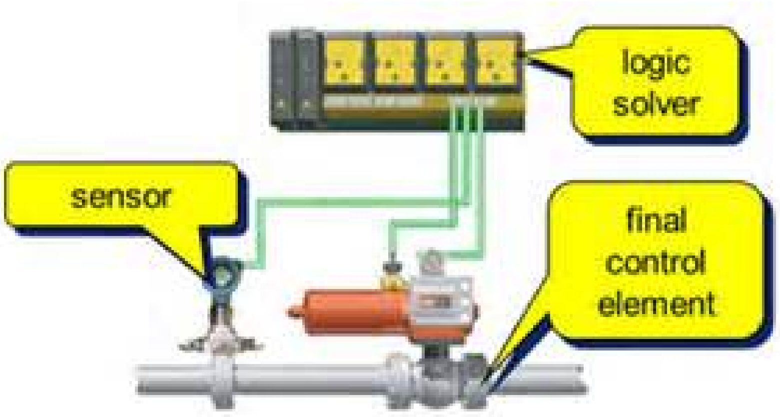
Functional Safety

&

Safety Integrity Levels



Presented by:

Ali Baghaei

Outlines

- Part 1
  - Introduction to Functional Safety
  - Definitions
- Part 2
  - SIL Target Evaluation
  - Risk Graph Method
- Part 3
  - SIL Verification
  - FTA Method
- Part 4
  - Course Review

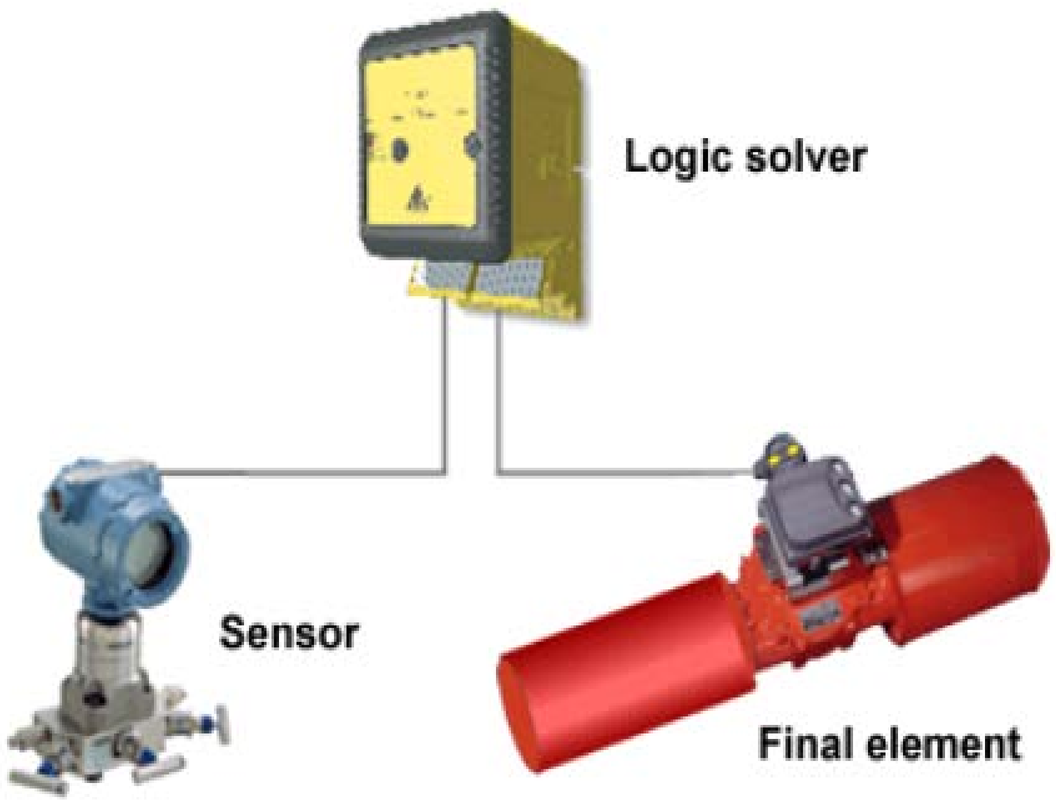
- Part 1: Definitions
  - Safety Related Systems
  - Functional Safety
  - Safety Lifecycle
  - Standards
  - Safety Integrity Levels

Safety Related Systems (SRS)

- Mechanical protection system
- Passive protection systems
- Non-SIS instrumented systems (BPCS)
- Alarms
- Safety Instrumented Systems (SIS)

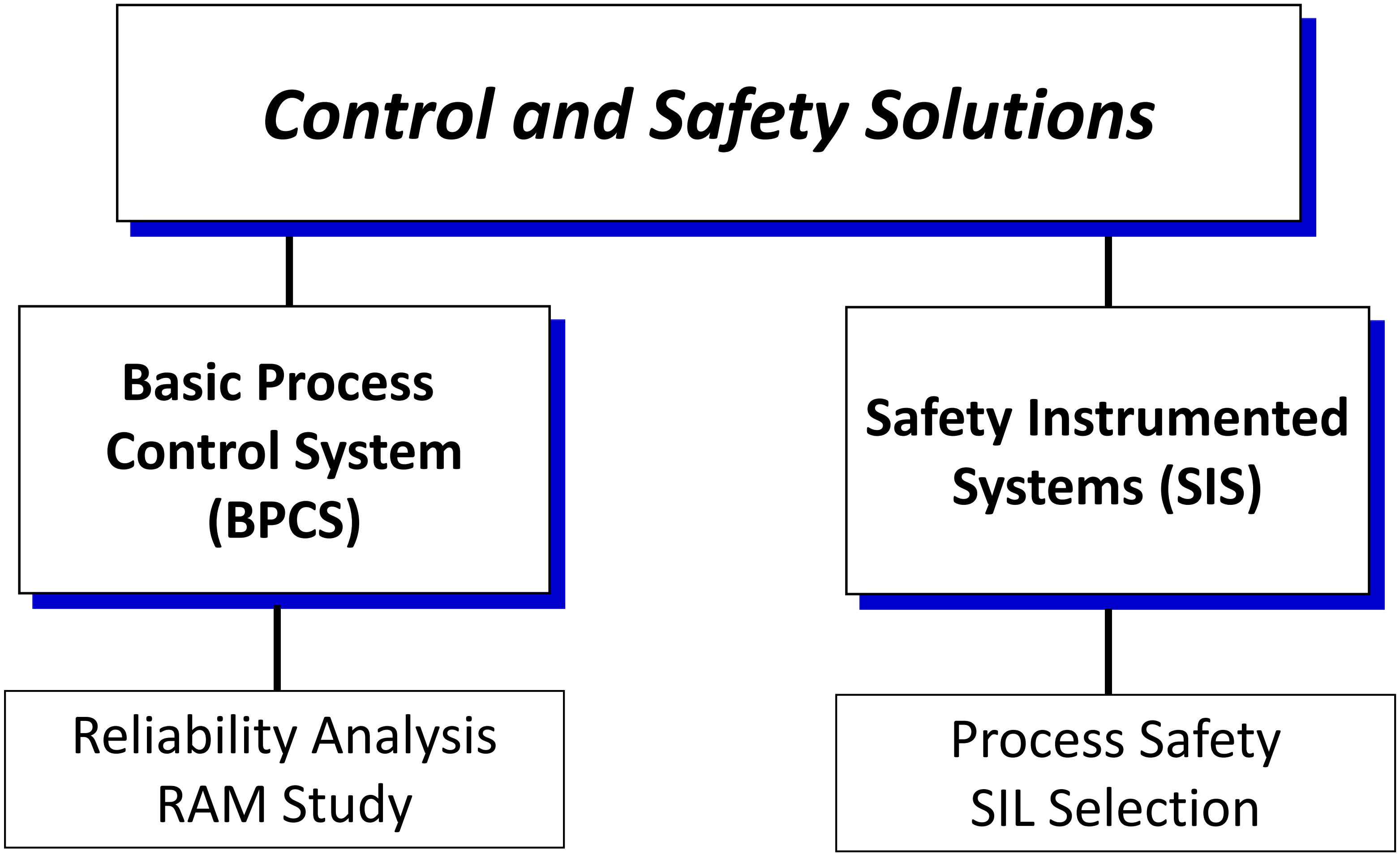
  trip system, shutdown system, interlock, instrumented protection system (IPS)

SIS Main Components



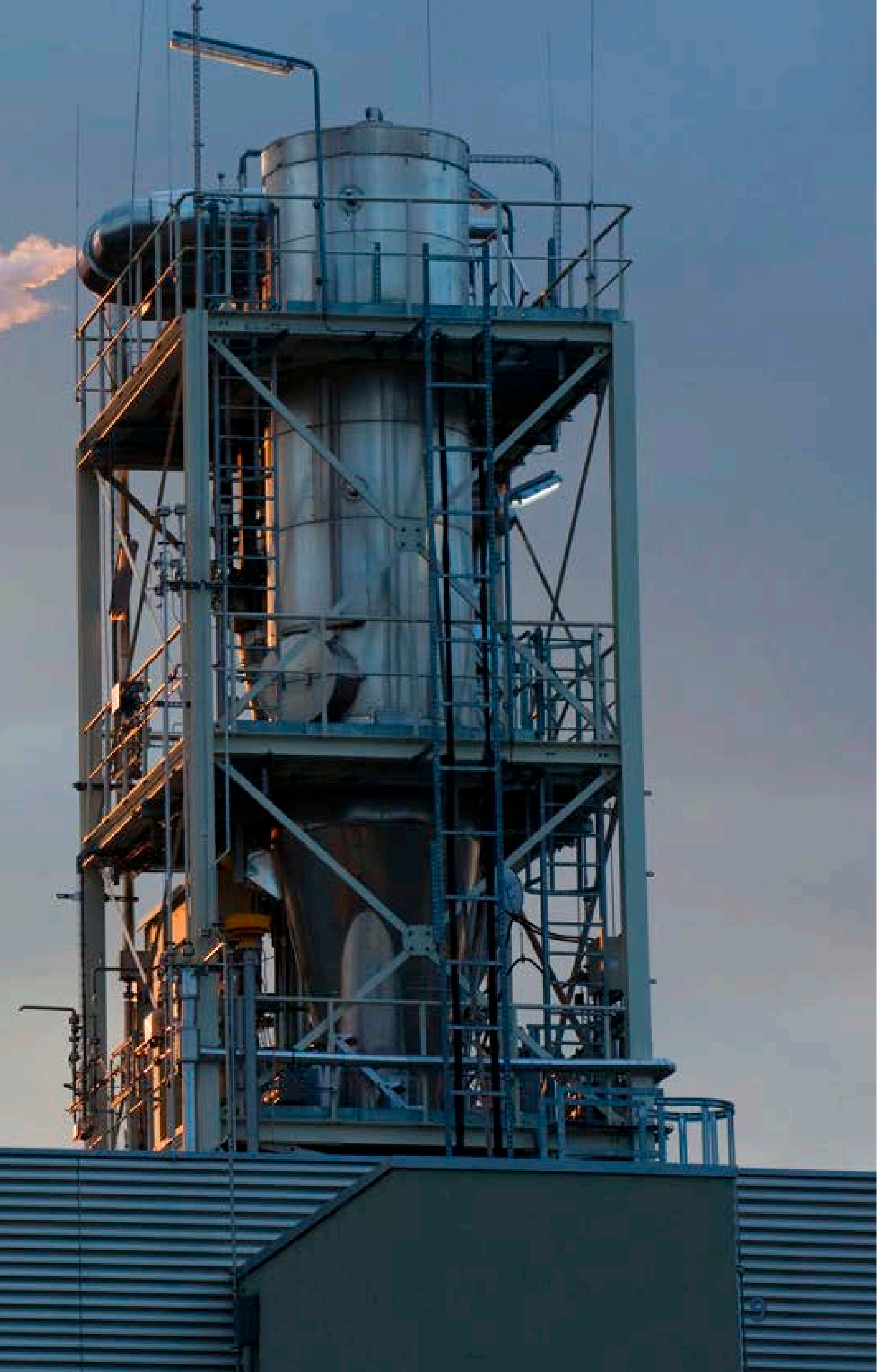
- The function of a Safety Instrumented System (SIS) is called a Safety Instrumented Function (SIF).
- More than one SIF may be assigned to a single SIS.

SIL Study vs. RAM Study



Functional Safety

The ability of a safety instrumented system (E/E/PE) 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-84.00.01: Application of Safety Instrumented Systems for the Process Industries


IEC 61511-1

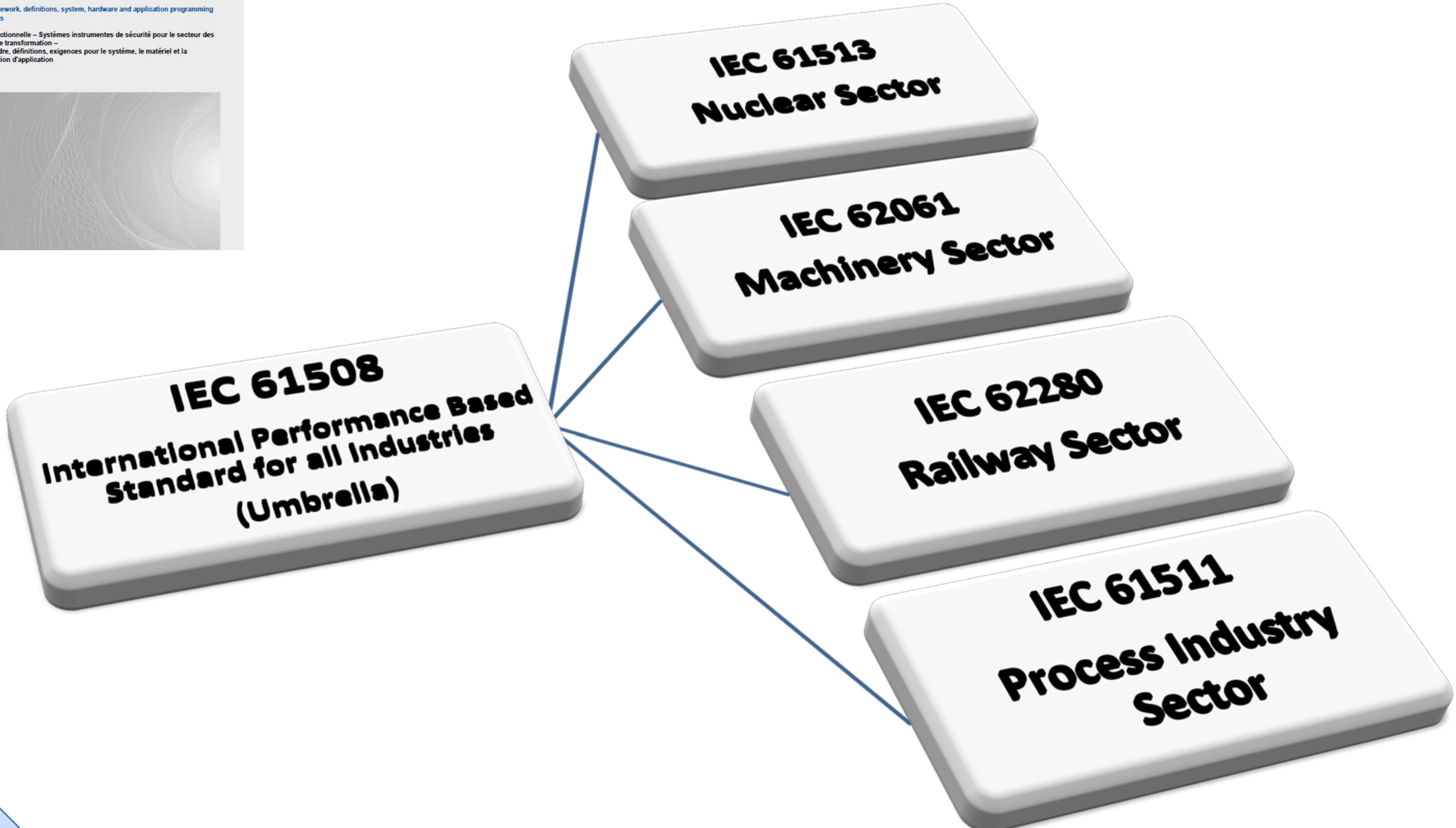
Edition 2.0 2016-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

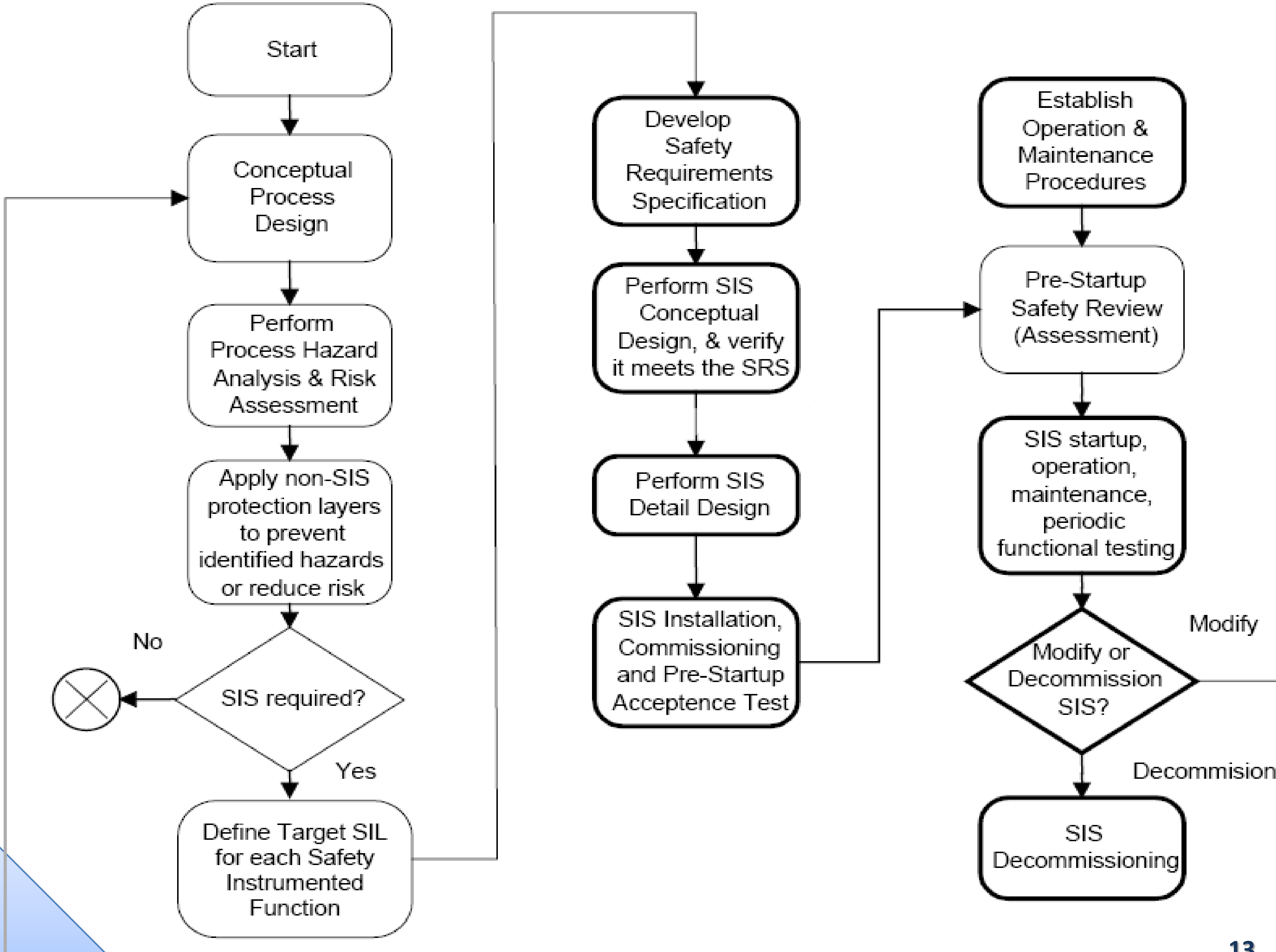
Functional safety – Safety instrumented systems for the process industry sector –
Part 1: Framework, definitions, system, hardware and application programming requirements

Sécurite fonctionnelle – Systèmes instrumentes de sécurité pour le secteur des industries de transformation –
Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application



Safety Lifecycle

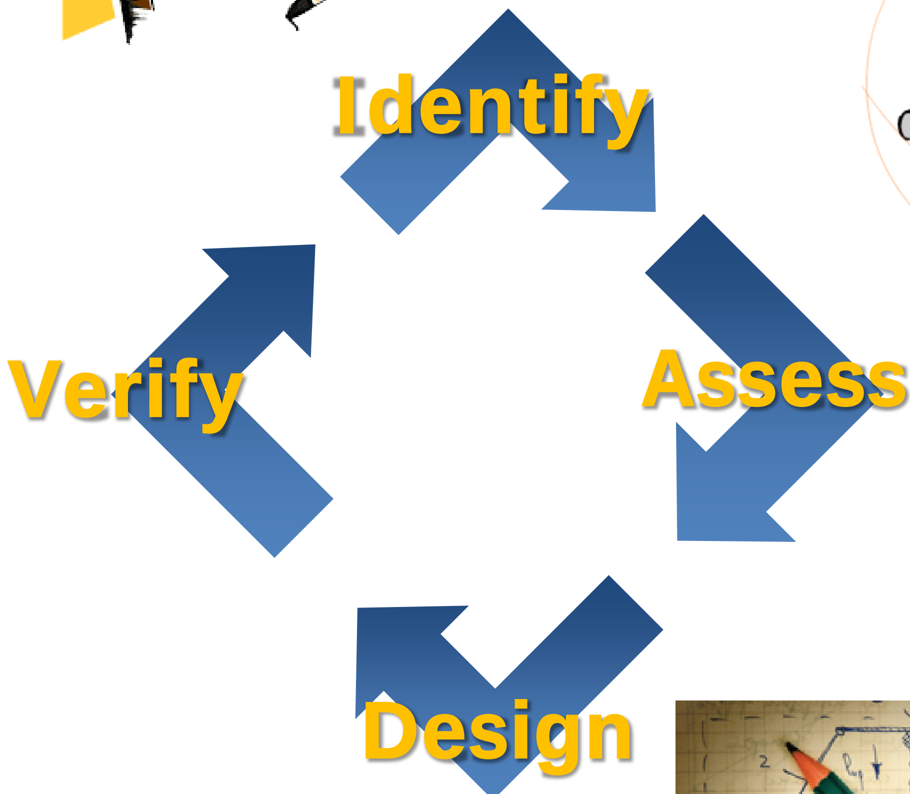
- The necessary activities involved in the implementation of safety instrumented functions, occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use.

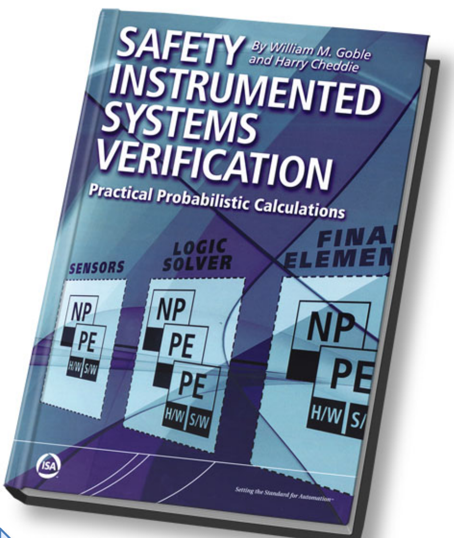


Start
Conceptual Process Design
Perform Process Hazard Analysis & Risk Assessment
Apply non-SIS protection layers to prevent identified hazards or reduce risk
No
SIS required?
Yes
Define Target SIL for each Safety Instrumented Function
Develop Safety Requirements Specification
Perform SIS Conceptual Design, & verify it meets the SRS
Perform SIS Detail Design
SIS Installation, Commissioning and Pre-Startup Acceptence Test
Establish Operation & Maintenance Procedures
Pre-Startup Safety Review (Assessment)
SIS startup, operation, maintenance, periodic functional testing
Modify
Modify or Decommission SIS?
Decommision
SIS Decommissioning


HAZARD
REVIEW


RISK


Identify
Assess
Design
Verify

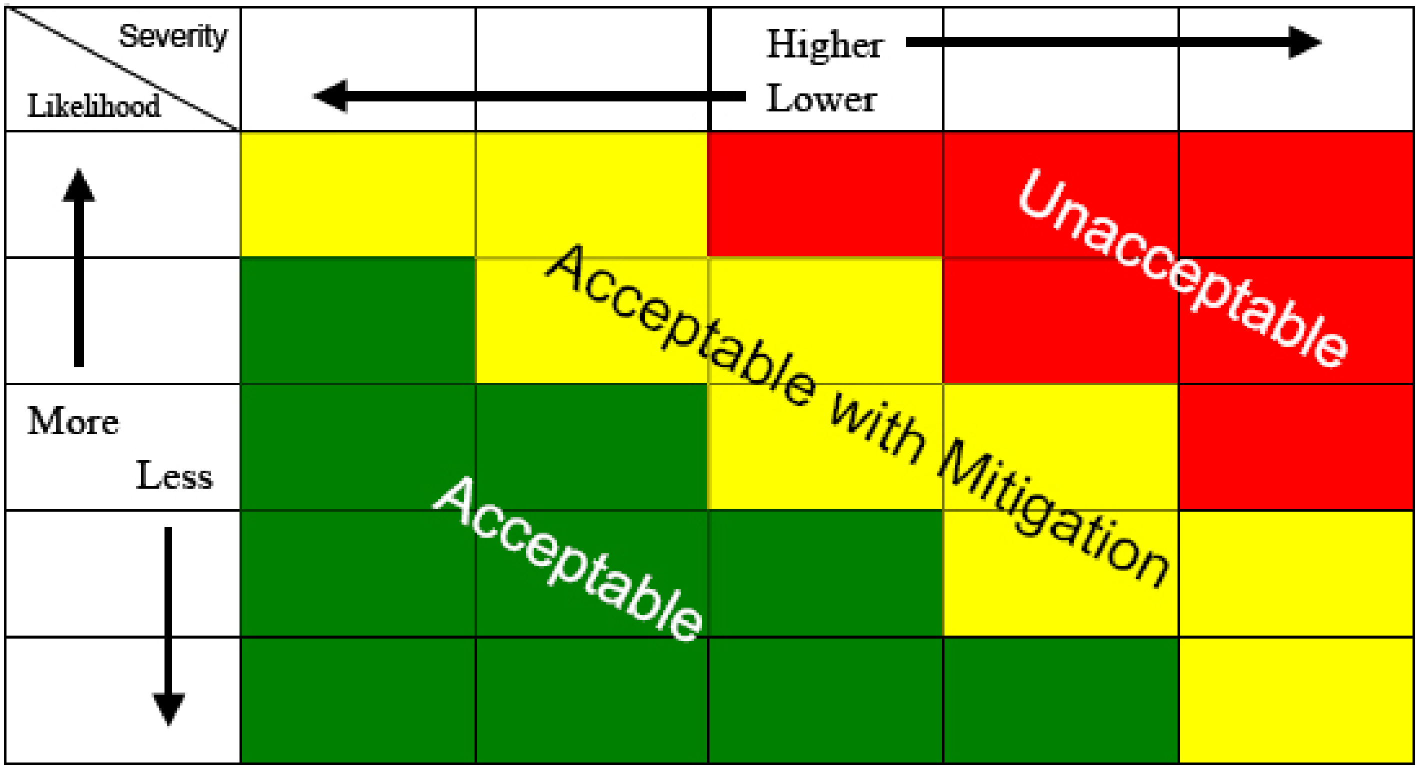

SAFETY INSTRUMENTED SYSTEMS VERIFICATION
By William M. Goble and Harry Cheddie
Practical Probabilistic Calculations
SENSORS
LOGIC SOLVER
NP
PE
H/W S/W
ISA

What is risk?

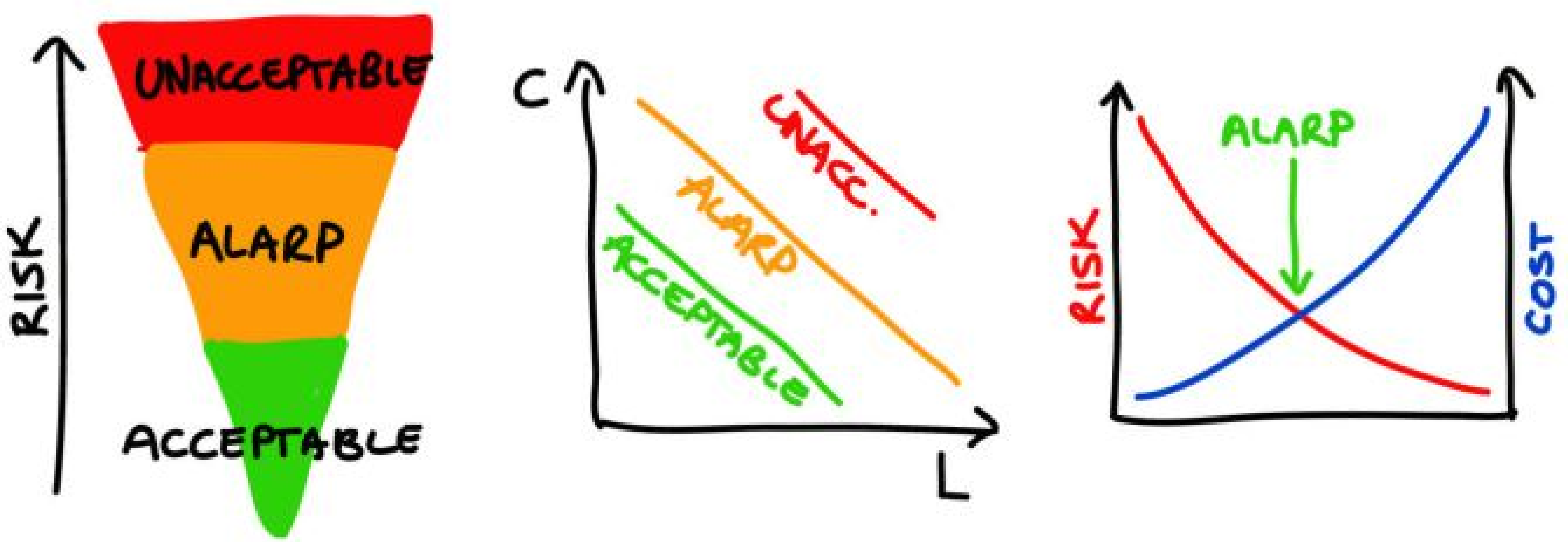
A Risk is the amount of harm that can be expected to occur during a given time period due to specific harm event.

$$\text{RISK}\ \frac{\text{Detriment}}{\text{Unit Time}} = \text{FREQUENCY}\ \frac{\text{Events}}{\text{Unit Time}} \times \text{SEVERITY}\ \frac{\text{Detriment}}{\text{Event}}$$

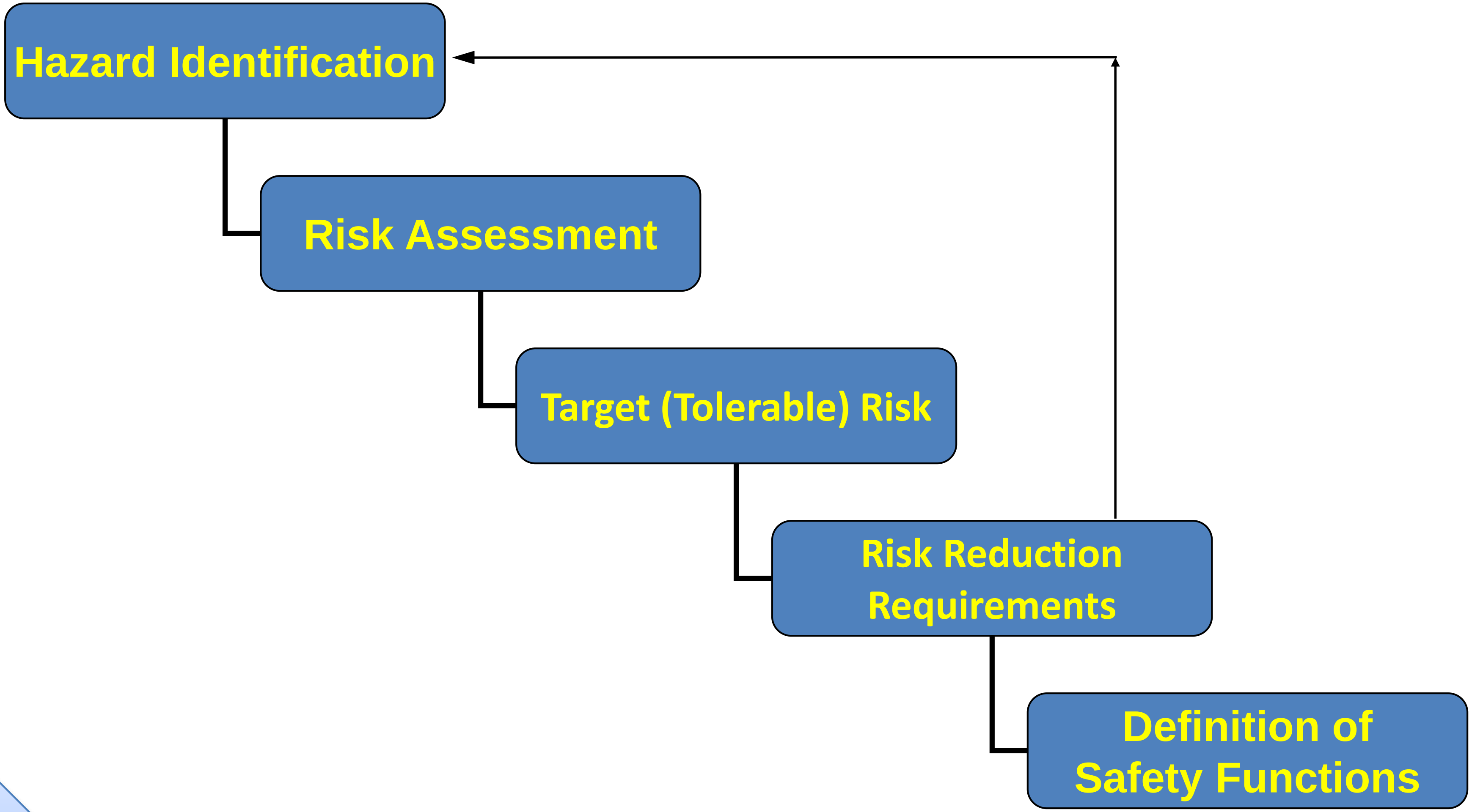
How much risk is acceptable?

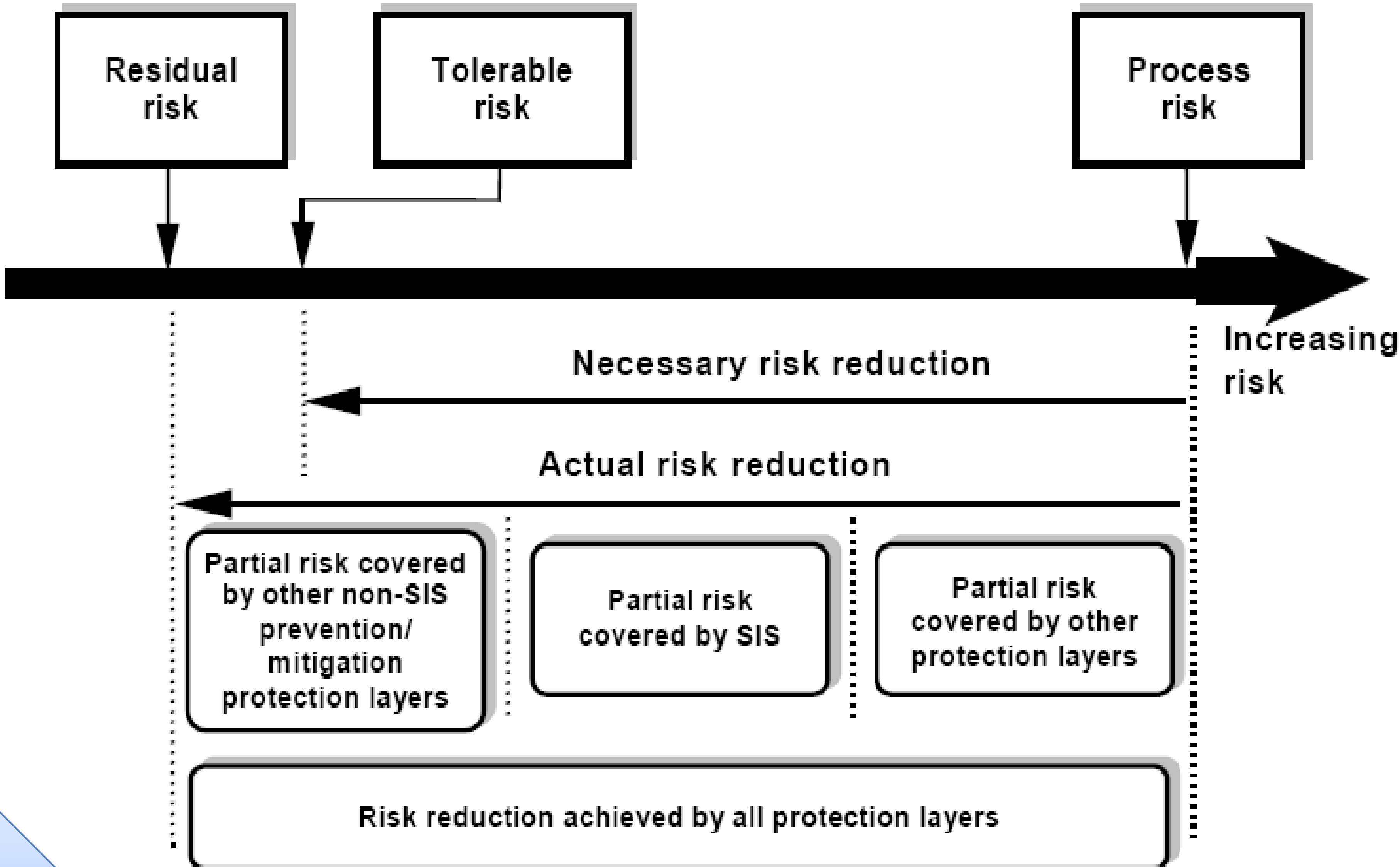


ALARP (As Low As Reasonably Practicable)



Risk Reduction




Residual risk
Tolerable risk
Process risk
Increasing risk
Necessary risk reduction
Actual risk reduction
Partial risk covered by other non-SIS prevention/ mitigation protection layers
Partial risk covered by SIS
Partial risk covered by other protection layers
Risk reduction achieved by all protection layers

Safety Integrity Level (SIL)

a relative level of risk-reduction provided by a safety function, or to specify a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a Safety Instrumented Function (SIF).

Safety Integrity Level (high/low demand mode)

SIL Rating	Range of PFD	Range of RRF
4	$10^{-5} \leq PFD < 10^{-4}$	100,000≥RRF>10,000
3	$10^{-4} \leq PFD < 10^{-3}$	10,000≥RRF>1,000
2	$10^{-3} \leq PFD < 10^{-2}$	1,000≥RRF>100
1	$10^{-2} \leq PFD < 10^{-1}$	100≥RRF>10

Mode of operation (of a SIF)

IEC 61511-1: 2016 para 3.2.39

way in which a SIF operates which may be either low demand mode, high demand mode or continuous mode

a) low demand mode: mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year.

b) high demand mode: mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year.

c) continuous mode: mode of operation where the SIF retains the process in a safe state as part of normal operation.

SIL for continuous operation mode

SIL Rating	Target frequency of dangerous failures to perform the safety instrumented function (per hour) = PFH
4	$10^{-9} \leq \lambda_D < 10^{-8}$
3	$10^{-8} \leq \lambda_D < 10^{-7}$
2	$10^{-7} \leq \lambda_D < 10^{-6}$
1	$10^{-6} \leq \lambda_D < 10^{-5}$

Stages of SIL Study

1. Target SIL Evaluation

What SIL should be allocated for the SIF?

2. SIL Verification

Does SIS fulfill Target SIL requirements?

- Part 2: Target SIL Evaluation
  - Layers of Protection Analysis
  - Risk Matrix
  - Risk Graph
  - Calibrated Risk Graph

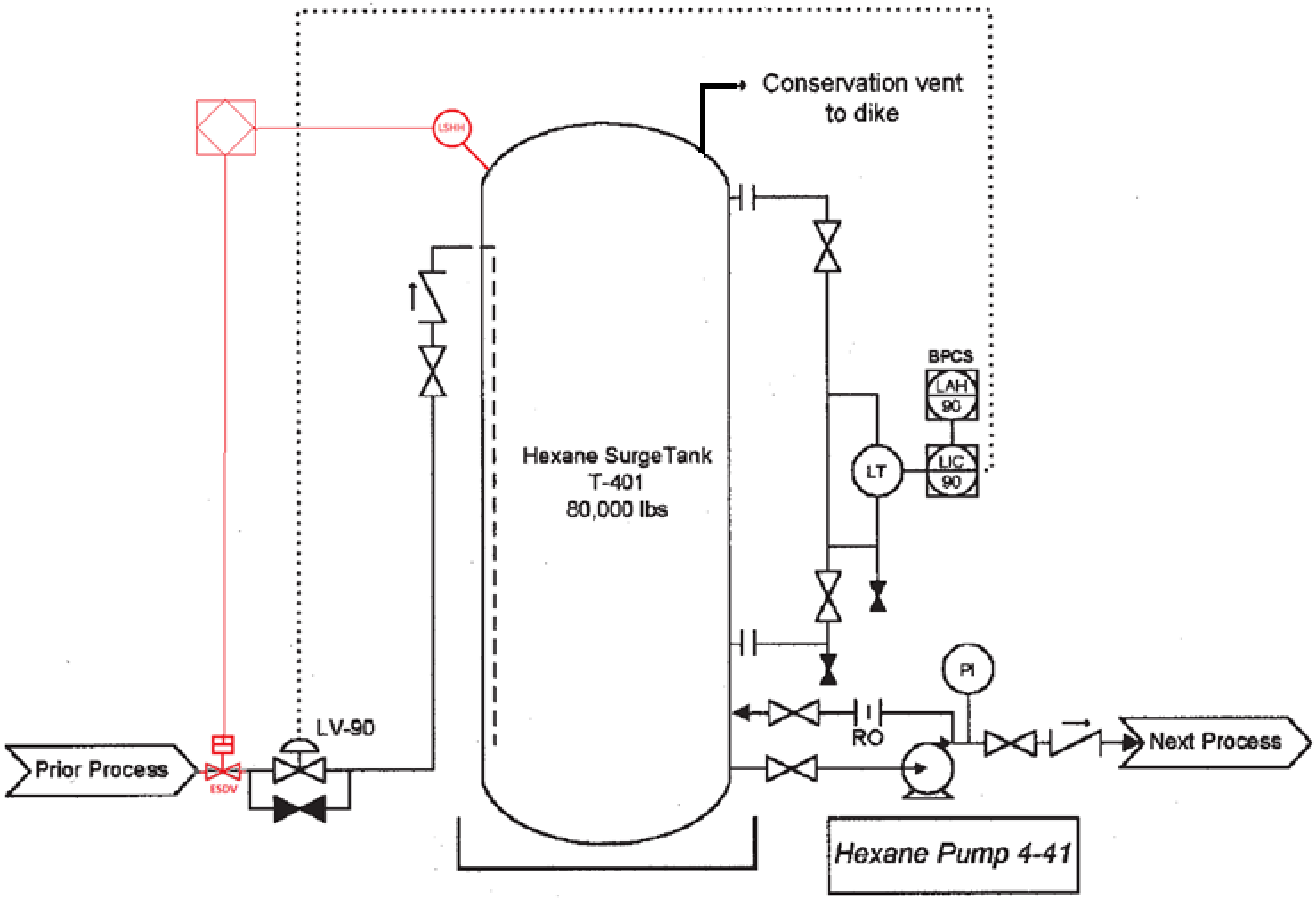
What you need...

- P&IDs
- Cause & Effect Charts
- HAZOP Report

Also:

- Process Description
- Logic Diagrams
- ESD Philosophy
- Control Philosophy
- Blowdown Philosophy
- Etc.

Working Example



Workshop

1. Perform a hazard identification e.g. HAZOP Study
2. Allocate Safety Instrumented Functions

What SIL do you expect?

Semi-Quantitative Technique
LAYERS OF PROTECTION ANALYSIS (LOPA)

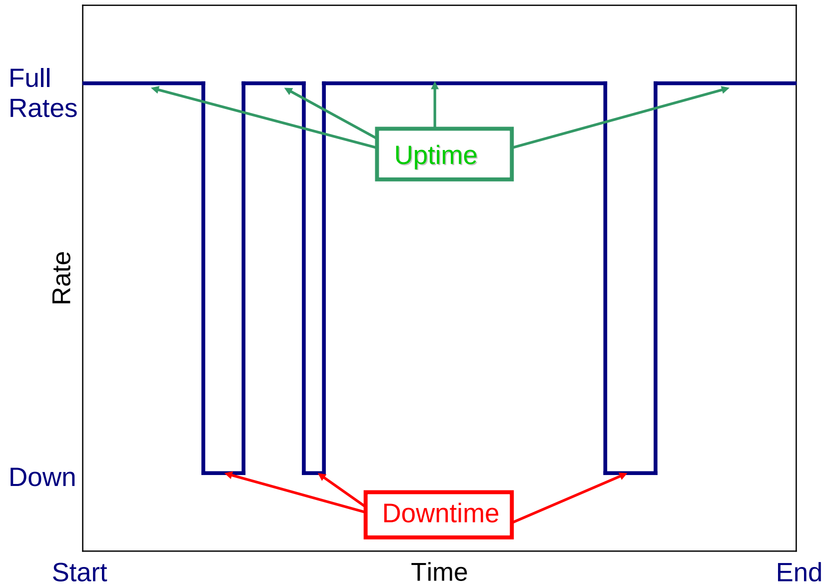
Abbreviations

- MTBF: Mean Time Between Failures
- MTTF: Mean Time To Fail
- MTTR: Mean Time To Repair (Repair vs. Restore)
- MDT: Mean Down Time

Failure: Strength vs. Stress

- All failures occur when **stress** exceeds the associated level of **strength**
  - **Heat**
  - **Humidity**
  - **Shock**
  - **Vibration**
  - **Electrical surge**
  - **Electrostatic discharge**
  - **Radio frequency interference**
  - **Mis-calibration**
  - **Maintenance errors**
  - **Operational errors**

Availability



$$\text{Actual Availability} = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}}$$

Average Availability = MTBF / (MTBF + MTTR)

Operational Availability = MTBM / (MDT+MTBM)

Failure Rate

- Definition: The probability that a system fails during a specified period of time.

- Dimensions: $Time^{-1}$

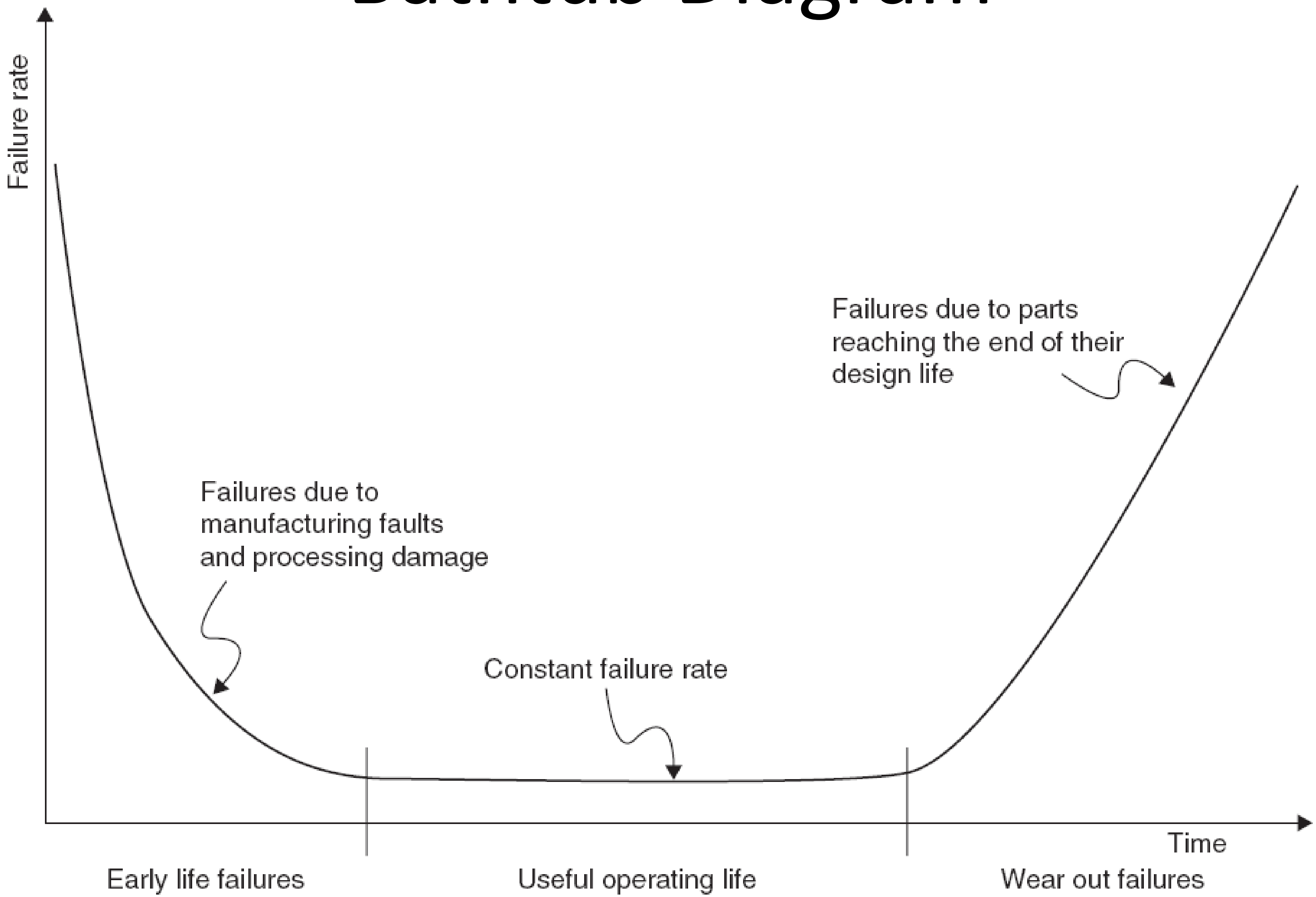
- How to calculate failure rate from statistical databases?

λ=(no. of faults)/(total working time of all items)

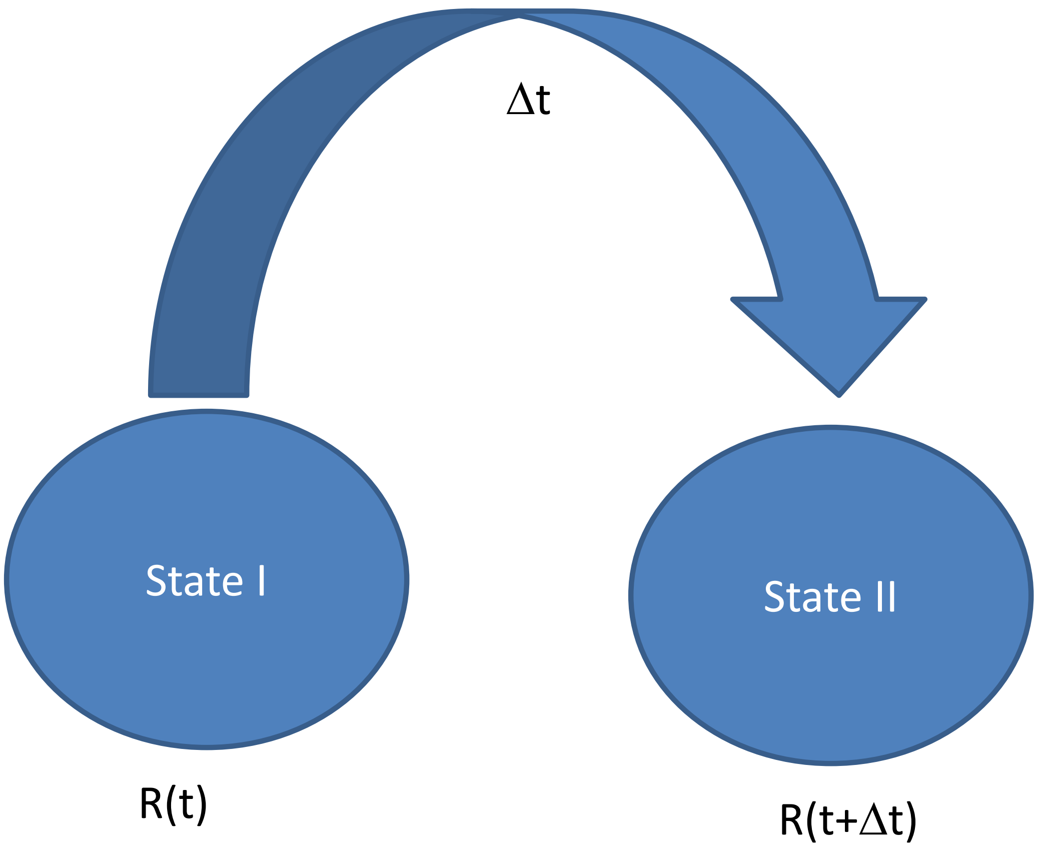
Source:

- Experience, accidents history, etc.
- Generic Data, e.g. OREDA, IEREDA, PERD, SERH, etc.
- Probabilistic Reliability Methods e.g. FTA, ETA, RBD, etc.

Bathtub Diagram



Reliability



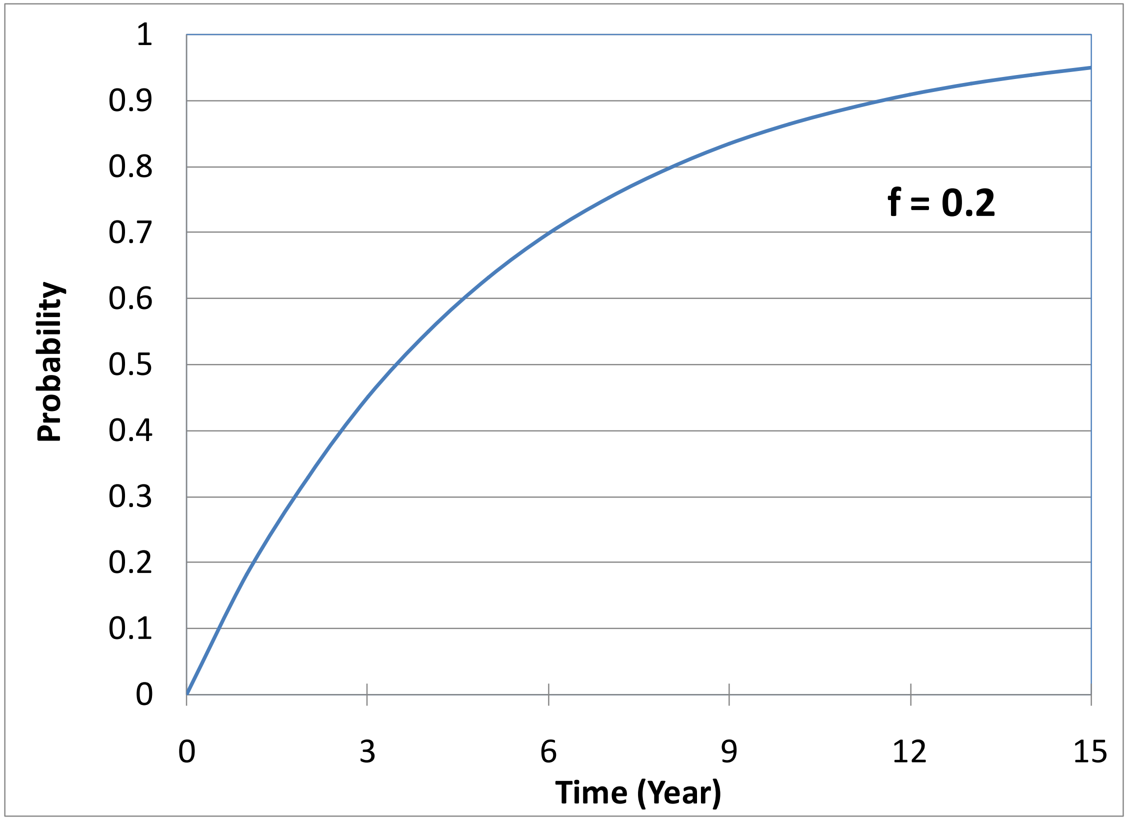
Failure probability

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

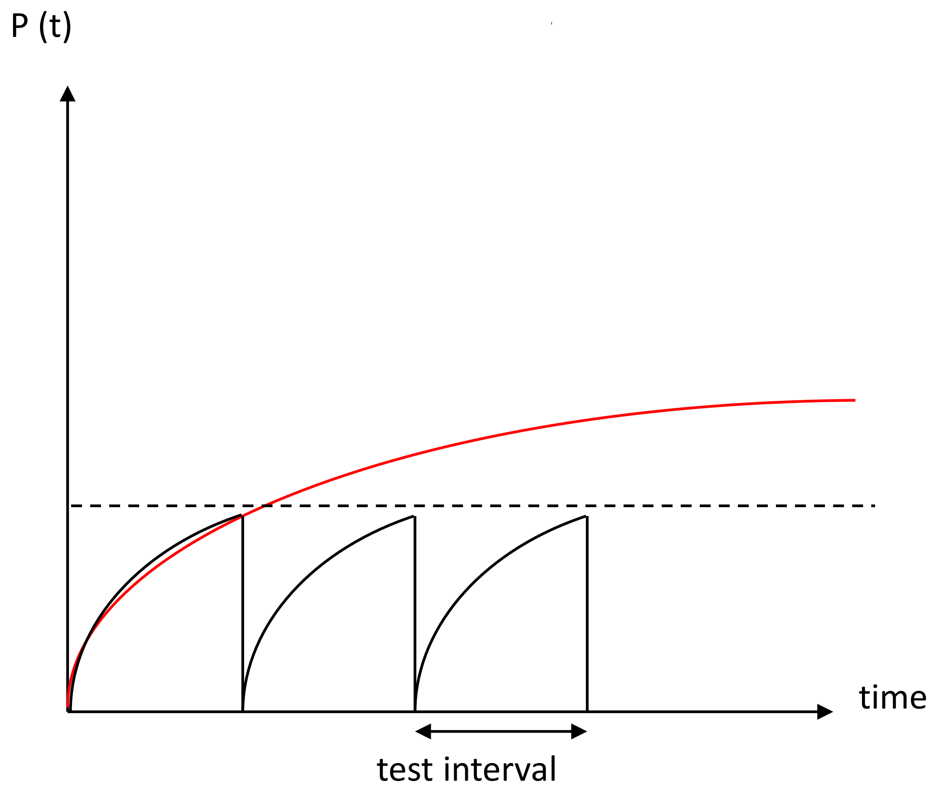
$R(t)=\exp(-\lambda t)$

$P=1-R$

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

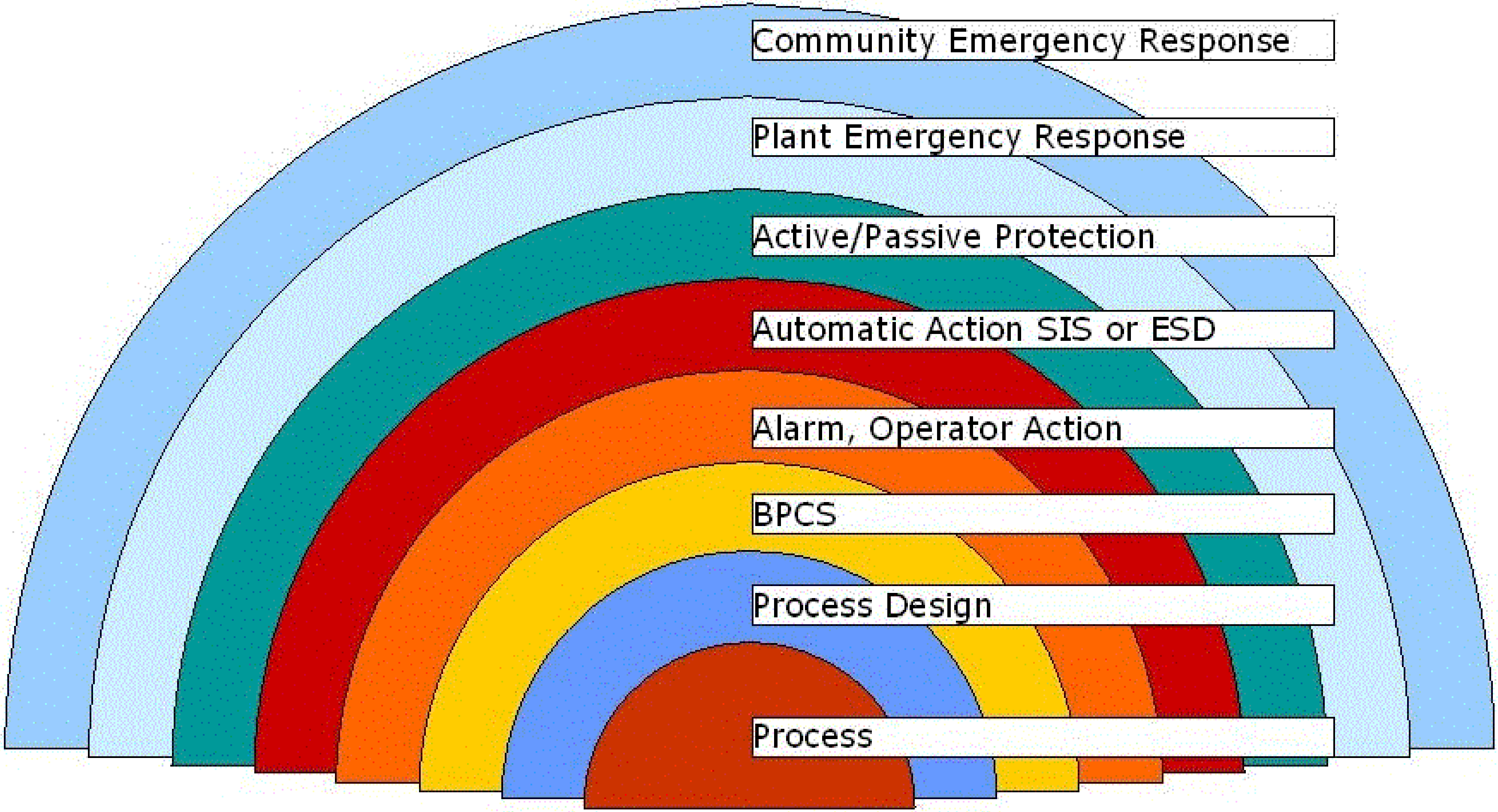


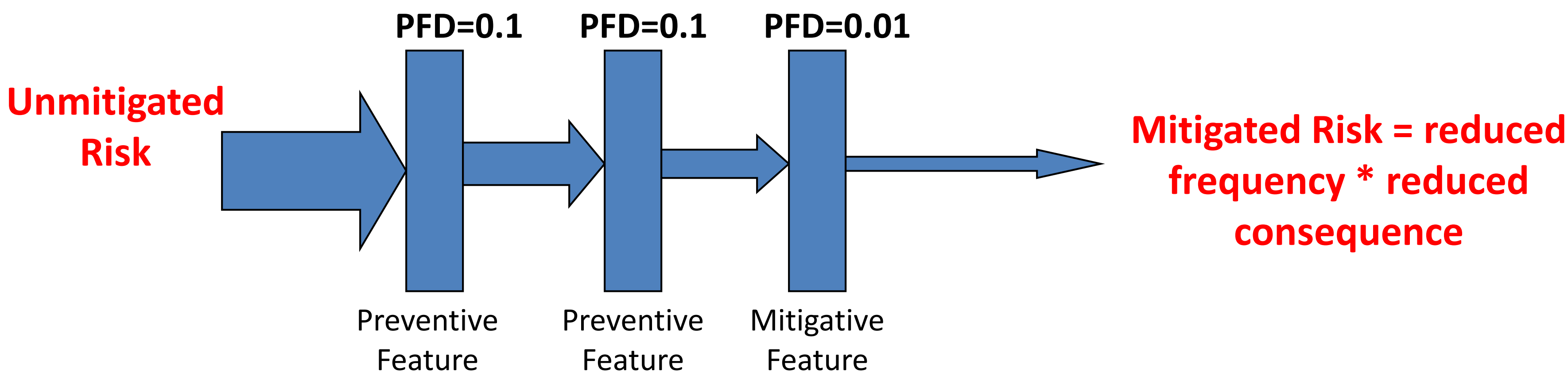
Reliability and Maintenance
Proof Test Coverage

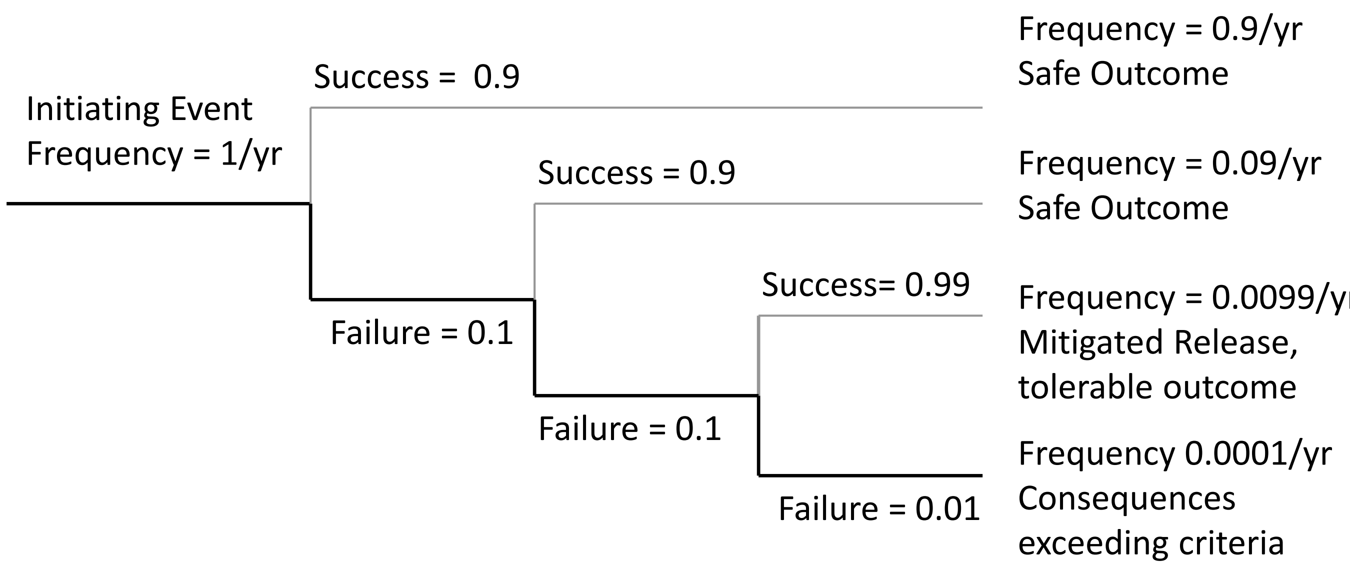


$$P_{avg} = \frac{\int_0^{TI} P(t)dt}{TI} \approx \frac{\lambda \times TI}{2} \quad if \;\; \lambda \times TI << 1$$

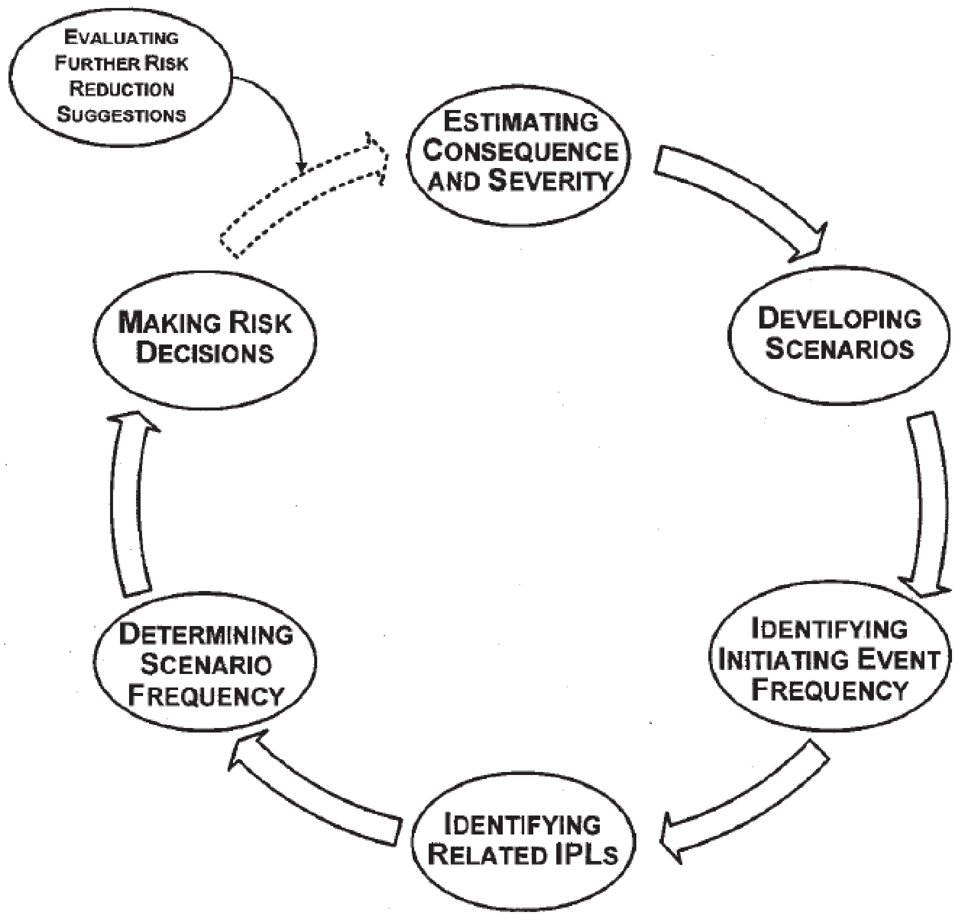
Layers of Protection Analysis



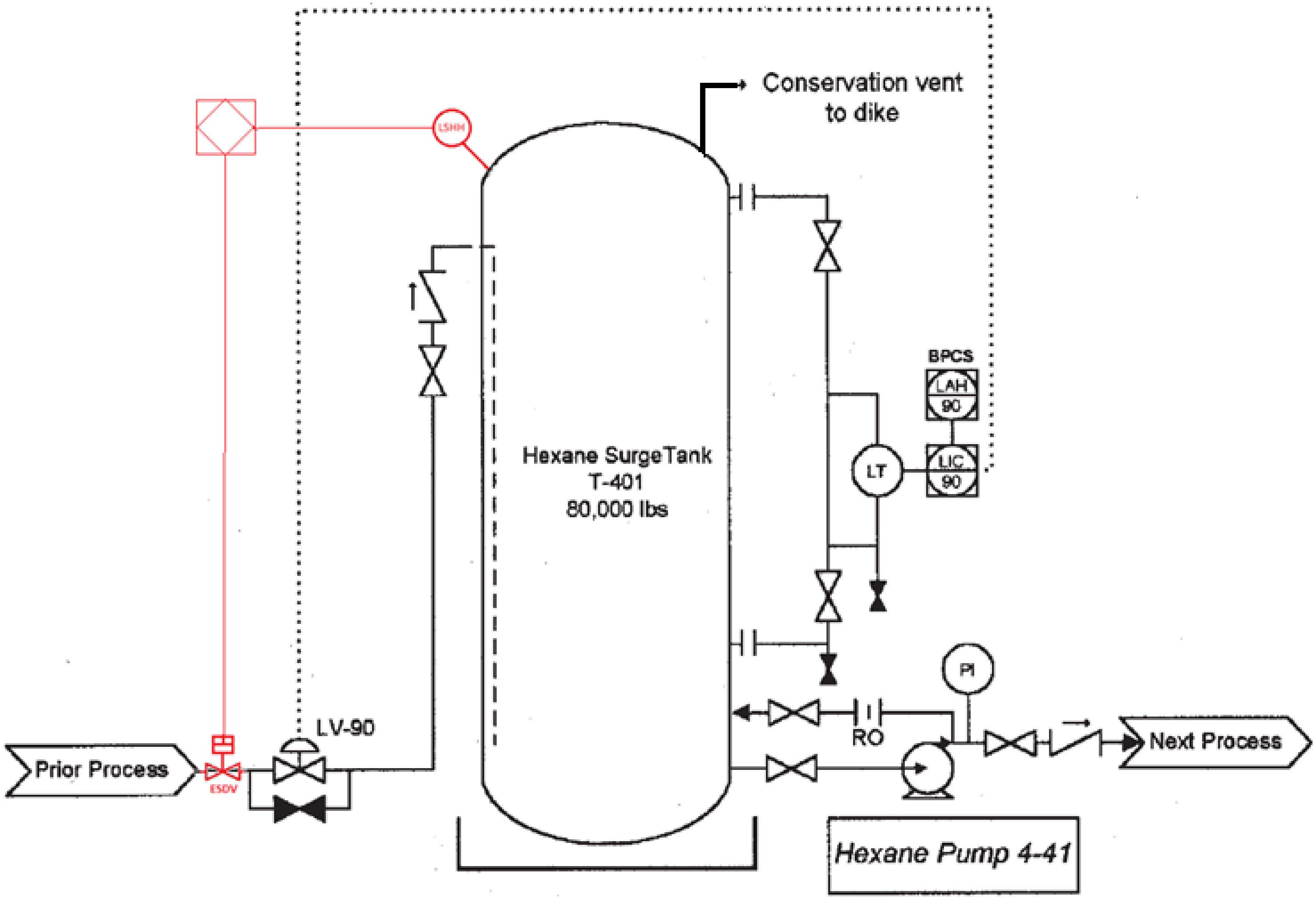

PFD=0.1
PFD=0.1
PFD=0.01
Unmitigated Risk
Mitigated Risk = reduced frequency * reduced consequence
Preventive Feature
Preventive Feature
Mitigative Feature


Initiating Event Frequency = 1/yr
Success = 0.9
Failure = 0.1
Success = 0.9
Failure = 0.1
Success= 0.99
Failure = 0.01
Frequency = 0.9/yr Safe Outcome
Frequency = 0.09/yr Safe Outcome
Frequency = 0.0099/yr Mitigated Release, tolerable outcome
Frequency 0.0001/yr Consequences exceeding criteria

Stages of LOPA



Working example…



Methods for Consequence Estimation

1. **Category Approach without Direct Reference to Human Harm**
2. **Qualitative Estimates with Human Harm**
3. **Qualitative Estimates with Human Harm with Adjustments for Postrelease Probabilities**
4. **Quantitative Estimates with Human Harm**

What do you select for the examp

1. Material Release
2. Fire
3. Fire exposure and harm
4. Fatality

… Any further escalations?

step 2

Define scenarios

Initiating Events → Consequences

Failure of Pump

Failure of BPCS

Material Release

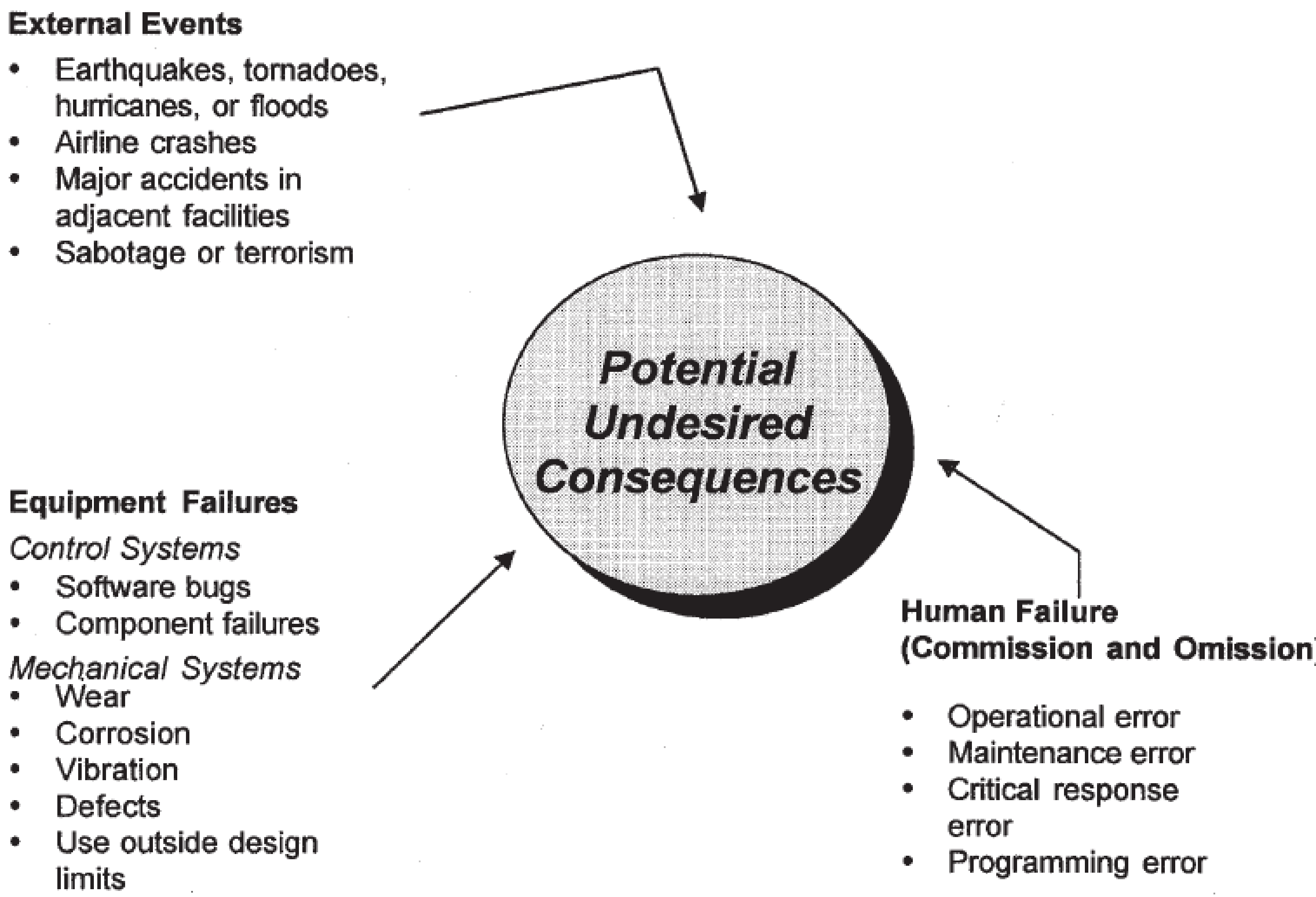
Fire

Fire Exposure

Fatality

step 3

Identifying Initiating Event Frequency



Initiating Event	Frequency Range from Literature (per year)	Example of a Value Chosen by a Company for Use in LOPA (per year)
Pressure vessel residual failure	10^{-5} to 10^{-7}	1×10^{-6}
Piping residual failure—100 m—Full Breach	10^{-5} to 10^{-6}	1×10^{-5}
Piping leak (10% section)—100 m	10^{-3} to 10^{-4}	1×10^{-3}
Atmospheric tank failure	10^{-3} to 10^{-5}	1×10^{-3}
Gasket/packing blowout	10^{-2} to 10^{-6}	1×10^{-2}
Turbine/diesel engine overspeed with casing breach	10^{-3} to 10^{-4}	1×10^{-4}
Third party intervention (external impact by backhoe, vehicle, etc.)	10^{-2} to 10^{-4}	1×10^{-2}
Crane load drop	10^{-3} to 10^{-4} per lift	1×10^{-4} per lift
Lightning strike	10^{-3} to 10^{-4}	1×10^{-3}
Safety valve opens spuriously	10^{-2} to 10^{-4}	1×10^{-2}
Cooling water failure	1 to 10^{-2}	1×10^{-1}
Pump seal failure	10^{-1} to 10^{-2}	1×10^{-1}
Unloading/loading hose failure	1 to 10^{-2}	1×10^{-1}
BPCS instrument loop failure *Note:* IEC 61511 limit is more than 1×10^{-5}/hr or 8.76×10^{-2}/yr (IEC, 2001)	1 to 10^{-2}	1×10^{-1}
Regulator failure	1 to 10^{-1}	1×10^{-1}
Small external fire (aggregate causes)	10^{-1} to 10^{-2}	1×10^{-1}
Large external fire (aggregate causes)	10^{-2} to 10^{-3}	1×10^{-2}
LOTO (lock-out tag-out) procedure* failure *overall failure of a multiple-element process	10^{-3} to 10^{-4} per opportunity	1×10^{-3} per opportunity
Operator failure (to execute routine procedure, assuming well trained, unstressed, not fatigued)	10^{-1} to 10^{-3} per opportunity	1×10^{-2} per opportunity

What is an IPL?

IPL must be:

- **specific** and designed to prevent that specific scenario
- **effective** in preventing the consequence when it functions as designed (provides a Risk Reduction Factor of 10 or greater),
- **independent** of the initiating event and the components of any other IPL already claimed for the same scenario,
- **auditable**; the assumed effectiveness in terms of consequence prevention and PFD must be capable of validation in some manner (by documentation, review, testing, etc.)

Find IPL’s for your scenario

- Inspection & Maintenance procedures
- BPCS
- LAH that needs operator intervention
- LSHH that activates ESD
- Conservative vent
- Dike
- Emergency response procedures

Determining the Frequency of Scenarios

$$f_i^{\text{fire}} = f_i^{\text{I}} \times \left(\prod_{j=1}^{J} \text{PFD}_{ij} \right) \times P^{\text{ignition}}$$

$$f_i^{\text{fire exposure}} = f_i^{\text{I}} \times \left(\prod_{j=1}^{J} \text{PFD}_{ij} \right) \times P^{\text{ignition}} \times P^{\text{person present}}$$

$$f_i^{\text{fire injury}} = f_i^{\text{I}} \times \left(\prod_{j=1}^{J} \text{PFD}_{ij} \right) \times P^{\text{ignition}} \times P^{\text{person present}} \times P^{\text{injury}} \quad \text{(fire)}$$

$$f_i^{\text{toxic}} = f_i^{\text{I}} \times \left(\prod_{j=1}^{J} \text{PFD}_{ij} \right) \times P^{\text{person present}} \times P^{\text{injury}} \quad \text{(toxic)}$$

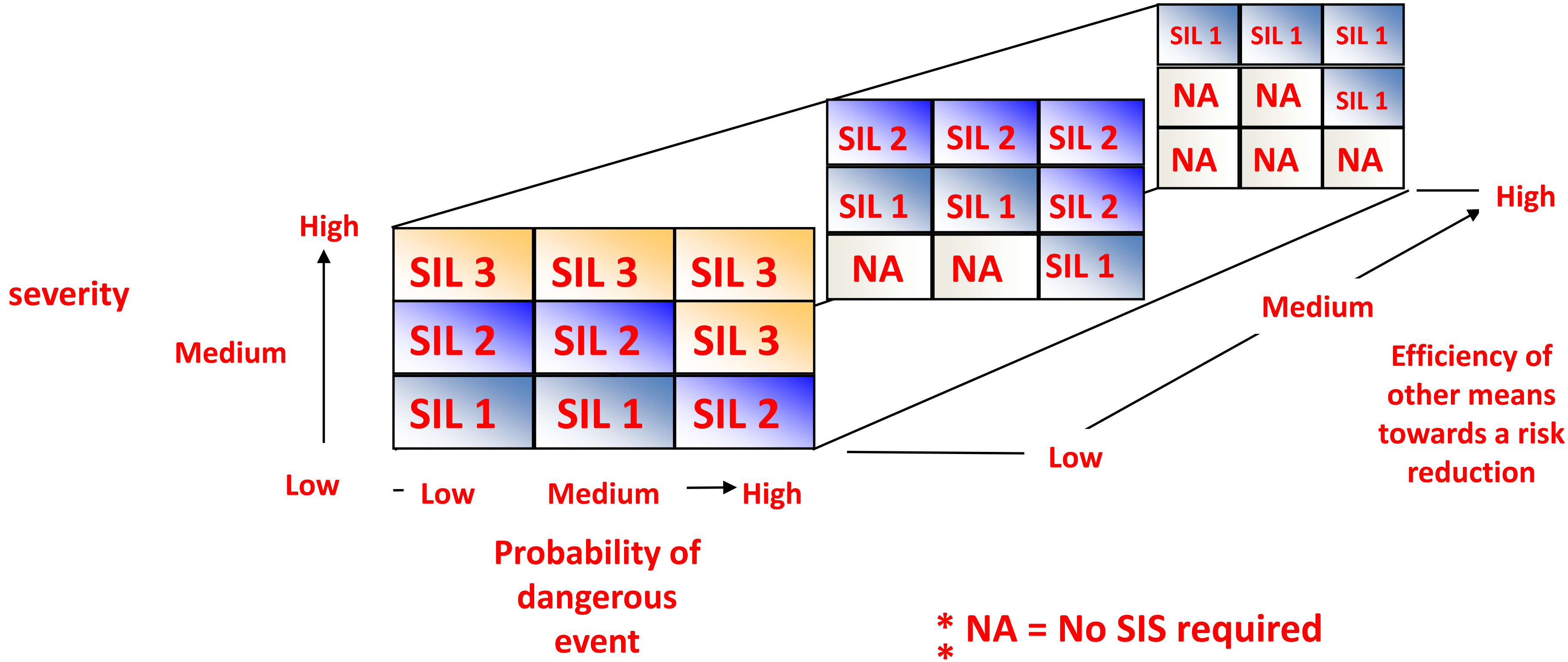
Calculate scenario rate

Step 6

Making Risk Decisions

1. **compare the calculated risk** with a predetermined **risk tolerance criteria**
2. **expert judgment** by a qualified risk analyst
3. **relative comparison among competing alternatives** for risk reduction

Qualitative Technique
Risk Matrix

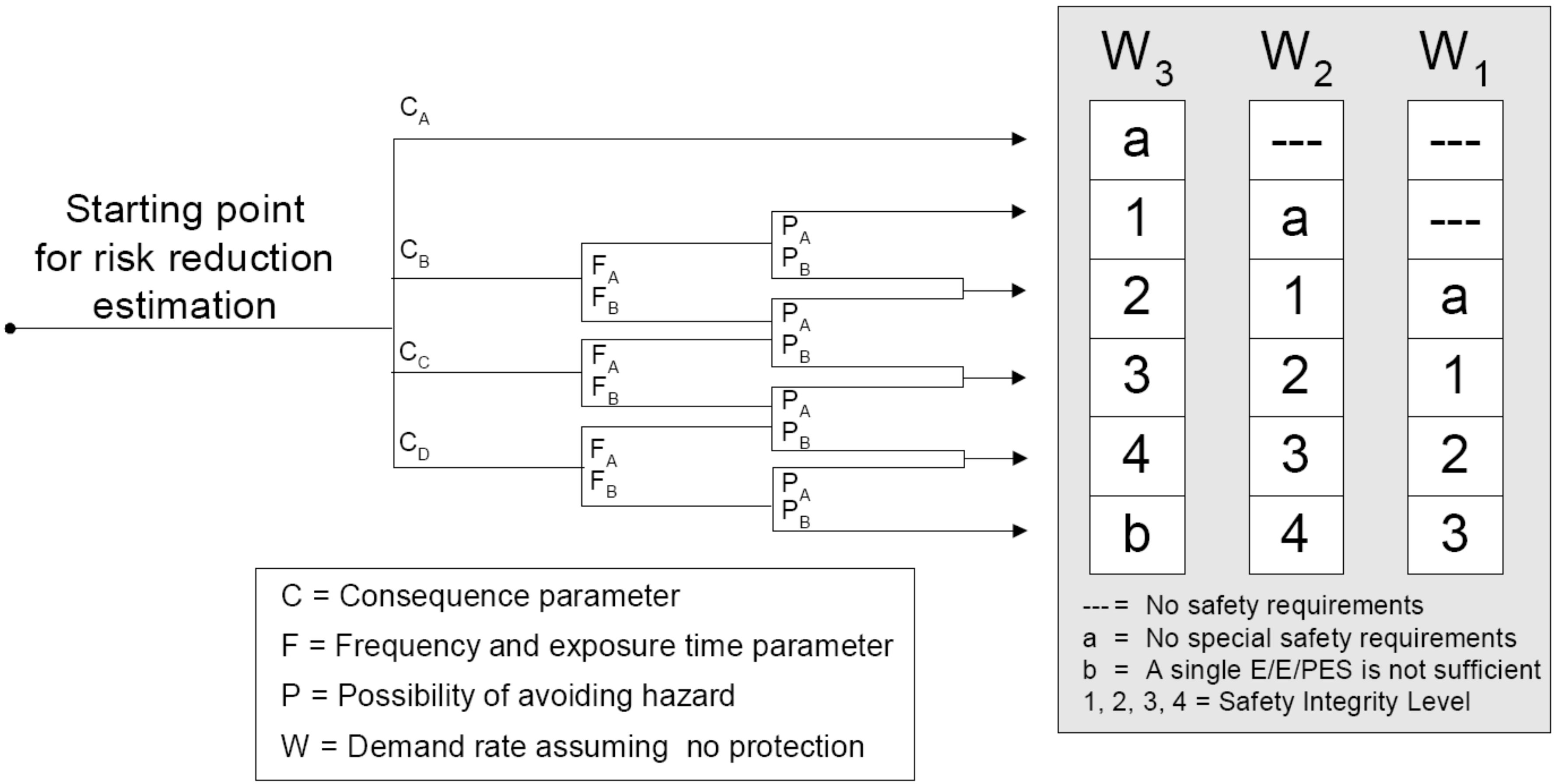


* NA = No SIS required
*

Target SIL Evaluation Techniques

3

Qualitative Technique
Risk Graph


Starting point for risk reduction estimation
C_A
C_B
C_C
C_D
F_A
F_B
P_A
P_B
W_3
W_2
W_1
a --- ---
1 a ---
2 1 a
3 2 1
4 3 2
b 4 3
--- = No safety requirements
a = No special safety requirements
b = A single E/E/PES is not sufficient
1, 2, 3, 4 = Safety Integrity Level
C = Consequence parameter
F = Frequency and exposure time parameter
P = Possibility of avoiding hazard
W = Demand rate assuming no protection

Consequence Parameter

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	

Consequence Parameter
(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

Exposure/Occupancy Parameter

Risk Parameter		Classification	Remarks
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 F_A 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.	

Prevention Capability Parameter

Risk Parameter		Classification	Remarks
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 Parameter

Risk Parameter		Classification	Remarks
Demand rate (W) The number of times per year that the hazardous event would occur in absence of safety-related loop under consideration.	W_1	Very low demand rate	5 The purpose of the W factor is to estimate the frequency of the hazard taking place without the addition of the safety-related loop
	W_2	Low demand rate	
	W_3	Relatively high demand rate	

Target SIL Evaluation Techniques

4

Semi-Qualitative Technique
Calibrated Risk Graph

UKOOA Calibrated 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	

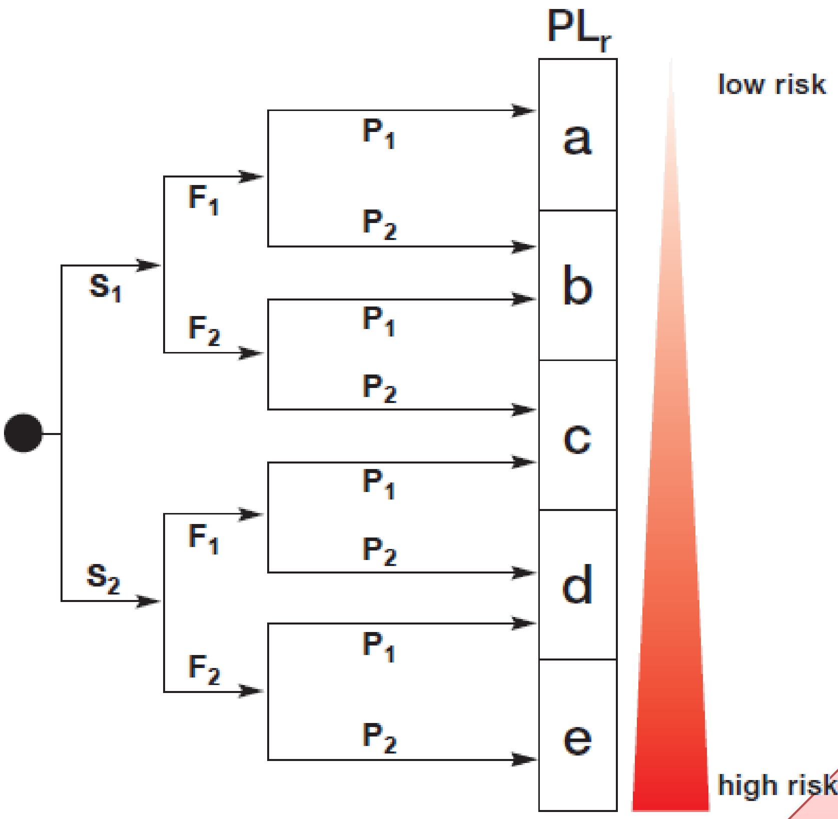
Performance Levels based on **EN/ISO 13849-1**

Safety of machinery - Safety-related parts of control systems

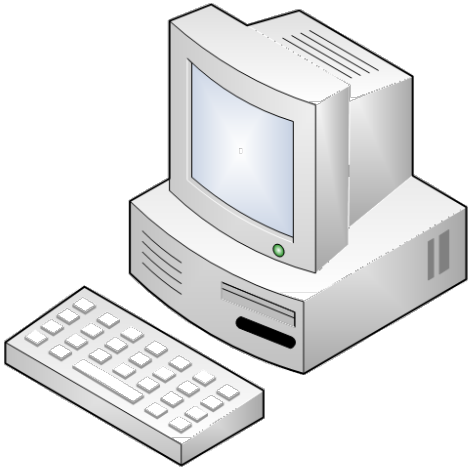
Risk estimation

To calculate the performance level required (PL_r).

S	**Severity of injury**
S1	slight (normally reversible injury)
S2	serious (normally irreversible injury or death)
F	**Frequency and/or exposure to hazard**
F1	seldom to less often and/or exposure time is short
F2	frequent to continuous and/or exposure time is long
P	**Possibility of avoiding hazard or limiting harm**
P1	possible under specific conditions
P2	scarcely possible



Software

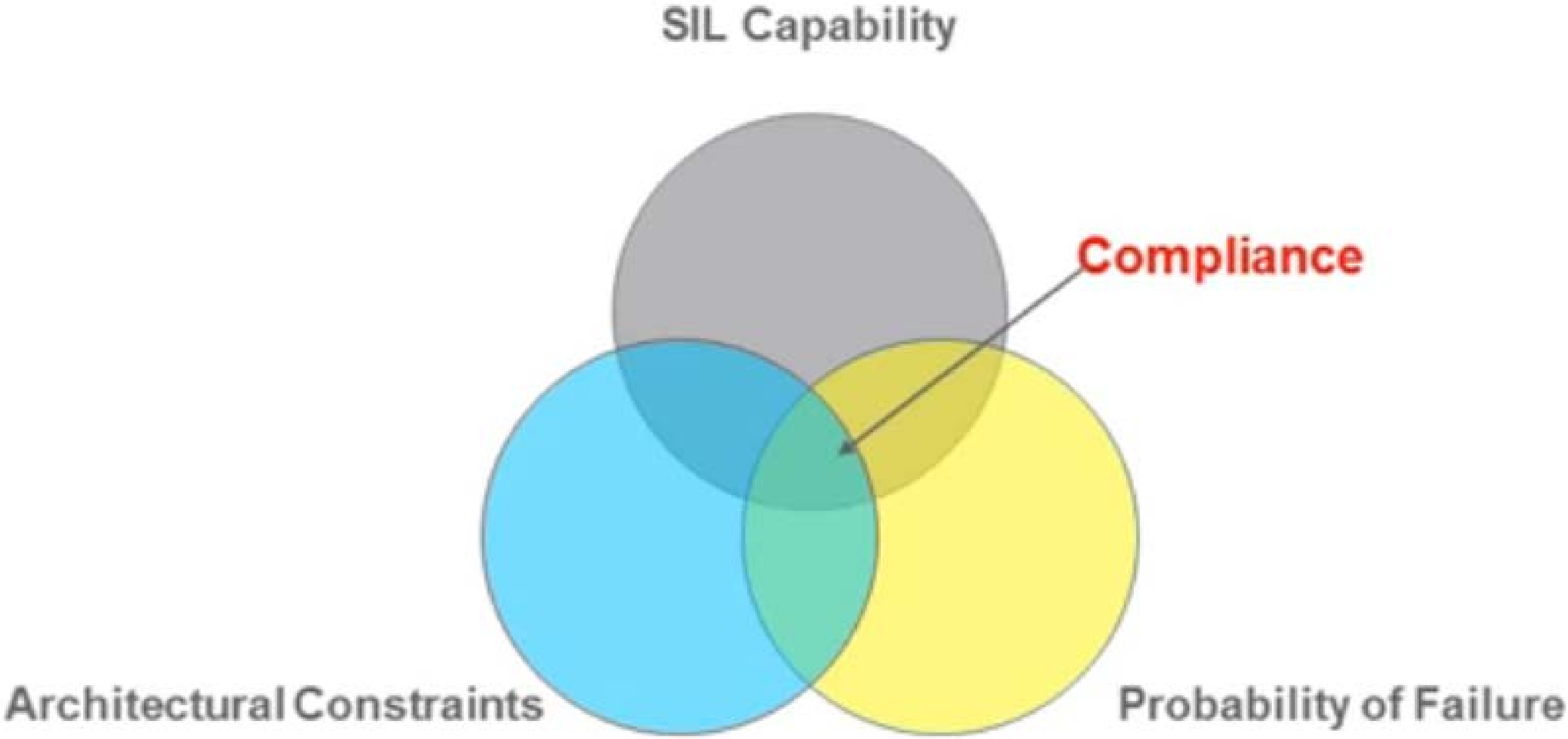


- exSILentia by exida, www.exida.com
- SILSolver by SIS-Tech, www.sis-tech.com
- SILCore by ACM (Canada), www.silcore.com
- AEShield by AE Solutions, www.aesolns.com

- Part 3: SIL Verification Techniques
  - Definitions
  - Reliability Data
  - Simplified Equations
  - FTA Technique
  - Markov Method

SIL Design Verification

- Random failure
- Architectural constraints
- Systematic integrity: Safety lifecycle
  - Proven in use or IEC 61508 compliant equipment
  - Functional safety management
  - Software requirements


SIL Capability
Compliance
Architectural Constraints
Probability of Failure

SIF Failure Modes

- Based on cause
  - Systematic Failures
  - Random Hardware Failures
- Based on consequence
  - Safe
  - Dangerous
- Based on diagnostic
  - Detected (overt)
  - Undetected (covert, hidden)

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

Failure Partitioning

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

Failure Rate Data

- OREDA - SINTEF
- PERD - CCPS
- TECDOC & EIREDA– IAEA
- SERH - Exida
- GS EP EXP 405 TOTAL
- www.sael-online.com
- …

Redundancy

Use of multiple elements or systems to perform the same function. It can be

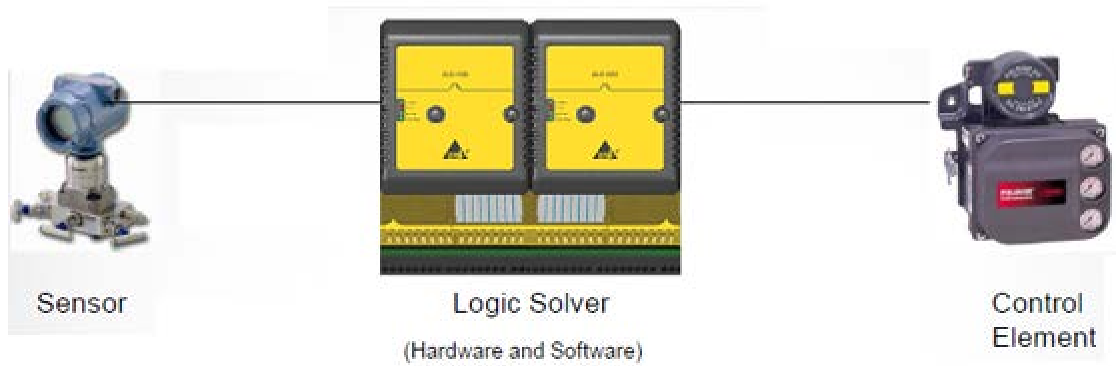
- identical redundancy
- diverse redundancy

HFT (Hardware Fault Tolerance): maximum number of failures that can be tolerated in a SIS component

SFF (Safe Failure Fraction): fraction of safe failures!

What is HFT for the following systems?

- 1oo1
- 1oo2
- 1oo3
- 2oo2
- 2oo3
- 2oo4



Architectural Constraints (Route 1_H) (IEC 61508 part 2 – table 2)

Safe Failure Fraction (SFF)	Type A elements			Type B elements		
	Hardware Fault Tolerance (HFT)			Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
<60%	SIL1	SIL2	SIL3	Not Allowed	SIL1	SIL2
60% - <90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
90% - <99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

Architectural Constraints (Route 2_H) (IEC 61511 part 1 – table 6)

Type A elements		
Hardware Fault Tolerance (HFT)		
0	1	2
SIL1	SIL2	SIL3

Note 1: for demand mode

Note 2: provided that the dominant failure mode is to the safe state, or dangerous failures are detected

Note 3: If the dominant failure is to dangerous state, and if there isn't effective diagnostics but it can be demonstrated 'limited adjustment' and 'prior use' (with extensive evidence)

Definitions

- Proof Test Intervals (TI) (directly affects PFD)
- De-energize to trip (DTT)
- Energize to trip (ETT)
- Diagnostic Coverage (DC)
- Common Cause Failure (β)

SIL Verification Techniques

1

Simplified Equations

Reference:
"Reliability, Maintainability and Risk" by David J. Smith, 4th Edition, 1993, Butterworth-Heinemann, ISBN 82-515-0188-1.

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 Between Failures (MTBF).

PFD_{avg}

- Converting MTTF to failure rate: $\lambda^{DU} = \frac{1}{MTTF^{DU}}$
- PFD_{avg}: $PFD_{avg} = \left[\lambda^{DU} \times \frac{TI}{2}\right]$
- PFD_{avg} (including systematic failures): $PFD_{avg} = \left[\lambda^{DU} \times \frac{TI}{2}\right] + \left[\lambda_F^{D} \times \frac{TI}{2}\right]$
- SIS PFD_{avg}: $PFD_{SIS} = PFD_S + PFD_L + PFD_{FE} + PFD_{PS}$

Voting Systems

- 1oo2

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

- 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

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

Voting Systems (contd.)

- 2oo3

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

- 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

- 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

$$PFD_{avg} = \left(\lambda^{DU}\right)^3 \times \left(TI\right)^3$$

Spurious Trip Rate (STR)

$$\lambda^{S} = \lambda^{SD}+\lambda^{SU}+\lambda^{DD}+\lambda^{S}_{F}$$

- $\lambda^{SD}+\lambda^{SU}$ 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

Simplified Equations

$$STR\,(MooN) = \frac{n!}{(n-m)!}\lambda \times (\lambda \times MTTR)^{m-1}$$

- 1oo1

$$STR = \lambda^S$$

- 1oo2

$$STR = 2 \times \lambda^S$$

- 1oo3

$$STR = 3 \times \lambda^S$$

- 2oo2

$$STR = 2 \times \left(\lambda^S\right)^2 \times MTTR$$

- 2oo3

$$STR = 6 \times \left(\lambda^S\right)^2 \times MTTR$$

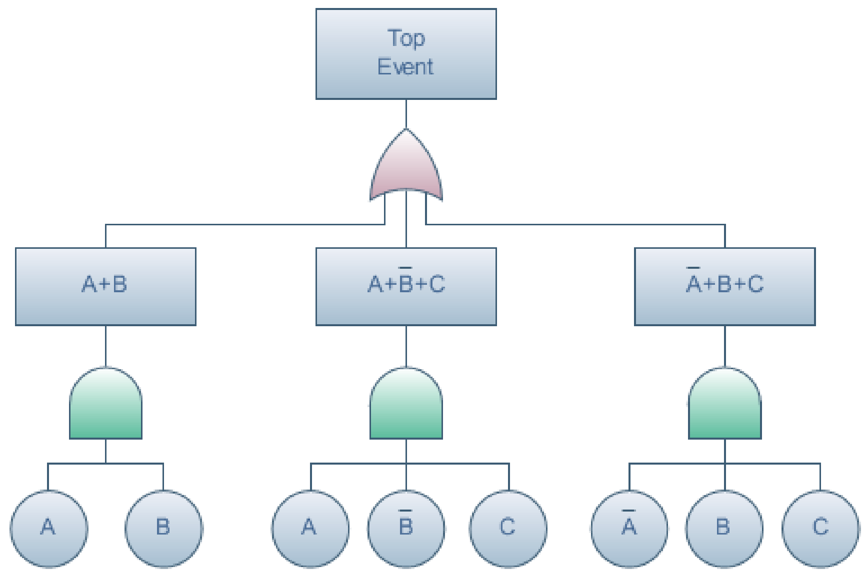
- 2oo4

$$STR = 12 \times \left(\lambda^S\right)^3 \times MTTR^2$$

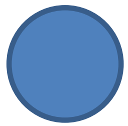
SIL Verification Techniques

2

Fault Tree Analysis

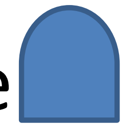


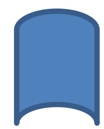
FTA Elements and Symbols
IEC 61025 - Fault tree analysis (FTA)

Basic Event 

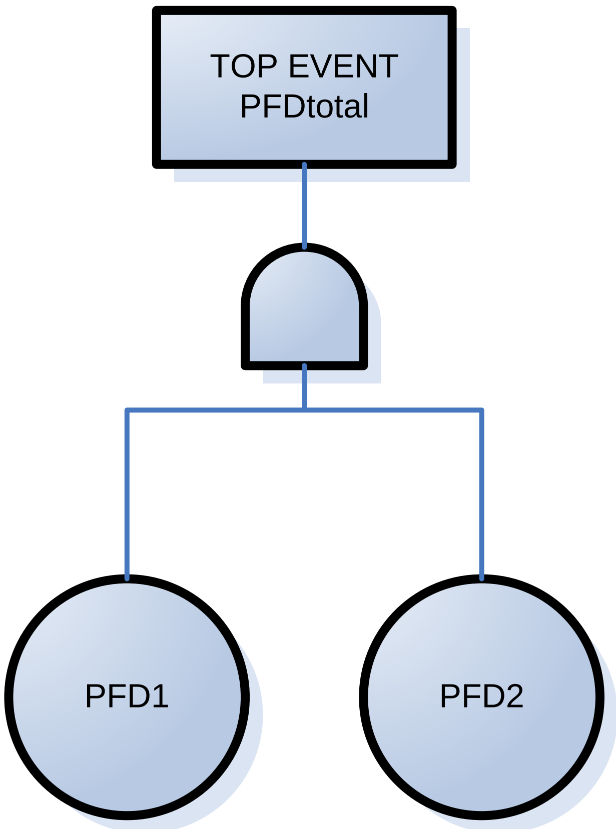
Top Event 

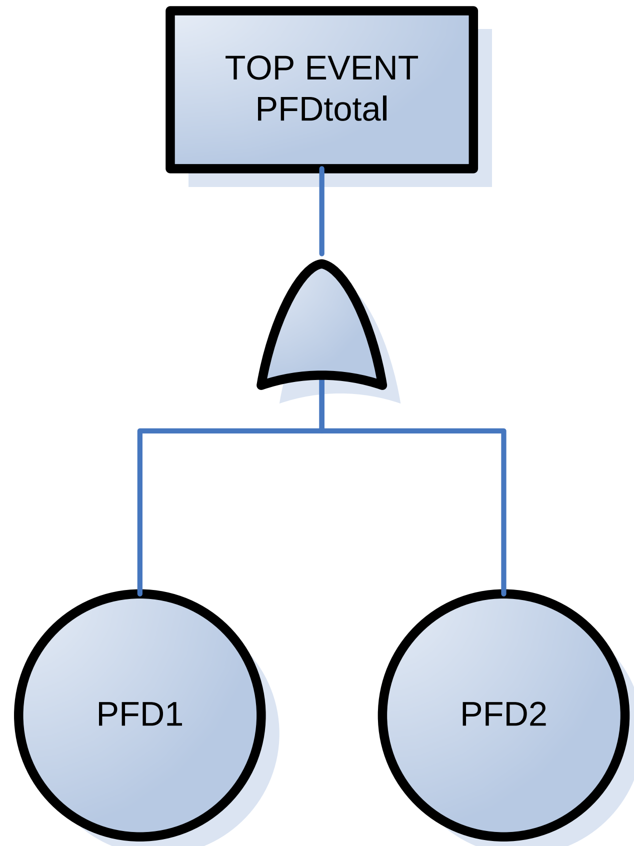
Intermediate Event 

AND Gate 

OR Gate 

FTA Logic





AND GATE:

$$P(A.B) = P(A) \times P(B)$$

OR GATE:

$$P(A+B) = P(A) + P(B) - P(A) \times P(B)$$

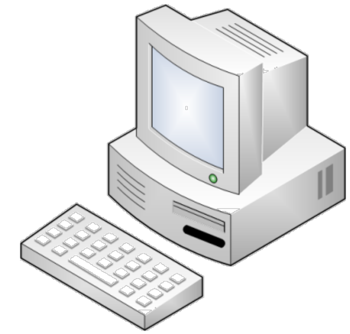
Procedure

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.

Software



- CAFTA

  http://www.epri.com/
- OpenFTA

  http://www.openfta.com/
- BlockSim

  http://www.reliasoft.com/
- Many more…

Working Example