Why standards for functional safety ? –

An introduction to the international standard IEC 61508

Jan Jacobson

SP Technical Research Institute of Sweden

phone +46 10 516 56 97

email jan.jacobson@sp.se

Our Core Areas

Process of innovation

- 9000 customers
- Wide technical range
- Experimental resources
- Strong research environments
- High scientific quality

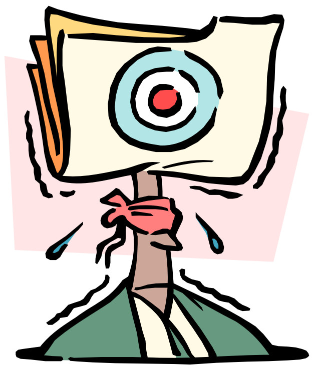
SP Technical Research Institute of Sweden

Contents

- What is risk?
- What is “functional safety” and “safety function”?
- Is there “high” and “low” safety?
- What is the IEC 61508 standard?
- ISO 26262 for the automotive industry
- Failure rate
- An example of calculation of probability of failure
- Experiences regarding dependable systems
- More to read

SP Technical Research Institute of Sweden

What is risk?



SP Technical Research Institute of Sweden

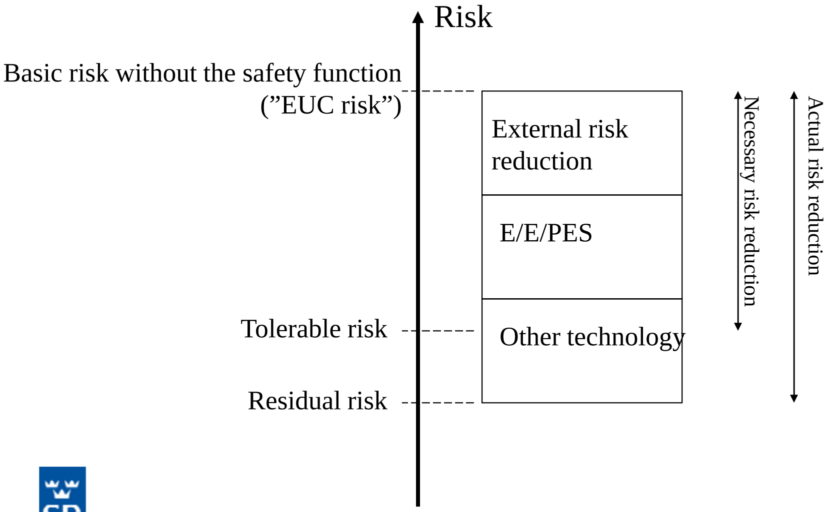
Elements of risk

Risk	Severity	Probability of occurrence
		- frequency and duration - probability of occurrence of hazardous event - possibility to avoid or limit the harm

Risk is a function of severity and probability.

SP Technical Research Institute of Sweden

Risk reduction



SP Technical Research Institute of Sweden

Risk reduction

- Risks will be reduced by
  - proper safety functions (correctly implemented)
  - expected system behaviour at fault
  - expected probability for faults
  - suitable development methods
  - suitable safety principles
  - ….

SP Technical Research Institute of Sweden

Failures of the systems

Dangerous failures may arise from:
- incorrect specifications of the system, hardware or software;
- omissions in the safety requirements specification (e.g. failure to develop all relevant safety functions during different modes of operation);
- random failures of hardware;
- systematic failures of hardware and software;
- common cause failures;
- human error;
- environmental influences (e.g. electromagnetic, temperature, mechanical phenomena);
- supply system voltage disturbances (e.g. loss of supply, reduced voltages, re-connection of supply).


www.autoliv.se

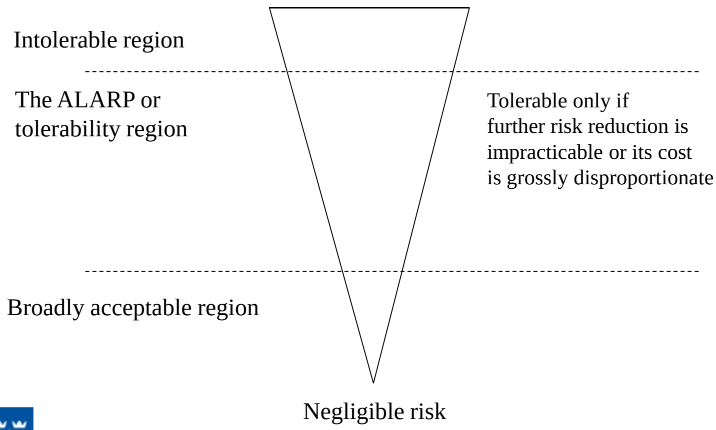
SP Technical Research Institute of Sweden

Example: Hydraulically operated guillotine

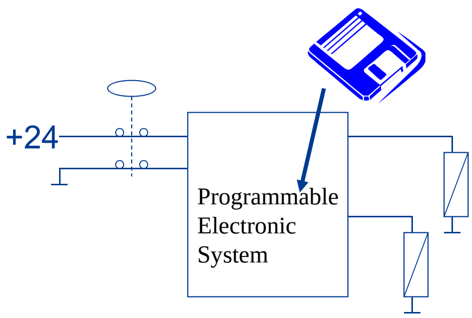
- ’hold-to-run’
- light curtain
- amputating his hand
- recently reconditioned
- replacing a hydraulic valve
- connections of ’up’ and ’down’ solenoids transposed
- HSE ’Out of Control’

SP Technical Research Institute of Sweden

ALARP (As Low As Reasonably Practicable)



SP Technical Research Institute of Sweden

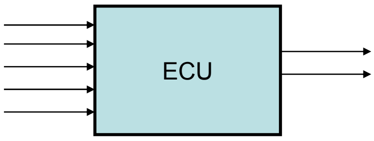


What is ”functional safety” and ”safety function”?

SP Technical Research Institute of Sweden

Functional safety

- Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.
- Functionality ≠ Functional safety
- Focus on development of functions must not reduce efforts for functional safety.
- It will be expensive to try to “add functional safety” late in the development process.



SP Technical Research Institute of Sweden

Safety function

- *”Function to be implemented by an E/E/PE safety-related system, other technology safety related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event”*
- Defined in standard IEC 61508

SP Technical Research Institute of Sweden

Safety requirements specification

- Overall safety requirements specification :
  safety functions AND safety integrity levels

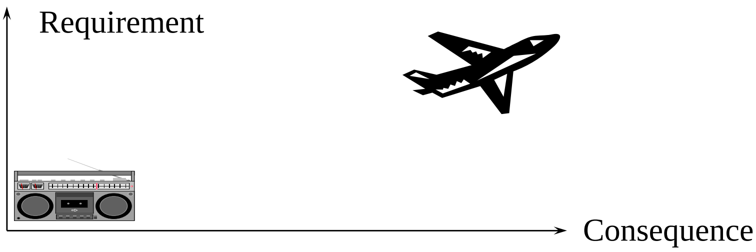
- Example:
  safety function: pressure monitoring (alarm at high pressure)
  safety integrity: 1 fault/10 years

SP Technical Research Institute of Sweden

Is there ”high” and ”low” safety?

SP Technical Research Institute of Sweden

Different safety requirements



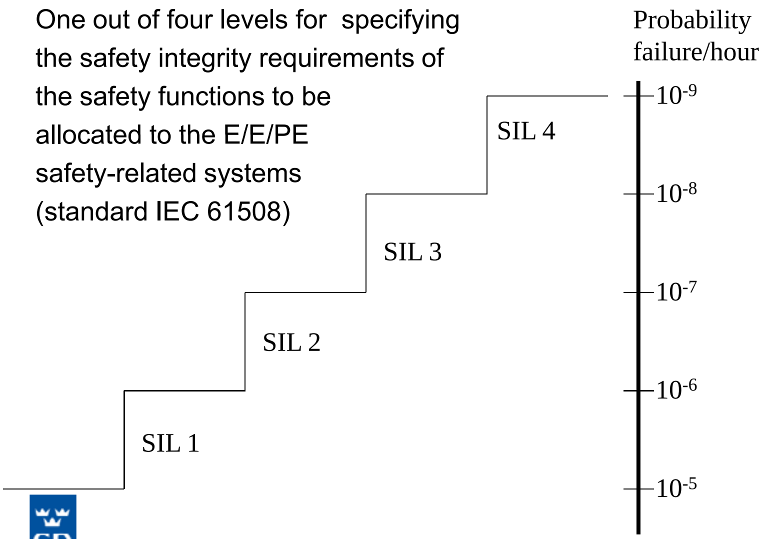
•Serious consequences – high requirements
•Moderate consequences – moderate requirements

… but the safety integrity level depends on other parameters also.

SP Technical Research Institute of Sweden

Safety Integrity Level (SIL)

One out of four levels for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems (standard IEC 61508)



SP Technical Research Institute of Sweden

Qualitative assessment of SIL

- Consequence
  - –C1 minor injury
  - –C2 serious permanent injury to one or more persons. Death to one person
  - –C3 death to several people
  - –C4 very many people killed
- Frequence & exposure
  - –F1 rare to more often
  - –F2 frequent to permanent
- Possibility of avoiding
  - –P1 Possible under certain conditions
  - –P2 Almost impossible
- Probability of the unwanted occurrence
  - –W1 very slight probability
  - –W2 slight probability
  - –W3 relatively high probability

SP Technical Research Institute of Sweden

Risk graph

Basic risk: Serious injury to person depending on uncontrolled start of remote controlled machine.

Safety function: Emergency stop. Estimated parameters are C2, F1, P1, W3.

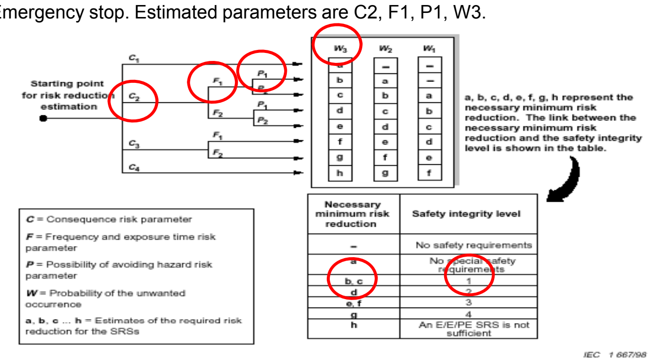
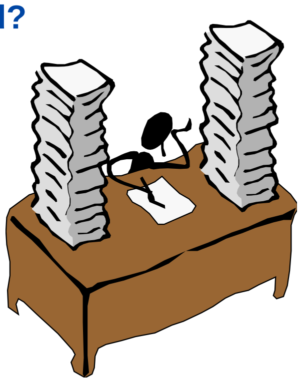


Figure D.2 – Risk graph: example (illustrates general principles only)

What is the IEC 61508 standard?



SP Technical Research Institute of Sweden

IEC 61508

Functional safety of
electrical/electronic/programmable electronic (E/E/PE)
safety related systems

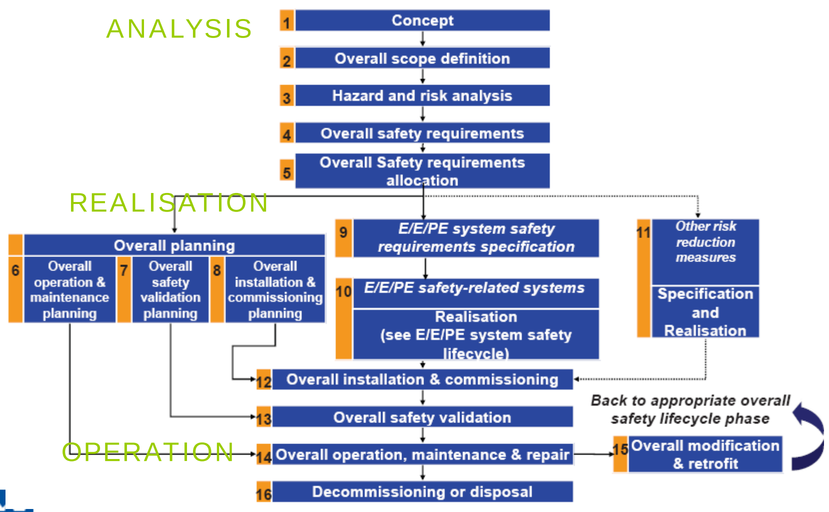
- Part 1: General requirements
- Part 2: Requirements for E/E/PE safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviation
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

SP Technical Research Institute of Sweden

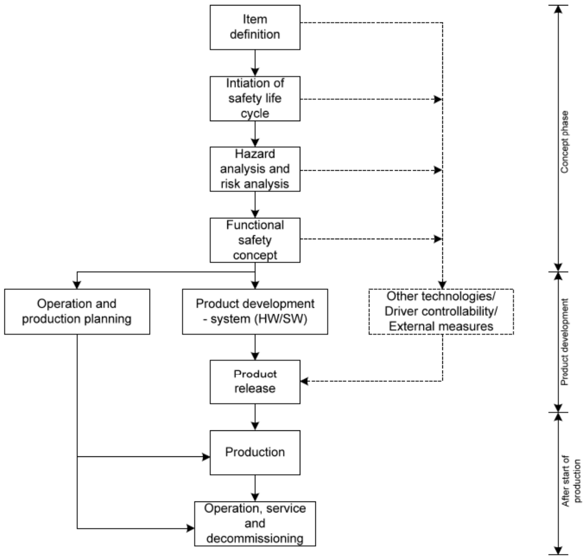
IEC 61508

- Generic standard, i.e. used as a base for generation of sector-specific standards
- Part 1-4 are ”basic safety publications”. These parts must be considered when developing sector-specific standards.
- IEC 61508 can be used when sector-specific standards do not exist
- Presently under maintenance
- Also as European standard (EN 61508) and national standards (e.g. DS/EN 61508 ’Funktionel sikkerhed for elektriske/elektroniske/programmerbare sikkerhedsrelaterede systemer’)

Overall safety lifecycle



Overall Safety Lifecycle



SP Techn

Example: Engineer microwaves hand

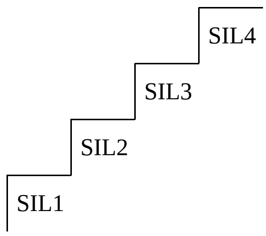
- commercial 10.5 kW microwave oven
- '.. a sensation of warmth in his hands..'
- electric interlocks at oven doors
- single channel control system
- 4 times per day?
- 200 times per day
- contacts welded

- HSE 'Out of Control'

SP Technical Research Institute of Sweden

Measures and techniques to control failures

- Target : To control failures during operation
- A combination of techniques and measures
- HR = Highly Recommended
- R = Recommended
- NR = Not Recommended
- - = No statement



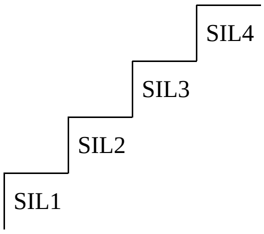
IEC 61508-2, Table A16

Technique/ measure	SIL 1	SIL 2	SIL 3	SIL 4
Programme sequence monitoring	HR Low coverage	HR Low coverage	HR Medium coverage	HR High coverage
On-line monitoring	R Low coverage	R Low coverage	R Medium coverage	R High coverage
…..				
Diverse hardware	-	-	R Medium coverage	R High coverage
…..				

SP Technical Research Institute of Sweden

Measures and techniques to avoid failures

- Target : To avoid failures during the different phases of the safety life cycle.
- A combination of techniques and measures
- HR = Highly Recommended
- R = Recommended
- NR = Not Recommended
- - = No statement



SP Technical Research Institute of Sweden

IEC 61508-2, Table B1 (during specification)

Technique/ measure	SIL 1	SIL 2	SIL 3	SIL 4
Project mangement	HR Low	HR Low	HR Medium	HR High
…..				
Semi-formal methods	R Low	R Low	HR Medium	HR High
…..				
Formal methods	-	-	R Medium	R High

SP Technical Research Institute of Sweden

IEC 61508-2, Table B5 (during validation)

Technique/ measure	SIL 1	SIL 2	SIL 3	SIL 4
Functional testing	HR mandatory	HR mandatory	HR mandatory	HR mandatory
…..				
Static analysis	-	R Low	R Medium	R High
…..				
Field experience	R Low	R Low	R Medium	NR

ISO 26262 for the automotive industry

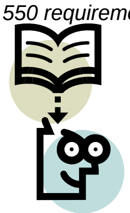
Draft International Standard ISO 26262

ISO 26262 Functional Safety – Road Vehicles

- 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

350 pages

550 requirements



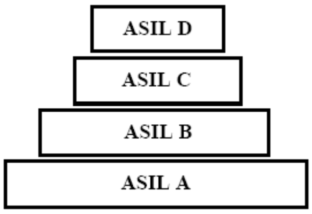
SP Technical Research Institute of Sweden

Motivation for a sector-specific standard

- Control and safety functions usually inseparable (not separate safety functions)
- Mass-market products, not low-volume
- How to handle subcontracting?
- Life cycle: Validation before start-of-production (not validation before installation)
- Risk analysis for road vehicles
- ”Techniques and measures” more suitable for road vehicles
- Human factors, driver part of the control loop

SP Technical Research Institute of Sweden

Automotive Safety Integrity Level



Draft standard ISO 26262

- All safety-related functions are expected to be assigned to an ASIL.
- ASIL D provides the highest risk reduction.

SP Technical Research Institute of Sweden

ASIL and Risk Classification (draft ISO 26262)

		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

- QM: Quality management => 26262 not applicable

SP Technical Research Institute of Sweden

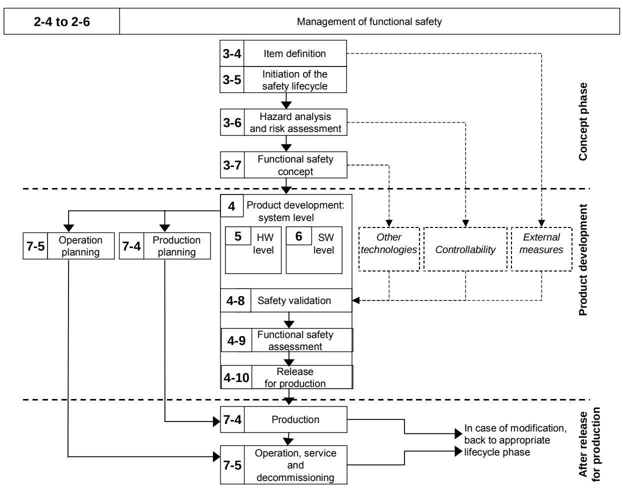
Examples of Hazard Analysis Using ISO 26262

- Airbag
  - Loss of airbag functionality in a crash situation is typically QM or ASIL A
  - Unintended airbag activation under normal driving is typically ASIL B or C
- Brake-by-wire
  - Unintended braking with maintained stability is typically ASIL B or C
  - Unintended braking on single wheel is typically ASIL D
  - Total symmetric loss of brake function (assume p-brake and engine-brake) is typically ASIL D
- Steer-by-wire
  - Loss of steer-by-wire functionality (S3, C3 and E4) gives ASIL D
- Head-lights
  - Loss of high-beam (assume low-beam functional) (S2, E3, C1) gives ASIL A

N.B. The hazard analysis may be different for other vehicles, drivers or traffic situations.
The above are only examples. There is no “always true ASIL”.

SP Technical Research Institute of Sweden

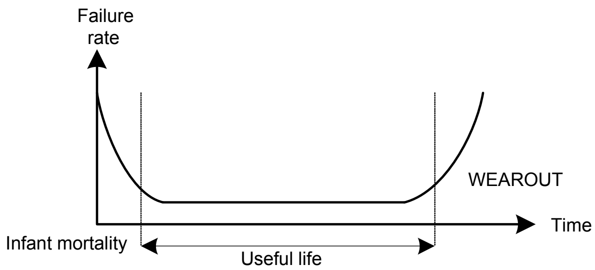
Safety lifecycle according to draft ISO 26262



SP Technical Research Institute of Sweden

Failure rate

Failure rate as a function of time



- Electronic components can be often described by the above curve.
- The failure rate is assumed constant during the usefil life.
- Exponential distribution is assumed.

$$f(t) = \lambda e^{-\lambda t}$$ ”Exponential probability density function”

SP Technical Research Institute of Sweden

Safe/dangerous and detected/undetected faults

The failure rate may be described through the consequences of a fault

S – Safe

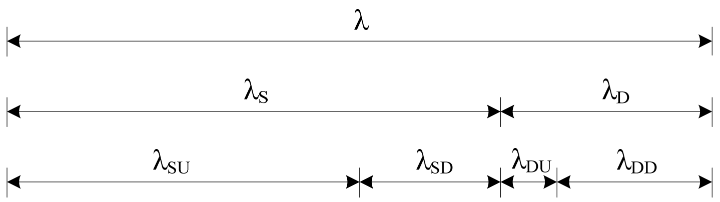
D – Dangerous

SU – Safe Undetected

SD – Safe Detected

DU – Dangerous Undetected

DD – Dangerous Detected



SP Technical Research Institute of Sweden

Diagnostic Coverage

- ” fractional decrease in the probability of dangerous hardware failures resulting from the operation of the automatic diagnostic tests”

$$DC = \frac{\sum \lambda_{DD}}{\sum (\lambda_{DU} + \lambda_{DD})}$$

- $0 \leq DC \leq 100\%$

SP Technical Research Institute of Sweden

Safe Failure Fraction

- ” fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure”

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}}$$

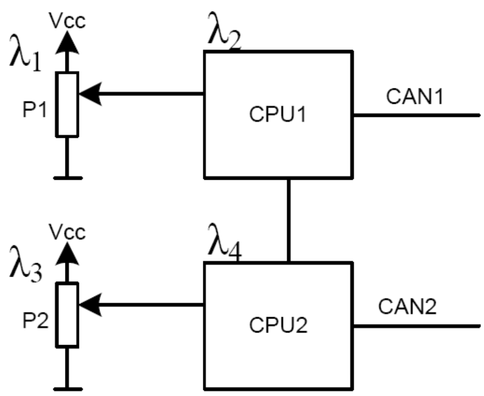
- 0 ≤ SFF ≤ 100%

SP Technical Research Institute of Sweden

An example of calculation of probability of failure

SP Technical Research Institute of Sweden

Example: Brake pedal sensing



- Failure rates:
- λ_1, λ_2, λ_3, λ_4
- (Failures/hour)

- What will be the
- total probability of
- dangerous failure
- per hour?

SP Technical Research Institute of Sweden

Example: Brake pedal sensing

- FMEA Failure Mode and Effects Analysis

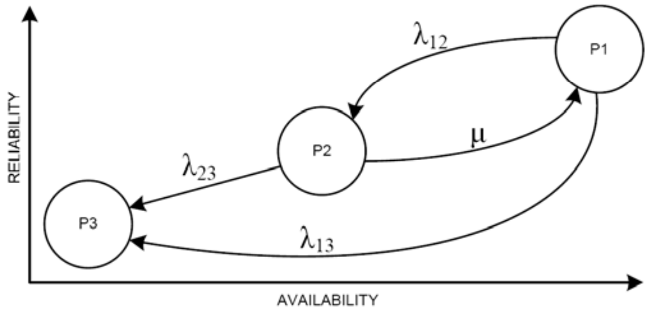
Monotoring function	Description
A- Comparison between redundant CPUs	The function continuously compares the potentiometer feed-back position values, performs control-flow tests of the CPUs and compares the communication channels. Any deviation between the redundant channels is handled by a special algorithm which forces the most incorrect channel into a passive safe-state.

Part 1 – Without considering monitoring functions							Part 2 – Taking the monitoring functions into account	
Comp.	Mode	Rate [FITs]	Distr. [%]	Effect	S [%]	D [%]	Monitoring function.	Coverage [%]
P1	SC	[700]	0.5	Either stucked at max or min position, or reduced range of the potentiometer	10	90	A	90
	OC		25	Floating feedback voltage	50	50	A	90
	D		65	Indicating the wrong position – continuously	30	70	A	90
	F		9.5	Indicating the wrong position - instantaneously	10	90	A	90
CPU1	F	[1300]	100	Indicating the wrong position	50	50	A	90

SP Technical Research Institute of Sweden

Example: Brake pedal sensing

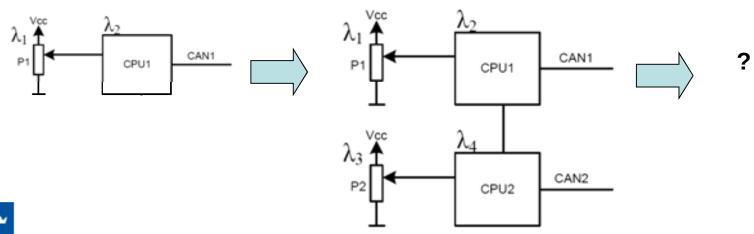
The Markov model



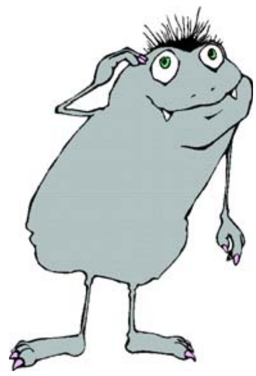
- State P1: Normal operation
- State P2: Degarded operation
  (Safe-state. Only one channel operating)
- State P3: Dangerous operation

Example: Brake pedal sensing

- FMEA, Markov modelling and calculations give
- the probability of failure per hour = 3,87 * 10^{-7}
- Will this be acceptable?
- Do we have to reduce the risk further?



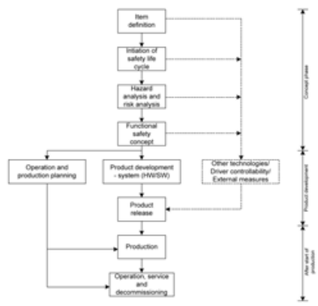
Experiences regarding dependable systems

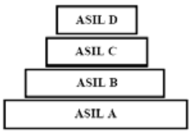


SP Technical Research Institute of Sweden

How to achieve functional safety?

- Overall safety lifecycle
- Risk management
- Safety functions
- Safety Integrity Level
- Avoid faults
- Control faults





SP Technical Research Institute of Sweden

Some important conclusions

- ”Zero risk” can never be achieved
- It is important to understand the risks associated with the system
- Risks impossible to tolerate must be reduced (ALARP)
- Safety thinking must be applied from the beginning
- Correct function does no necessarily imply a safe system

SP Technical Research Institute of Sweden

Some views on IEC 61508

- The probability-based thinking may be hard to learn
- Not perfect for automotive applications
- Large differences compared with earlier sector-specific standards
- The decision to apply IEC61508 must be taken early in a development project
- An extensive standard, hard for many small or medium-sized organisations to learn
- Large amounts of documentation generated

SP Technical Research Institute of Sweden

Development acc. to the Safety Life Cycle

- Objective: Obtain functional safety through systematic development work

- Not to produce documentation by
- reverse engineering.

- Supporting the safety work,
- not an extra burden for the developer

- Who is responsible for
- the functional safety?

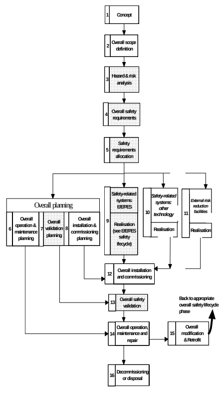


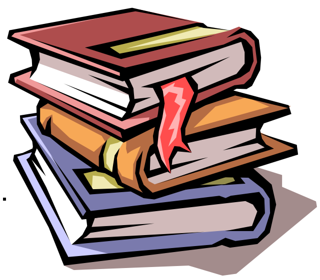
Fig. 1 Overall safety lifecycle

SP Technical Research Institute of Sweden

Documentation

- Size?
- Structure?
- Fit the establish quality management of the company.

- The progress of the work
- for dependability is indicated
- by the progress of the documentation.



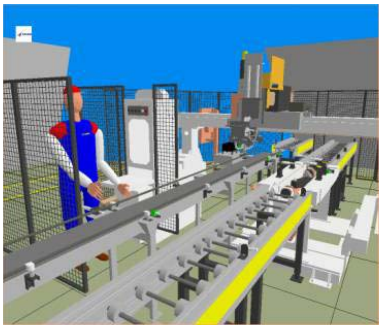
SP Technical Research Institute of Sweden

More to read …

SP Technical Research Institute of Sweden

Sector-specific standards

- IEC 62061 Machinery
- IEC 61511 Process industry
- IEC 61513 Nuclear industry
- ISO 26262 Road vehicles



Källa: www.euromation.se

SP Technical Research Institute of Sweden

More to read …

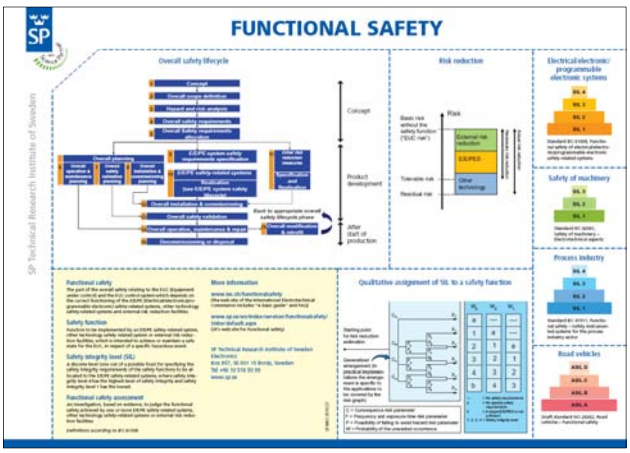
www.iec.ch/functionalsafety
(the web site of the International Electrotechnical Commission includes ”A basic guide” och FAQ)

http://www.sp.se/en/index/research/safeprod/Sidor/default.aspx
(SafeProd - a research project on functional safety in complex products)

DS-håndbog 148:2004, *Functional Safety* at DKK 712,-.
(www.ds.dk)

SP Technical Research Institute of Sweden

Functional Safety poster

- Download SP INFO 2010:27 at http://www.sp.se/en/publications/Sidor/Publikationer.aspx
- 

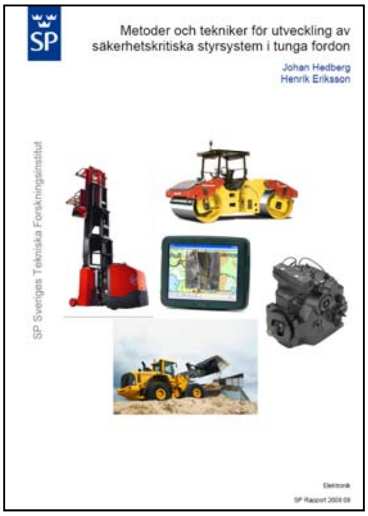
SP Technical Research Institute of Sweden

Download on Heavy Vehicles

- SP Report 2008:08
- ”Metoder och tekniker för
- utveckling av säkerhetskritiska
- styrsystem i tunga fordon ”

- at
- http://www.sp.se/en/publications/Sidor/Publikationer.aspx

- (only available in Swedish)



SP Technical Research Institute of Sweden

Download the AutoVal reports

SP reports no
2007:13
2007.14
2007:15

(only no 2007:13 available on paper)

- To be found at www.sp.se under ”Publications” and ”Electronics and ICT”

SP Technical Research Institute of Sweden