Safety Integrity Levels (SIL)

Ali Baghaei

Process Safety Specialist

Email: ali.baghaei@gmail.com

Tel: +98-912-4785416

Contents

Functional Safety

“Part of the overall safety relating to the equipment under control (EUC) and the EUC control system which depends on the correct functioning of the electrical / electronic / programmable electronic (E/E/PE) safety-related systems, other technology safety-related systems and external risk reduction facilities”

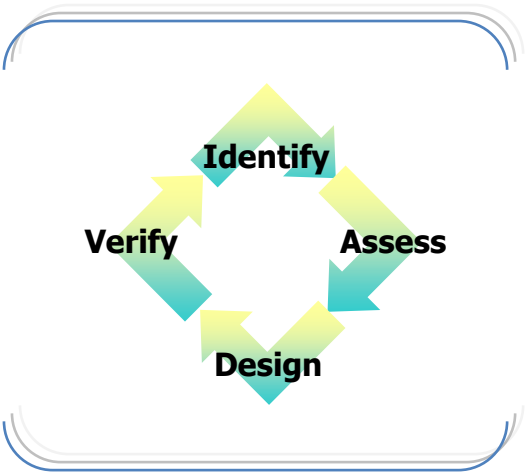
The ability of a safety instrumented system or other means of risk reduction to carry out the actions necessary to achieve or to maintain a safe state for the process and its associated equipment.

Applicable Standards

- **IEC-61508**: Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety Related Systems
- **IEC-61511**: Functional safety – safety instrumented systems for the process industry sector
- **ANSI/ISA-84.01**: Application of Safety Instrumented Systems for the Process Industries
- **IEC 62280-1**: Railway applications - Communication, signaling and processing systems - Part 1: Safety-related communication in closed transmission systems
- **IEC/EN 62061**: Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems
- **ISO 13849-1**: Safety of machinery -- Safety-related parts of control systems

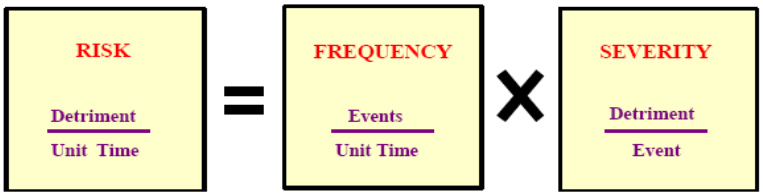
Safety Lifecycle

The necessary activities involved in the implementation of safety instrumented functions, occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use.



Risk

A Risk is the amount of harm that can be expected to occur during a given time period due to specific harm event. There is no such thing as zero risk. Therefore the concept of defining and accepting a tolerable risk for any particular activity prevails.



ماتریس ریسک

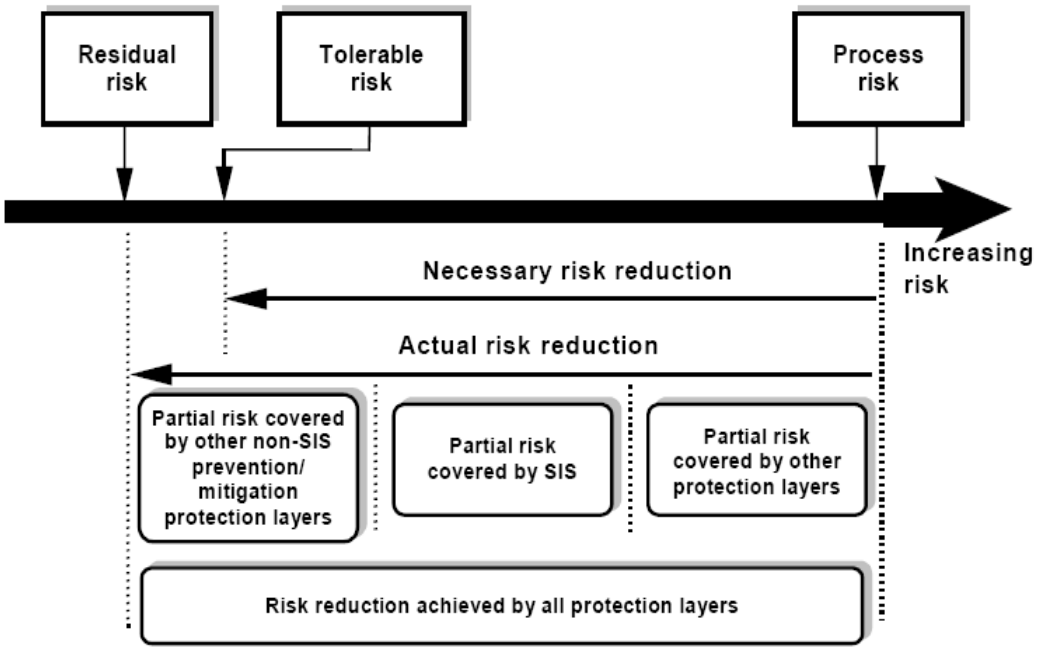
عواقب ⟵		ایمنی	محیط زیست	بهداشت	سرمایه (تولید)	دسته	۱	۲	۳	۴	۵
						تاریخچه	هرگز در صنعت دیده نشده	در صنعت اتفاق افتاده	در شرکت نفت اتفاق افتاده	در یک شرکت فرعی اتفاق افتاده	در واحد عملیاتی اتفاق افتاده
						احتمال	۱۰۰۰ سال	۱۰۰ سال	۳۰ سال	۵ سال	۱سال
						احتمال ⟵					
		چند کشته،کشتار عمومی یا خسارت بسیار زیاد به دارائی	خسارت طولانی مدت دور ریزی زیاد نفت و مواد شیمیایی ، بازسازی ممکن نیست	مرگ یا بیماری شغلی که منجر به مرگ می‌شود، مانند سرطان	خسارت خیلی زیاد، از دست رفتن واحد و یا تولید	۵	۵	۱۰	۱۵	۲۰	۲۵
		یک کشته ، اثرات حاد سلامت روی عموم یا خسارت عمده به دارائی	خسارت متوسط، دور ریزی معمول نفت و مواد شیمیایی، بازسازی بیش از یک سال طول می‌کشد	آسیب ناتوان کننده کلی، بیماری شغلی برگشت ناپذیر، مانند سوختگی با مواد خورنده	خسارت زیاد از دست دادن تولید برای چندین هفته	۴	۴	۸	۱۲	۱۶	۲۰
		آسیب جدی، غیبت طولانی از محیط کار، اثرات جزئی روی سلامت عموم	تأثیرحاد، دور ریزی جزئی، بازسازی طی یک سال	آسیب ناتوان کننده جزئی، بیماری شغلی، مانند کم شدن شنوایی، ارتعاش دست	خسارت محلی به تجهیزات، توقف واحد برای یک،دو هفته	۳	۳	۶	۹	۱۲	۱۵
		درمان دارویی، نیاز به چند روز استراحت، تاثیر و خسارت ناچیز روی محیط	تأثیر گذرا، دور ریزی کم نفت و مواد شیمیایی، بازسازی فوری	درمان دارویی، بیماری بدون زمان از دست رفته، مانند سوختگی پوست	خسارت جزئی به تجهیزات، قطع تولید برای چند روز	۲	۲	۴	۶	۸	۱۰
		کمکهای اولیه، بازگشت به کار همان روز یا روز بعد	تأثیر جزئی،دور ریزی ناچیز نفت و مواد شیمیایی ، بدون بازسازی	کمکهای اولیه جزئی، بیماری شغلی با اثرات ناچیز روی سلامتی	خسارت خیلی کم بدون قطع تولید	۱	۱	۲	۳	۴	۵

ناحیه غیر قابل قبول. به غیر از شرایط خاص و غیر معمول، این ریسک قابل قبول نمی باشد.

ناحیه قابل تحمل. تنها در صورتی که مطابق اصل ALARP ، کاهش ریسک از نظر منطقی، عملی نباشد. .

ناحیه قابل قبول. بایستی سعی شود که با بهبود مستمر، ریسک در این ناحیه نگاه داشته شود.

A sample for Risk Matrix



Concept of Risk Reduction

Risk Reduction

SIS achieves risk reduction by reducing the frequency/severity of the hazardous event. The amount of risk reduction achieved is indicated by the risk reduction factor (RRF):

RRF = probability of risk in state 1 / probability of risk in state 2

Safety Integrity Levels

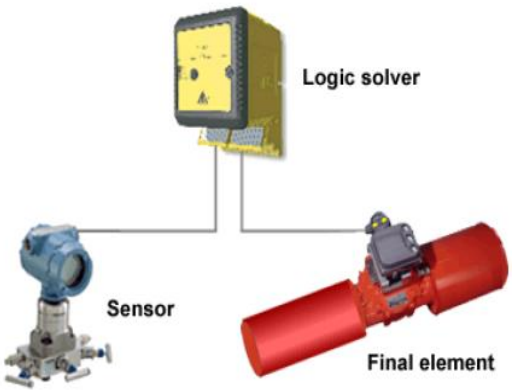
A SILn system is a short way of saying "system developed using appropriate techniques and measures to ensure that the system meets the systematic failure requirements of a specific safety function X at SILn".

SIL Rating	Range of PFD	Range of RRF
B	A Single E/E/PES is not sufficient	
4	$10^{-5} \leq PFD < 10^{-4}$	$100,000 \geq RRF > 10,000$
3	$10^{-4} \leq PFD < 10^{-3}$	$10,000 \geq RRF > 1,000$
2	$10^{-3} \leq PFD < 10^{-2}$	$1,000 \geq RRF > 100$
1	$10^{-2} \leq PFD < 10^{-1}$	$100 \geq RRF > 10$
A	No Special Safety Requirements	
--	No Safety Requirements	

Safety Related Systems

- Passive protection systems

- Alarms
- Non-instrumented systems
- Safety Instrumented Systems (SIS)
  aka: trip system, shutdown system, interlock, instrumented protection system (IPS)



Typical structure of a Safety Instrumented System (SIS)

The action of a Safety Instrumented System (SIS) is called a Safety Instrumented Function (SIF). More than one SIF may be assigned to a single SIS.

Stages of SIL Study

1. **Target SIL Evaluation**
2. **SIL Verification**

Required Documents for SIL Evaluation

- P&ID
- Cause & Effect Charts
- HAZOP Report
- Process Description
- Logic Diagrams
- ESD Philosophy
- Control Philosophy
- Blowdown Philosophy

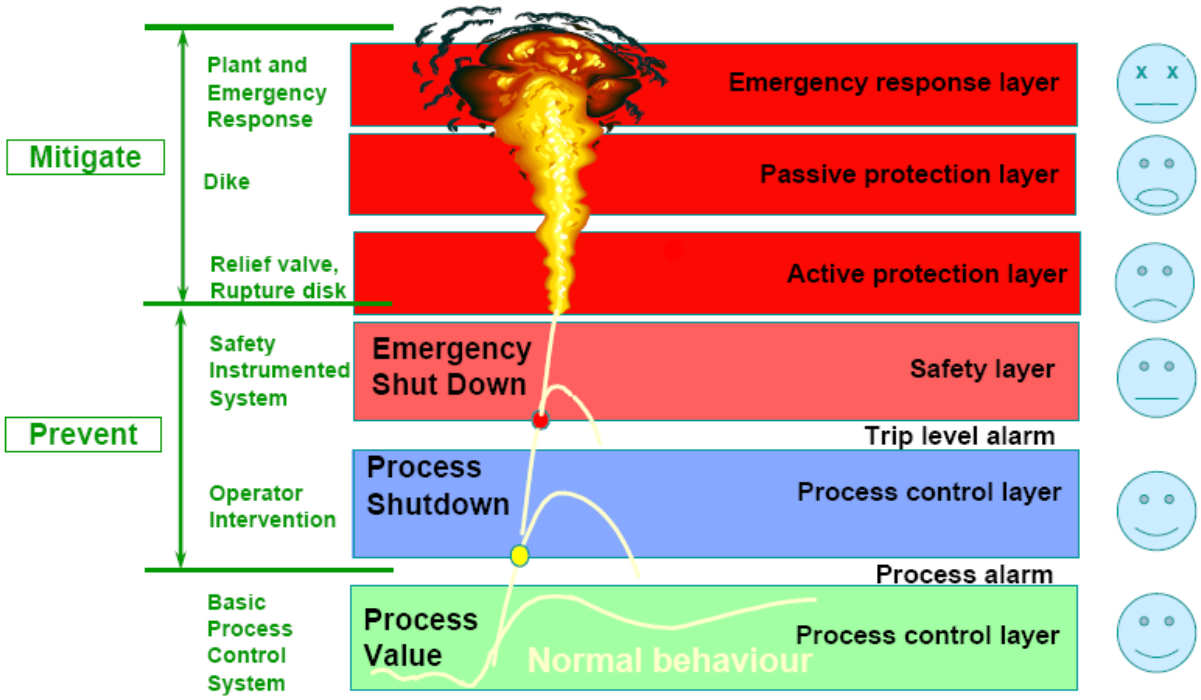
SIL Target Evaluation Study

- **Quantitative Technique**
- **Qualitative Techniques**

Layers of Protection

1. Basic Process Control System (BPCS).
2. Automated shutdown sequences in the process control system combined with operator intervention to shut down the process.
3. Safety Instrumented System (SIS). It is a safety system independent of the process control system. It has separate sensors, valves and logic system. No process control is performed in this system; its only role is safety.

4. Active protection layer such as valves or rupture disks designed to provide a relief point that prevents a rupture, large spill or other uncontrolled release that can cause an explosion or fire.
5. Passive protection layer like a dike or other passive barrier that serves to contain a fire or channel the energy of an explosion in a direction that minimizes the spread of damage.
6. Emergency Response Plan (ERP).

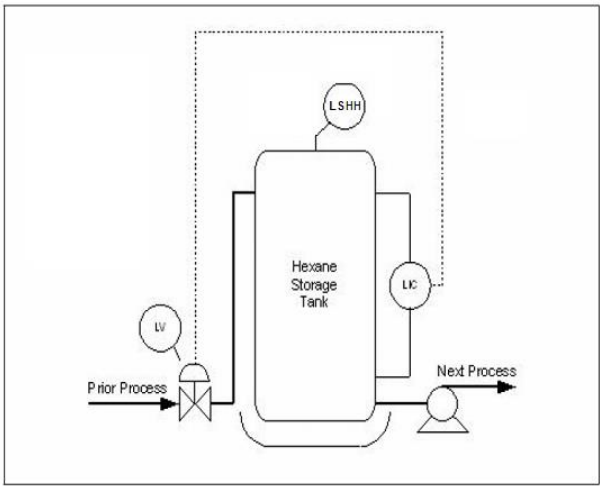


Concept of Layers of Protection

Quantitative Method

See also IEC 61511-3:2003, Annex B

Example:



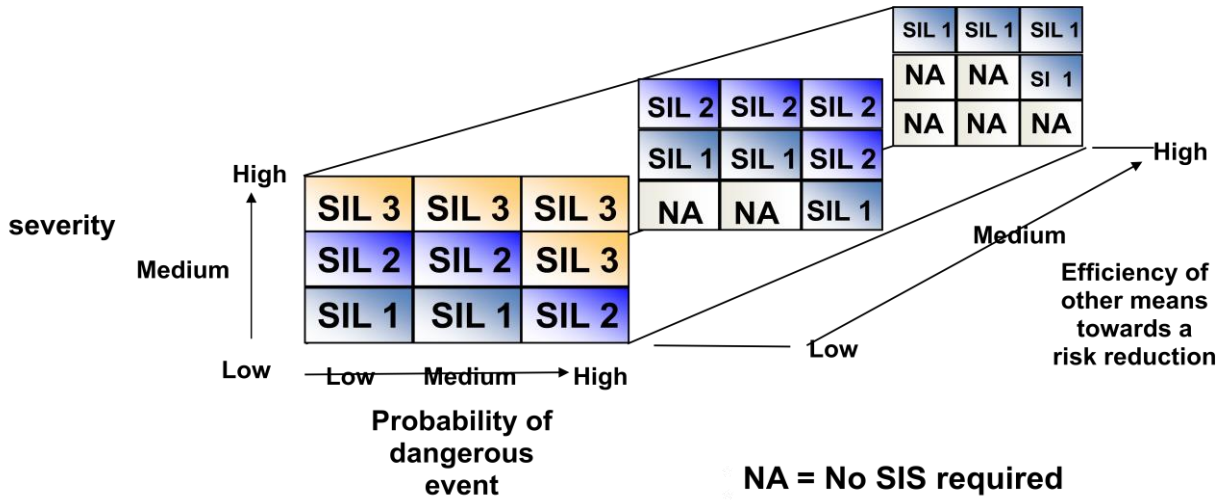
Tolerable Frequency of Fatality: 1e-5 per year

Failure rate of BPCS	Failure Rate of Dike	Probability of Ignition	Probability of personnel in area	Probability of fatality
0.1	0.01	1.0	0.5	0.5

- Frequency of Fire: 0.1 × 0.01 × 1.0 = 1e-3
- Frequency of Fatality: 1e-3 × 0.5 × 0.5 = 2.5 e-4
- Risk Reduction Factor: 2.5e-4 / 1e-5 = 25

Qualitative Methods

Risk Matrix



Risk Graph

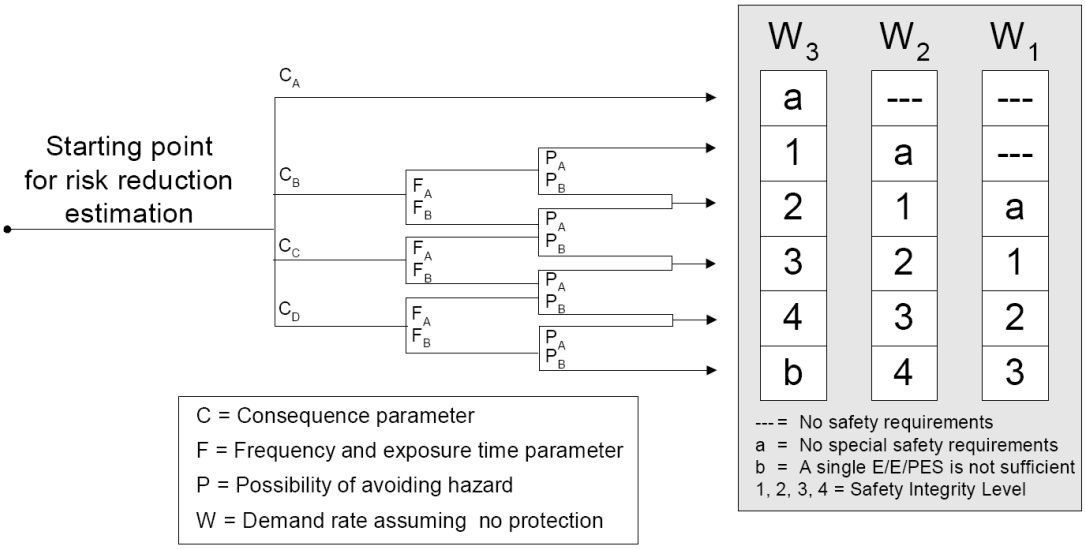
According to IEC 61511, the semi-qualitative method of the calibrated risk graph enables the safety integrity level of a safety-related loop to be determined from knowledge of the risk factors associated with the process and basic process control system.

The approach uses a number of parameters, which together describe the nature of the hazardous situation when safety-related loops fail or are not available. One parameter is chosen from each of four sets, and the selected parameters are then combined to decide the SIL allocated to the safety-related loop. These parameters allow a graded assessment of the risk to be made, and represent key risk assessment factors.

Risk graph method is widely used for reasons outlined in section below. The risk graph and the descriptions of its four parameters and the ranges for each parameter are shown in Figure and Table below, respectively. This methodology can be applied for safety protection, environmental protection or asset protection. When the safety integrity level of a safety-related loop is assessed for different protections (safety, environmental and/or asset), the most conservative SIL target shall be chosen for this loop.

As risk graph method is a semi-quantitative technique it does not require precise hazard rates, consequences, and values for other parameters of the method. Hence, no special calculations or complex modeling is required. Moreover, it can be applied as a team exercise, similar to HAZOP, so that individual bias can be avoided. This way, all team members (e.g. from design, operations, and maintenance) will acquire a comprehensive understanding of process hazards and risks.

Another advantage of this method is fast conclusion process because it does not require a detailed study of relatively minor hazards and it can be used to assess many hazards relatively quickly. It is also useful as a screening tool to identify hazards which need more detailed assessment and minor hazards which do not need additional protection.



Risk Graph

Consequence		
C_A	Minor injury	
C_B	0.01 to 0.1 probable fatalities per event	
C_C	>0.1 to 1.0 probable fatalities per event	
C_D	>1.0 probable fatalities per event	
Exposure		
F_A	<10% of Time	
F_B	≥10% of Time	
Avoidability/Unavoidability		
P_A	>90% probability of avoiding hazard	<10% probability hazard cannot be avoided
P_B	≤90% probability of avoiding hazard	≥10% probability hazard cannot be avoided
Demand Rate		
W_1	<1 in 30 years	
W_2	1 in >3 to 30 years	
W_3	1 in >0.3 to 3 years	

Risk Parameter		Classification	Remarks
Consequence (C) Number of fatalities	C_A	Minor injury	1. The classification system has been developed to deal with injury and death to people. 2. For the interpretation of C_A, C_B; C_C and C_D, the consequences of the accident and normal healing should be taken into account.
	C_B	Serious injury or one death	
	C_C	Multiple deaths	
	C_D	Catastrophic	
Occupancy (F) This is calculated by determining the proportional length of time the area exposed to the hazard is occupied during a normal working period. Note 1 If the time in the hazardous area is different depending on the shift being operated then the maximum should be selected. Note 2 It is only appropriate to use FA where it can be shown that the demand rate is random and not related to when occupancy could be higher than normal. The latter is usually the case with demands which occur at equipment start-up or during the investigation of abnormalities.	F_A	Rare to more frequent exposure in the hazardous zone.	3. See remark 1, above.
	F_B	Frequent to permanent exposure in the hazardous zone.	
Probability of avoiding the hazardous event (P) if the protection system fails to operate.	P_A	Adopted if all conditions in remark 4 are satisfied	4. P_A should only be selected if all the following are true: - facilities are provided to alert the operator that the safety related loop has failed; - independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area; - the time between the operator being alerted and a hazardous event occurring exceeds 1 hour or is definitely sufficient for the necessary actions.
	P_B	Adopted if all the conditions are not satisfied	
Demand rate (W) The number of times per year	W_1	Very low demand rate	5. The purpose of the W factor is to estimate the frequency of the hazard
	W_2	Low demand rate	

that the hazardous event would occur in absence of safety-related loop under consideration.	W_3	Relatively high demand rate	taking place without the addition of the safety-related loop

Consequence Parameters – Environmental

Risk parameter		Classification	Comments
Consequence (C)	C_A	A release with minor damage that is not very severe but is large enough to be reported to plant management	A moderate leak from a flange or valve Small scale liquid spill Small scale soil pollution without affecting ground water
	C_B	Release within the fence with significant damage	A cloud of obnoxious vapour travelling beyond the unit following flange gasket blow-out or compressor seal failure
	C_C	Release outside the fence with major damage which can be cleaned up quickly without significant lasting consequences	A vapour or aerosol release with or without liquid fallout that causes temporary damage to plants or fauna
	C_D	Release outside the fence with major damage which cannot be cleaned up quickly or with lasting consequences	Liquid spill into a river or sea A vapour or aerosol release with or without liquid fallout that causes lasting damage to plants or fauna Solids fallout (dust, catalyst, soot, ash) Liquid release that could affect groundwater

SIL Verification Techniques

- Simplified Equations
- FTA
- Markov Method

Available Software for SIL Verification

- ExSILEntia by exida, www.exida.com
- SILSolver by SIS-Tech, www.sis-tech.com
- SILCore by ACM (Canada), www.silcore.com
- AEShield by AE Solutions, www.aesolns.com

SIS Failures

A Safety Instrumented System (SIS) may fail in different modes. These failure modes may be:

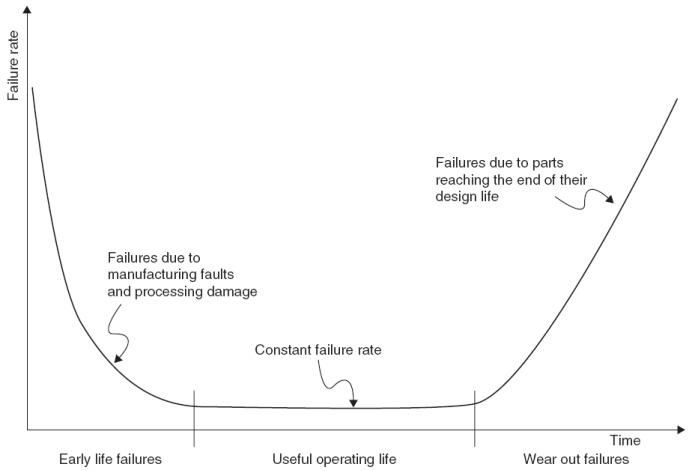
- Failure Modes (causes):
  - Systematic Failures: specification, design, implementation (wiring/tubing errors, inadequate electrical/pneumatic power supply, improper or blocked-in connections to the process, installation of wrong sensor or final control component), Software errors, operation and modification
  - Random Hardware Failures
- Failure Modes (results):
  - Safe
  - Dangerous
  - Detected (overt)
  - Undetected (covert, hidden)

Therefore failures are divided as follows:

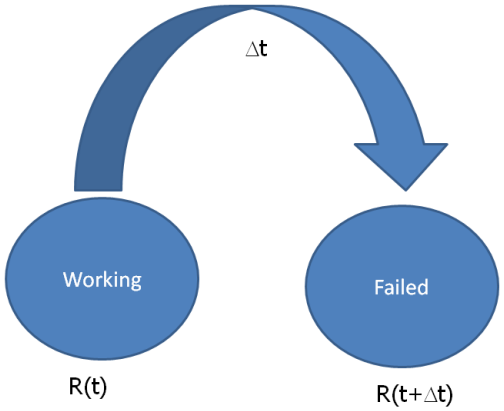
- Safe/Detected: λ^{SD}
- Safe/Undetected: λ^{SU}
- Dangerous/Detected: λ^{DD}
- Dangerous/Undetected: λ^{DU}

Primary Definitions:

- Failure Frequency
- Mean Time To Fail (MTTF)
- Probability of Failure upon Demand (PFD)
- Test intervals (TI) (directly affects PFD)



Reliability



$R(t+\Delta t)=R(t) - \lambda \Delta t\, R(t)$

$R(t)=\exp(-\lambda t)$

$P = 1- R$

$P(t) = 1- \exp(-\lambda t)$

- Instantaneous PFD: $PFD(t) = 1 - e^{-\lambda t}$
  - When $\lambda t<0.1$: $PFD(t) \approx \lambda t$

$$e^{-\lambda t} = 1 - \lambda t + \frac{\lambda^2 t^2}{2} - \frac{\lambda^3 t^3}{6} + \frac{\lambda^4 t^4}{24} - \dots$$

$$PFD_{avg} = \frac{1}{TI}\int_0^{TI} 1 - e^{-\lambda t} dt$$

$$PFD_{avg} = 1 + \frac{e^{-\lambda TI} - 1}{\lambda TI} \quad \textbf{for } \lambda t<0.1 \quad PFD_{avg} = \frac{\lambda TI}{2}$$

Working Example:

Vendor data for "NAMUR proximity switch NJ2-12GM-N (SJ2-N*)" are as follows:

λ_{total} = 29 FIT , SFF = 76%

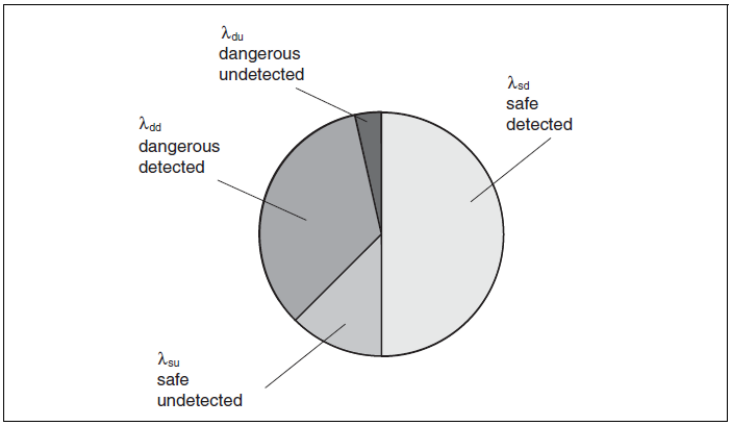
Complete the following table:

Proof Test Interval	PFD_{avg}	SIL Capability
1 year		
2 years		
5 years		

Other Definitions:

- Mean Time To Repair (MTTR)
- Availability = MTTF / (MTTF+MTTR)
- De-energize to trip (DTT)
- Energize to trip (ETT)
- Diagnostic Coverage Factor
  - $C = \lambda^D / \lambda$
- Spurious Trip: $MTTF^{Spurious}$
- Safe Failure Fraction (SFF):

Fraction of the failure rate, which does not have the potential to put the safety related system in a hazardous state.



- Safety Integrity:

"The probability of a Safety Instrumented Function satisfactorily performing the required safety functions under all stated conditions within a stated period of time."

Common Cause Failure

A failure, which is the result of one or more events causing coincident failures of two or more separate channels in a multiple channel system, leading to a system failure. Common cause is characterized by Beta Factor (Common Cause Factor):

$$\beta = \lambda^C / \lambda$$

Beta factor is calculated by a scoring model. The parameters are calculated as follows:

- $S = X + Y$ to obtain the value of β (for undetected failures)
- $S_D = X(1 + Z) + Y$ to obtain the value of β_D (for detected failures)

See IEC61508:2010, Part 6, Pages 88&89

Item	Logic subsystem		Sensors and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Separation/segregation				
Are all signal cables for the channels routed separately at all positions?	1,5	1,5	1,0	2,0
Are the logic subsystem channels on separate printed-circuit boards?	3,0	1,0		
Are the logic subsystems physically separated in an effective manner? For example, in separate cabinets.	2,5	0,5		
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?			2,5	1,5
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?			2,5	0,5
Diversity/redundancy				
Do the channels employ different electrical technologies for example, one electronic or programmable electronic and the other relay?	8,0			
Do the channels employ different electronic technologies for example, one electronic, the other programmable electronic?	6,0			
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc?			9,0	
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?			6,5	
Is low diversity used, for example hardware diagnostic tests using the same technology?	2,0	1,0		
Is medium diversity used, for example hardware diagnostic tests using different technology?	3,0	2,0		
Were the channels designed by different designers with no communication between them during the design activities?	1,5	1,5		
Are separate test methods and people used for each channel during commissioning?	1,0	0,5	1,0	2,0
Is maintenance on each channel carried out by different people at different times?	3,0		3,0	
Complexity/design/application/maturity/experience				
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	0,5	0,5	0,5	0,5
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	0,5	1,0	1,0	1,0
Is there more than 5 years experience with the same hardware used in similar environments?	1,0	1,5	1,5	1,5
Is the system simple, for example no more than 10 inputs or outputs per channel?		1,0		
Are inputs and outputs protected from potential levels of over-voltage and over-current?	1,5	0,5	1,5	0,5
Are all devices/components conservatively rated (for example, by a factor of 2 or more)?	2,0		2,0	
Assessment/analysis and feedback of data				
Have the results of the failure modes and effects analysis or fault-tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		3,0		3,0
Were common cause failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)		3,0		3,0
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0,5	3,5	0,5	3,5
Procedures/human interface				
Is there a written system of work to ensure that all component failures (or degradations) are detected, the root causes established and other similar items inspected for similar potential causes of failure?		1,5	0,5	1,5
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	1,5	0,5	2,0	1,0
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.) intended to be independent of each other, are not to be relocated?	0,5	0,5	0,5	0,5
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0,5	1,0	0,5	1,5
Does the system have low diagnostic coverage (60 % to 90 %) and report failures to the level of a field-replaceable module?	0,5			
Does the system have medium diagnostics coverage (90 % to 99 %) and report failures to the level of a field-replaceable module?	1,5	1,0		
Does the system have high diagnostics coverage (>99 %) and report failures to the level of a field-replaceable module?	2,5	1,5		
Do the system diagnostic tests report failures to the level of a field-replaceable module?			1,0	1,0

Item	Logic subsystem		Sensors and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Competence/training/safety culture				
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures?	2,0	3,0	2,0	3,0
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures?	0,5	4,5	0,5	4,5
Environmental control				
Is personnel access limited (for example locked cabinets, inaccessible position)?	0,5	2,5	0,5	2,5
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3,0	1,0	3,0	1,0
Are all signal and power cables separate at all positions?	2,0	1,0	2,0	1,0
Environmental testing				
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10,0	10,0	10,0	10,0

NOTE 1 A number of the items relate to the operation of the system, which may be difficult to predict at design time. In these cases, the designers should make reasonable assumptions and subsequently ensure that the eventual user of the system is made aware of, for example, the procedures to be put in place in order to achieve the designed level of safety integrity. This could be by including the necessary information in the accompanying documentation.

NOTE 2 The values in the *X* and *Y* columns are based on engineering judgement and take into account the indirect as well as the direct effects of the items in column 1. For example, the use of field-replaceable modules leads to

– repairs being carried out by the manufacturer under controlled conditions instead of (possibly incorrect) repairs being made under less appropriate conditions in the field. This leads to a contribution in the *Y* column because the potential for systematic (and, hence, common cause) failures is reduced;

– a reduction in the need for on-site manual interaction and the ability quickly to replace faulty modules, possibly on-line, so increasing the efficacy of the diagnostics for identifying failures before they become common-cause failures. This leads to a strong entry in the *X* column.

Table D.2 – Value of *Z* – programmable electronics

Diagnostic coverage	Diagnostic test interval		
	Less than 1 min	Between 1 min and 5 min	Greater than 5 min
≥ 99 %	2,0	1,0	0
≥ 90 %	1,5	0,5	0
≥ 60 %	1,0	0	0

Table D.3 – Value of *Z* – sensors or final elements

Diagnostic coverage	Diagnostic test interval			
	Less than 2 h	Between 2 h and two days	Between two days and one week	Greater than one week
≥ 99 %	2,0	1,5	1,0	0
≥ 90 %	1,5	1,0	0,5	0
≥ 60 %	1,0	0,5	0	0

	Corresponding value of β or β_D for the:	
Score (S or S_D)	PES	Sensors or actuators
120 or above	0.5%	1%
70 to 120	1%	2%
45 to 70	2%	5%
Less than 45	5%	10%

NOTE The maximum levels of β_D shown in this table are lower than would normally be used, reflecting the use of the techniques described elsewhere in this technical report for the reduction in the probability of systematic failures as a whole, and of Common cause failures as a result of this.

Values of β_D lower than 0.5% for the PES and 1% for the sensors would be difficult to justify.

Redundancy

Use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy).

HFT = maximum number of failures that can be tolerated in a SIS component

Architectural Constraints on type A safety-related systems

Safe failure fraction	**Hardware fault tolerance (see note 2)**		
	0	**1**	**2**
< 60 %	SIL1	SIL2	SIL3
60 % – < 90 %	SIL2	SIL3	SIL4
90 % – < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.
NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.
NOTE 3 See annex C for details of how to calculate safe failure fraction.

Architectural Constraints on type B safety-related systems

Safe failure fraction	**Hardware fault tolerance (see note 2)**		
	0	**1**	**2**
< 60 %	Not allowed	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4

NOTE 1 See 7.4.3.1.1 to 7.4.3.1.4 for details on interpreting this table.
NOTE 2 A hardware fault tolerance of N means that N + 1 faults could cause a loss of the safety function.
NOTE 3 See annex C for details of how to calculate safe failure fraction.

Subsystem type A: A subsystem can be regarded as type A if, for the components required to achieve the safety function

- the failure modes of all constituent components are well defined; and
- the behavior of the subsystem under fault conditions can be completely determined; and

- there is sufficient dependable failure data from field experience to show that the claimed rates of failure for detected and undetected dangerous failures are met.

Subsystem type B: A subsystem shall be regarded as type B, if for the components required to achieve the safety function

- the failure mode of at least one constituent component is not well defined; or
- the behavior of the subsystem under fault conditions cannot be completely determined; or
- there is insufficient dependable failure data from field experience to support claims for rates of failure for detected and undetected dangerous failures.

Simplifying, one can say that as long as programmable or highly integrated electronic components are used, a subsystem must be considered as type B.

Failure Rate Data

- OREDA - SINTEF
- PERD - CCPS
- IEREDA
- MIL
- SERH - Exida (www.sael-online.com)
- …

Simplified Equations

Assumptions:

- Component failure and repair rates are assumed to be constant over the life of the SIF.
- Once a component has failed in one of the possible failure modes it cannot fail again in one of the remaining failure modes.
- The equations assume similar failure rates for redundant components.
- The Test Interval (TI) is assumed to be much shorter than the Mean Time To Failure (MTTF).

- SIS PFD_{avg}:

$$\mathrm{PFD}_{\mathrm{SIS}} = \sum \mathrm{PFD}_{\mathrm{Si}} + \sum \mathrm{PFD}_{\mathrm{Ai}} + \sum \mathrm{PFD}_{\mathrm{Li}} + \sum PFD_{PSi}$$

- Converting MTTF to failure rate:

$$\lambda^{DU} = \frac{1}{MTTF^{DU}}$$

- PFD_{avg}:

$$\mathrm{PFD}_{\mathrm{avg}} = \left[\lambda^{DU} \times \frac{\mathrm{TI}}{2}\right]$$

- PFD_{avg} (including systematic failures):

$$\mathrm{PFD}_{\mathrm{avg}} = \left[\lambda^{DU} \times \frac{\mathrm{TI}}{2}\right] + \left[\lambda_F^D \times \frac{TI}{2}\right]$$

Full equations:

- **1oo2**

$$\mathrm{PFD}_{\mathrm{avg}} = \left[\left((1-\beta)\times\lambda^{DU}\right)^2 \times \frac{TI^2}{3}\right] + \left[(1-\beta)\times\lambda^{DU}\times\lambda^{DD}\times MTTR\times TI\right] + \left[\beta\times\lambda^{DU}\times\frac{TI}{2}\right] + \left[\lambda_F^D\times\frac{TI}{2}\right]$$

- **1oo3**

$$PFD_{avg} = \left[\left(\lambda^{DU}\right)^3\times\frac{TI^3}{4}\right] + \left[\left(\lambda^{DU}\right)^2\times\lambda^{DD}\times MTTR\times TI^2\right] + \left[\beta\times\left(\lambda^{DU}\times\frac{TI}{2}\right)\right] + \left[\lambda_F^D\times\frac{TI}{2}\right]$$

- **2oo2**

$$\mathrm{PFD}_{\mathrm{avg}} = \left[\lambda^{DU}\times TI\right] + \left[\beta\times\lambda^{DU}\times TI\right] + \left[\lambda_F^D\times\frac{TI}{2}\right]$$

- **2oo3**

$$\mathrm{PFD}_{\mathrm{avg}} = \left[(\lambda^{DU})^2\times(TI)^2\right] + \left[3\lambda^{DU}\times\lambda^{DD}\times MTTR\times TI\right] + \left[\beta\times\lambda^{DU}\times\frac{TI}{2}\right] + \left[\lambda_F^D\times\frac{TI}{2}\right]$$

- **2oo4**

$$PFD_{avg} = \left[\left(\lambda^{DU}\right)^3\times(TI)^3\right] + \left[4\left(\lambda^{DU}\right)^2\times\lambda^{DD}\times MTTR\times(TI)^2\right] + \left[\beta\times\lambda^{DU}\times\frac{TI}{2}\right] + \left[\lambda_F^D\times\frac{TI}{2}\right]$$

Simplified equations:

Voting type	Equation
1oo1	$PFD_{avg} = \lambda^{DU}\times\frac{TI}{2}$
1oo2	$PFD_{avg} = \frac{\left[\left(\lambda^{DU}\right)^2\times TI^2\right]}{3}$
1oo3	$PFD_{avg} = \frac{\left[\left(\lambda^{DU}\right)^3\times TI^3\right]}{4}$
2oo2	$PFD_{avg} = \lambda^{DU}\times TI$
2oo3	$PFD_{avg} = \left(\lambda^{DU}\right)^2\times TI^2$
2oo4	$PFD_{avg} = \left(\lambda^{DU}\right)^3\times(TI)^3$

Spurious Trip Rate (STR)

$$STR = \lambda^S + \lambda^{DD} + \lambda_F^S$$

In the above equation:

- λ^S is the safe or spurious failure rate for the component,
- λ^{DD} is the dangerous detected failure rate for the component,
- λ_F^S is the safe systematic failure rate for the component

Voting type	Equation
1oo1	$STR = \lambda^S$
1oo2	$STR = 2 \times \lambda^S$
1oo3	$STR = 3 \times \lambda^S$
2oo2	$STR = 2 \times (\lambda^S)^2 \times MTTR$
2oo3	$STR = 6 \times (\lambda^S)^2 \times MTTR$
2oo4	$STR = 12 \times (\lambda^S)^3 \times MTTR^2$

Table B.2 – Average probability of failure on demand for a proof test interval of six months and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	1,1E-04			5,5E-04			1,1E-03		
	60 %	4,4E-05			2,2E-04			4,4E-04		
	90 %	1,1E-05			5,7E-05			1,1E-04		
	99 %	1,5E-06			7,5E-06			1,5E-05		
1oo2	0 %	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
2oo2 (see Note 2)	0 %	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,3E-05			1,1E-04			2,3E-04		
	99 %	3,0E-06			1,5E-05			3,0E-05		
1oo2D (see Note 3)	0 %	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04
	60 %	1,4E-06	4,9E-06	9,3E-06	7,1E-06	2,5E-05	4,7E-05	1,4E-05	5,0E-05	9,3E-05
	90 %	4,3E-07	1,3E-06	2,4E-06	2,2E-06	6,6E-06	1,2E-05	4,3E-06	1,3E-05	2,4E-05
	99 %	6,0E-08	1,5E-07	2,6E-07	3,0E-07	7,4E-07	1,3E-06	6,0E-07	1,5E-06	2,6E-06
2oo3	0 %	2,2E-06	1,1E-05	2,2E-05	1,2E-05	5,6E-05	1,1E-04	2,7E-05	1,1E-04	2,2E-04
	60 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,3E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06
1oo3	0 %	2,2E-06	1,1E-05	2,2E-05	1,1E-05	5,5E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04
	60 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	90 %	2,2E-07	1,1E-06	2,2E-06	1,1E-06	5,6E-06	1,1E-05	2,2E-06	1,1E-05	2,2E-05
	99 %	2,6E-08	1,3E-07	2,6E-07	1,3E-07	6,5E-07	1,3E-06	2,6E-07	1,3E-06	2,6E-06

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	5,5E-03			1,1E-02			5,5E-02		
	60 %	2,2E-03			4,4E-03			2,2E-02		
	90 %	5,7E-04			1,1E-03			5,7E-03		
	99 %	7,5E-05			1,5E-04			7,5E-04		
1oo2	0 %	1,5E-04	5,8E-04	1,1E-03	3,7E-04	1,2E-03	2,3E-03	5,0E-03	8,8E-03	1,4E-02
	60 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	90 %	1,2E-05	5,6E-05	1,1E-04	2,4E-05	1,1E-04	2,2E-04	1,5E-04	6,0E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,4E-05	6,6E-05	1,3E-04
2oo2 (see Note 2)	0 %	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,3E-03			1,1E-02		
	99 %	1,5E-04			3,0E-04			1,5E-03		
1oo2D (see Note 3)	0 %	1,5E-04	5,8E-04	1,1E-03	3,8E-04	1,2E-03	2,3E-03	5,0E-03	9,0E-03	1,4E-02
	60 %	7,7E-05	2,5E-04	4,7E-04	1,7E-04	5,2E-04	9,5E-04	1,3E-03	3,0E-03	5,1E-03
	90 %	2,2E-05	6,6E-05	1,2E-04	4,5E-05	1,3E-04	2,4E-04	2,6E-04	6,9E-04	1,2E-03
	99 %	3,0E-06	7,4E-06	1,3E-05	6,0E-06	1,5E-05	2,6E-05	3,0E-05	7,4E-05	1,3E-04
2oo3	0 %	2,3E-04	6,5E-04	1,2E-03	6,8E-04	1,5E-03	2,5E-03	1,3E-02	1,5E-02	1,9E-02
	60 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,3E-03	3,9E-03	5,9E-03
	90 %	1,2E-05	5,7E-05	1,1E-04	2,7E-05	1,2E-04	2,3E-04	2,4E-04	6,8E-04	1,2E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,7E-06	1,3E-05	2,6E-05	1,5E-05	6,7E-05	1,3E-04
1oo3	0 %	1,1E-04	5,5E-04	1,1E-03	2,2E-04	1,1E-03	2,2E-03	1,4E-03	5,7E-03	1,1E-02
	60 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	90 %	1,1E-05	5,6E-05	1,1E-04	2,2E-05	1,1E-04	2,2E-04	1,1E-04	5,6E-04	1,1E-03
	99 %	1,3E-06	6,5E-06	1,3E-05	2,6E-06	1,3E-05	2,6E-05	1,3E-05	6,5E-05	1,3E-04

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.3 – Average probability of failure on demand for a proof test interval of one year and mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	2,2E-04			1,1E-03			2,2E-03		
	60 %	8,8E-05			4,4E-04			8,8E-04		
	90 %	2,2E-05			1,1E-04			2,2E-04		
	99 %	2,6E-06			1,3E-05			2,6E-05		
1oo2	0 %	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,0E-06	4,4E-05	8,8E-05	1,9E-05	8,9E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
2oo2 (see Note 2)	0 %	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,5E-05			2,2E-04			4,5E-04		
	99 %	5,2E-06			2,6E-05			5,2E-05		
1oo2D (see Note 3)	0 %	4,5E-06	2,2E-05	4,4E-05	2,4E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	60 %	2,8E-06	9,8E-06	1,9E-05	1,4E-05	4,9E-05	9,3E-05	2,9E-05	9,9E-05	1,9E-04
	90 %	8,5E-07	2,6E-06	4,8E-06	4,3E-06	1,3E-05	2,4E-05	8,5E-06	2,6E-05	4,8E-05
	99 %	1,0E-07	2,8E-07	5,0E-07	5,2E-07	1,4E-06	2,5E-06	1,0E-06	2,8E-06	5,0E-06
2oo3	0 %	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,2E-05	2,4E-04	4,5E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	9,5E-06	4,5E-05	8,8E-05	2,1E-05	9,1E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06
1oo3	0 %	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	60 %	1,8E-06	8,8E-06	1,8E-05	8,8E-06	4,4E-05	8,8E-05	1,8E-05	8,8E-05	1,8E-04
	90 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05
	99 %	4,8E-08	2,4E-07	4,8E-07	2,4E-07	1,2E-06	2,4E-06	4,8E-07	2,4E-06	4,8E-06

Architecture	DC	λ_D = 2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	1,1E-02			2,2E-02			>1E-01		
	60 %	4,4E-03			8,8E-03			4,4E-02		
	90 %	1,1E-03			2,2E-03			1,1E-02		
	99 %	1,3E-04			2,6E-04			1,3E-03		
1oo2	0 %	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03	1,8E-02	2,4E-02	3,2E-02
	60 %	1,1E-04	4,6E-04	9,0E-04	2,8E-04	9,7E-04	1,8E-03	3,4E-03	6,6E-03	1,1E-02
	90 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,9E-06	2,4E-05	4,8E-05	2,6E-05	1,2E-04	2,4E-04
2oo2 (see Note 2)	0 %	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,5E-03			2,2E-02		
	99 %	2,6E-04			5,2E-04			2,6E-03		
1oo2D (see Note 3)	0 %	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,9E-03	1,8E-02	2,5E-02	3,4E-02
	60 %	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03	3,9E-03	7,1E-03	1,1E-02
	90 %	4,4E-05	1,3E-04	2,4E-04	9,1E-05	2,7E-04	4,8E-04	5,8E-04	1,4E-03	2,5E-03
	99 %	5,2E-06	1,4E-05	2,5E-05	1,0E-05	2,8E-05	5,0E-05	5,4E-05	1,4E-04	2,5E-04
2oo3	0 %	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,8E-03	5,6E-03	4,8E-02	5,0E-02	5,3E-02
	60 %	1,6E-04	5,1E-04	9,4E-04	4,8E-04	1,1E-03	2,0E-03	8,4E-03	1,1E-02	1,5E-02
	90 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
	99 %	2,5E-06	1,2E-05	2,4E-05	5,1E-06	2,4E-05	4,8E-05	3,1E-05	1,3E-04	2,5E-04
1oo3	0 %	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,7E-03	1,3E-02	2,3E-02
	60 %	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03	1,0E-03	4,5E-03	8,9E-03
	90 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03
	99 %	2,4E-06	1,2E-05	2,4E-05	4,8E-06	2,4E-05	4,8E-05	2,4E-05	1,2E-04	2,4E-04

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.4 – Average probability of failure on demand for a proof test interval of two years and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	4,4E-04			2,2E-03			4,4E-03		
	60 %	1,8E-04			8,8E-04			1,8E-03		
	90 %	4,4E-05			2,2E-04			4,4E-04		
	99 %	4,8E-06			2,4E-05			4,8E-05		
1oo2	0 %	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	8,9E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,9E-05	8,9E-05	1,8E-04	3,9E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,5E-06	2,2E-05	4,4E-05	9,1E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06
2oo2 (see Note 2)	0 %	8,8E-04			4,4E-03			8,8E-03		
	60 %	3,5E-04			1,8E-03			3,5E-03		
	90 %	8,8E-05			4,4E-04			8,8E-04		
	99 %	9,6E-06			4,8E-05			9,6E-05		
1oo2D (see Note 3)	0 %	9,0E-06	4,4E-05	8,8E-05	5,0E-05	2,2E-04	4,4E-04	1,1E-04	4,6E-04	9,0E-04
	60 %	5,7E-06	2,0E-05	3,7E-05	2,9E-05	9,9E-05	1,9E-04	6,0E-05	2,0E-04	3,7E-04
	90 %	1,7E-06	5,2E-06	9,6E-06	8,5E-06	2,6E-05	4,8E-05	1,7E-05	5,2E-05	9,6E-05
	99 %	1,9E-07	5,4E-07	9,8E-07	9,5E-07	2,7E-06	4,9E-06	1,9E-06	5,4E-06	9,8E-06
2oo3	0 %	9,5E-06	4,4E-05	8,8E-05	6,2E-05	2,3E-04	4,5E-04	1,6E-04	5,0E-04	9,3E-04
	60 %	3,6E-06	1,8E-05	3,5E-05	2,1E-05	9,0E-05	1,8E-04	4,7E-05	1,9E-04	3,6E-04
	90 %	8,9E-07	4,4E-06	8,8E-06	4,6E-06	2,2E-05	4,4E-05	9,6E-06	4,5E-05	8,9E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,3E-07	4,6E-06	9,2E-06
1oo3	0 %	8,8E-06	4,4E-05	8,8E-05	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04
	60 %	3,5E-06	1,8E-05	3,5E-05	1,8E-05	8,8E-05	1,8E-04	3,5E-05	1,8E-04	3,5E-04
	90 %	8,8E-07	4,4E-06	8,8E-06	4,4E-06	2,2E-05	4,4E-05	8,8E-06	4,4E-05	8,8E-05
	99 %	9,2E-08	4,6E-07	9,2E-07	4,6E-07	2,3E-06	4,6E-06	9,2E-07	4,6E-06	9,2E-06

Architecture	DC	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	2,2E-02			4,4E-02			>1E-01		
	60 %	8,8E-03			1,8E-02			8,8E-02		
	90 %	2,2E-03			4,4E-03			2,2E-02		
	99 %	2,4E-04			4,8E-04			2,4E-03		
1oo2	0 %	1,1E-03	2,7E-03	4,8E-03	3,3E-03	6,5E-03	1,0E-02	6,6E-02	7,4E-02	8,5E-02
	60 %	2,8E-04	9,7E-04	1,8E-03	7,5E-04	2,1E-03	3,8E-03	1,2E-02	1,8E-02	2,5E-02
	90 %	5,0E-05	2,3E-04	4,5E-04	1,1E-04	4,6E-04	9,0E-04	1,1E-03	2,8E-03	4,9E-03
	99 %	4,7E-06	2,3E-05	4,6E-05	9,5E-06	4,6E-05	9,2E-05	5,4E-05	2,4E-04	4,6E-04
2oo2 (see Note 2)	0 %	4,4E-02			8,8E-02			>1E-01		
	60 %	1,8E-02			3,5E-02			>1E-01		
	90 %	4,4E-03			8,8E-03			4,4E-02		
	99 %	4,8E-04			9,6E-04			4,8E-03		
1oo2D (see Note 3)	0 %	1,1E-03	2,7E-03	4,8E-03	3,4E-03	6,6E-03	1,1E-02	6,7E-02	7,7E-02	9,0E-02
	60 %	3,8E-04	1,1E-03	1,9E-03	9,6E-04	2,3E-03	4,0E-03	1,3E-02	1,9E-02	2,6E-02
	90 %	9,0E-05	2,6E-04	4,8E-04	1,9E-04	5,4E-04	9,8E-04	1,5E-03	3,2E-03	5,3E-03
	99 %	9,6E-06	2,7E-05	4,9E-05	1,9E-05	5,4E-05	9,8E-05	1,0E-04	2,8E-04	5,0E-04
2oo3	0 %	2,3E-03	3,7E-03	5,6E-03	8,3E-03	1,1E-02	1,4E-02	1,9E-01	1,8E-01	1,7E-01
	60 %	4,8E-04	1,1E-03	2,0E-03	1,6E-03	2,8E-03	4,4E-03	3,2E-02	3,5E-02	4,0E-02
	90 %	6,3E-05	2,4E-04	4,6E-04	1,6E-04	5,1E-04	9,4E-04	2,4E-03	4,0E-03	6,0E-03
	99 %	4,8E-06	2,3E-05	4,6E-05	1,0E-05	4,7E-05	9,2E-05	6,9E-05	2,5E-04	4,8E-04
1oo3	0 %	4,6E-04	2,2E-03	4,4E-03	1,0E-03	4,5E-03	8,9E-03	2,4E-02	3,7E-02	5,5E-02
	60 %	1,8E-04	8,8E-04	1,8E-03	3,6E-04	1,8E-03	3,5E-03	3,1E-03	9,9E-03	1,8E-02
	90 %	4,4E-05	2,2E-04	4,4E-04	8,8E-05	4,4E-04	8,8E-04	4,6E-04	2,2E-03	4,4E-03
	99 %	4,6E-06	2,3E-05	4,6E-05	9,2E-06	4,6E-05	9,2E-05	4,6E-05	2,3E-04	4,6E-04

NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Table B.5 – Average probability of failure on demand for a proof test interval of ten years and a mean time to restoration of 8 h

Architecture	DC	λ_D = 0,5E-07			λ_D = 2,5E-07			λ_D = 0,5E-06		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	2,2E-03			1,1E-02			2,2E-02		
	60 %	8,8E-04			4,4E-03			8,8E-03		
	90 %	2,2E-04			1,1E-03			2,2E-03		
	99 %	2,2E-05			1,1E-04			2,2E-04		
1oo2	0 %	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	1,9E-05	8,9E-05	1,8E-04	1,1E-04	4,6E-04	9,0E-04	2,7E-04	9,6E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,3E-05	1,1E-04	2,2E-04	5,0E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,5E-06	2,2E-05	4,4E-05
2oo2 (see Note 2)	0 %	4,4E-03			2,2E-02			4,4E-02		
	60 %	1,8E-03			8,8E-03			1,8E-02		
	90 %	4,4E-04			2,2E-03			4,4E-03		
	99 %	4,5E-05			2,2E-04			4,5E-04		
1oo2D (see Note 3)	0 %	5,0E-05	2,2E-04	4,4E-04	3,7E-04	1,2E-03	2,3E-03	1,1E-03	2,7E-03	4,8E-03
	60 %	2,9E-05	9,9E-05	1,9E-04	1,7E-04	5,1E-04	9,5E-04	3,8E-04	1,1E-03	1,9E-03
	90 %	8,4E-06	2,6E-05	4,8E-05	4,3E-05	1,3E-04	2,4E-04	9,0E-05	2,6E-04	4,8E-04
	99 %	8,9E-07	2,6E-06	4,8E-06	4,5E-06	1,3E-05	2,4E-05	8,9E-06	2,6E-05	4,8E-05
2oo3	0 %	6,2E-05	2,3E-04	4,5E-04	6,8E-04	1,5E-03	2,5E-03	2,3E-03	3,7E-03	5,6E-03
	60 %	2,1E-05	9,0E-05	1,8E-04	1,6E-04	5,0E-04	9,3E-04	4,7E-04	1,1E-03	2,0E-03
	90 %	4,6E-06	2,2E-05	4,4E-05	2,7E-05	1,1E-04	2,2E-04	6,3E-05	2,4E-04	4,5E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,3E-06	1,1E-05	2,2E-05	4,6E-06	2,2E-05	4,4E-05
1oo3	0 %	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03
	60 %	1,8E-05	8,8E-05	1,8E-04	8,8E-05	4,4E-04	8,8E-04	1,8E-04	8,8E-04	1,8E-03
	90 %	4,4E-06	2,2E-05	4,4E-05	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04
	99 %	4,4E-07	2,2E-06	4,4E-06	2,2E-06	1,1E-05	2,2E-05	4,4E-06	2,2E-05	4,4E-05

Architecture	DC	λ_D =2,5E-06			λ_D = 0,5E-05			λ_D = 2,5E-05		
		β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %	β = 2 % β_D = 1 %	β = 10 % β_D = 5 %	β = 20 % β_D = 10 %
1oo1 (see Note 2)	0 %	>1E-01			>1E-01			>1E-01		
	60 %	4,4E-02			8,8E-02			>1E-01		
	90 %	1,1E-02			2,2E-02			>1E-01		
	99 %	1,1E-03			2,2E-03			1,1E-02		
1oo2	0 %	1,8E-02	2,4E-02	3,2E-02	6,6E-02	7,4E-02	8,5E-02	>1E-01	>1E-01	>1E-01
	60 %	3,4E-03	6,6E-03	1,1E-02	1,2E-02	1,8E-02	2,5E-02	>1E-01	>1E-01	>1E-01
	90 %	3,8E-04	1,2E-03	2,3E-03	1,1E-03	2,8E-03	4,9E-03	1,8E-02	2,5E-02	3,5E-02
	99 %	2,4E-05	1,1E-04	2,2E-04	5,1E-05	2,3E-04	4,5E-04	3,8E-04	1,3E-03	2,3E-03
2oo2 (see Note 2)	0 %	>1E-01			>1E-01			>1E-01		
	60 %	8,8E-02			>1E-01			>1E-01		
	90 %	2,2E-02			4,4E-02			>1E-01		
	99 %	2,2E-03			4,5E-03			2,2E-02		
1oo2D (see Note 3)	0 %	1,8E-02	2,5E-02	3,3E-02	6,6E-02	7,7E-02	9,0E-02	1,6E+00	1,5E+00	1,4E+00
	60 %	3,9E-03	7,1E-03	1,1E-02	1,3E-02	1,9E-02	2,6E-02	2,6E-01	2,7E-01	2,8E-01
	90 %	5,7E-04	1,4E-03	2,5E-03	1,5E-03	3,1E-03	5,2E-03	2,0E-02	2,7E-02	3,5E-02
	99 %	4,6E-05	1,3E-04	2,4E-04	9,5E-05	2,7E-04	4,9E-04	6,0E-04	1,5E-03	2,5E-03
2oo3	0 %	4,8E-02	5,0E-02	5,3E-02	1,9E-01	1,8E-01	1,7E-01	4,6E+00	4,0E+00	3,3E+00
	60 %	8,3E-03	1,1E-02	1,4E-02	3,2E-02	3,5E-02	4,0E-02	7,6E-01	7,1E-01	6,6E-01
	90 %	6,9E-04	1,5E-03	2,6E-03	2,3E-03	3,9E-03	5,9E-03	4,9E-02	5,4E-02	6,0E-02
	99 %	2,7E-05	1,2E-04	2,3E-04	6,4E-05	2,4E-04	4,6E-04	7,1E-04	1,6E-03	2,6E-03
1oo3	0 %	4,7E-03	1,3E-02	2,3E-02	2,4E-02	3,7E-02	5,5E-02	2,5E+00	2,0E+00	1,6E+00
	60 %	1,0E-03	4,5E-03	8,9E-03	3,0E-03	9,8E-03	1,8E-02	1,7E-01	1,8E-01	1,9E-01
	90 %	2,2E-04	1,1E-03	2,2E-03	4,6E-04	2,2E-03	4,4E-03	4,8E-03	1,3E-02	2,4E-02
	99 %	2,2E-05	1,1E-04	2,2E-04	4,4E-05	2,2E-04	4,4E-04	2,2E-04	1,1E-03	2,2E-03

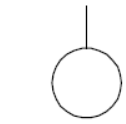
NOTE 1 This table gives example values of PFD_G, calculated using the equations in B.3.2 and depending on the assumptions listed in B.3.1. If the sensor, logic or final element subsystem comprises of only one group of voted channels, then PFD_G is equivalent to PFD_S, PFD_L or PFD_{FE} respectively (see B.3.2.1).

NOTE 2 The table assumes $\beta = 2 \times \beta_D$. For 1oo1 and 2oo2 architectures, the values of β and β_D do not affect the average probability of failure.

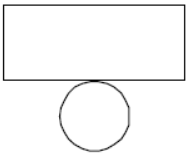
NOTE 3 The safe failure rate is assumed to be equal to the dangerous failure rate and K = 0,98.

Fault Tree Analysis

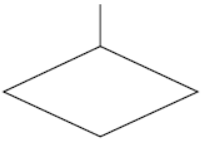
Fault tree analysis (FTA) is a top down, Deductive reasoning failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. This analysis method is mainly used in the field of Safety engineering and Reliability engineering to understand how systems can fail, to identify the best ways to reduce risk or to determine (or get a feeling for) event rates of a safety accident or a particular system level (functional) failure.



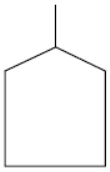
Basic Event



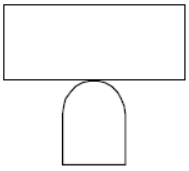
Boxed Basic Event



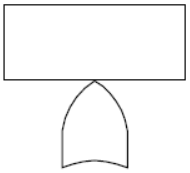
Undeveloped Event



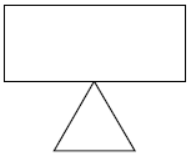
House Event



AND Gate

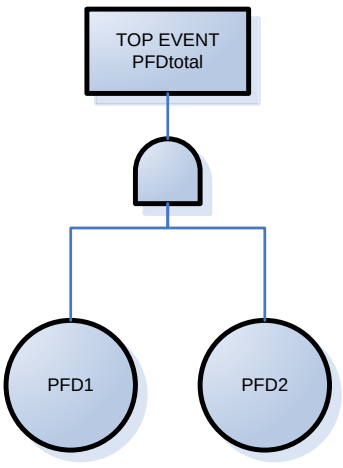


OR Gate



Transfer Gate

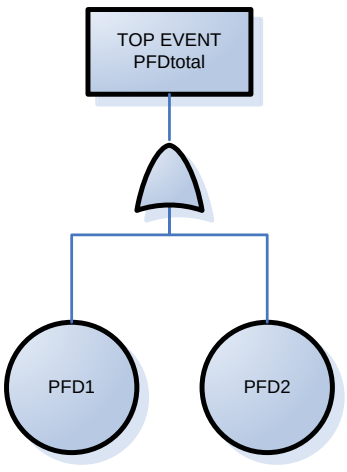
Transfer



AND Gate

$PFD_{total} = PFD_1 \times PFD_2$

$PFD_{total} = PFD_1 \times PFD_2 \times \ldots \times PFD_N$



OR Gate

$PFD_{total} = PFD_1 + PFD_2 - PFD_1 \times PFD_2$

$(1\text{-}PFD_{total}) = (1\text{-}PFD_1) \times (1\text{-}PFD_2) \times \ldots \times (1\text{-}PFD_N)$

Procedure

1. SIF Description and Application Information
2. Top Event Identification
3. Construction of the FTA
4. Qualitative Examination of the Fault Tree Structure
5. Quantitative FTA Evaluation

Top events:

- For SIL determination, the Top Event is the probability of the SIF to fail on process demand for a given safety function.
- For availability purposes, the top event is spurious trip of SIF.

Typical HIPPS System