EDA122/DIT061 Fault-Tolerant Computer Systems
DAT270 Dependable Computer Systems

Welcome to Lecture 9

Safety Assessment and Technical Management

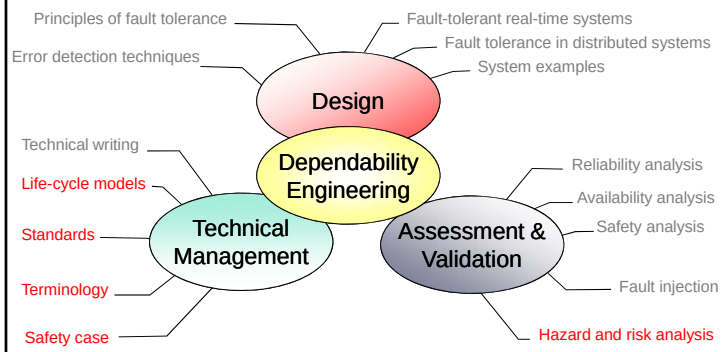
List of topics in this and the next two lectures

Design
- Specification of dependability and safety requirements

Assessment and Validation
- Hazard analysis
- Risk analysis
- Hardware failure rate prediction

Technical management
- Life-cycle models
- Standards - IEC 61508 and ISO 26262
- Safety case

Topics marked in red are covered in this lecture and the next two lectures (including the guest lecture by Jan Jacobson, SP)



Reading list for lecture 9, 10 and 11

- Chapter 1 – Introduction
  - Terminology, life cycle models, cost, legal aspects
- Chapter 2 – Safety Criteria
  - Terminology, requirements, role of standards, safety case
- Chapter 3 – Hazard Analysis
  - FMEA, HAZOP, FTA, Hazard Analysis within the development lifecycle
- Chapter 4 – Risk analysis
  - IEC 61508, risk classification, Safety Integrity Levels
- Chapter 5 – Developing Safety-Critical Systems
  - Life cycle models, safety management
- Chapter 7 – System Reliability
  - Hardware reliability prediction, Mil Hdbk 217

Outline

- Specification of dependability and safety requirements
- Development life-cycles models
- Hazard analysis
- Risk analysis
- Risk classification

Safety requirements

- In safety-related systems, the safety issues are often covered by a separate ***safety requirements document***
- Safety requirements can be both ***functional*** and ***non-functional***
- Describes what the system ***must do*** (functional), and what it ***should not do*** (non-functional)

Non-functional vs. Functional Requirements

- ***Non-functional requirements*** describes properties of the system such as *dependability*, *safety*, *maintainability*, *cost*, *power consumption*, *size*, *weight*, *etc*.
- ***Functional requirements*** describes the service that the system shall deliver
- Two categories of functional requirements
  - ***Primary functionality***
    - Service delivered in response to normal inputs
  - ***Secondary functionality***
    - Service delivered in response to abnormal inputs and/or in the presence of faults and errors.

Ways to express dependability and safety requirements

Non-functional properties

- Reliability
- Availability
- Safety
- Maintainability
- Safety integrity level (SIL)

Functional features

- Fault tolerance
- Failsafe operation
- Error masking
- Error detection
- System recovery

(See Chapter 2.2 System requirements, pp. 19 – 25 in the course book)

Different definitions of integrity

The term *integrity* is used in different contexts covering both functional and non-functional aspects of a system!

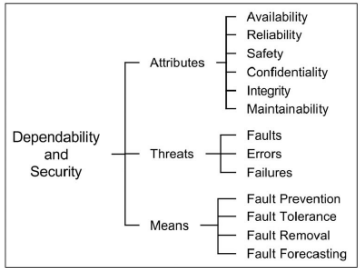
Course book:

> ***Safety integrity*** *is the likelihood of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time*
>
> ***Data integrity:*** *Data integrity is the ability of a system to prevent damage to its own database and to detect, and possibly correct, errors that do occur*
>
> ***System integrity****: The integrity of a system is its ability to detect faults in its own operation and to inform a human operator*

"Basic Concepts and Taxonomy of Dependable and Secure Computing":

> ***Integrity****: absence of improper system alterations*

The Dependability and Security Tree



Availability: readiness for correct service

Reliability: continuity of correct service

Safety: absence of catastrophic consequences on user(s) or the environment

Integrity: absence of improper system alterations

Maintainability: ability to undergo modifications and repairs

From "Basic Concepts and Taxonomy of Dependable and Secure Computing"

Safety Integrity Levels (SILs) IEC 61508

Safety integrity level	Continuous mode of operation (probability of failure per year)	Demand mode of operation (probability of failure to perform its designed function on demand)
4	$>10^{-5}$ to $< 10^{-4}$	$>10^{-5}$ to $< 10^{-4}$
3	$>10^{-4}$ to $< 10^{-3}$	$>10^{-4}$ to $< 10^{-3}$
2	$>10^{-3}$ to $< 10^{-2}$	$>10^{-3}$ to $< 10^{-2}$
1	$>10^{-2}$ to $< 10^{-1}$	$>10^{-2}$ to $< 10^{-1}$

(See Chapter 4.6 Levels of integrity, Table 4.10, p. 72 in the course book)

Ways to express functional dependability and safety requirements

Non-functional properties

- Reliability
- Availability
- Safety
- Maintainability
- Safety integrity level (SIL)

Functional features

- Fault tolerance
- Failsafe operation
- Error masking
- Error detection
- System recovery

Specifying fault-tolerant and fail-safe operation

- Fault-tolerant and fail-safe operation can be specified as illustrated by the following examples:

  FO/FS:
  - The system shall tolerate one fault (FO = Fail Operational) and shut-down safely (FS = Fail Safe) after the second fault.

  FO/FO/FS:
  - The system shall tolerate two faults (FO/FO = Fail Operational after two faults) and shut-down safely (FS = Fail Safe) after the third fault.

(See “Basic Concepts and Taxonomy of Dependable and Secure Computing”, pp. 29)

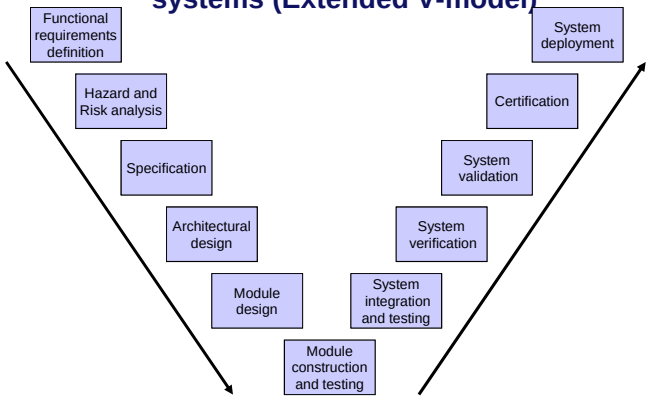
Outline

- Dependability and safety requirements specification
- Development life-cycles models
- Hazard analysis
- Risk analysis
- Risk classification

Life-cycle models

- Life-cycles models are used to organize the development, operation and maintenance of complex systems
- We will look at three development life-cycle models for safety-critical computer systems:
  - An extension of the V-model – from the course book
  - Life-cycle model from IEC 61508 – Generic standard
  - Life-cycle model from ISO 26262 – New safety standard for automotive electronic systems (lecture 10 and 11)
- Safety life-cycle models will be discussed in the guest lecture by Jan Jacobson from SP – Technical Research Institute of Sweden (www.sp.se)

Development life-cycle model for safety-critical systems (Extended V-model)



Limitations of the V-model

- The V-model is an approximation of the development process
- In practice, the various stages are not performed in a strictly sequential manner
- Hazard and risk analysis is shown as a requirements definition activity, but should be conducted during the entire life-cycle.
- The V-model does not capture the necessary, and sometimes costly, iterations that are needed in all development projects.
- Nor does it capture *all activities and relationships* within a development project.
- The V-model represents ***one*** view of the development process

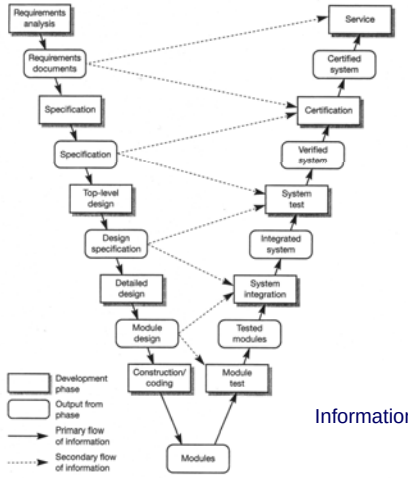


Figure 5.1 A "V" development lifecycle model.

Information flow in the V-model

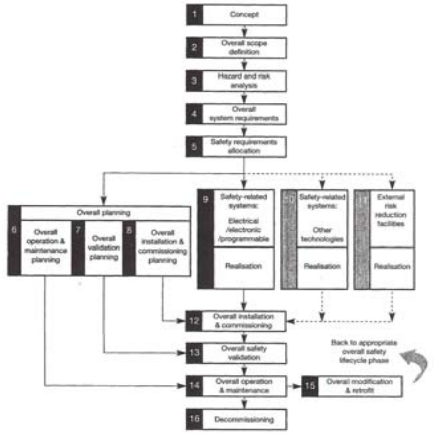
IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

- Generic standard
- Intended to be a template for industry-specific standards
- Three major and four subsidiary sections, and an introduction:
  - Part 0 – Functional safety IEC 61508
  - Part 1 – General requirements
  - Part 2 – Requirements for electrical/electronic/programmable electronic safety-related systems
  - Part 3 – Software requirements
  - Part 4 – Definitions and abbreviations (Definitions)
  - Part 5 – Examples and methods for the determination of safety integrity levels (Guidelines for applications of part 1)
  - Part 6 – Guidelines for application of part 2 and 3
  - Part 7 – Overview of techniques and measures (Bibliography of techniques)

Definition of safety lifecycle in IEC 61508

"*The necessary activities involving safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when any safety-related systems are no longer available for use*"

Note: The IEC 1508 draft standard mentioned in the course book has now become an accepted standard IEC 61508



The overall safety lifecycle model for IEC 61508

Examples of sector standards based on IEC 61508

- IEC 61511 Process industries
- IEC 61513 Nuclear power plants
- IEC 62061 Machinery sector
- IEC 61800-5-2 Power drive systems
- ISO 26262 Road vehicles – functional safety

Outline

- Dependability and safety requirements specification
- Development life-cycles models
- Hazard analysis
- Risk analysis
- Risk classification

Hazard and Risk
Definitions

*"A **hazard** is a situation in which there is actual or potential danger to people or the environment."*

***"Risk** is a combination of the frequency or probability of a specified hazardous event, and its consequence."*

(Quotes from the course book)

Tasks involved in identifying safety requirements

- ***Identification of the hazards*** associated with the system
- ***Risk classification of these hazards***
- Determination of methods for dealing with hazards
- Assignment of appropriate reliability and availability requirements
- Determination of an appropriate safety integrity level (SIL)
- Specification of development methods appropriate to this safety integrity level.

(See Chapter 2.3 Safety requirements, pp. 25 – 26 in the course book)

Hazard Analysis

- The purpose of a hazard analysis is to identify
  - the hazards associated with a safety-critical system, and
  - all events that may lead to a hazard
- Hazard analysis is not a single method – it is an ***activity*** that involves *a* ***combination of different analysis and assessment techniques***
- Hazard analysis should be conducted throughout the development life-cycle

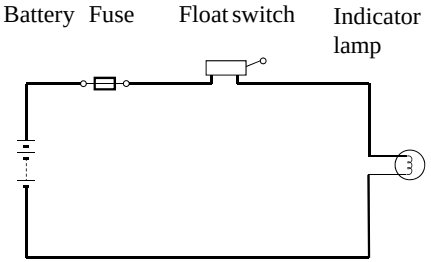
Hazard Analysis Techniques

- We will briefly look at three hazard analysis techniques:
  - fault-tree analysis (FTA)
  - failure mode and effects analysis (FMEA)
  - hazard and operability studies (HAZOP) (lecture 10)
- Examples of other techniques:
  - event tree analysis (ETA)
  - functional failure analysis (FFA)

Fault Tree Analysis (FTA)

- Graphical method that starts with a hazardous event and works backwards to identify the causes of the ”top event”
- Top-down analysis
- Intermediate events related to the top event are combined by using logical operations such as AND and OR.
- IEC 1025 international standard, 1990

Brake fluid warning lamp



Fault tree for brake fluid warning

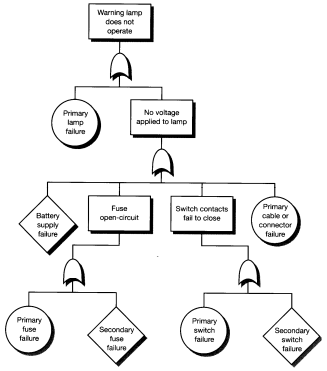


Figure 3.10 A fault tree for a brake fluid warning lamp system.

Failure Mode and Effects Analysis (FMEA)

- **Manual analysis** to determine the consequences of components, module or subsystem failures
- Bottom-up analysis
- Requires access to detailed design
- Documented in a spreadsheet where each failure mode, and its possible causes and consequences are described
- Conducted with a special software tool or a standard spreadsheet program.
- IEC 812 International Standard, 1985

(See Chapter 3 Hazard Analysis, pp. 34 – 35 and 38 – 39 in the course book)

FMEA for a microswitch

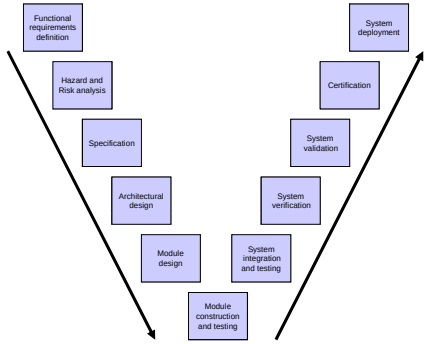
Ref No.	*Unit*	*Failure mode*	*Possible cause*	*Local effects*	*System effects*	*Remedial action*
1	Tool guard switch	Open-circuit contacts	(a) faulty component (b) excessive current (c) extreme temperature	Failure to detect tool guard in place	Prevents use of machine – system fails safe	Select switch for high reliability and low probability of dangerous failure Rigid quality control on switch procurement
2		Short-circuit contacts	(a) faulty component (b) excessive current	System incorrectly senses guard to be closed	Allows machine to be used when guard is absent – dangerous failure	Modify software to detect switch failure and take appropriate action
3		Excessive switch-bounce	(a) ageing effects (b) prolonged high currents	Slight delay in sensing state of guard	Negligible	Ensure hardware design prevents excessive current through switch

Figure 3.3 A simple FMEA chart.

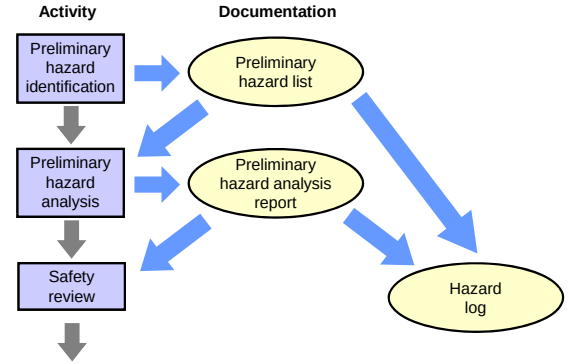
FMEA - Characteristics

- Focuses on single failures
- Often applied late in the development process
- Demanding, time-consuming, and expensive
- Not possible to apply exhaustively at the component-level for complex systems - needs to be focused to critical parts
- Boring – need for automated analysis
- Useful for an approximate analysis at the subsystem or module level (analysis based on failure mode assumptions)

How can we conducted Hazard Analysis within the development life-cycle?
(Not shown in the V-model)



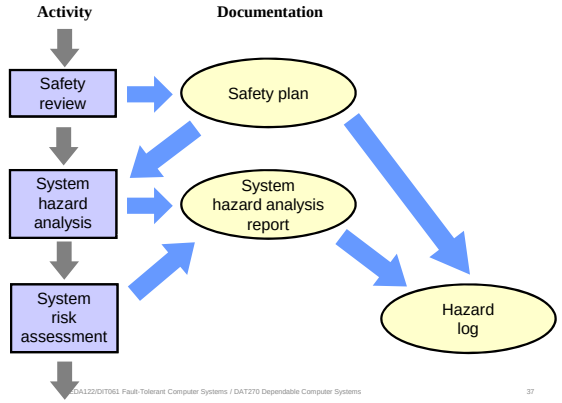
Hazard Analysis within the Development Lifecycle



Elements of a Preliminary Hazard Analysis

- A brief description of the system and its environment
- An overview of the system's function and its safety features
- The safety objectives of the system
- Justification of the risk and integrity level assignments
- Target failure rates and safety levels
- Sources of any data used within the analysis
- A bibliography of all documents used.

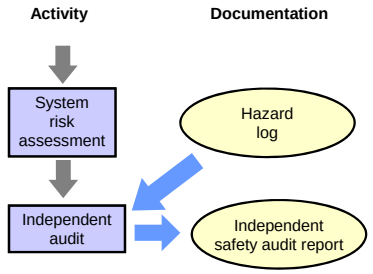
Hazard Analysis within the Development Lifecycle



Outline

- Dependability and safety requirements specification
- Development life-cycles models
- Hazard analysis
- Risk analysis
- Risk classification

Hazard Analysis within the Development Lifecycle



Risk analysis

- Risk analysis predicts the *probability* and *severity* of accidents
- ”*An accident is an unintended event or sequence of events that causes death, injury, environmental or material damage*” (Quote from course book)

Risk analysis - Example

In a country with a population of 10 000 000 approximately 500 people are killed in traffic accidents each year. In average each person spend 500 hours per year in situations where they are exposed to the risk of traffic accidents.

What is the risk of being killed in a traffic accident?

The risk is simply

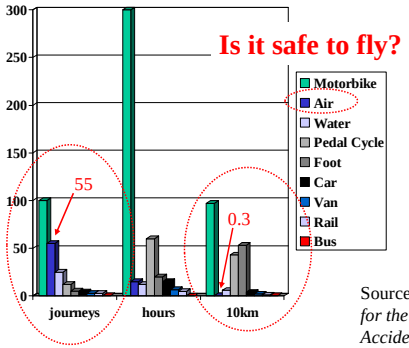
$(500 / 10^7) / 500 = 10^{-7}$ deaths/hour

Outline

- Dependability and safety requirements specification
- Life-cycles models
- Hazard analysis
- Risk analysis
- Risk classification

Number of deaths in transport

(per 100 Million passengers)



Source: *Royal Society for the Prevention of Accidents and Michael Paulitsch, EADS*

Risk classification

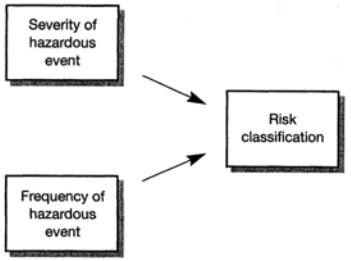


Figure 4.2 Determination of risk classification.

Severity classifications of hazards

- Industries developing safety-related systems classify hazards in terms of their severity
- Severity classification varies between different industries
- We will look at severity classifications used in:
  - IEC 61508
  - Civil aircraft
  - Military systems

Consequence categories in IEC 61508

Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Minor injuries at worst

Likelihood of occurrence in IEC 61508

Category	Definition	Range (failures per year)
Frequent	Many times in system lifetime	$> 10^{-3}$
Probable	Several times in system lifetime	10^{-3} to 10^{-4}
Occasional	Once in system lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in system lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	$< 10^{-7}$

Risk classification in IEC 61508

Table 4.6 Risk classifications from draft IEC 1508.

	Consequences			
Frequency	*Catastrophic*	*Critical*	*Marginal*	*Negligible*
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

Table 4.7 Interpretation of risk classes from draft IEC 1508.

Risk class	*Interpretation*
I	Intolerable risk
II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained
III	Tolerable risk if the cost of risk reduction would exceed the improvement gained
IV	Negligible risk

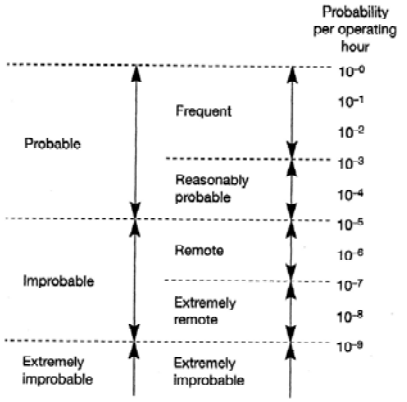


Figure 4.1 Hazard probability classes for aircraft systems.

Severity vs. allowed probability for civil aircraft

Table 4.11 Relationship between the severity of an effect and its allowable probability for civil aircraft systems.

Category	*Severity of effect*	*Maximum probability per operating hour*
Normal		10^{0}
		10^{-1}
Nuisance		10^{-2}
Minor	Operating limitation; emergency procedures	10^{-3}
		10^{-4}
Major	Significant reduction in safety margins; difficult for crew to cope with adverse conditions; passenger injuries	10^{-5}
		10^{-6}
Hazardous	Large reductions in safety margins; crew extended because of workload or environmental conditions. Serious injury or death of a small number of occupants	10^{-7}
		10^{-8}
Catastrophic	Multiple deaths, usually with loss of aircraft	10^{-9}

Hazard severity categories for civil aircraft

Table 4.1 Hazard severity categories for civil aircraft.

Category	*Definition*
Catastrophic	Failure condition which would prevent continued safe flight and landing
Hazardous	Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions, to the extent that there would be: (1) a large reduction in safety margins or functional capabilities (2) physical distress or higher workload such that the flight crew could not be relied on to perform their tasks accurately or completely (3) adverse effects on occupants, including serious or potentially fatal injuries to a small number of those occupants
Major	Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to occupants, possibly including injuries
Minor	Failure conditions which would not significantly reduce aircraft safety, and which would involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some inconvenience to occupants
No effect	Failure conditions which do not affect the operational capability of the aircraft or increase crew workload

Accidents severity categories for military systems

Table 4.2 Accident severity categories for military systems.

Category	*Definition*
Catastrophic	Multiple deaths
Critical	A single death, and/or multiple severe injuries or severe occupational illnesses
Marginal	A single severe injury or occupational illness, and/or multiple minor injuries or minor occupational illnesses
Negligible	At most a single minor injury or minor occupational illness

Military risk classes

Table 4.4 Accident risk classes for military systems.

	Consequences			
Frequency	*Catastrophic*	*Critical*	*Marginal*	*Negligible*
Frequent	A	A	A	B
Probable	A	A	B	C
Occasional	A	B	C	C
Remote	B	C	C	D
Improbable	C	C	D	D
Incredible	D	D	D	D

Table 4.5 Interpretation of risk classes for military systems.

Risk class	*Interpretation*
A	Intolerable
B	Undesirable, and will only be accepted when risk reduction is impracticable
C	Tolerable with the endorsement of the Project Safety Review Committee
D	Tolerable with the endorsement of the normal project reviews

Overview of Lecture 10

- Hazard analysis - continued
  - Hazard and operability studies (HAZOP)
- ISO 26262 – Functional Safety for Automotive Systems
- Acceptability of risk
- Assignment of safety integrity levels
- Safety case
- Hardware failure rate prediction

- Preparations:
  - Chapter 2.4, 3.4, 4.1 – 4.6, 7.3, and 14.4 in the course book.
  - Lecture slides

Overview of Lecture 11

- Guest lecture by Jan Jacobson, SP Technical Research Institute of Sweden, Borås.
- Topic: IEC 61508 and ISO 26262
- Preparations:
  - Section 5.1 – 5.3, and 14.5 (IEC 1508) in the course book.
  - Lecture slides