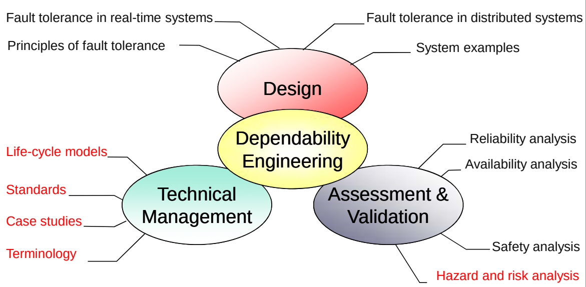
EDA122/DIT061 Fault-Tolerant Computer Systems

Welcome to Lecture 10

Safety Assessment and Technical Management

Topics marked in red are covered in lecture 8, lecture 10, and the guest lecture by Jan Jacobson, SP



List of topics for lecture 8, 10 and 11

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

Reading list for lecture 8, 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

- Risk analysis
  - Acceptability of risk - ALARP
  - Assignment of Safety Integrity Levels
- ISO 26262
- Hazard analysis
  - Hazard and operability studies (HAZOP)
- Safety case
- Hardware reliability prediction

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)

Risk classification

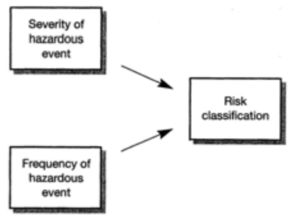


Figure 4.2 Determination of risk classification.

Severity classifications of hazards

- Industries developing safety-related systems classify hazards in terms of their severity
- Severity classification varies between different industries
- In lecture 8, we look at severity classifications used in:
  - IEC 61508
  - Civil aircraft
  - Military systems

Acceptability of risk in IEC 61508
ALARP – as low as is reasonably practicable

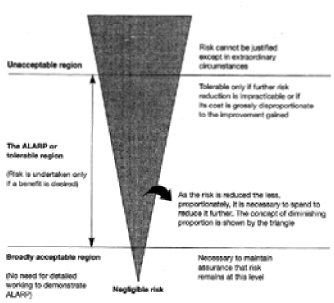


Figure 4.3 Levels of risk from draft IEC 1508.

Risk reduction

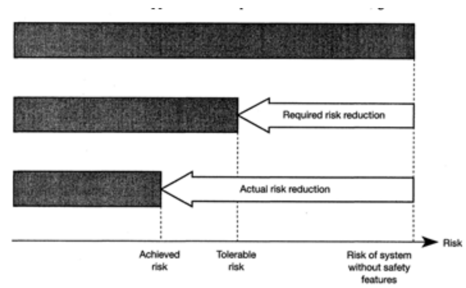


Figure 4.4 The process of risk reduction.

Outline

- Risk analysis
  - Acceptability of risk – ALARP
  - Assignment of Safety Integrity Levels (SILs)
- ISO 26262
- Hazard analysis
  - Hazard and operability studies (HAZOP)
- Safety case
- Hardware reliability prediction

Assignment of integrity levels

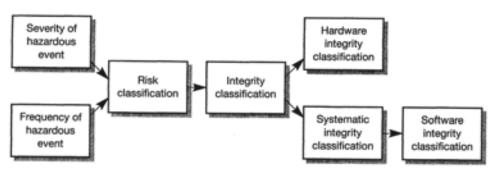


Figure 4.5 Assignment of integrity levels.

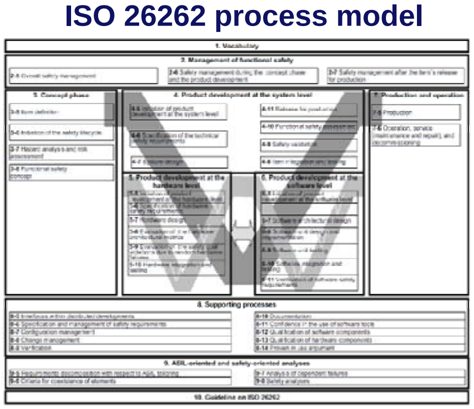
Outline

- Risk analysis
  - Acceptability of risk - ALARP
  - Assignment of Safety Integrity Levels
- ISO 26262
- Hazard analysis
  - Hazard and operability studies (HAZOP)
- Safety case
- Hardware reliability prediction

ISO 26262 Road Vehicles – Functional Safety

– *Part 1: Vocabulary*
– *Part 2: Management of functional safety*
– *Part 3: Concept phase*
– *Part 4: Product development: system level*
– *Part 5: Product development: hardware level*
– *Part 6: Product development: software level*
– *Part 7: Production and operation*
– *Part 8: Supporting processes*
– *Part 9: ASIL-oriented and safety-oriented analyses*
– *Part 10: Guideline on ISO 26262*

ISO 26262 process model



ISO 26262: How safety is achieved

"*System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (for example: mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic etc).*

Although ISO 26262 is concerned with E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered." (quote from ISO 26262, part 2)

Note: E/E systems means electrical and electronic systems

ISO 26262: Summary
(text from part 2 of the standard)

ISO 26262:

- provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;
- provides an automotive specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs);
- uses ASILs for specifying applicable requirements of ISO 26262 for avoiding unreasonable residual risk; and
- provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved.
- provides requirements for the relation with suppliers.

ISO 26262: What influences safety?

"*Functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and by the management processes.*" (quote from the standard)

ASIL – Automotive Safety Integrity Classes

- **QM** – Quality management (No safety integrity class assigned.)
- **ASIL A** – lowest safety integrity
- **ASIL B**
- **ASIL C**
- **ASIL D** – highest safety integrity

ASIL – Automotive Safety Integrity

- The ASIL for an item (array of systems or system or function) is determined during hazard analysis and risk assessment.
- The ASIL depends on three factors:
  - **Severity** of potential harm to endangered persons such as the driver and the passengers of the vehicle, pedestrians, cyclists and occupants of other vehicles.
  - **Probability of exposure –** the probability that endangered persons are exposed to an hazardous event.
  - **Controllability** – the probability that the driver or an other endangered person can control the hazardous event and thereby avoid the specific harm.

ISO26262: Classes of severity

Class	Description
S0	No injuries
S1	Light and moderate injuries
S2	Severe and life-threatening injuries (survival probable)
S3	Life-threatening injuries (survival uncertain), fatal injuries

ISO26262: Classes of probability of exposure

Class	Description
E0	Incredible
E1	Very low probability
E2	Low probability
E3	Medium probability
E4	High probability

Note: No probability values is specified by the standard.

ISO26262: Classes of controllability

Class	Description
C0	Controllable
C1	Simply controllable
C2	Normally controllable
C3	Difficult to control or uncontrollable

ISO 26262: ASIL determination

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Outline

- Risk analysis
  - Acceptability of risk - ALARP
  - Assignment of Safety Integrity Levels
- ISO 26262
- Hazard analysis
  - Hazard and operability studies (HAZOP)
- Safety case
- Hardware reliability prediction

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 and operability study (HAZOP)

- Invented by ICI (Imperial Chemical Industries), a British chemical company in the early 1960's.
- Method for structured study of safety-critical processes and systems
- Performed by a team of engineers and experts
- Aims to identify the consequences of ***deviations*** from normal operation
- Guide words are used to systematically generate questions of "what if" nature

Table 3.1 Possible guide word interpretations in different applications.

Guide word	*Chemical plant*	*Computer-based system*
No	No part of the intended result is achieved	No data or control signal exchanged
More	A quantitative increase in the physical quantity	A signal magnitude or a data rate is too high
Less	A quantitative decrease in the physical quantity	A signal magnitude or a data rate is too low
As well as	The intended activity occurs, but with additional results	Redundant data sent in addition to intended value
Part of	Only part of the intended activity occurs	Incomplete data transmitted
Reverse	The opposite of what was intended occurs, for example reverse flow within a pipe	Polarity of magnitude changes reversed
Other than	No part of the intended activity occurs, and something else happens instead	Data complete but incorrect
Early	Not used	Signal arrives too early with reference to clock time
Late	Not used	Signal arrives too late with reference to clock time
Before	Not used	Signal arrives earlier than intended within a sequence
After	Not used	Signal arrives later than intended within a sequence

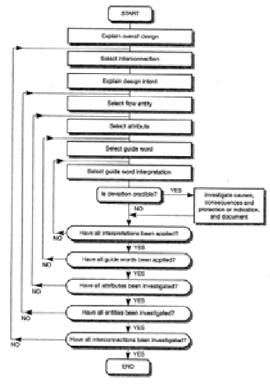


Figure 3.4 A flowchart of the HAZOP study process.

Item	*Inter-connection*	*Attribute*	*Guide word*	*Cause*	*Consequence*	*Recommendation*
1	Sensor supply line	Supply voltage	No	PSU, regulator or cable fault	Lack of sensor signal detected and system shuts down	
2			More	Regulator fault	Possible damage to sensor	Consider overvoltage protection
3			Less	PSU or regulator fault	Incorrect temperature reading	Include voltage monitoring
4		Sensor current	More	Sensor fault	Incorrect temperature reading, possible loading of supply	Monitor supply current
5			Less	Sensor fault	Incorrect temperature reading	As above
6	Sensor output	Voltage	No	PSU, sensor or cable fault	Lack of sensor signal detected and system shuts down	
7			More	Sensor fault	Temperature reading too high – results in decrease in plant efficiency	Consider use of duplicate sensor
8			Less	Sensor mounted incorrectly or sensor failure	Temperature reading too low – could result in overheating and possible plant failure	As above

Figure 3.5 Part of a simplified HAZOP results table for a temperature sensor.

Outline

- Risk analysis
  - Acceptability of risk - ALARP
  - Assignment of Safety Integrity Levels
- ISO 26262
- Hazard analysis
  - Hazard and operability studies (HAZOP)
- **Safety case**
- Hardware reliability prediction

Safety Case

- A safety case is a record of all activities that ensure the safety of a system throughout its life time.
- The safety case must contain a rigorous argumentation for the safety of the system
- Constitutes the collected evidence that a system is safe.
- Mandatory for certification by regulating authorities
- Often used for internal purposes by the system manufacturer, also for products that do not require certification

Contents of a Safety Case
(Example)

- A description of the safety-related system
- Evidence of competence of personnel involved in any safety activity
- A specification of safety requirements
- The results of hazard and risk analysis
- The results of design analysis showing that the system design meets all the required safety targets
- The verification and validation strategy
- Records of safety reviews
- Records of any incidents which occur throughout the life of the system
- Records of all changes to the system and justification of its continued safety

(See Chapter 14.4, pp. 364-365 in course book)

Outline

- Risk analysis
  - Acceptability of risk - ALARP
  - Assignment of Safety Integrity Levels
- ISO 26262
- Hazard analysis
  - Hazard and operability studies (HAZOP)
- Safety case
- **Hardware reliability prediction**

Hardware failure rates

- Ways of improving reliability of hardware
  - Decrease temperature
  - Decrease electrical stress (derating)
  - Reduce number of components or increase integration
  - Increase quality of components
  - Improve physical environment
    - Reduce exposure to moisture
    - Reduce exposure to vibrations

Examples of Failure Rate Prediction for Hardware

- MIL-HDBK-217, Military handbook, US Department of Defense, Parts Stress Model (Revision F Notice 2, released February 1995)
- Telcordia SR-332, Issue 2 (released Sept 2006)

Failure Rate Prediction Mil-Hdbk-217F

$\lambda_p = (C_1\Pi_T + C_2\Pi_E)\Pi_Q\Pi_L$ failures / 10^6 hours

λ_p is the part failure rate
C_1 is related to die complexity
Π_T is related to ambient temperature
C_2 is related to the package type
Π_E is determined by the operating environment
Π_Q is determined by the part quality
Π_L represents the learning factor and is determined by the experience of the manufacturer.

Telcordia SR-332 (Bellcore)

$\lambda_{SS} = \lambda_G \Pi_Q\Pi_S\Pi_T$ failures / 10^6 hours

λ_{SS} is the steady state failure rate
λ_G is the generic steady state failure rate (table look up based on field data)
Π_Q is determined by the part quality
Π_S is determined by the electrical stress
Π_T is related to operating temperature

Standards for hardware reliability prediction

- **MIL-HDBK-217 Part Stress & Part Count**
  MIL-HDBK-217 F Notice 2.
- **217Plus - Based on Handbook of 217PlusTM**
  Reliability Prediction Models, 26 May 2006 by Reliability Information Analysis Center (RIAC).
- **Telcordia Issue 2 -** Reliability Prediction Procedure for Electronic Equipment, SR-332, Issue 2, September 2006
- **IEC 62380 (RDF 2003)**
  Updated version of RDF 2000 UTEC 80810 method – French Telecom reliability prediction Standard. It includes most of the same components as MIL-HDBK-217.

Standards for hardware reliability prediction

- **FIDES Guide 2009**
  The FIDES methodology is applicable to all domains using electronics: aeronautical, naval, military, production and distribution of electricity, automobile, railway, space, industry, telecommunications, data processing, home automation, household appliances.
- **BRT - British Telecom -** British Telecom Module for reliability prediction based on British Telecom document HRD-4 or HRD-5.
- **GJB299 -** Chinese reliability standard.
- **Siemens SN29500.1 -** Siemens reliability standard.

Overview of Lecture 11

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

Overview of Lecture 12

More on N-version programming and Recovery Blocks.
Study of failures in high-performance computing systems.

Read *before the lecture:*

- Reprints:
  1. A Large Scale Experiment in N-version Programming (Skip Section 4, Model of Independence)
  2. An Evaluation of Software Fault Tolerance in a Practical System (skip Section 5, Analysis of Results)
  3. A Large-Scale Study of Failures in High-Performance Computing Systems.