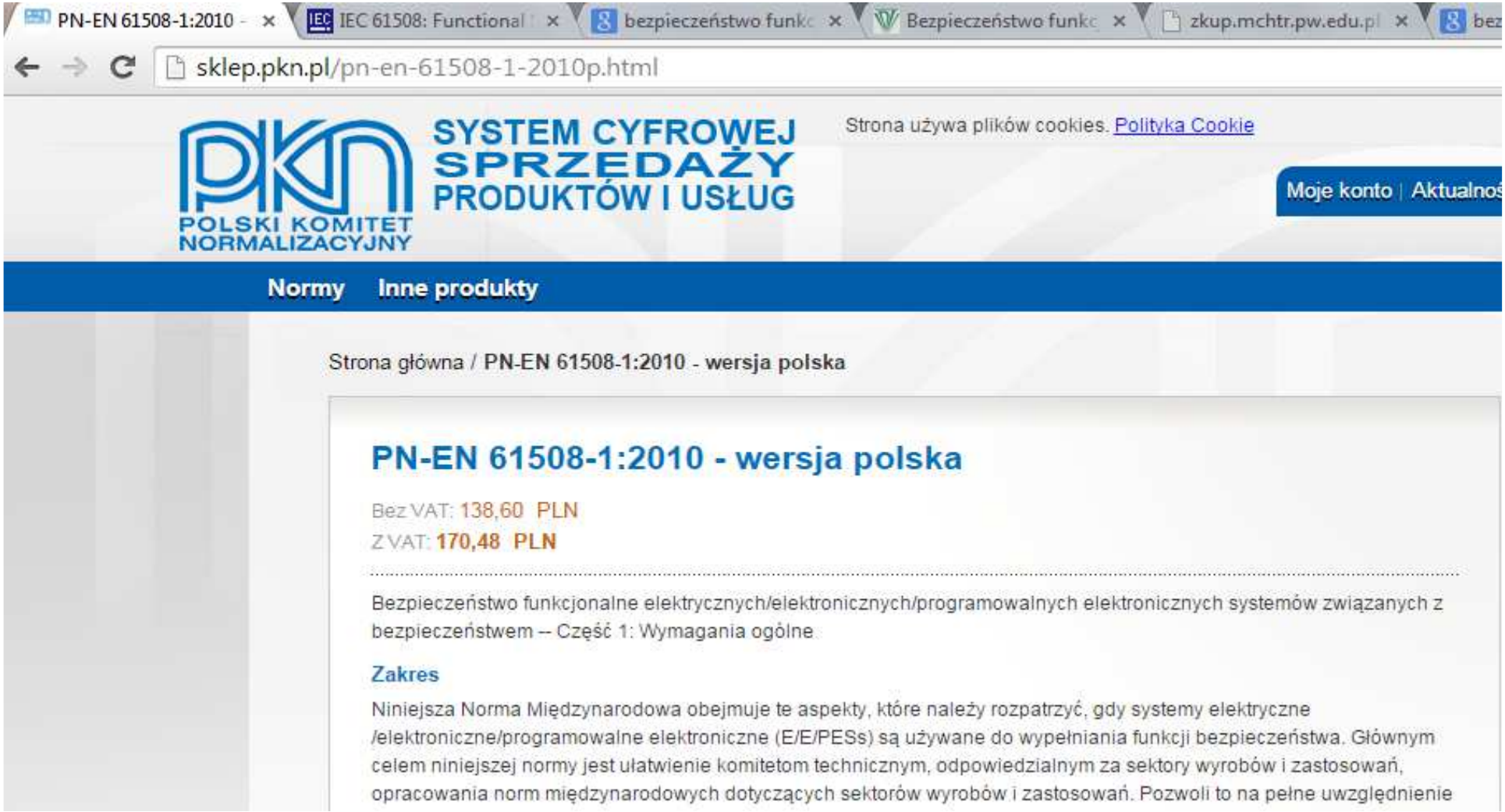
The S+ IEC 61508 single file is a compilation of the seven-part official IEC standard in English, enriched with the following information:

- track changes displayed in red, highlight all changes of the technical content made to edition 1.0

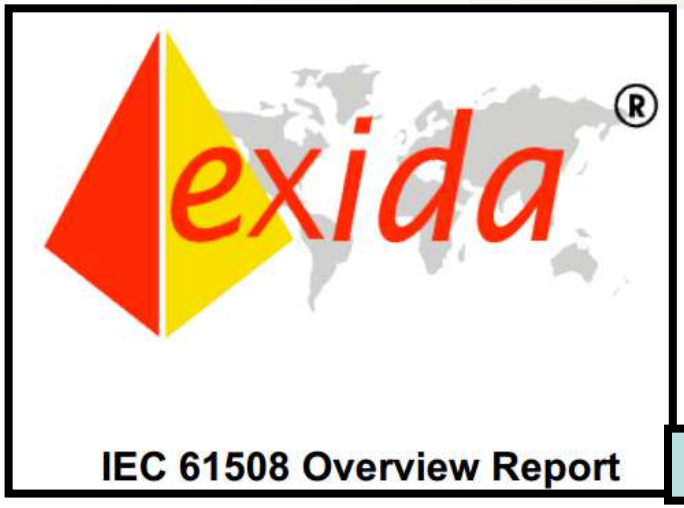
~3KCHF

IEC 61508 – gdzie kupić? jak czytać?

http://sklep.pkn.pl/



IEC 61508 – Baaaardzo dużo informacji w sieci



A Summary of the IEC 61508 Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

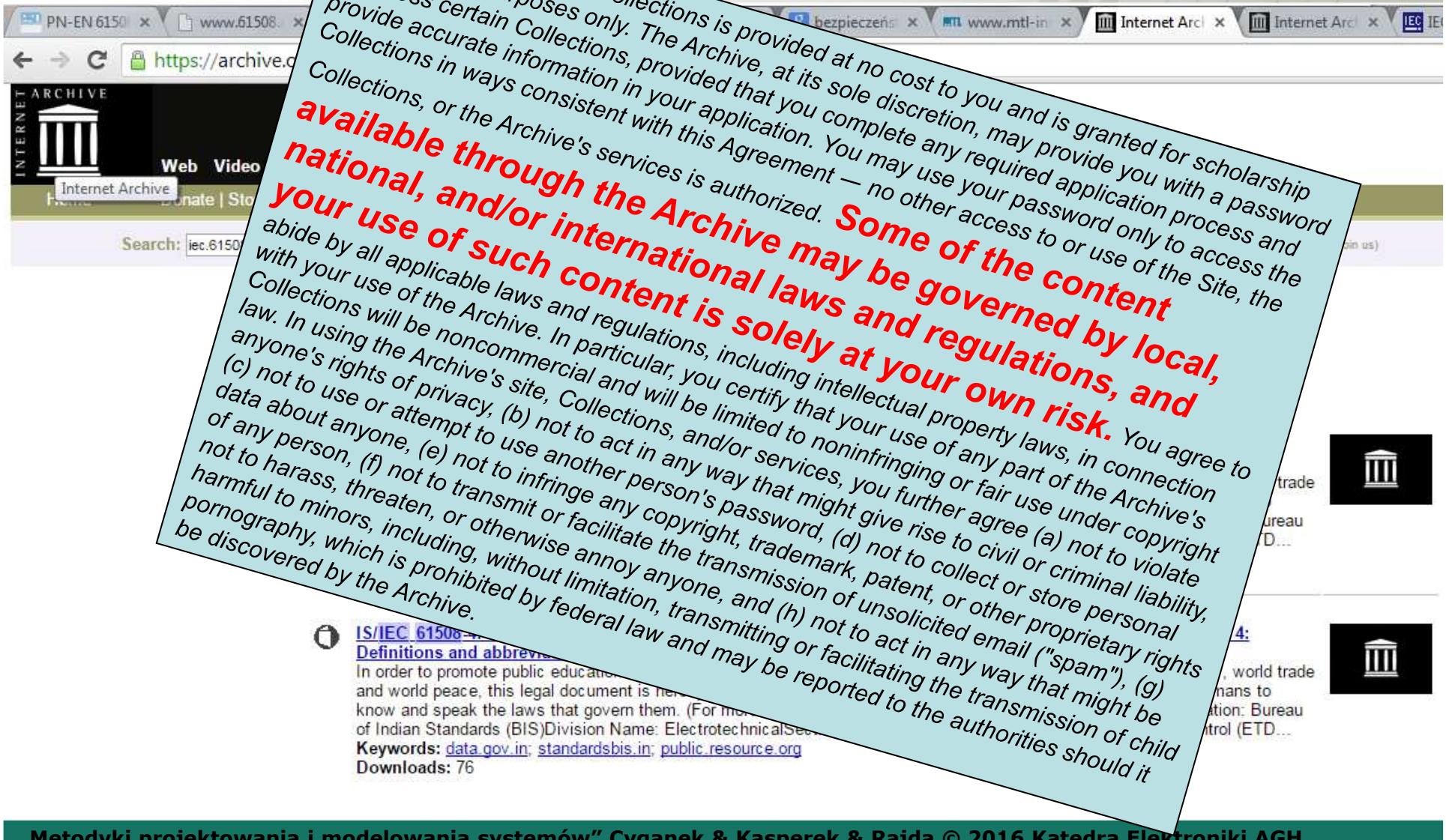
http://www.win.tue.nl/~mvdbrand/courses/sse/1213/iec61508_overview.pdf

https://www.youtube.com/watch?v=wve6_3oArmw

Systemy automatyki budynku realizujące funkcje bezpieczeństwa – struktury sprzętu

Marcin JACHIMSKI , Zbigniew MIKOŚ , Grzegorz WRÓBEL AGH Akademia Górniczo-Hutnicza, Katedra Energoelektroniki i Automatyki Systemów Przetwarzania Energii

IEC 61508 – Baaaardzo dużo informacji w sieci



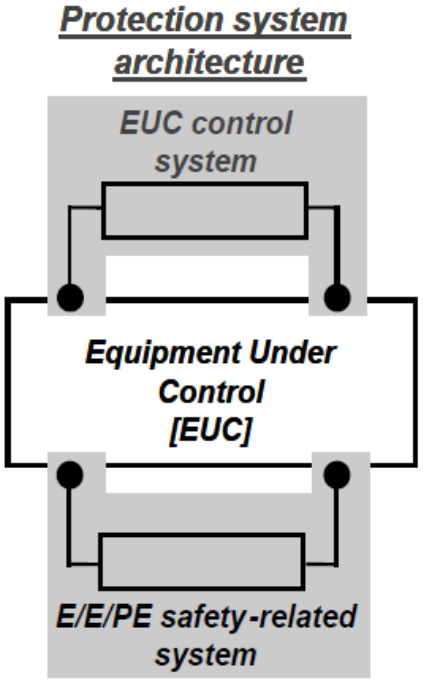
IEC 61508

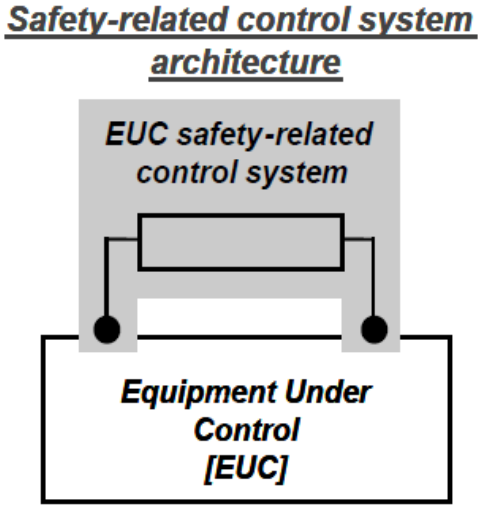
Bezpieczeństwo funkcjonalne związanych z bezpieczeństwem systemów elektrycznych/elektronicznych/programowalnych systemów elektronicznych

Na podstawie normy IEC 61508 definiowane są wymogi w stosunku do systemów bezpieczeństwa w zakresie bezpieczeństwa urządzeń niezależnie od zastosowania. Nie chodzi przy tym wyłącznie o harmonizację prawodawstwa krajowego z normami międzynarodowymi. Chodzi natomiast w większym stopniu o stosowane coraz częściej do zadań związanych z bezpieczeństwem urządzenia i czujniki wyposażone w mikroprocesory.

- Część 1: Wprowadza koncepcję bezpieczeństwa funkcjonalnego i prezentuje przegląd norm z rzędu IEC 61508.
- Część 2: Wymogi odnośnie do związanych z bezpieczeństwem systemów elektrycznych/elektronicznych/programowalnych systemów elektronicznych
- Część 3: Wymogi dotyczące oprogramowania
- Część 4: Pojęcia i skróty
- Część 5: Przykłady ustalania stopnia nienaruszalności bezpieczeństwa
- Część 6: Dyrektywa wykonawcza do cz. 2 i 3
- Część 7: Wskazówki wykonawcze dot. procedur i sposobów postępowania

Bezpieczeństwo funkcjonalne –definicje za IEC 61508





Funkcja bezpieczeństwa to funkcja do zaimplementowania przez system E/E/PE związany z bezpieczeństwem, system związany z bezpieczeństwem wykonany w innej technice lub zewnętrzne urządzenie do zmniejszania ryzyka, którego przeznaczeniem jest osiągnięcie lub utrzymanie stanu bezpiecznego EUC, w odniesieniu do konkretnego zdarzenia zagrażającego

Nienaruszalność bezpieczeństwa to prawdopodobieństwo, że system związany z bezpieczeństwem wykona właściwie wymagane funkcje bezpieczeństwa w określonych warunkach i w określonym przedziale czasowym.

Poziom nienaruszalności bezpieczeństwa (SIL) poziom dyskretny (jeden z czterech możliwych) do wyszczególnienia wymagań nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, które powinny być przypisane w systemach E/E/PE związanych z bezpieczeństwem, przy czym poziom nienaruszalności bezpieczeństwa 4 jest poziomem najwyższym, a poziom nienaruszalności bezpieczeństwa 1 poziomem najniższym.

Poziom nienaruszalności bezpieczeństwa (SIL *Safety Integrity Level*)

Poziom nienaruszalności bezpieczeństwa	Rodzaj pracy na rzadkie przywołanie(średnie prawdopodobieństwo uszkodzenia wykonania jego zaprojektowanej funkcji na żądanie)	Rodzaj pracy na częste przywołanie lub ciągły (prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę)
4	od $\geq 10^{-5}$ do $<10^{-4}$	od $\geq 10^{-9}$ do $<10^{-8}$
3	od $\geq 10^{-4}$ do $<10^{-3}$	od $\geq 10^{-8}$ do $<10^{-7}$
2	od $\geq 10^{-3}$ do $<10^{-2}$	od $\geq 10^{-7}$ do $<10^{-6}$
1	od $\geq 10^{-5}$ do $<10^{-1}$	od $\geq 10^{-6}$ do $<10^{-5}$

Bezpieczeństwo funkcjonalne – awers i rewers
Pomiary Automatyka Robotyka 1/2008
prof. dr inż. Tadeusz Missala
Przemysłowy Instytut Automatyki i Pomiarów, Warszawa

Rodzaj pracy	Typ systemu związanego z bezpieczeństwem	
	Sterowanie	Ochrona
Na rzadkie przywołanie	Wymaga się, aby system sterowania pracował w krótkich odstępach czasu, np. ABS.	Systemy ochronne, których liczba zadziałań jest mała w porównaniu z liczbą testów sprawdzających (np. system odcięcia instalacji chemicznej)
Ciągły/na częste przywołanie	Wymaga się, aby system pracował mniej lub więcej ciągle w długich przedziałach czasu, np. stymulator pracy serca.	Systemy ochronne, których liczba zadziałań jest duża w porównaniu z liczbą testów sprawdzających (np. fotoelektryczny system ochrony maszyny)

Poziom nienaruszalności bezpieczeństwa (SIL *Safety Integrity Level*)

Risk graph according to IEC 61508/61511

		W3	W2	W1
C1		–	–	–
C2	P1	SIL 1	–	–
	P2	SIL 1	SIL 1	–
	P1	SIL 2	SIL 1	SIL 1
	P2	SIL 3	SIL 2	SIL 1
C3	F1	SIL 3	SIL 3	SIL 2
	F2	SIL 4[1)]	SIL 3	SIL 3
C4		–	SIL 4[1)]	SIL 3

Consequences
- **C1** minor injury
- **C2** serious permanent injury to one or more persons; death of one person.
- **C3** death of several persons
- **C4** very many people killed

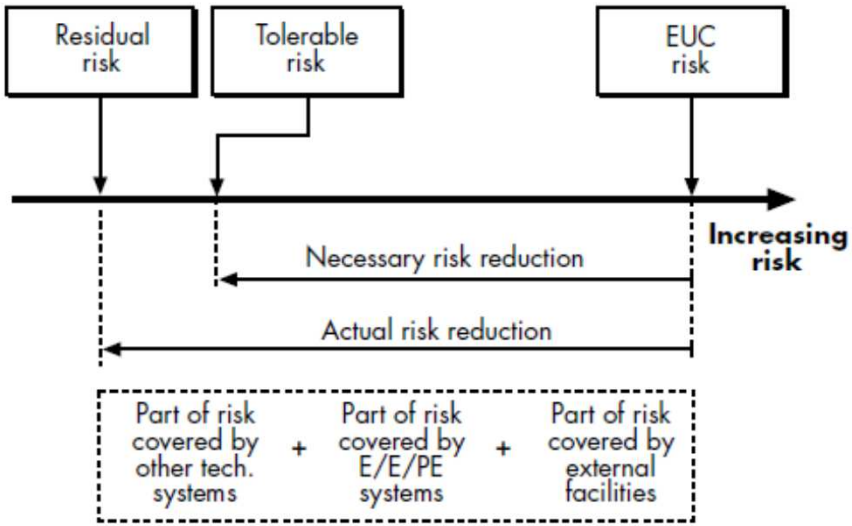
Exposure time
- **F1** rare to more often
- **F2** frequent to permanent

Avoidance of hazard
- **P1** possible under certain circumstances
- **P2** almost impossible

Probability of unwanted occurance
- **W1** very slight
- **W2** slight
- **W3** relatively high

Analiza ryzyka...

An introduction to Functional Safety and IEC 61508
AN9025
Members of The MTL Instruments Group plc



The development of safety functions, which embody the main principles of the standard, requires the following steps:

- *Identify and analyse the risks;*
- *Determine the tolerability of each risk;*
- *Determine the risk reduction necessary for each intolerable risk;*
- *Specify the safety requirements for each risk reduction, including their safety integrity levels (SILs);*
- *Design safety functions to meet the safety requirements;*
- *Implement the safety functions;*
- *Validate the safety functions.*

Analiza ryzyka...

Osiągnięcie wymaganego poziomu nienaruszalności bezpieczeństwa jest możliwe poprzez zwiększenie odporności sprzętu na awarie lub zwiększenie odsetka bezpiecznych uszkodzeń tego sprzętu (takich, które nie prowadzą do sytuacji niebezpiecznych) [15]. W PN-EN 61508 proponuje się różne techniki, których zastosowanie pozwala osiągnąć pożądany poziom SIL. Na przykład odsetek bezpiecznych uszkodzeń można zwiększyć poprzez zastosowanie technik zwiększających prawdopodobieństwo wykrycia uszkodzeń i ich prawidłową obsługę (takich jak np. diagnostyka). Inną techniką jest zastosowanie sprzętu na tyle niezawodnego, że spełniającego określone wcześniej wymogi nienaruszalności bezpieczeństwa. Jeszcze inną techniką jest zastosowanie sprzętu odpornego na wewnętrzne awarie, co oznacza, że zostaną podjęte dodatkowe środki (takie jak np. redundancja) w celu uniknięcia sytuacji niebezpiecznych nawet jeśli nastąpiło uszkodzenie. W przypadku zastosowania redundancji lub redundancji w połączeniu z diagnostyką, poszczególne struktury wielokanałowe wpływają w różny sposób na poziom bezpieczeństwa realizowanych funkcji, dostępność systemu oraz tolerancję uszkodzeń.

Systemy automatyki budynku realizujące funkcje bezpieczeństwa – struktury sprzętu
Marcin JACHIMSKI , Zbigniew MIKOŚ , Grzegorz WRÓBEL AGH Akademia Górniczo-Hutnicza, Katedra Energoelektroniki i Automatyki Systemów Przetwarzania Energii

Analiza ryzyka...

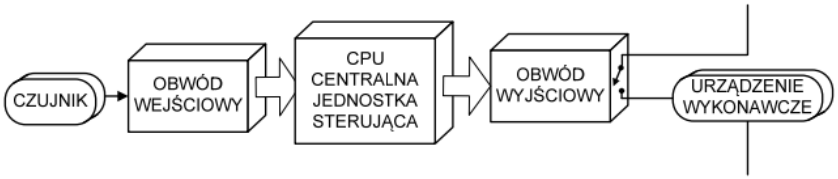
Nadmiarowe struktury wielokanałowe oznacza się kodem skrótowym MooN(D), który oznacza strukturę N kanałową o sposobie głosowania „M kanałów z N dostępnych". M oznacza liczbę sprawnych kanałów z pośród N dostępnych, która wystarcza do prawidłowej realizacji funkcji bezpieczeństwa. Opcjonalnie specyfikowana na końcu kodu skrótowego litera D oznacza kanały z diagnostyką.

Stosowane są następujące systemy:

- *1oo1 jedno wyjście z jednego,*
- *1oo2 jedno wyjście z dwu,*
- *2oo2 dwa wyjścia z dwu,*
- *2oo3 dwa wyjścia z trzech,*
- *1oo2D jedno wyjście z jednego z diagnostyką,*
- *1oo2D jedno wyjście z dwu z diagnostyką,*
- *2oo3D dwa wyjścia z trzech z diagnostyką.*

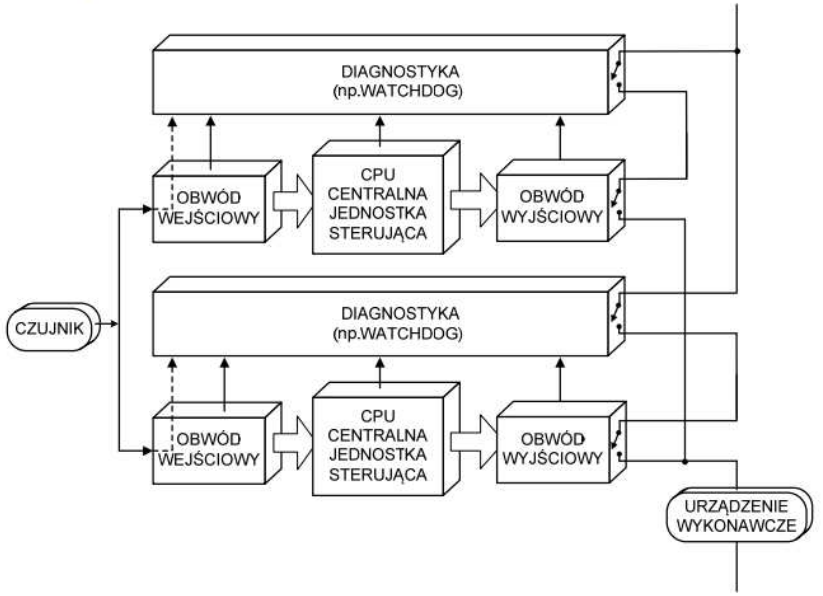
Analiza ryzyka...

Własności struktury jednokanałowej 1oo1:
- minimalna konfiguracja,
- brak dodatkowych środków bezpieczeństwa.



Rys. 4. Struktura jednokanałowa 1oo1

Własności struktury dwukanałowej z diagnostyką 2oo2D:
- budowa oparta na podstawie dwóch struktur 1oo1D,
- zwiększona dostępność.

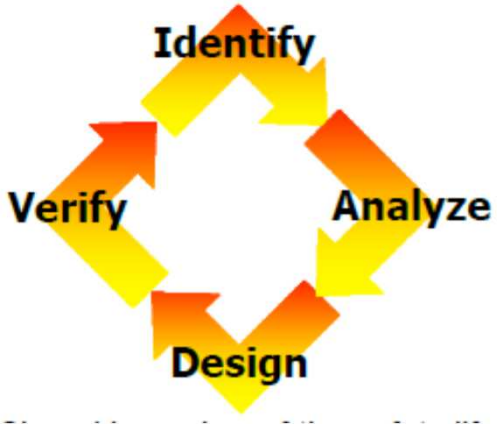


Rys. 9. Struktura dwukanałowa z diagnostyką 2oo2D

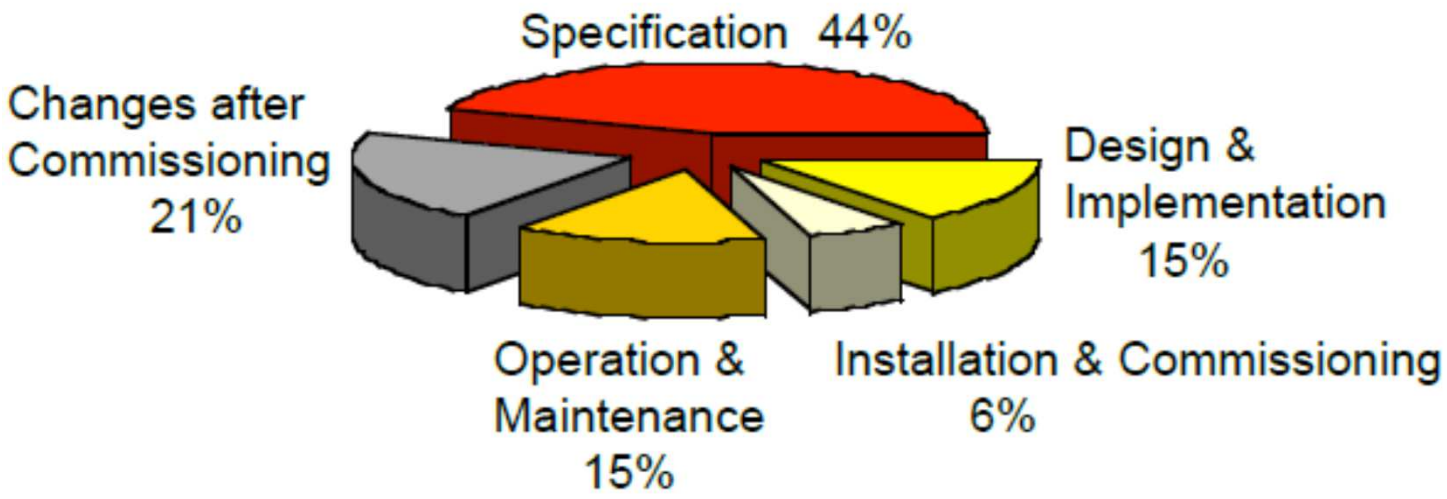
Systemy automatyki budynku realizujące funkcje bezpieczeństwa – struktury sprzętu

Marcin JACHIMSKI , Zbigniew MIKOŚ , Grzegorz WRÓBEL AGH Akademia Górniczo-Hutnicza, Katedra Energoelektroniki i Automatyki Systemów Przetwarzania Energii

IEC 61508 *Safety lifecycle*



Przyczyna wypadków



The safety life cycle concept came from studies done by the Health Safety Executive (HSE) in the United Kingdom. The HSE studied accidents involving industrial control systems and classified accident causes as shown above.

IEC 61508 *Functional Safety Assesment*

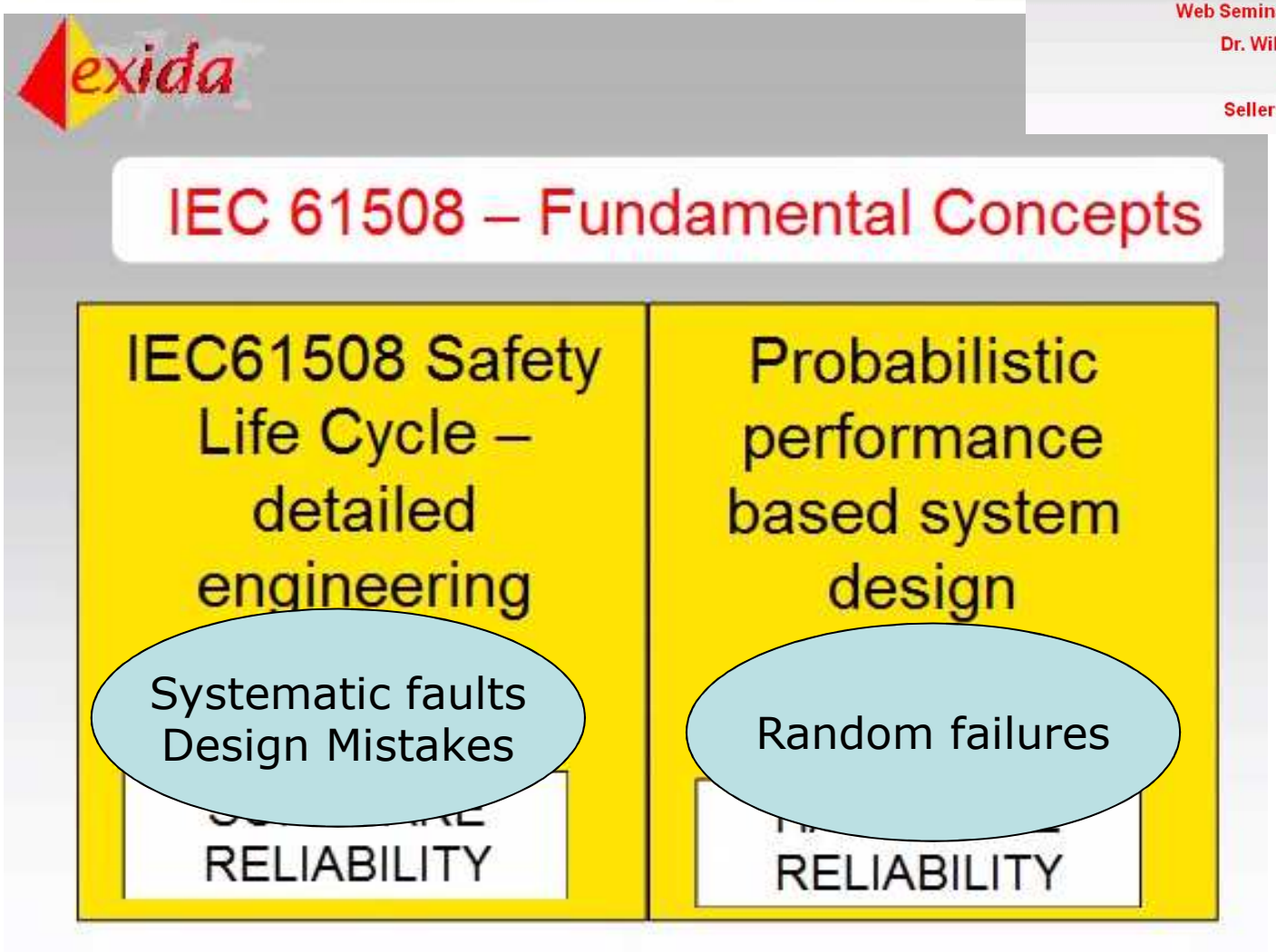
Minimum level of Independence	Consequence			
	A	B	C	D
Independent person	HR	HR[1]	NR	NR
Independent department	-	HR[2]	HR[1]	NR
Independent organization (see note 2 of 8.2.12)	-	-	HR[2]	HR
Typical consequences could be: Consequence A - minor injury (for example temporary loss of function); Consequence B - serious permanent injury to one or more persons, death to one person; Consequence C - death to several people; Consequence D - very many people killed. Abbreviations – HR - highly recommended, NR – not recommended				

Table 1: Assessment independence level as a function of consequence.

Minimum level of Independence	Safety integrity level			
	1	2	3	4
Independent person	HR	HR[1]	NR	NR
Independent department	-	HR[2]	HR[1]	NR
Independent organization	-	-	HR[2]	HR

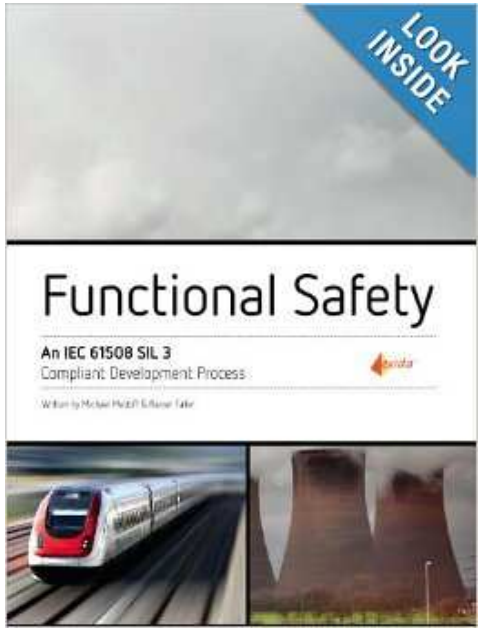
Table 2: Assessment independence level for E/E/PE and software life cycle activities.

IEC 61508 - koncept



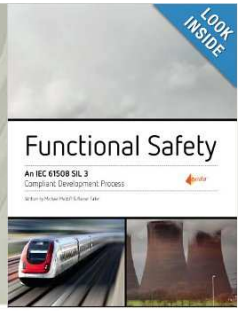
Metodyka zgodna z IEC 61508
Zagadnienia

- *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*
- *Verification*



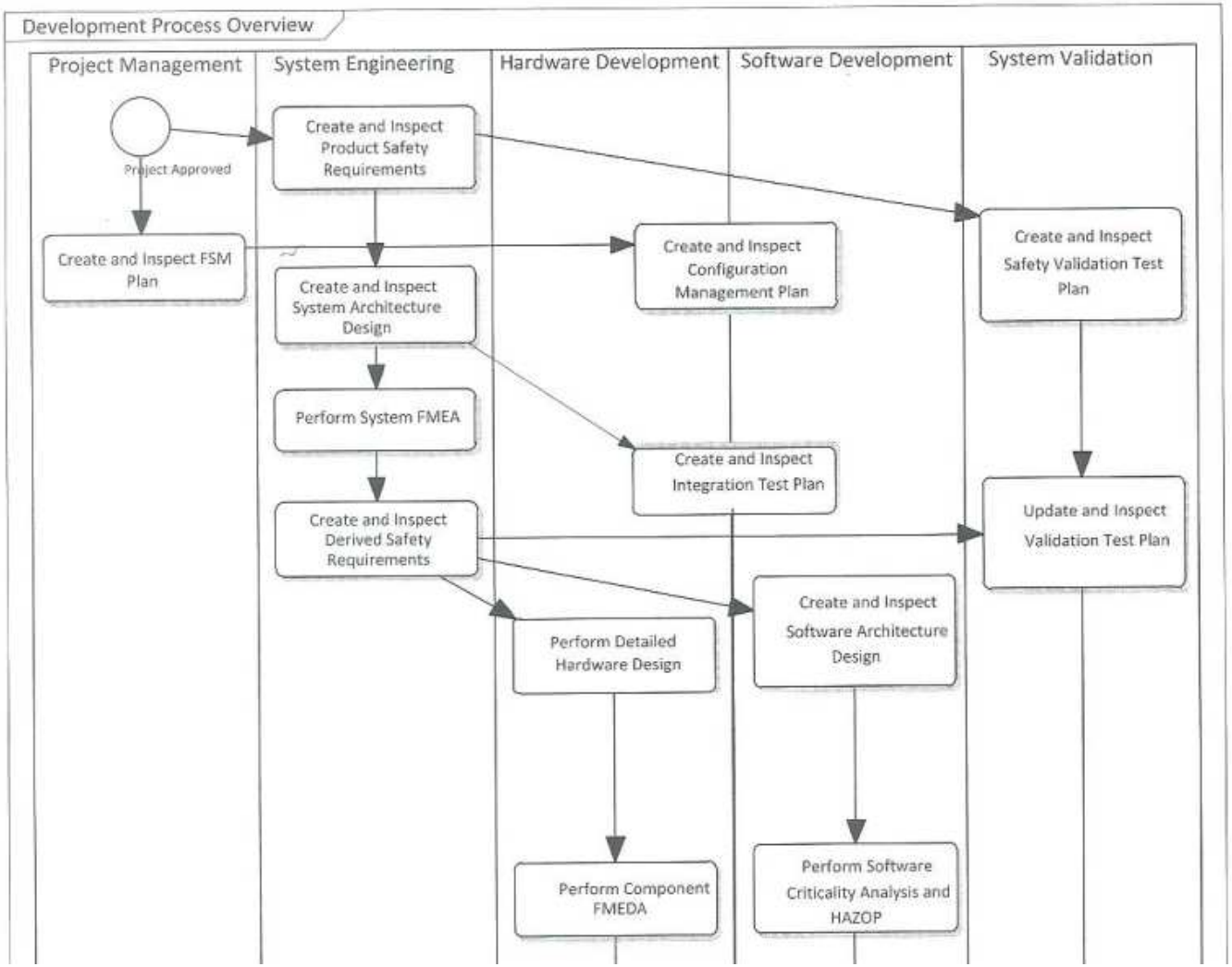
Functional Safety - An IEC 61508 SIL 3 Compliant Development Process
November 20, 2010
by Michael Medoff & Rainer Faller

Metodyka zgodna z IEC 61508
Development Process Overview

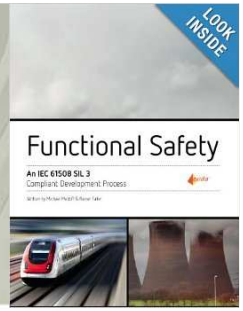


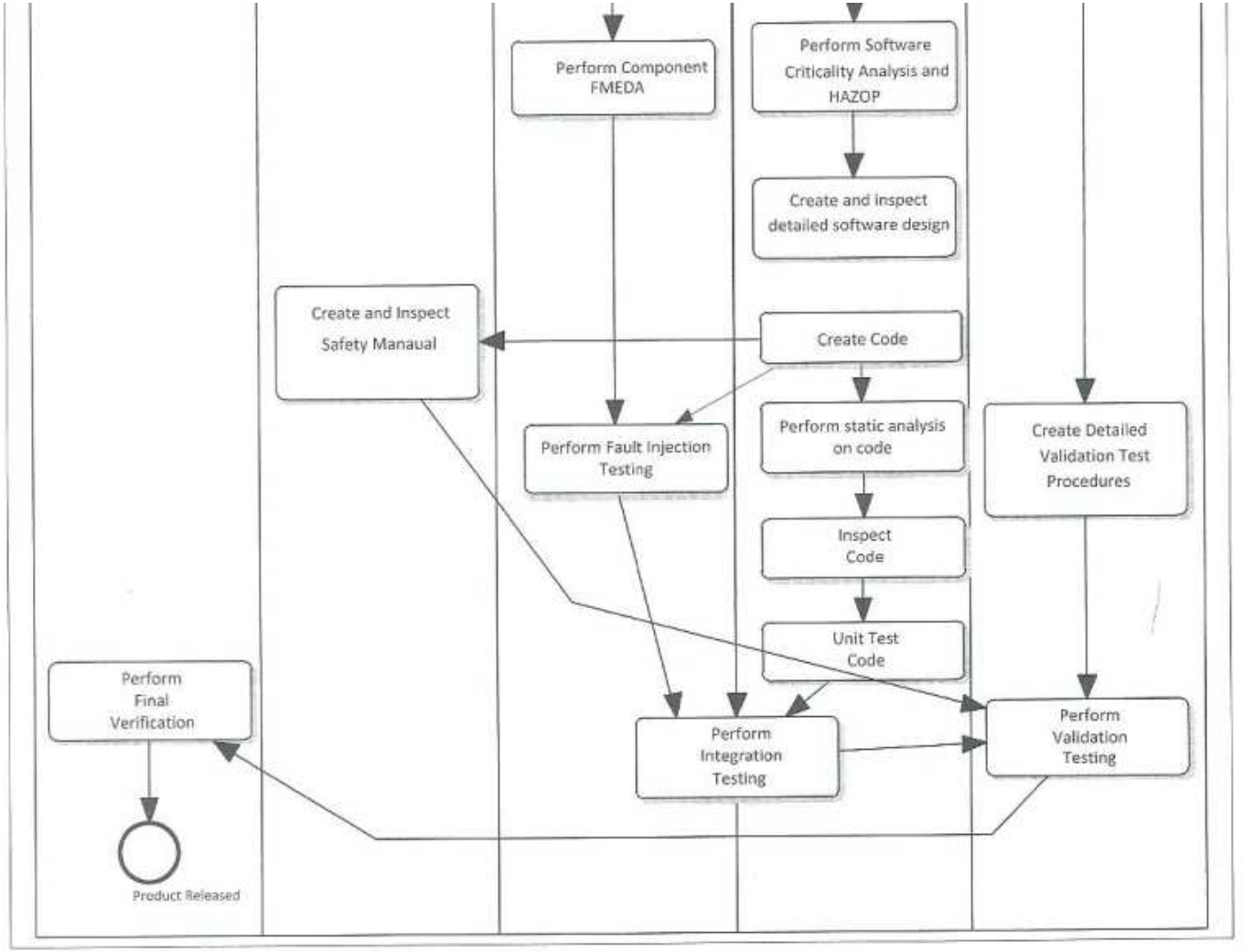
FMEA – Failure Mode and Effects Analysis

FMEDA – Failure Modes, Effects and Diagnostic Analysis

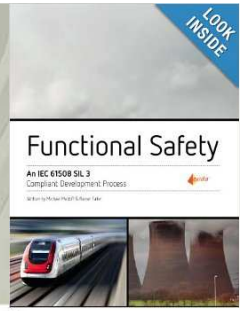


Metodyka zgodna z IEC 61508
Development Process Overview





Metodyka zgodna z IEC 61508
Development Process Overview



Phase	Process Steps in Phase
Safety Requirements	Create and Inspect Product Safety Requirements
Safety Validation Test Planning	Create and Inspect Safety Validation Test Plan.
System Architecture Design	• Create and inspect System Architecture Design • Perform System FMEA • Create and Inspect Derived Safety Requirements • Create and Inspect Integration Test Plan
Hardware Design	• Perform Detailed Hardware Design • Perform Hardware FMEDA • Perform Fault Injection Testing
Software Design	• Create and Inspect Software Architecture • Perform Software Criticality Analysis and HAZOP • Create and Inspect Detailed Software Design
Implementation	• Create Code • Perform Static Analysis • Inspect Code • Unit Test Code
Integration and Safety Validation Test Execution	• Perform Integration Testing • Perform Validation Testing

Metodyka zgodna z IEC 61508
Documentation

3.1 Requirements of IEC 61508

- Documentation shall be available to those who need it to perform specific duties defined by the standard.
- Documents shall have meaningful titles or names indicating the scope of the contents
- Documents shall have some form of index arrangements to allow ready access to the information required in the standard
- Documents shall have a revision attribute to make it possible to identify different revisions of the document
- Documents shall have a revision history to document what changed in each version
- Documents shall be structured to make it possible to search for relevant information
- All relevant documents shall be created, revised, amended, reviewed, and approved under the control of an appropriate document control system

Metodyka zgodna z IEC 61508
Documentation

The ideal DMS and associated process has the following requirements:

1. All official documents required for safety compliance are stored in the Document Management System (DMS). The DMS is a system used to organize, find, and store documents. The DMS shall have the following requirements:
    - The ability to store both electronic and paper documents
    - The ability to manage multiple versions of each document.
    - The ability to check out documents so that only one person can change the document at a time.

    The following desired attributes of the DMS are not required, but it is recommended that they be considered when choosing and DMS:
    - The ability to present the document structure in multiple, configurable hierarchies.
    - The ability to do a keyword search and a full text search on all electronic documents.
    - The ability to archive documents onto a secondary removable medium.
    - The ability to track approvals of a document.
    - Support for security which limits whom can access certain documents.

Metodyka zgodna z IEC 61508
Documentation

2. Not all information must be stored in documents. Some information, such as requirements, schematics and design models, may be stored in repositories of Computer Aided Software Engineering (CASE) tools. However, if access is limited to the repositories, then documents or reports must be generated from the tools so that everyone who requires the information has access to it. If important safety information is to be stored in a repository, this must be documented in the Functional Safety Management (FSM) plan.
3. All documents shall be stored electronically if possible.
4. All documents shall have a unique document number assigned to them. This number may be assigned by the DMS.
5. All documents shall have a unique document name assigned to them. This name should be chosen by the author.

Metodyka zgodna z IEC 61508
Documentation

6. All documents shall have a document type assigned to them. At a minimum, the following document types shall be supported:
    - Safety Requirements Specification
    - Functional Safety Management Plan
    - Safety Validation Plan
    - Configuration Management Plan
    - Safety Manual
    - Architecture design description
    - Detailed Design Specification
    - Development Tools and coding standards
    - Hardware Design Documents
    - Electronic Schematics
    - Software Design Documents
    - Source Code
    - Software System Integration Test Results
    - Programmable Electronics integration test results
    - Safety Validation Test Results
    - Impact Analysis Results

Metodyka zgodna z IEC 61508
Documentation

7. All documents shall be assigned to a project
8. All documents shall be assigned to a product or set of products
9. All documents shall have a standard template applied. This template consists of the following items:
    - Title page containing the following:
        - Company Name
        - Title of Document
        - Type of Document
        - Project Name
        - Product Name
        - Author(s)
        - Document Number
        - Revision Number
        - Date of Current Revision
        - Copyright information

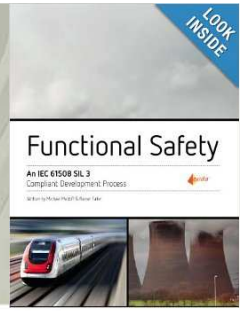
Metodyka zgodna z IEC 61508
Documentation

- Revision History Page containing the following
  - Revision History Table containing the following
    - Column for date of revision
    - Column for author of revision
    - Column for revision number defined as follows:
      - 0.x for any revisions prior to document approval
      - 1.0 for first approved version
      - 1.x for any minor revisions
      - Y.0 for any major revisions (Y = 2, 3, 4….)
    - Column for description of changes
    - Header Row
    - One Row for every revision.
- Table of Contents
- List of Required Reviewers and Approvers
- Body of document

Metodyka zgodna z IEC 61508
Documentation

10. Document Content
    - All standard document types shall have a template available that consists of the standard document template plus a document specific template. These templates will be listed in Appendix A of this document.
    - All documents shall include both graphical and natural language descriptions if appropriate.
    - All safety critical documents shall have a checklist at the end of the template that should be filled out prior to or during the document review.
11. Documents shall be organized so that it is easy to find and retrieve documents. It is desired that documents can be retrieved via multiple of the following mechanisms:
    - By knowing or entering document number
    - By knowing or entering document name
    - By entering part of a name, viewing all documents that match that name or part of name, and choosing a document from the list.
    - By viewing a list of projects, choosing a project, viewing all documents associated with that project, and choosing a document from that list.
    - By viewing a list of products, choosing a product, viewing all documents associated with that product, and choosing a document form that list
    - By viewing a list of all documents created or modified within a certain date range, and choosing a document from that list
    - By viewing all documents form a particular author, and choosing a document from that list
    - By viewing all documents of a particular type, and choosing a document from that list

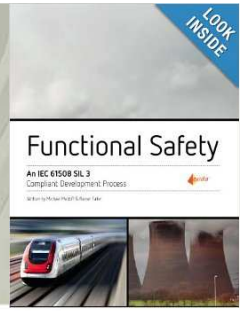
Metodyka zgodna z IEC 61508
Documentation



12. The document management system shall be available to everyone in the organization who needs to access the documents in order to perform their job. The document management system may limit access to documents so that each user can only access the documents they need in order to perform their job.
13. The document management system shall be completely backed up periodically. At least one backup should be stored on site and another backup should be stored off site. The backups should be updated periodically so that more recent documents are not lost in a disaster scenario.
14. Periodically or at least once per year, attempt to restore a system by using the backups. This will verify that the backups and backup process are working properly.

+Definicje procedur
- Tworzenie nowego dokumentu
- Wysłanie dokumentu do zatwierdzenia
- Zatwierdzanie dokumentu
- Zarządzanie zmianami wersji dokumentu

Metodyka zgodna z IEC 61508
Configuration Management



Configuration management applies throughout all phases of the development process and establishes how change is controlled and documented. It provides the means to build a product in a reliable and repeatable way. If your organization already has a configuration management procedure, you should compare the requirements from IEC 61508 to your procedure. Update your process as necessary to be compliant with IEC 61508.

4.1 Requirements of IEC 61508

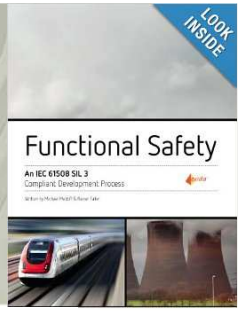
- Apply administrative and technical controls throughout the safety lifecycle in order to manage changes and thus ensure that the specified requirements for functional safety continue to be satisfied
- Guarantee that all necessary operations have been carried out to demonstrate that the required safety integrity has been achieved
- Maintain accurately and with unique identification all configuration items which are necessary to maintain the integrity of the E/E/PE safety-related system
- Apply change control procedures to prevent unauthorized modifications, to document modification requests, to analyze the impact of the proposed modification and to approve or reject the request
- Document configuration information to permit a subsequent audit
- Document and control the release of safety related software.
- Guarantee the composition and building of all product and/or software baselines (including the rebuilding of earlier baselines).

Metodyka zgodna z IEC 61508
Configuration Management

4.1.1 A Summation of the Requirements

- Identify and Control changes
- Ensure changes are being properly implemented
- Ensure changes are documented properly
- Ensure that changes are reported to those that may be impacted by the change
- Ensure that all configuration items are uniquely identified
- Guarantee that product can be built correctly in a repeatable way

Metodyka zgodna z IEC 61508
Configuration Management



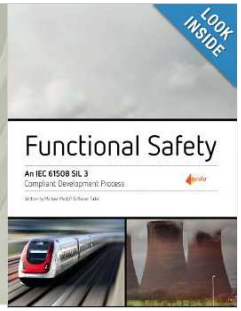
4.4 Version Control

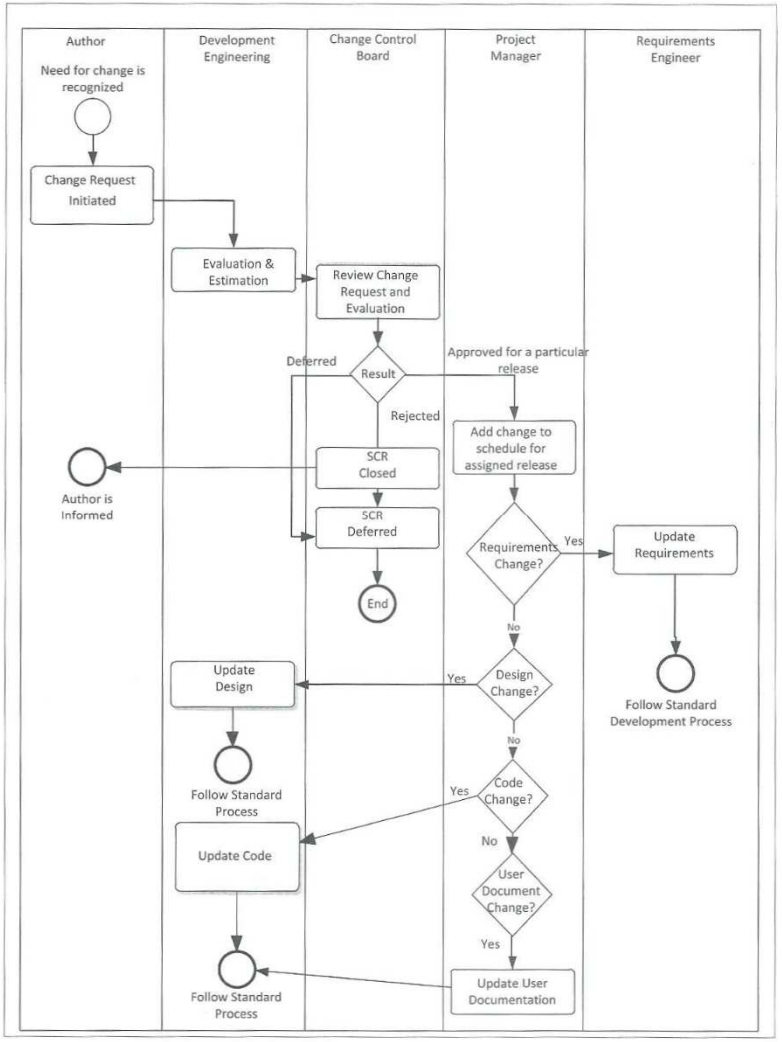
Version control manages the versions of a particular configuration item such that the following is achieved:

1. A new unique revision number is assigned to each item each time the item is changed.
2. Comments describing each change are required to be entered before submission of change.
3. Comments describing each change, date of change, author, and revision number can be extracted for every revision.
4. Every revision of electronically stored configuration items can be extracted in its original form.
5. Unauthorized access and modification to files is prevented.
6. A mechanism for locking electronically stored configuration items, forcing serialized change to any given file.
7. Allows for branches to be created which allow for parallel concurrent software development and the ability to later merge changes made by different people.

The version control system is usually the software that manages version control. Configuration items must be submitted to version control by the time they are made part of a baseline. However, configuration items can be submitted to version control prior to being part of a baseline. Submitting an item to version control alone does not make it subject to change control.

Metodyka zgodna z IEC 61508
Configuration Management





SCR – System Change Request

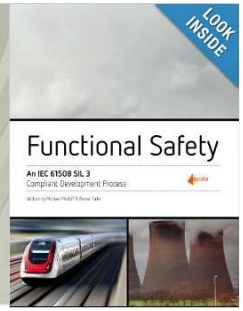
Type:
- New Feature
- New Product
- Fault
- Optimisation

Status:
- New
- Evaluation
- CBB review
- Approved
- Deffered
- Not a problem
- Complete
- Test
- Fixed
- Failed
- Feadback

Severity:
- High
- Medium
- Low

Priority:
- Urgent
- Blocking
- High
- Medium
- Low

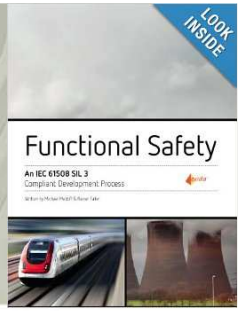
Metodyka zgodna z IEC 61508
Functional Safety Management



5.1 Requirements of IEC 61508

- Specify the activities to be carried out for all those who are involved in developing the product.
- Specify the responsibilities of all those who are involved in developing the product.
- Coordinate all safety related activities.
- Specify the policy and strategy for achieving functional safety
- Ensure prompt follow up and satisfactory resolution to action items.
- Ensure that all persons working on the project have the appropriate competence to carry out the duties that they have to perform.
- Ensure that all suppliers have an appropriate quality management system in place.

Metodyka zgodna z IEC 61508
Functional Safety Management



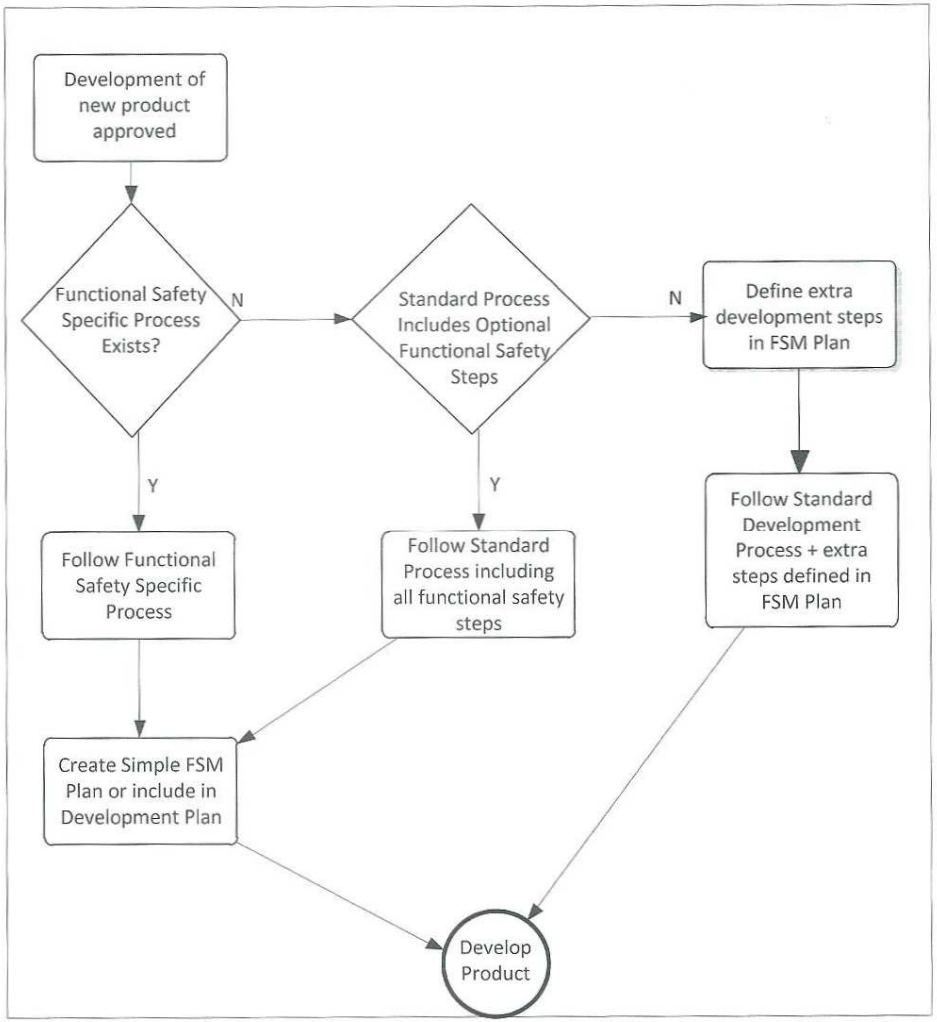


Figure 5.1 Three Possible Paths to Develop IEC 61508 Compliant Products

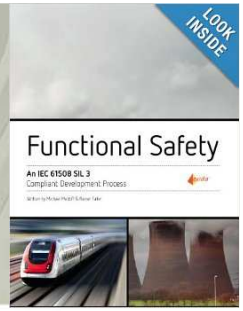
Role:

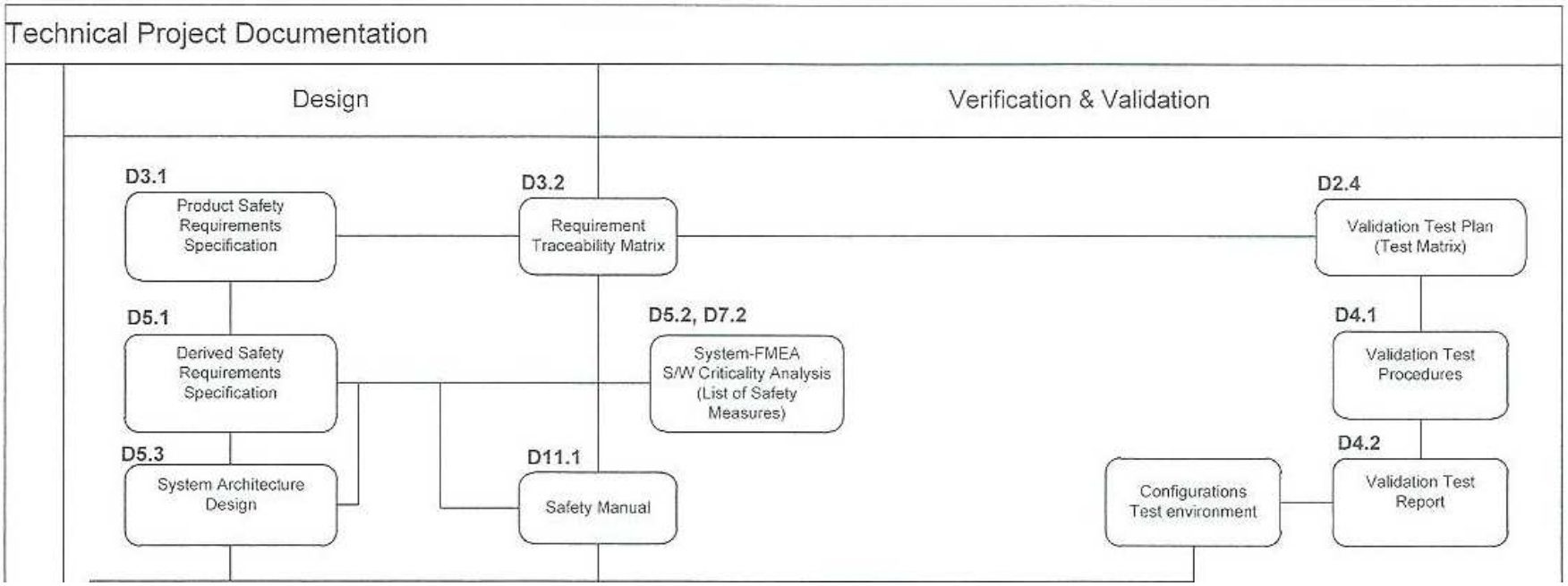
- *Product Manager (PrdM)*
- *Project Manager (PM)*
- *System Safety Architect (SSA)*
- *Functional Safety Cordinator (FSC)*
- *Test Team Leader (TTL)*
- *Internal Reviewers (IR)*
- *Quality Management (QM)*

i grupy

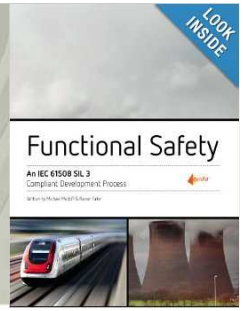
- *Product Release Board (PRB)*
- *Change Control Board (CCB)*

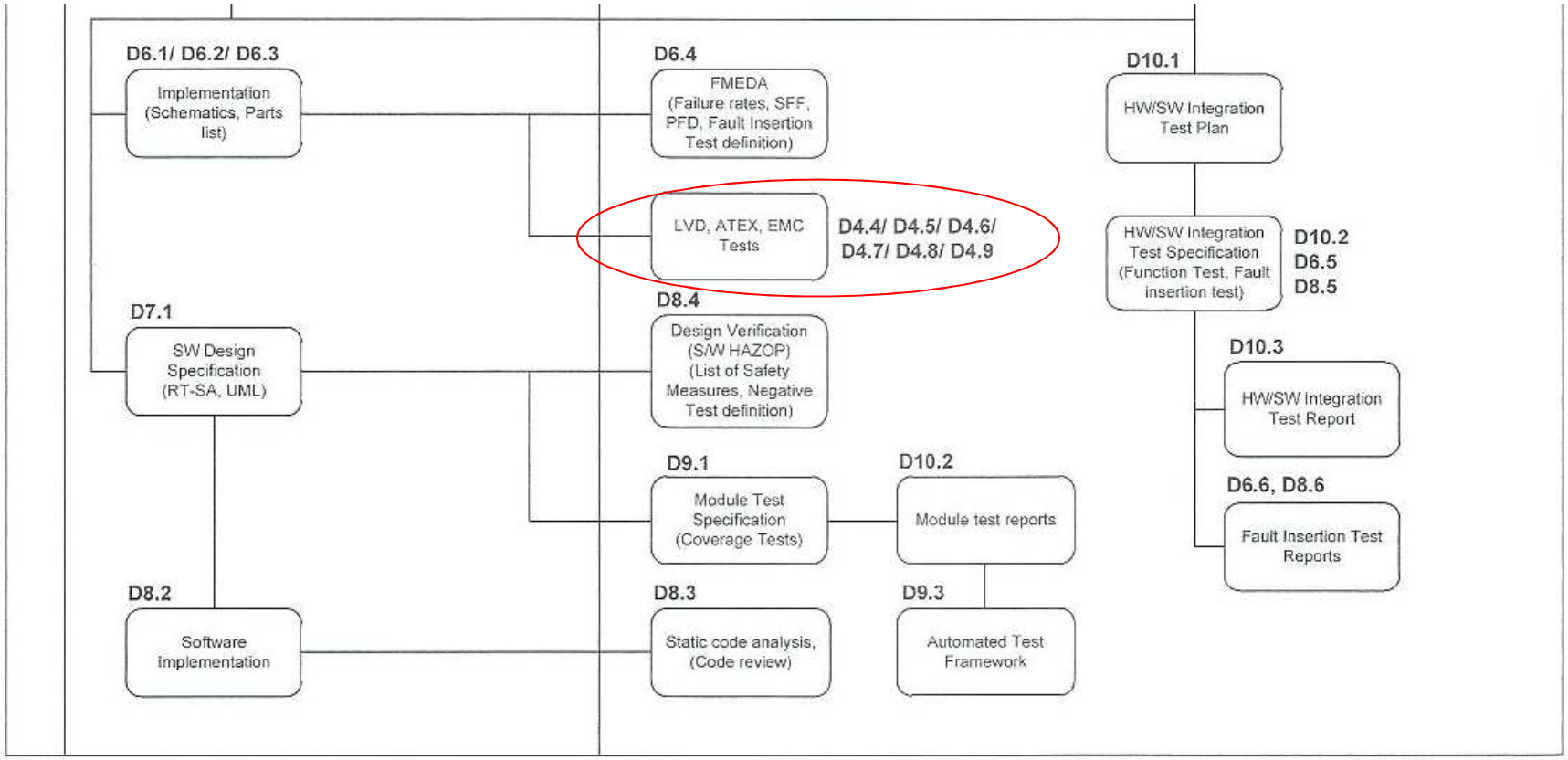
Metodyka zgodna z IEC 61508
Functional Safety Management



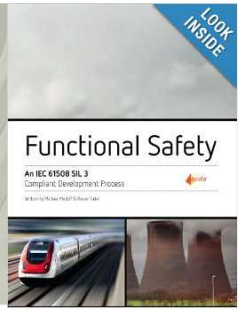


Metodyka zgodna z IEC 61508
Functional Safety Management





Metodyka zgodna z IEC 61508
Functional Safety Management



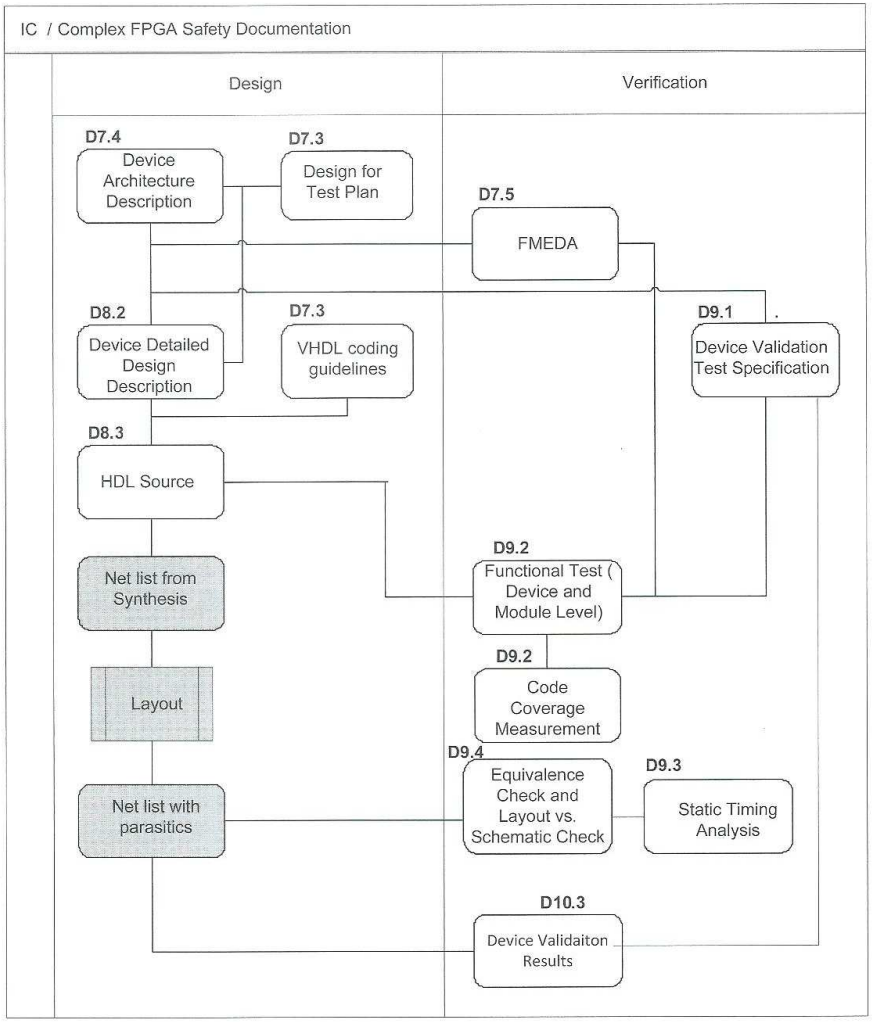
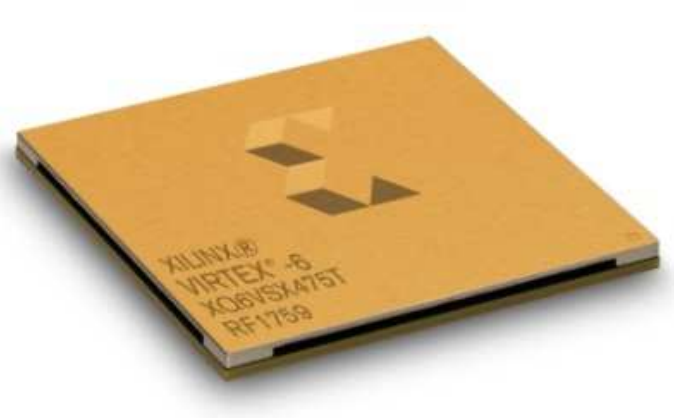
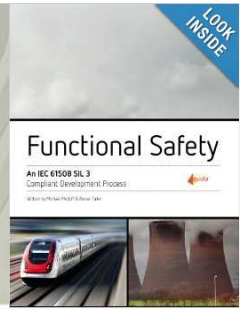


Figure 5.3 IC Safety Documentation



Przykładowy zestaw Dokumentujący układ FPGA

Metodyka zgodna z IEC 61508
Functional Safety Management



Input documents	
Doc id	**Name - Description**
D1.1	Market Specification – Defines customer and commercial goals
D1.2	System requirement specifications – Product specific requirements based on customer and commercial goals.

Output documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D3.1	Safety requirements spec. – Documents safety functions and safety integrity requirements	FSC, DM	PrdM	All

Verification documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D3.2	Safety requirements spec. Inspection report	FSC	PrdM	n/a
D3.3	Traceability between the product safety requirements and the perceived safety needs	FSC	PrdM	n/a
D3.4	Completed Safety Requirements Checklist	IR	PrdM	n/a

Dokumenty: *Create and Inspect Product Safety Requirements*

Metodyka zgodna z IEC 61508
Functional Safety Management

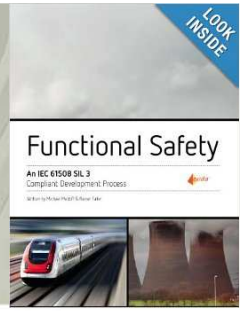
Input documents	
Doc id	**Name - Description**
D1.2	System requirement specification
D3.1	Safety requirements spec.

Output documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D2.4	(Validation) Test Plan – Plan showing how all requirements will be validated by documenting test objectives.	FSC	TL	DM, TL
D4.8	Environmental Stress and EMC / EMI Test specification	Test Team	TL	DM, TL

Verification documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D3.5	Safety Validation Plan Inspection Report	FSC	PrdM	n/a
D3.6	Forward Traceability from safety requirements to safety validation tests	FSC	PrdM	n/a
D3.7	Backward Traceability from safety validation tests to safety requirements	FSC	PrdM	n/a
D3.8	Completed Safety Validation Test Plan Checklist	IR	PrdM	n/a

Dokumenty: *Create and Inspect Safety Validation Test Plan*

Metodyka zgodna z IEC 61508
Functional Safety Management

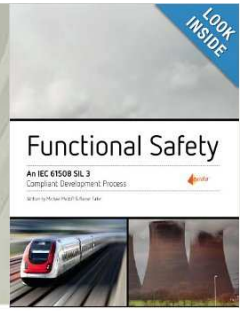


Input documents	
Doc id	**Name - Description**
D1.2	System requirement specification
D3.1	Safety requirements spec.
D5.1	System architecture description
D5.3	Derived Safety Requirements
D5.2	System-FMEA

Output documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D6.1	Circuit descriptions	Design team	HW sub-PM	All HW-dev
D6.2	Circuit diagrams	Design team	HW sub-PM	All HW-dev
D6.3	Layouts, part lists	Design team	HW sub-PM	All HW-dev
D6.4	Device Safety Requirements	Design team	HW sub-PM	All HW-dev
D9.1	Device Validation Test Plan and Procedures	Design team	HW sub-PM	All HW-dev
D7.4	Device Architecture Description	Design team	HW sub-PM	All HW-dev
D8.2	Device Detailed Design Description	Design team	HW sub-PM	All HW-dev
D8.3	HDL Source Code	Design team	HW sub-PM	All HW-dev

Dokumenty:
Detailed Hardware Design and Component FMEDA

Metodyka zgodna z IEC 61508
Functional Safety Management



Verification documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D6.4	Component FMEDA	Design team exida	HW sub-PM FSC	n/a
D6.5	Fault insertion test spec. – Test plan where faults are inserted in order to verify the FMEDA results.	Design team	HW sub-PM FSC	All HW-dev. TL
D9.2	Functional Test Plans and Results (Device and Module Level)	Design team	HW sub-PM	All HW-dev
D7.3	Design for Test (DFT) Plan	Design team	HW sub-PM	All HW-dev
D9.4	Equivalence Check and Layout vs. Schematic Check (LVS)	Design team	HW sub-PM	All HW-dev
D9.3	Static Timing Analysis	Design team	HW sub-PM	All HW-dev
D6.6	Hardware Inspection Report	Design Team	HW sub-PM	n/a
D6.7	Component De-rating Analysis	Design Team	HW sub-PM	HW sub-PM
D7.5	HDL Inspection Report	Design Team	HW sub-PM	n/a
D6.8	Communications Analysis (if relevant)	Design Team	FSC, SSA	HW sub-PM, SW sub-PM
D7.6	Design Rule Check Results	Design Team	HW sub-PM	All HW-dev

Dokumenty:
Detailed Hardware Design and Component FMEDA

Metodyka zgodna z IEC 61508
Functional Safety Management

Input documents	
Doc id	**Name - Description**
D1.2	System requirement specification
D3.1	Safety requirements spec.
D5.1	System architecture description

Output documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D7.1	Software architecture description	Design team	SW Sub-PM	FSC, DM

Verification documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D7.2	Safety criticality analysis and HAZOP – Documents which components are safety related and which are not.	Design team exida	FSC	SSA, DM
D7.6	Qualification and Confidence-from-Use for pre-existing software components – Documents previous use and/or previous verification done for existing components which are being re-used.	SSA, FSC	DM	n/a
D7.7	Software architecture inspection report	Design Team	PrdM	n/a
D7.8	Forward and backward traceability between software safety requirements and software architecture	Design Team	FSC	SW-sub PM
D7.9	Completed Software Architecture and Design Checklist	IR	PrdM	n/a

Dokumenty:
Software Architecture Design and Critically Analysis and HAZOP (*Hazard and Operability Study*)

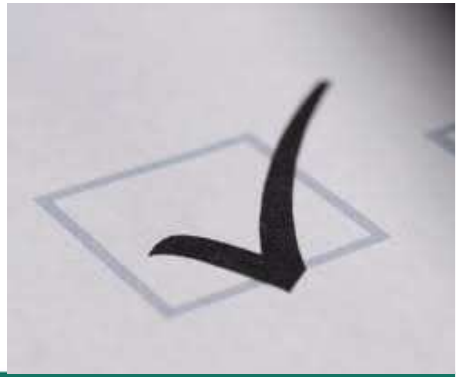
IEC61882
„Hazard and operability studies (HAZOP studies) – Application guide”

Metodyka zgodna z IEC 61508
Functional Safety Management

Input documents	
Doc id	**Name - Description**
D3.1	Safety requirements spec.
D11.1	Safety Manual
D2.4	(Validation) Test Plan – Plan showing how all requirements will be validated by documenting test objectives.

Output documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D4.1	Safety validation test specification – Documents detailed test procedures used to validate that each safety requirement has been met.	Test Team	TL	FSC DM SSA

Detailed Validation Procedures



Metodyka zgodna z IEC 61508
Functional Safety Management

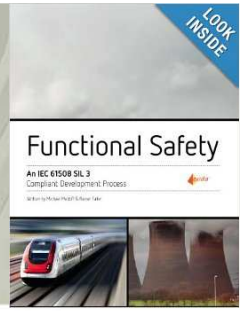
Input documents	
Doc id	**Name - Description**
D1.2	System requirement specification
D3.1	Safety requirements spec.
D7.1	Software architecture description
D7.2	Safety criticality analysis
D7.3	Software design and coding guidelines

Detailed Software Design

Output documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D8.2	Detailed Software design description	Design team	SW Sub-PM	Peer-to-peer

Verification documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D8.6	Detailed Software Design Inspection Report	Design team exida	FSC	SSA, DM
D7.9	Completed Software Architecture and Design Checklist	IR	PrdM	n/a
D7.10	Forward Traceability between software safety derived requirements and detailed software design	Design Team	FSC	SW-sub PM

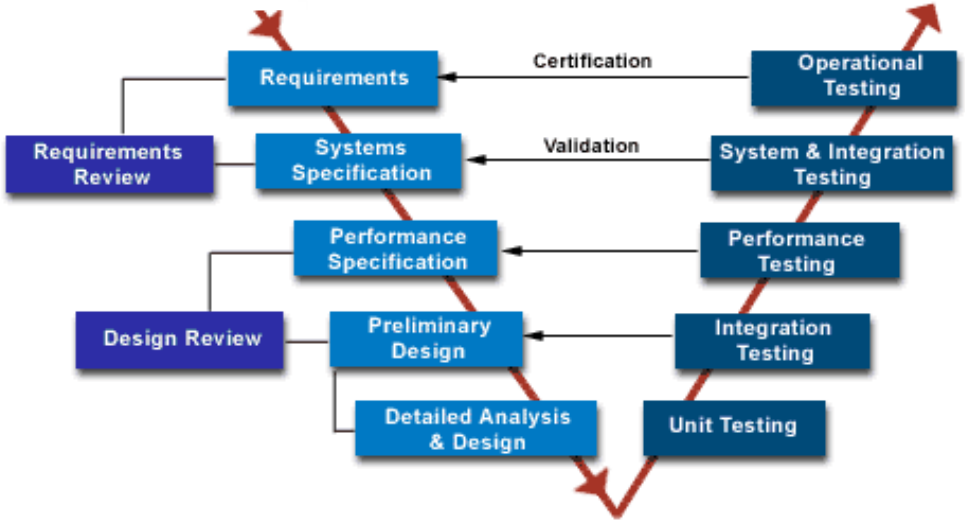
Metodyka zgodna z IEC 61508
Functional Safety Management



Input documents	
Doc id	**Name - Description**
D5.1	System architecture description
D7.1	Software architecture description
D7.2	Safety criticality analysis

Verification documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D10.1	HW/SW Integration Test Plan	Design team exida	FSC	SSA, DM
D10.2	HW/SW Integration Test Specification	Design team exida	FSC	SSA, DM

Integration Test Plan



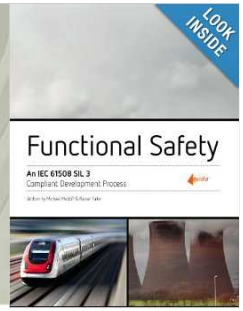
Metodyka zgodna z IEC 61508
Functional Safety Management

Inspect Code &
Static Analysis on Code

Input documents	
Doc id	**Name - Description**
D5.1	System architecture description
D7.1	Software architecture description
D8.2	Detailed Software design description
D7.2	Safety criticality analysis and HAZOP – Documents which components are safety related and which are not.

Output documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D8.2	Source Code	Design team	SW Sub-PM	n/a
D8.3	Source Code Inspection Reports	Design team	SW Sub-PM	n/a
D8.3	Static Analysis Results	Design team	SW Sub-PM	n/a

Metodyka zgodna z IEC 61508
Functional Safety Management

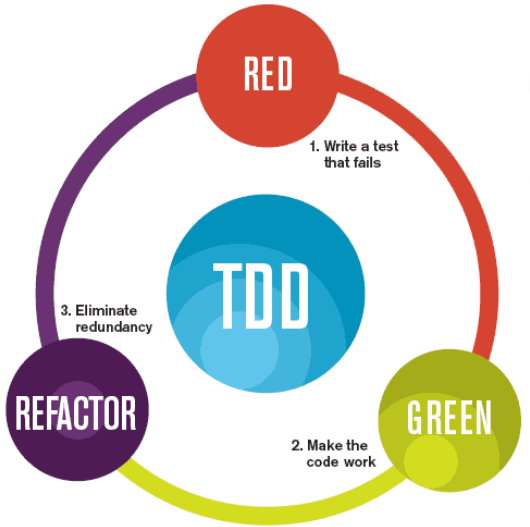


Unit Test Code

The code is tested on the unit level prior to being integrated with other code. All data must be recorded and analyzed for discrepancies between expected and real results.

Input documents	
Doc id	**Name - Description**
D8.2	Software design description
D8.3	Commented source code
D8.4	Safety criticality analysis including Software HAZOP

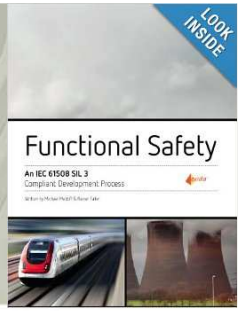
Output documents				
Doc id	**Name - Description**	**Author**	**Approval**	**Review**
D9.5	Unit Test Plans	Design team	SW Sub-PM	n/a
D9.6	Unit Test Results	Design team	SW Sub-PM	n/a
D9.7	Forward Traceability between detailed software design and module test specifications	Design Team	FSC	SW-sub PM
D9.8	Forward Traceability between detailed software design and software verification	Design Team	FSC	SW-sub PM



The mantra of Test-Driven Development (TDD) is "red, green, refactor."

Keep on a straight path with proper unit testing.

Metodyka zgodna z IEC 61508
Functional Safety Management



5.2.5 Development Tools

The Functional Safety Management plan should document all development tools used on the project. The following information should be documented for each tool:

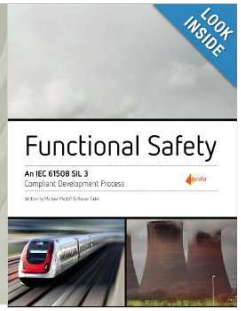
Type – A general classification of the tool

Tool, Version – The specific name of the tool and the version number used on the project

Criticality – A classification of the effect on safety that the tool could have. The following classifications should be used [1], Part 4, section 3.2.11::

- T1 – generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system,
  NOTE – T1 examples include: a text editor or a requirements or design support tool with no automatic code generation capabilities; configuration control tools.
- T2 – supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software.
  NOTE – T2 examples include: a test harness generator; a test coverage measurement tool; a static analysis tool.
- T3 – generates outputs which can directly or indirectly contribute to the executable code of the safety related system.
  NOTE – T3 examples include: a tool to change set-points during system operation; an optimizing compiler where the relationship between the source code program and the generated object code is not obvious; a compiler that incorporates an executable run-time package into the executable code.

Metodyka zgodna z IEC 61508
Functional Safety Management



Type	Tool, Version	Criticality	Tool Suitability
Safety requirements tracking	SafetyCaseDB, V6	T1	Not required for T1
CASE	Sparx Enterprise Architect, V6	T1, without code generation	Not required for T1
CASE	iLogix Rhaposdy for C, V5	T3, with code generation	Confidence from use and software HAZOP.
Change request Error tracking		T1	Not required for T1
Configuration management		T1	Not required for T1
Version control		T3	Confidence from use and software HAZOP.
Make	NMAKE32	T3	Confidence from use and software HAZOP.
IDE – Editor, Print beautifier	Microsoft Visual Studio	T1	Not required for T1
Compiler	IAR, Keil, Intel	T3	Confidence from use and software HAZOP
Linker / locater, target loader		T3	Confidence from use and software HAZOP
Static analysis tool	PC-LINT with exida control file	T2	Software HAZOP
VHDL analysis tool	SpyGlass	T2	Confidence from use.
Test coverage analysis	Not used, manual coverage determination	T2	Not Applicable
Test automation		T2	Software HAZOP
Preferred component database	Exida Electrical and Mechanical Component Reliability Handbook (EMCRH)	T2	Publicly available third party database
CAD PCB layout system		T2	Confidence from use

Metodyka zgodna z IEC 61508
Safety Requirements/ Validation Test Planning

6.1 Requirements of IEC 61508

- Specify the safety functions or element safety functions to be implemented for a given subsystem or product
- Specify the safety integrity requirements for a given subsystem or product
- Specify the requirements such that they are well understood and able to be validated
- Verify that the requirements are complete and correct

7.1 Requirements of IEC 61508

- Plan how each safety requirement will be validated to show that the safety related system meets all of the requirements for safety in terms of the required safety functions and the required safety integrity
- Plan the validation after the safety requirements review as a means to verify the sufficiency of the safety requirements and that requirements are non-ambiguous and able to be validated

Dziękujemy...