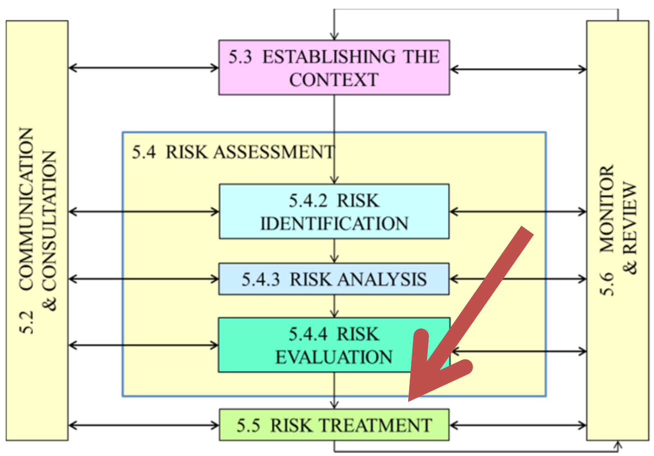
Qualitative Risk Analysis

Risk Management – Functional Reliability

Prepared by Ferenc Birloni, PhD
2017

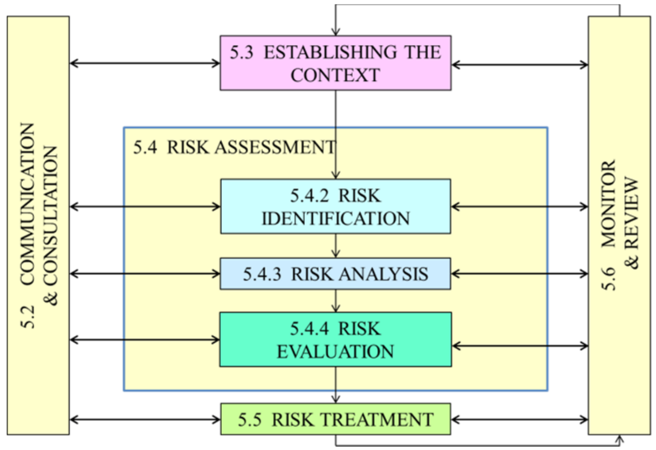
Warm Up

- **CAN YOU RECALL THAT YOU AVOIDED RISK?**
- **DID YOU CONFIDENTIALLY ACCEPT RISK?**
- **DID YOU REDUCE RISK IN YOUR LIFE?**



Monitoring and Review

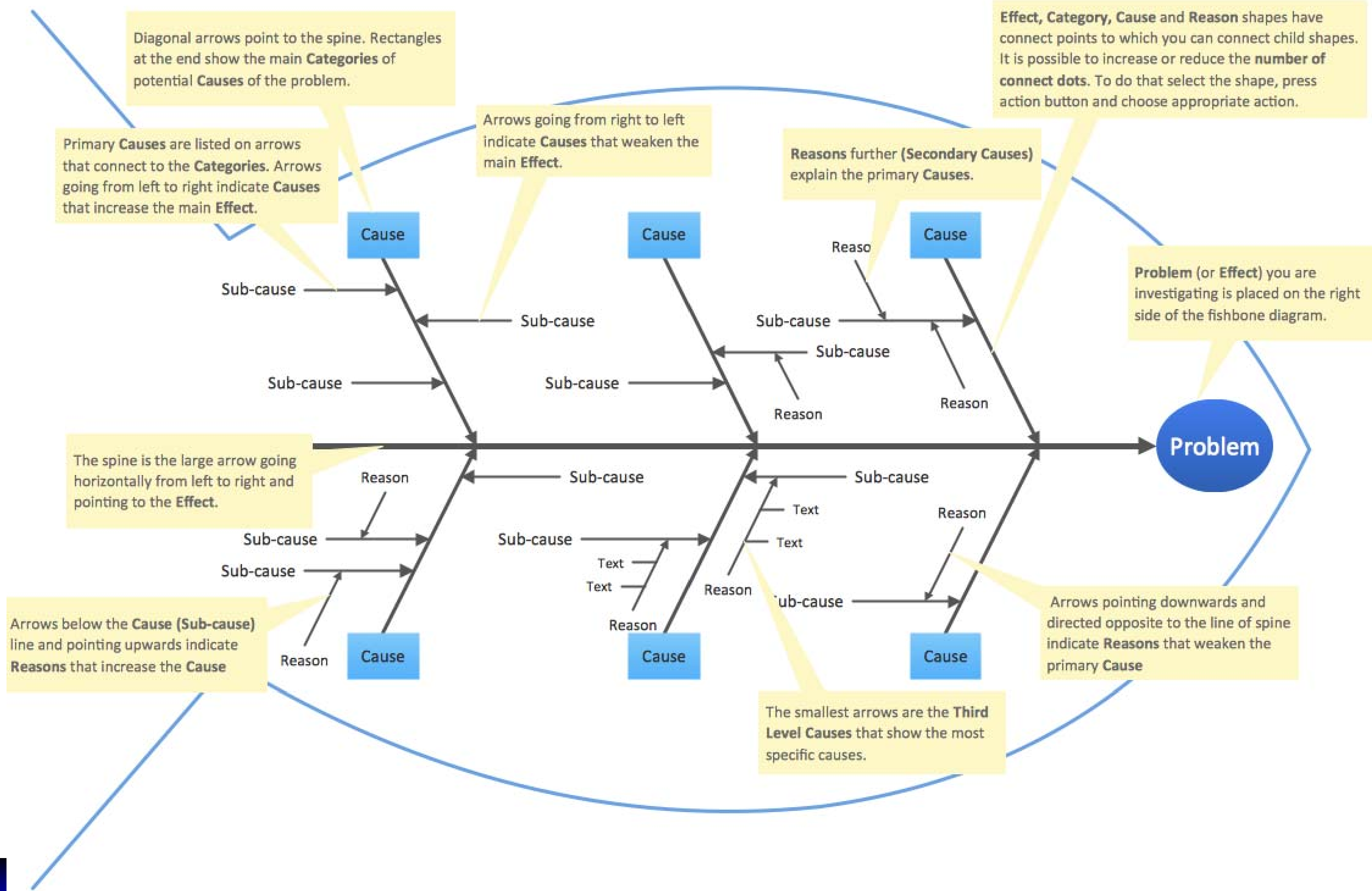
- **Planned, regular** monitoring of the risks and risk management framework is critical
- Monitoring and review is undertaken by **risk owners** and management
- **Independent review** of the risk management framework



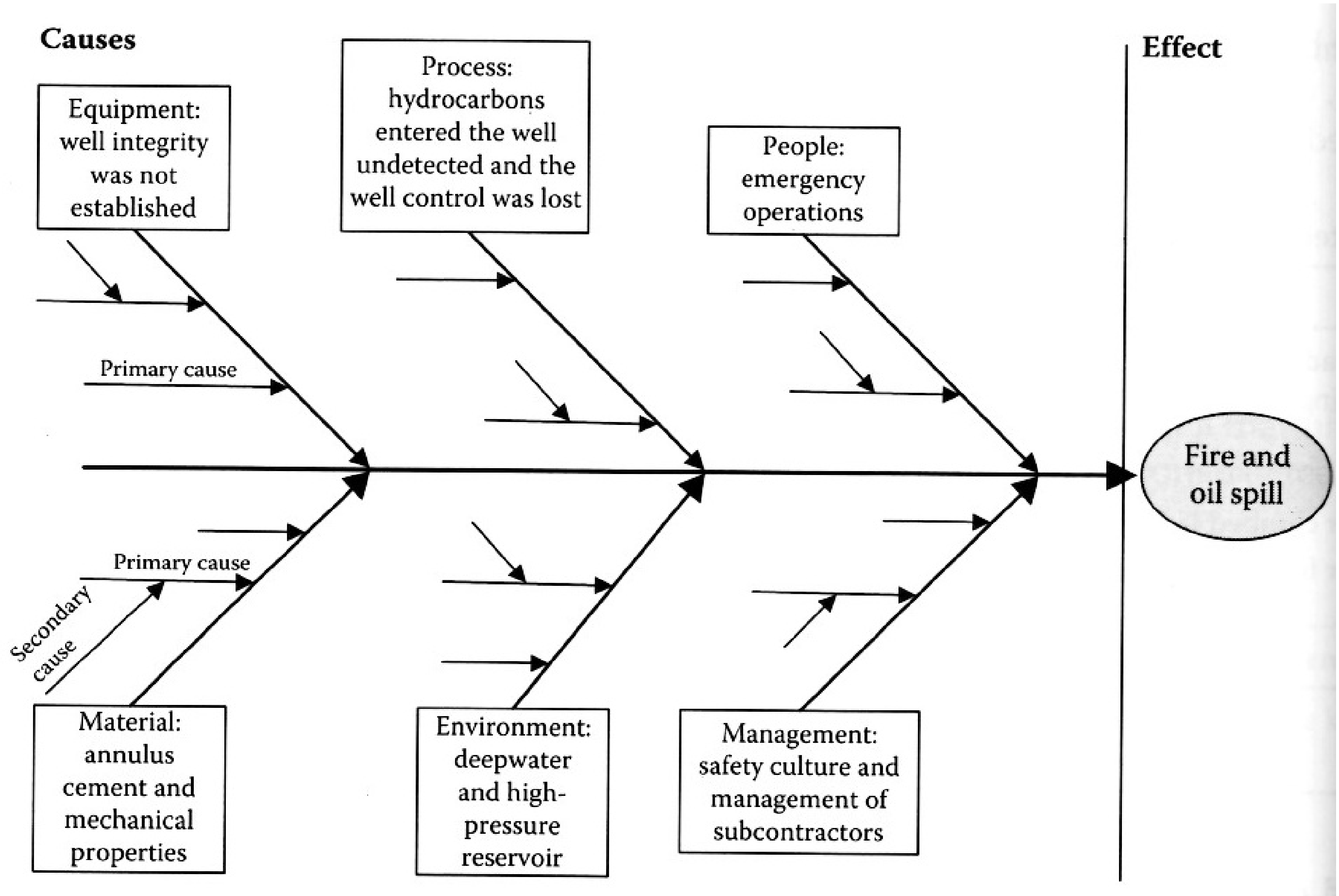
SUMMARY FOR TODAY

- ✓ Risk Assessment Methods – Logic trees
- ✓ Risk Analysis on Safety Instrumented Systems
- ✓ Risk Analysis with Risk Graphs

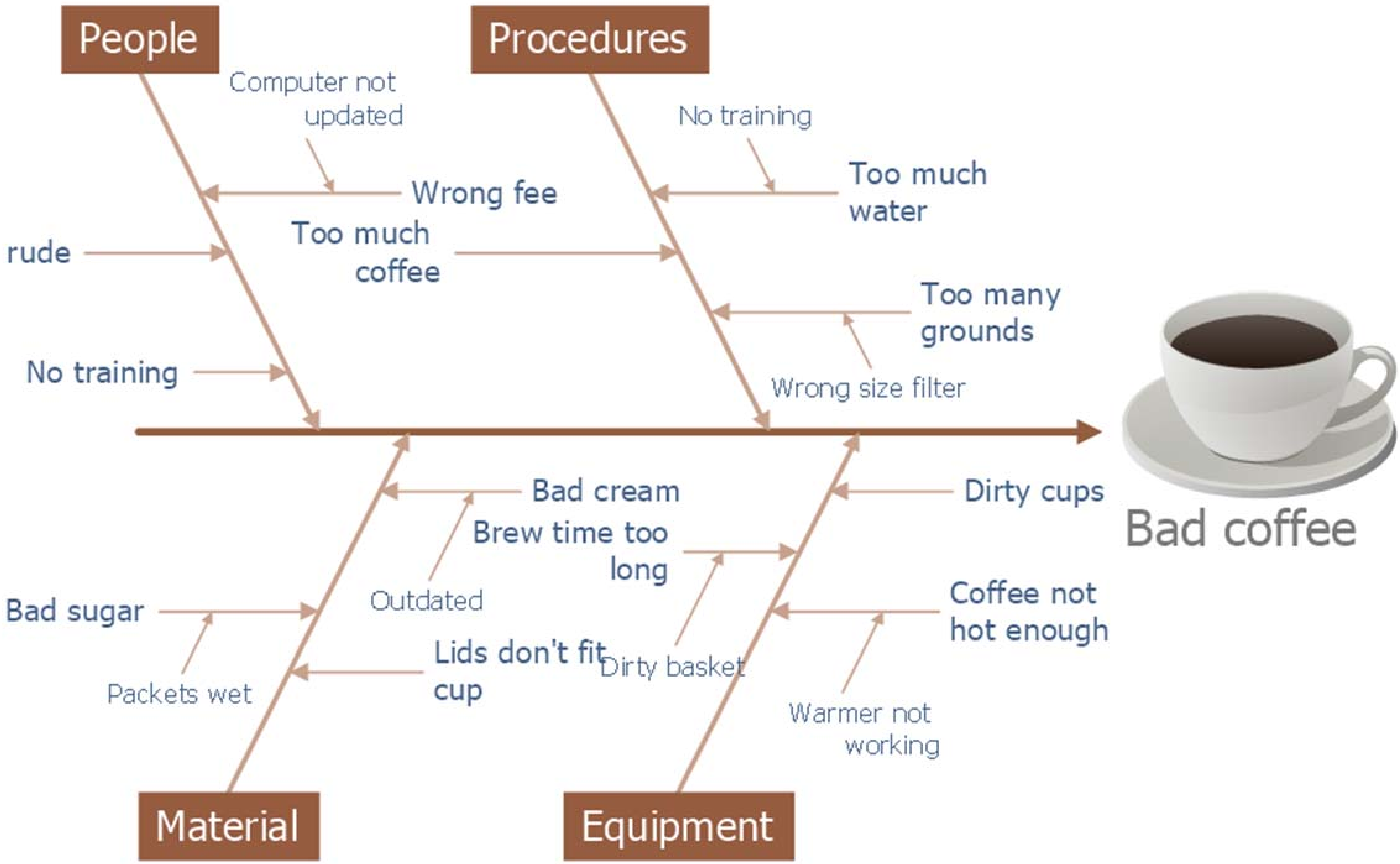
Fishbone Explained



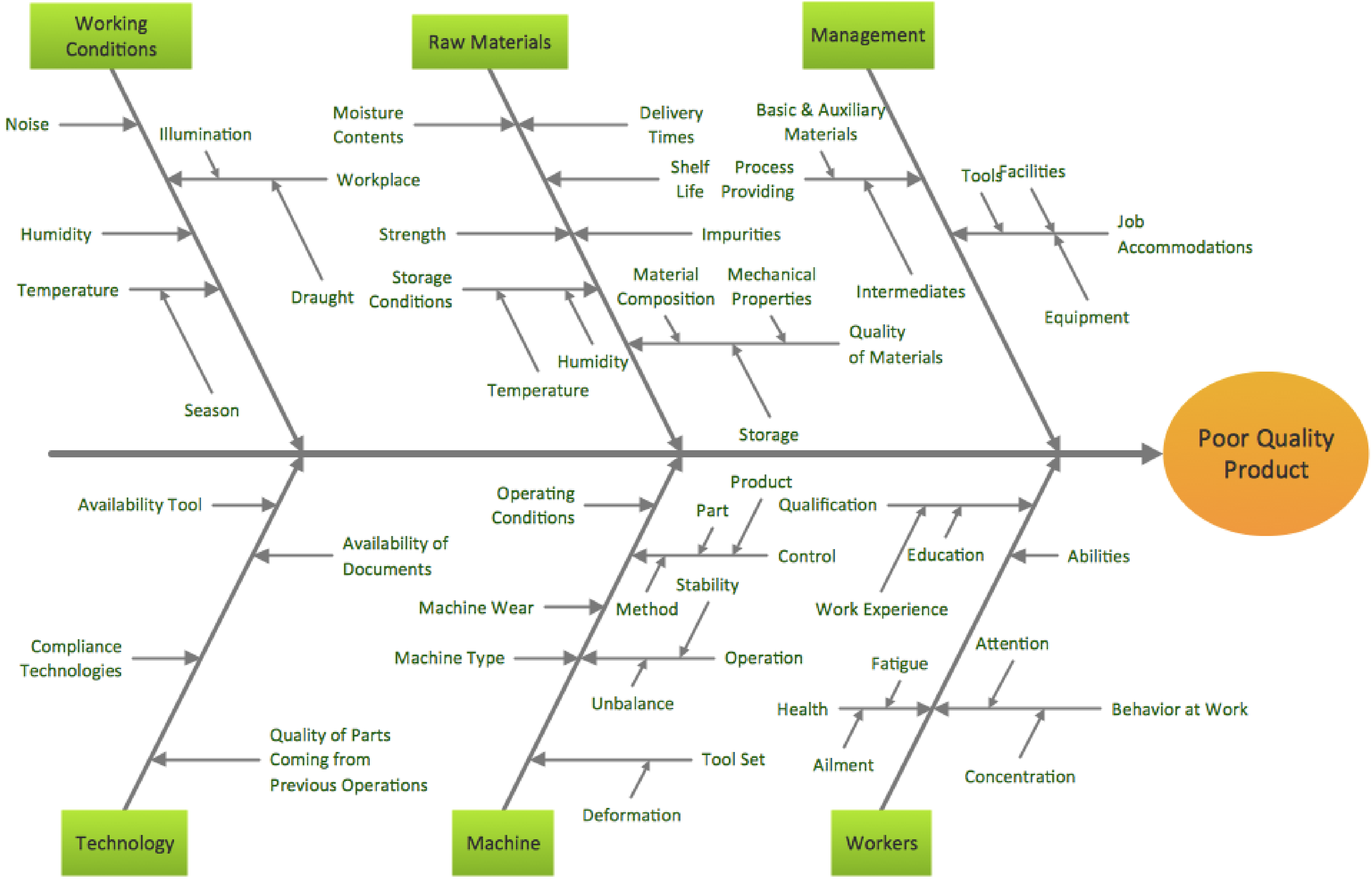
Ishikawa Diagram – Oil Split



Fishbone – Simple Analysis

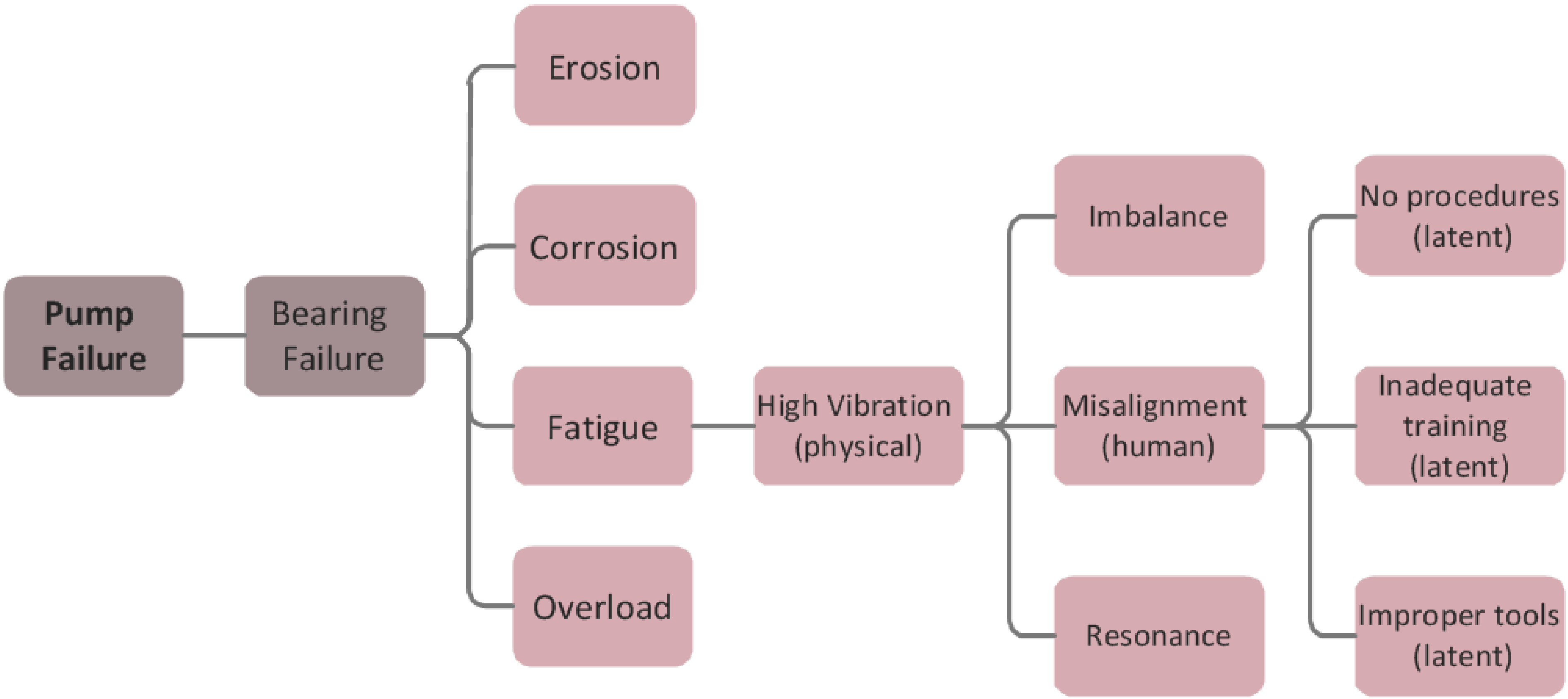


Fishbone Diagram - Causes of Low-Quality Output



Root Cause Analysis Tree

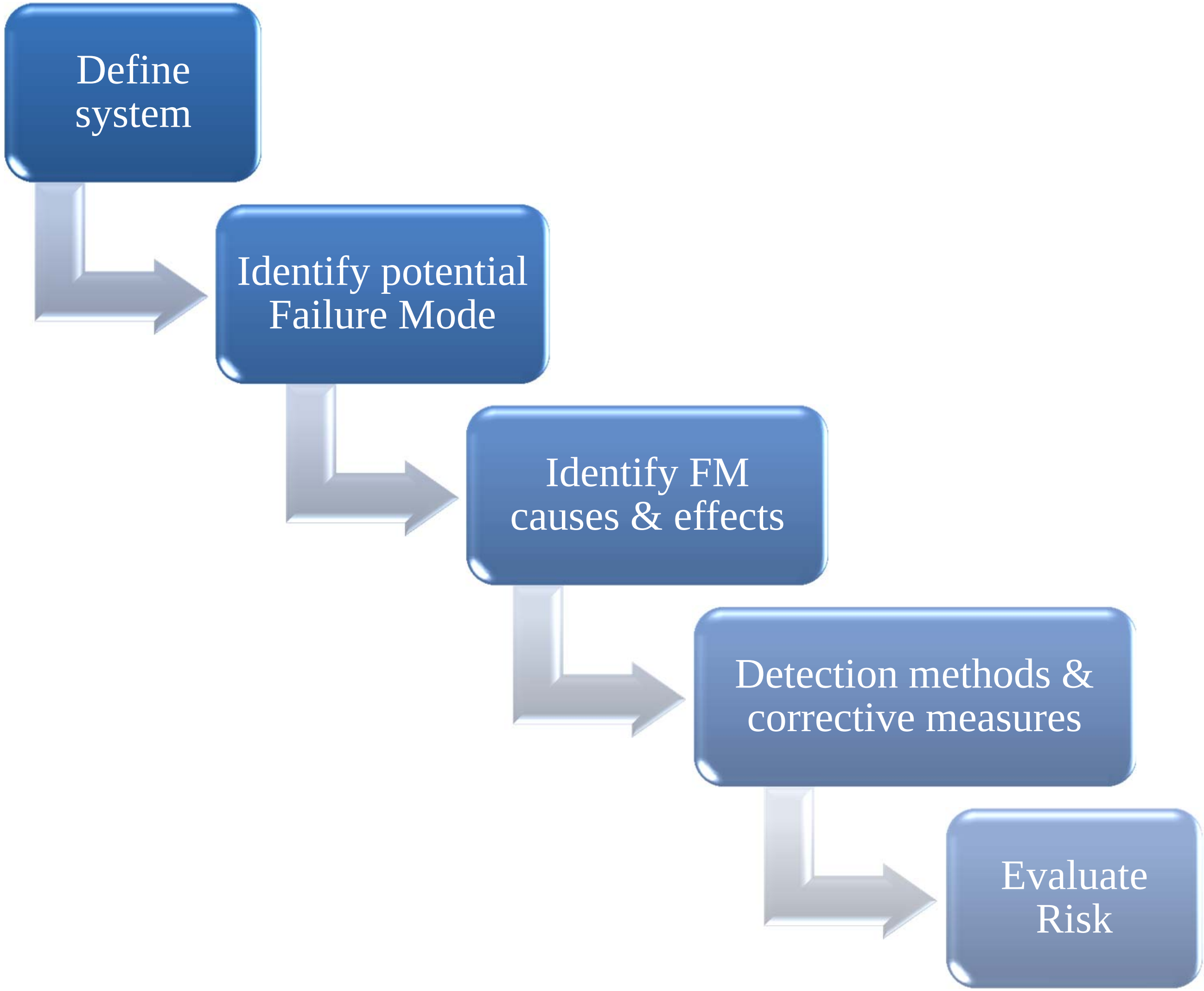
Undesirable Outcome in Mechanical Engineering



Further Risk Assessment Methods

- **FMEA – Fault Mode Effect Analysis**
- FMECA – Fault Mode & Critical Analysis
- ETA – Event Tree Analysis
- **FTA – Fault Tree Analysis**
- AEMA – Action Error Mode Analysis
- HAZOP – Hazard and Operability study

FMEA Model


Define system
Identify potential Failure Mode
Identify FM causes & effects
Detection methods & corrective measures
Evaluate Risk

FMEA – Warehouse example

THE UNIVERSITY OF MELBOURNE

Source & Type	Failure Mode	Effect on Total Perf	Causes	Controls	SEV	OCC	DET	RPN

SEV – severity of the effects of the failure (1-low, 10- high)
OCC – probability of failure occurring (1-low, 10- high)
DET – likelihood failure is detected (10-low, 1- high)
RPN – Risk Priority Number = SEV x OCC x DET

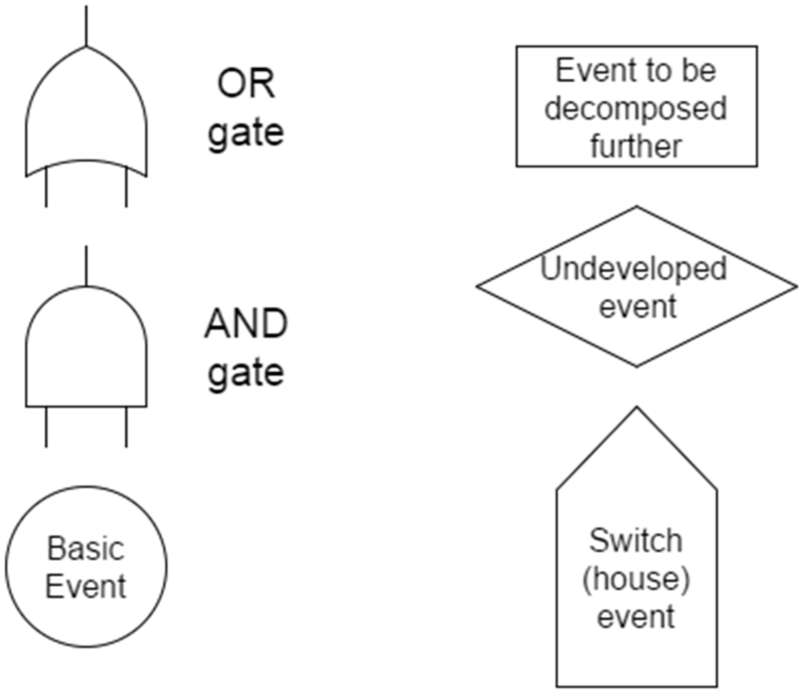
FMEA – Warehouse example 1

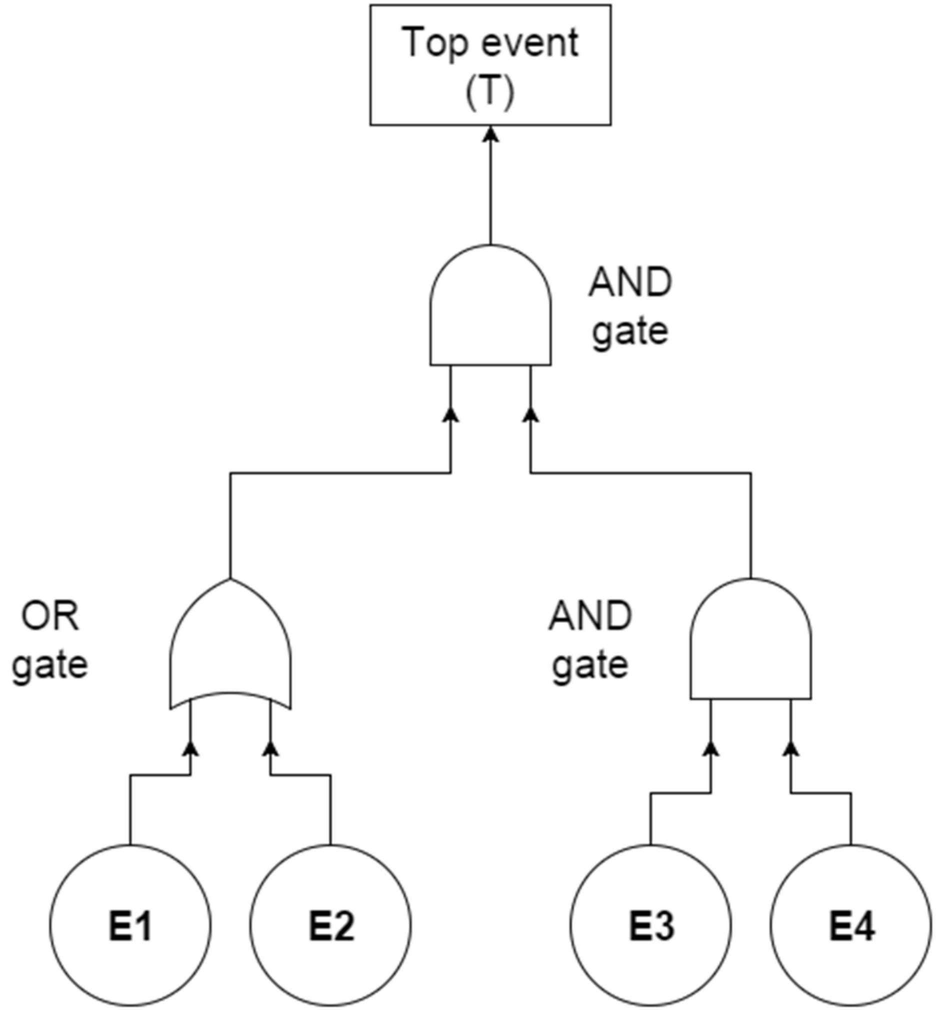
Source & Type	Failure Mode	Effect on Total Perf	Causes	Controls	SEV	OCC	DET	RPN
PM Risks (Internal)	Budget overrun	Failure to finish project within budget	Financial control is lost	Increase tech & financial monitoring, and auditing of project activities	9	6	5	270
	Time overrun	Failure to start operation on time	Technical monitoring by PM is reduced due to design/construction or contractor problem	Increase periodical tech control & progress track	9	5	8	360
	Party disputes	Delay in finishing, & loss to client	Various reasons among parties	Resolve problems as they appear	7	4	5	140
	Personnel problems on-site	Pers. problems that can lead to chaos	Bad planning – lack of on-site organization	Periodic meetings to solve problems	5	4	4	80
Technological, quality, performance risk	Changes in project technology	Failure to cope with changes	PM staff is not prepared to accept changes	Meetings to make PM staff aware of changes	6	6	6	216
	Quality problems	Failure to meet project requirements	Good quality standards not set properly	Quality manual to prepare and train	8	5	6	240

FMEA – Warehouse example 2

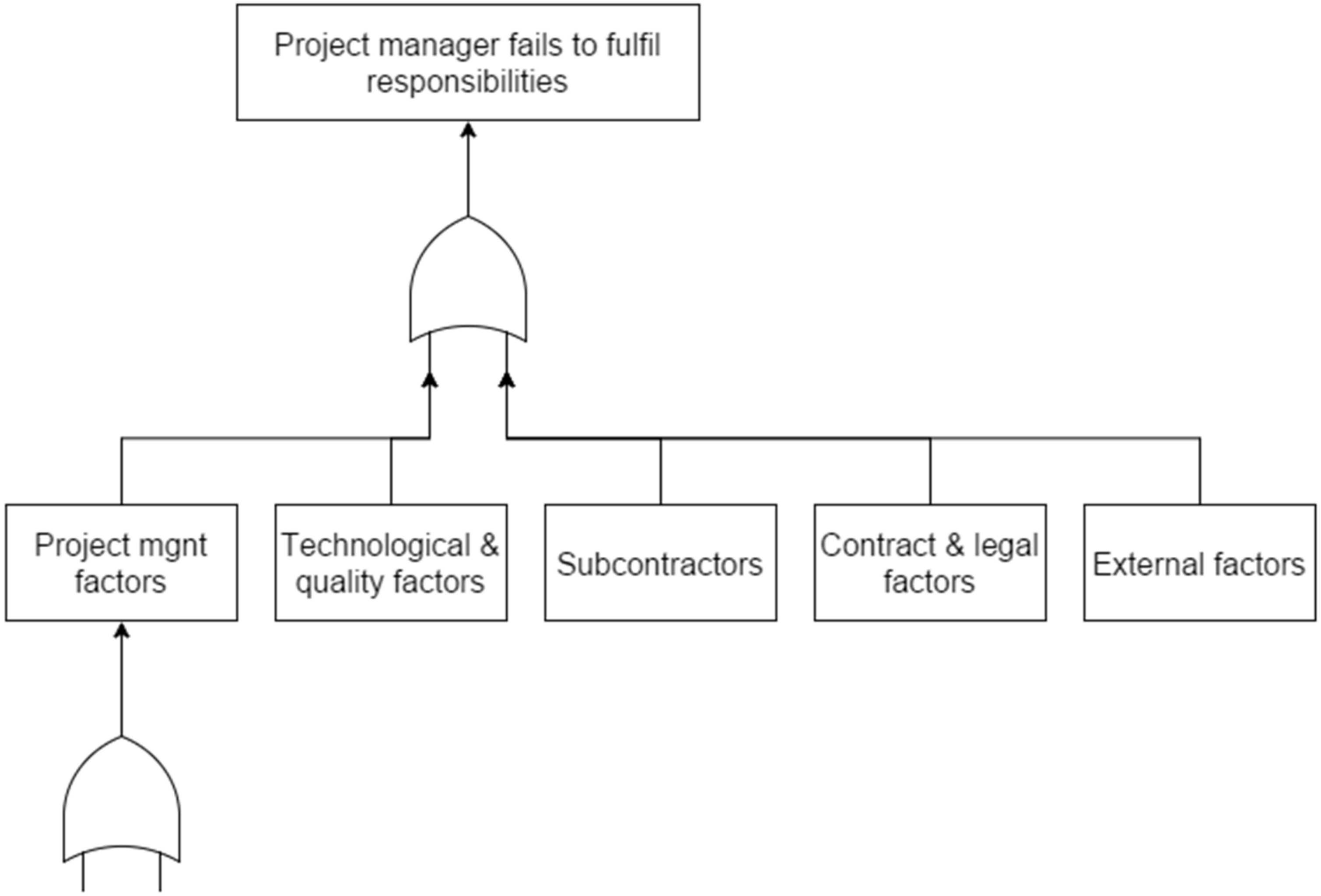
Source & Type	Failure Mode	Effect on Total Perf	Causes	Controls	SEV	OCC	DET	RPN
Contractors risk (External)	Contractor failure to finish on time	Failure to deliver to the client's expectation	PM lacks control over contractor	PM engagement in the selection of the contractor	7	4	6	168
	Incompetent contractor	Failure to meet project requirements	PM lacks control over the chosen contractor	Enforce adherence to PM procedures	6	3	8	144
	Inefficient subcontractors	Problems in delivery & subcontract work	Improper contractor or subcontractor issue	Check, control or mediate	5	6	4	120
Contractual & legal risks	Contractual problem with client	Disputes with the client	PM misunderstood the requirements	Explain to client the scope of services	4	4	5	80
		Failure to complete PM services	PM failed to fulfil his responsibilities	Negotiate new terms or provisional precautions	3	4	5	60

Success / Fault Tree Model

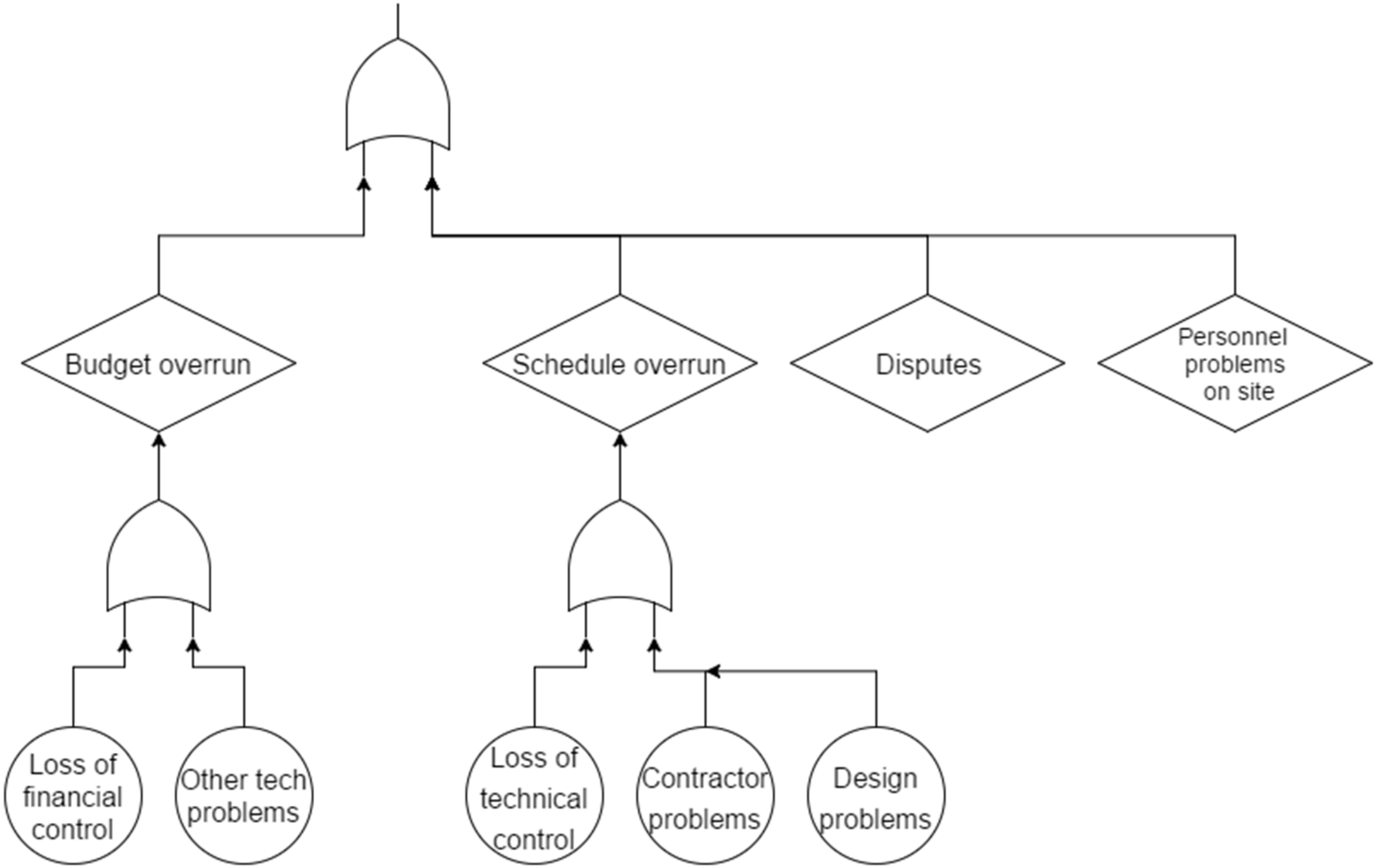




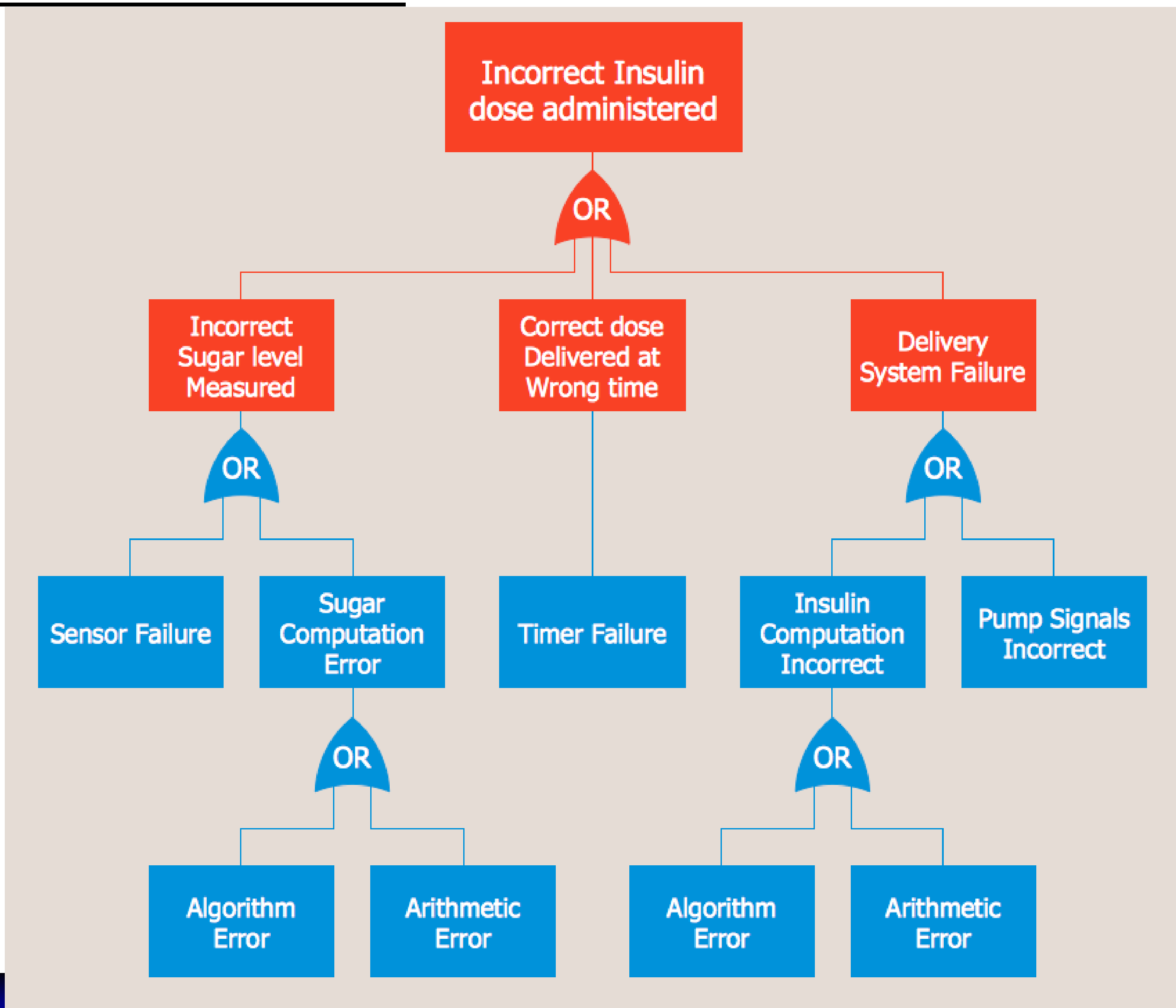
FT model of PM failure – example 1.



FT model of PM failure – example2.



FT Analysis – Functionnally Critical

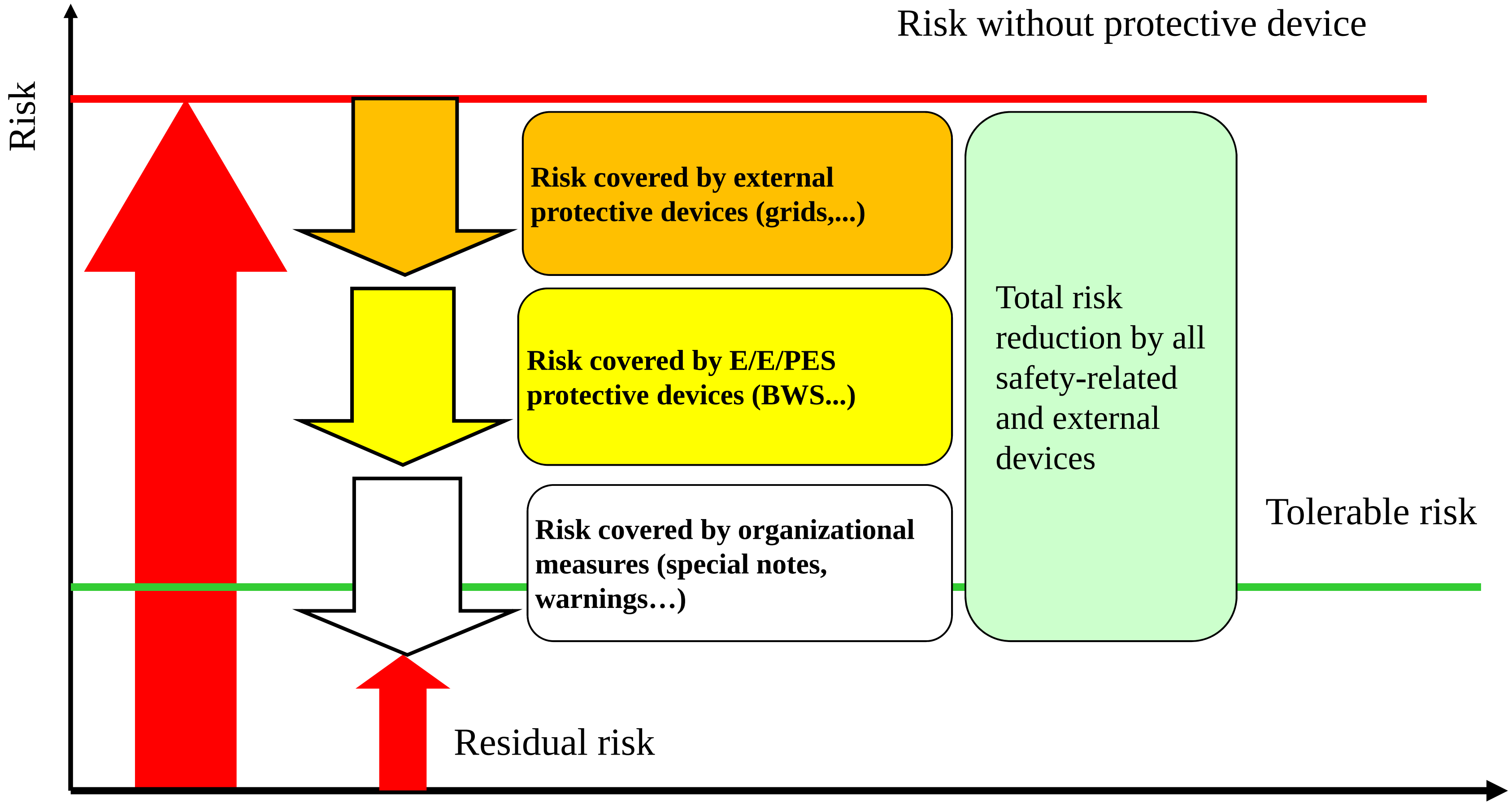


Logic Trees Compared

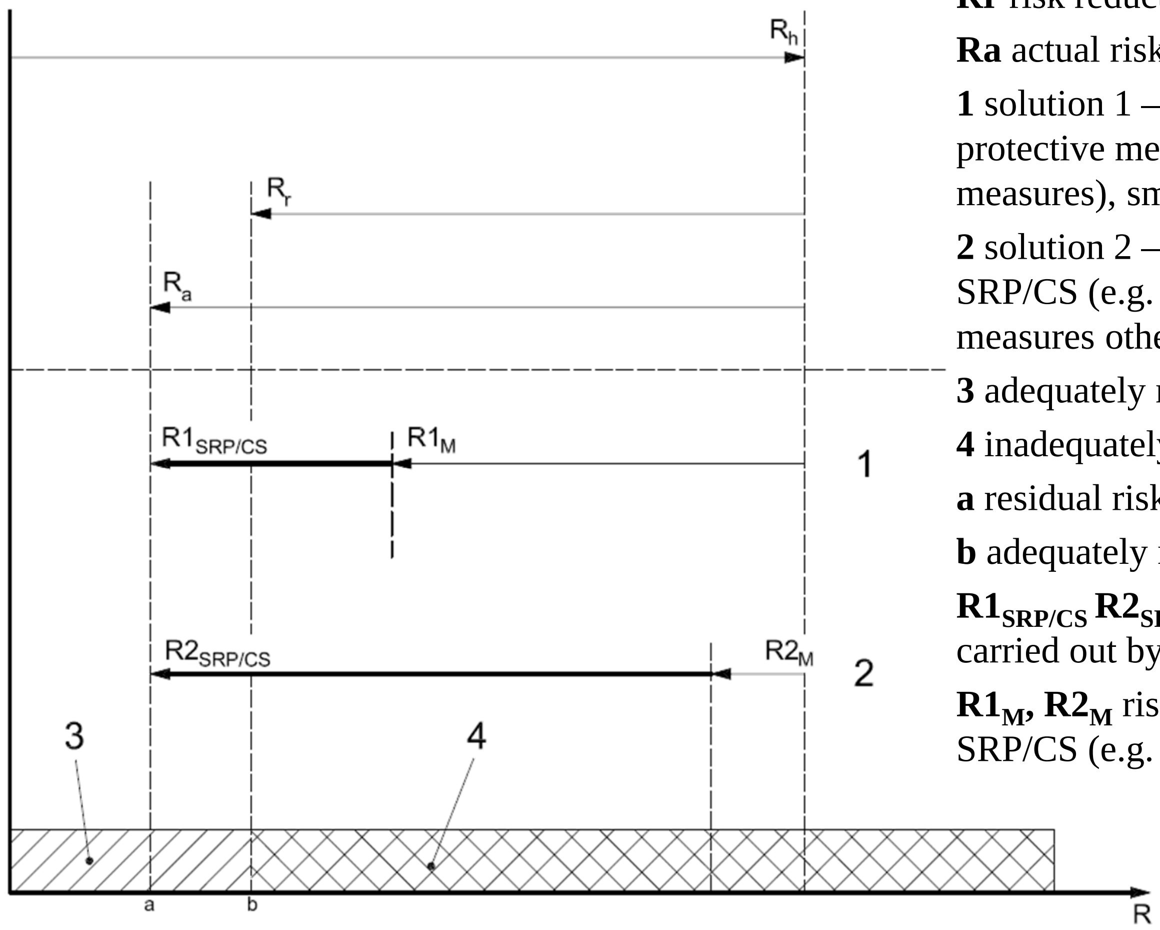
Logic Tree	Analysis Outcomes	Mathematical Foundation	Data Required	Advantages	Limitations
Fault Tree	Probability of failure Cut sets	Boolean logic Probability and reliability theory	System knowledge Failure modes & probabilities	Focusing on components and failure modes	Complex systems requiring use of specialised SW
Success Tree	Probability of success Cut sets	Boolean logic Probability and reliability theory	System knowledge Success modes & probabilities	Focusing on success modes	Complex systems requiring use of specialised SW
Event Tree	Probability of scenarios and consequences	Probability theory	Events, sequencing Outcome spaces	Multiple outcomes Conceptually simple to develop & solve	Binary outcomes
Probability Tree	Probability of any uncertain event in a joint probability distribution	Probability theory Bayes theorem	Events, sequencing Outcome spaces Probabilities Consequences	Multiple outcomes Conceptually simple to develop & solve	Difficult to display, understand, & solve for large tree
Decision Tree	Determine the best decision strategy under uncertainty	Bayes theorem Utility theory	Events, sequencing Outcome spaces Probabilities Consequences	Conceptually simple to develop & solve	Difficult to display, understand, & solve for large tree

FUNCTIONAL SAFETY SYSTEMS

How much safety is necessary?



Risk Reduction Process



Rh the risk before protective measures are applied

Rr risk reduction required from protective measures

Ra actual risk reduction achieved with protective measures

1 solution 1 — important part of risk reduction due to protective measures other than SRP/CS (e.g. mechanical measures), small part of risk reduction due to SRP/CS

2 solution 2 — important part of risk reduction due to the SRP/CS (e.g. light curtain), small part due to protective measures other than SRP/CS (e.g. mechanical measures)

3 adequately reduced risk

4 inadequately reduced risk

a residual risk obtained by solutions 1 and 2

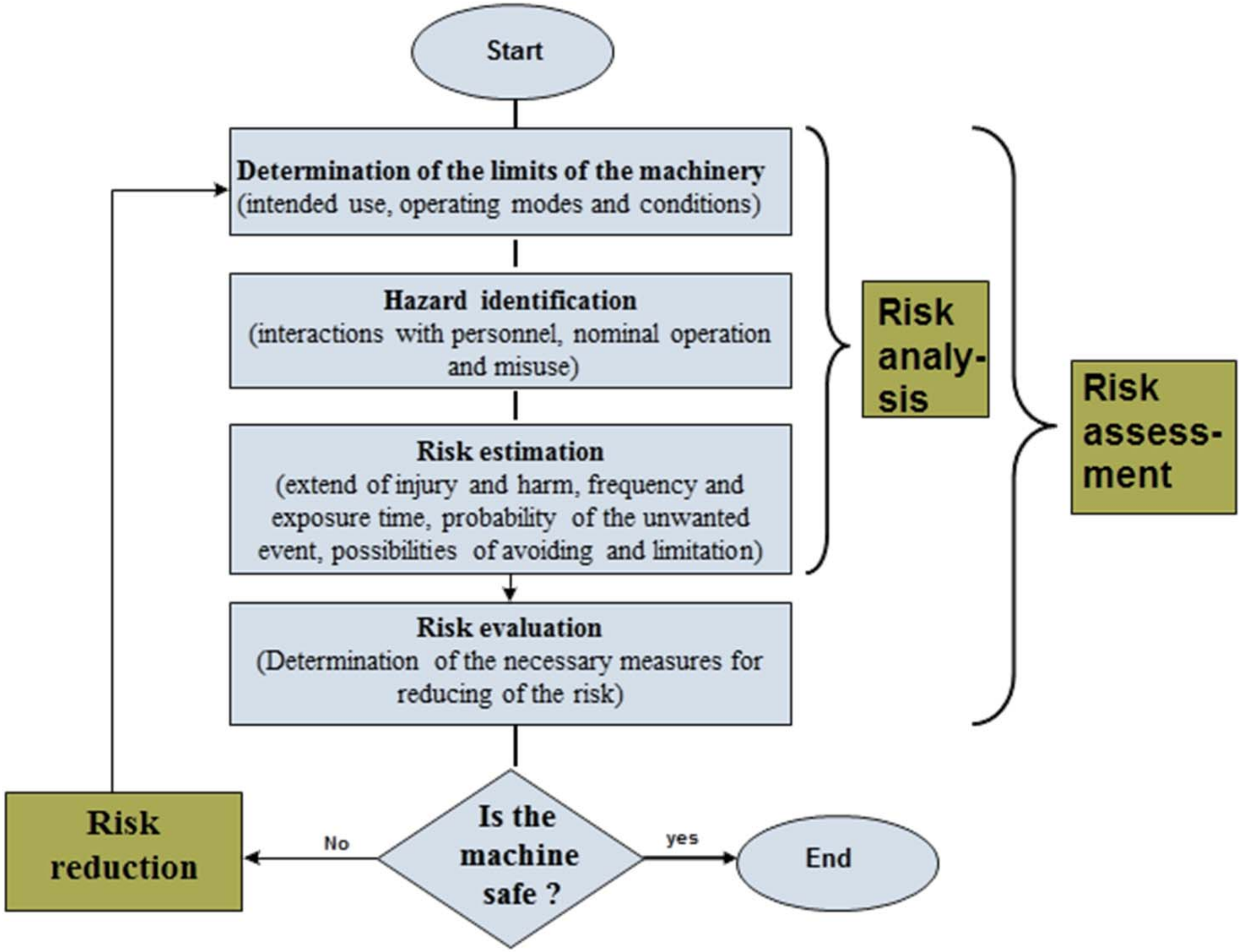
b adequately reduced risk

$\mathbf{R1_{SRP/CS}}$ $\mathbf{R2_{SRP/CS}}$ risk reduction from the safety function carried out by the SRP/CS

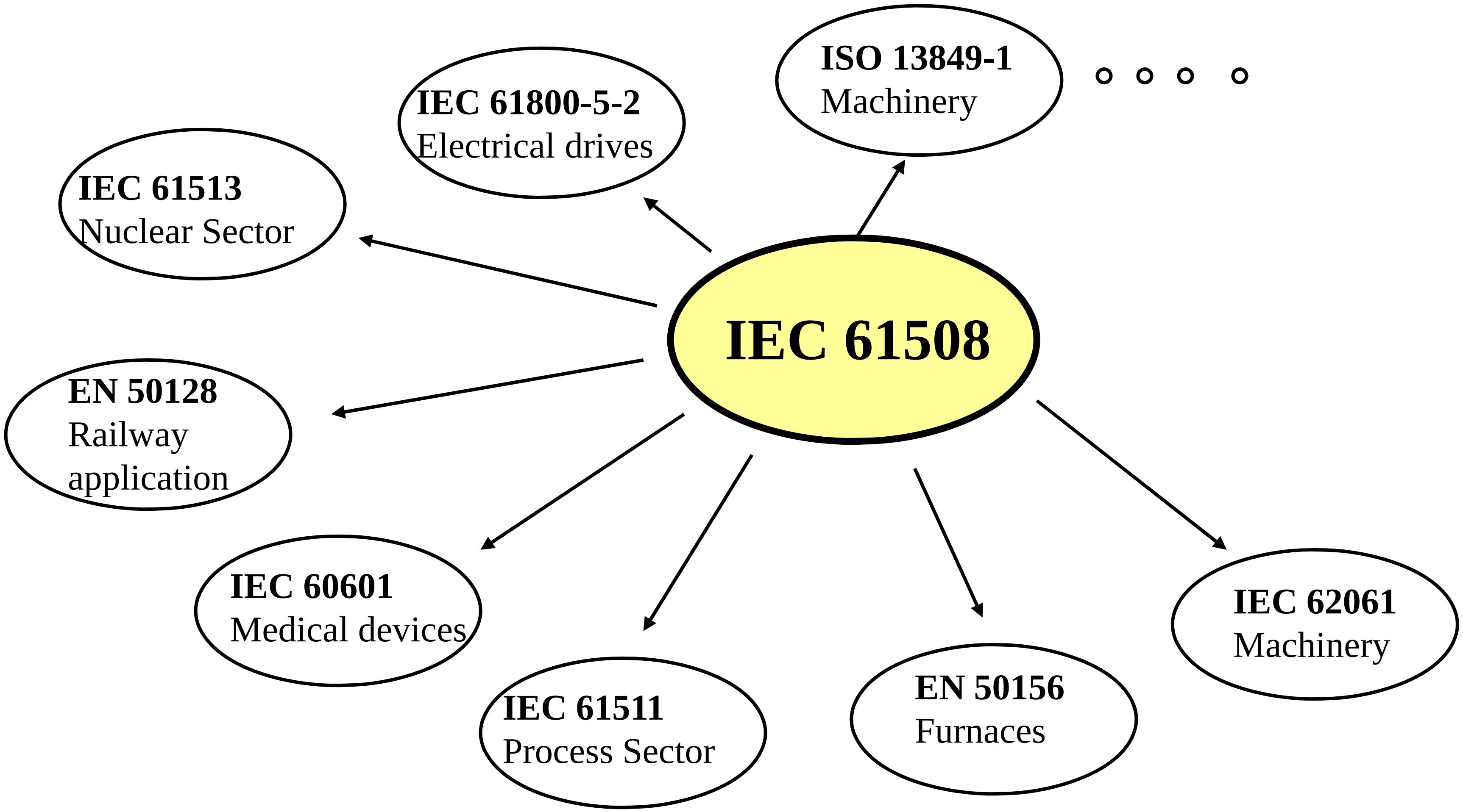
$\mathbf{R1_M}$, $\mathbf{R2_M}$ risk reduction from protective measures other than SRP/CS (e.g. mechanical measures)

EN ISO 14121

- Iterative Process to Achieve the Required Safety Level



Generic and Specific Standards



SIL – Target Failure Measures

1. target failure measures for a safety function operating in
   low demand mode of operation

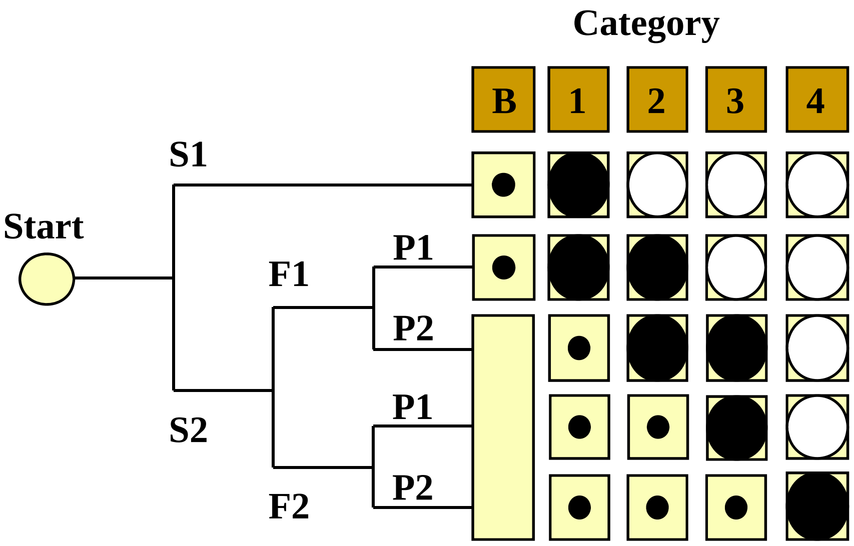
Safety integrity level (SIL)	Low demand mode of operation (Average probability of failure to perform its design function on demand (PFD))
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

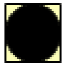
2. target failure measures for a safety function operating in
   high demand or continuous mode of operation

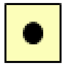
Safety integrity level (SIL)	High demand or continuous mode of operation (Probability of a dangerous failure per hour (PFH))
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

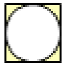
Risk Graph ISO 13849:1999 (superseded)

- **Severity of injury**
  - **S1** slight (usually reversible) injury
  - **S2** serious (usually irreversible) injury, including death
- **Frequency and/or exposure time for hazard**
  - **F1** seldom to less often and/or short duration of exposure time
  - **F2** frequent to continuous and/or long duration of exposition
- **Possibilities of avoiding the hazard**
  - **P1** possible under certain conditions
  - **P2** almost impossible
- **Choice of category**
  - **B, 1 to 4** categories for safety related parts of controls

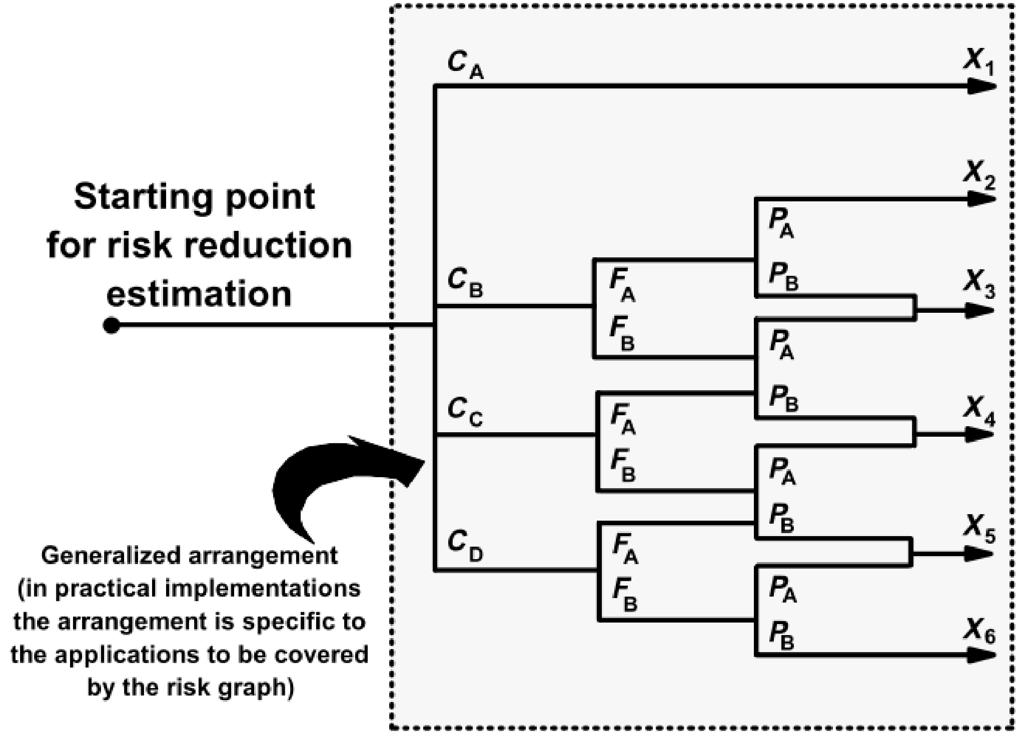



preferred categories for reference point


possible categories, requiring additional measures


measures, which concerning the applied risk may be over-dimensioned

Risk Graph – Analysis



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 risk parameter

F = Frequency and exposure time risk parameter

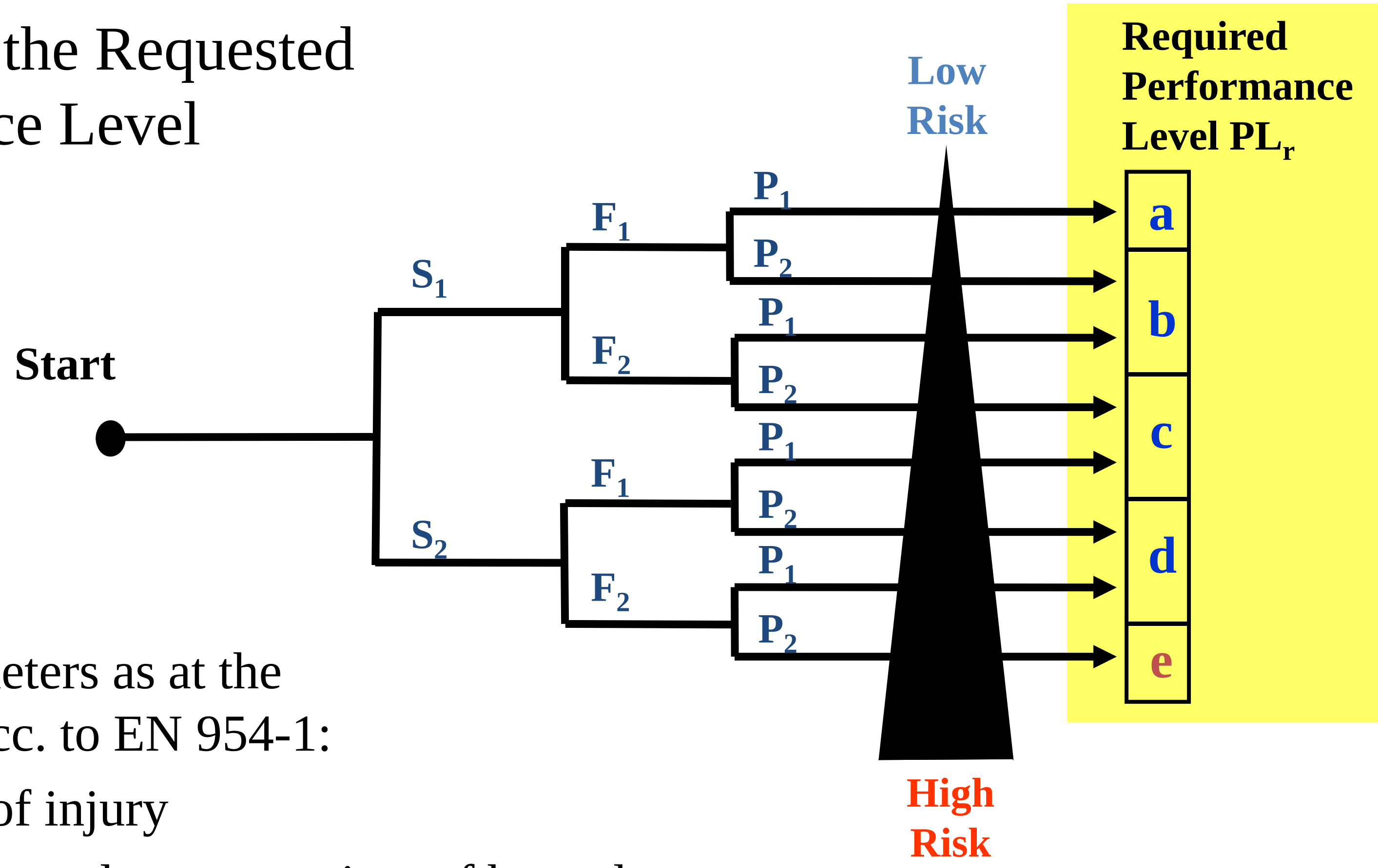
P = Possibility of failing to avoid hazard risk parameter

W = Probability of the unwanted occurrence

Risk Analysis PLr (ISO 13849-1)

THE UNIVERSITY OF MELBOURNE

Determine the Requested Performance Level



Same parameters as at the risk graph acc. to EN 954-1:

S: Severity of injury

F: Frequency and exposure time of hazard

P: Possibility of avoiding the hazard

Parameters of Risk Analysis - EN 62061

Severity of possible harm Se

Consequences	Se
irreversible: death, losing an eye or arm	4
irreversible: broken limb(s), loosing a finger(s)	3
reversible: requiring attention from a medical practitioner	2
reversible: requiring first aid	1

Parameters of Risk Analysis - EN 62061

THE UNIVERSITY OF MELBOURNE

Frequency and duration of exposure Fr

Frequency of exposure	Fr (Duration > 10 min)
≤ 1 per h	5
< 1 per h to ≥ 1 per day	5
< 1 per day to ≥ 1 per 2 weeks	4
< 1 per 2 weeks to ≥ 1 per year	3
< 1 per year	2

Where the duration is shorter than 10 min, the value may be decreased to the next level.

Parameters of Risk Analysis - EN 62061

Probability of occurrence of a hazardous event Pr

Probability of occurrence	Pr
very likely	5
likely	4
possible	3
rarely	2
negligible	1

Parameters of Risk Analysis - EN 62061

THE UNIVERSITY OF MELBOURNE

Avoiding / limiting harm Av

Possibility of avoiding or limiting harm	Av
impossible	5
rarely	3
possible	1

Determination of Required SIL - EN 62061

THE UNIVERSITY OF MELBOURNE

1. Determining of the extent of harm Se

2. Determining of the class Cl

Parameter		Value
Frequency and duration of the exposure	Fr	5
Probability of the unwanted event	Pr	4
Possibility of avoiding and limiting of harm	Av	3
	Sum (class Cl):	12

Determination of Required SIL - EN 62061

Severity Se	Class Cl				
	4	5 to 7	8 to 10	11 to 13	14 to 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

OM: other measures

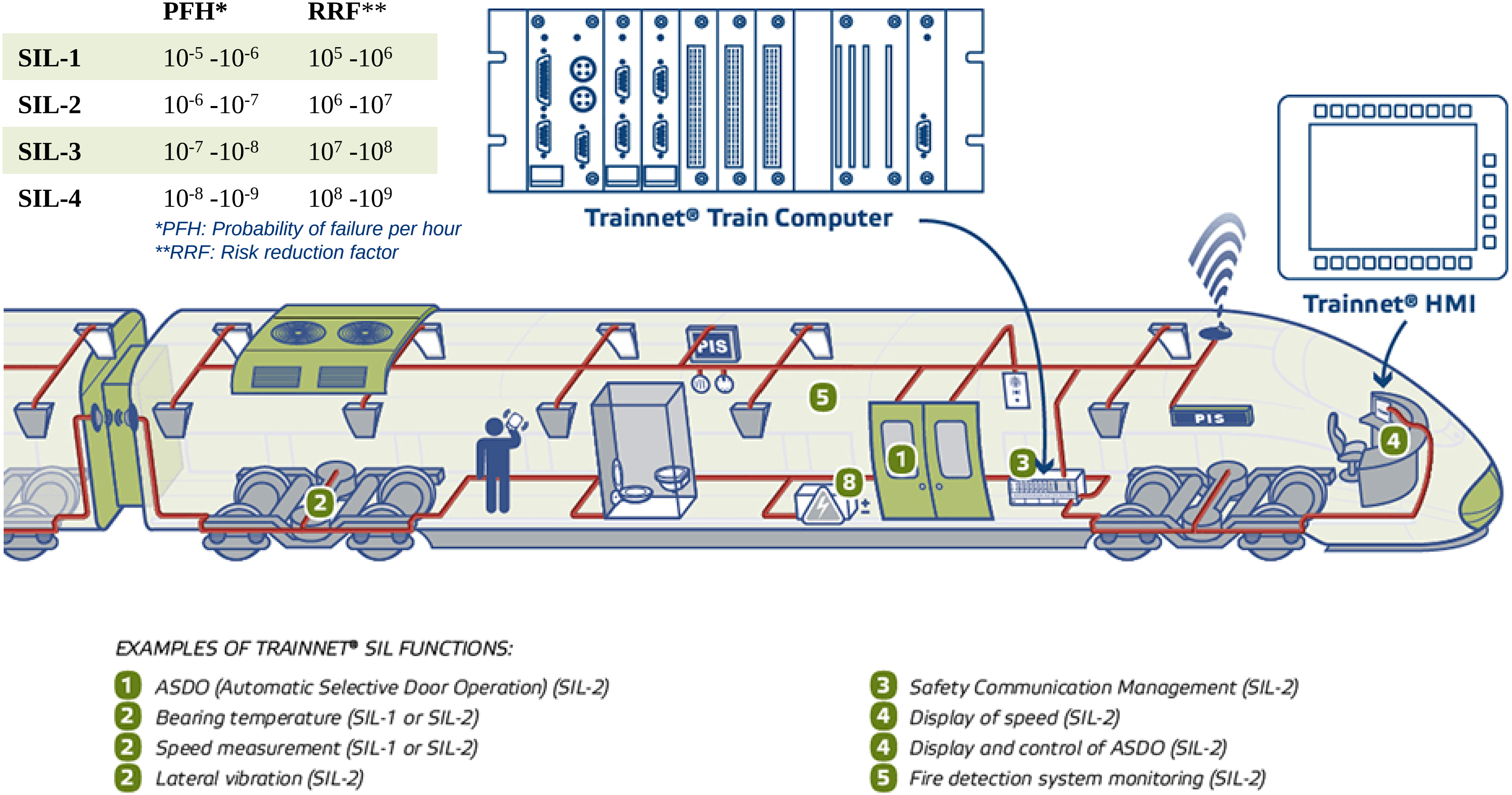
Comparison of the various Safety Classification Systems

EN 62061 Safety Integrity Level (SIL)	IEC 61508 Safety Integrity Level (SIL)	EN ISO 13849-1 Performance Level (PL)	EN 954-1 Category (Cat)
-	-	a	B
1	1	b	1
		c	2
2	2	d	3
3	3	e	4
	4		

SIL – Train System Example

	PFH*	RRF**
SIL-1	10^{-5} -10^{-6}	10^{5} -10^{6}
SIL-2	10^{-6} -10^{-7}	10^{6} -10^{7}
SIL-3	10^{-7} -10^{-8}	10^{7} -10^{8}
SIL-4	10^{-8} -10^{-9}	10^{8} -10^{9}

**PFH: Probability of failure per hour*
***RRF: Risk reduction factor*



http://www.eke-electronics.com/safety-integrity-level-sil-railway-applications

MACHINE CONTROL SYSTEM – EXAMPLE

Risk Assessment

Deal with hazards from two point of view

- hazards to the machine operator
- hazards to people in the environment of machinery

Risk Graph – Qualitative method to determine SIL from the assessment of Risk Factors

Classification Example 1

Risk Parameter		Classifications	Comments
Consequence (C)	C_1	Minor injury	For the interpretation of C, the consequences of the accident and normal healing should be taken into account
	C_2	Serious permanent injury to one or more persons	
	C_3	Death of several people	
	C_4	A large number of people killed	
Frequency and exposure time in hazardous zone (F)	F_1	Rare to more frequent exposure in the hazardous zone	
	F_2	Frequent to permanent exposure in the hazardous zone	

Classification Example 2

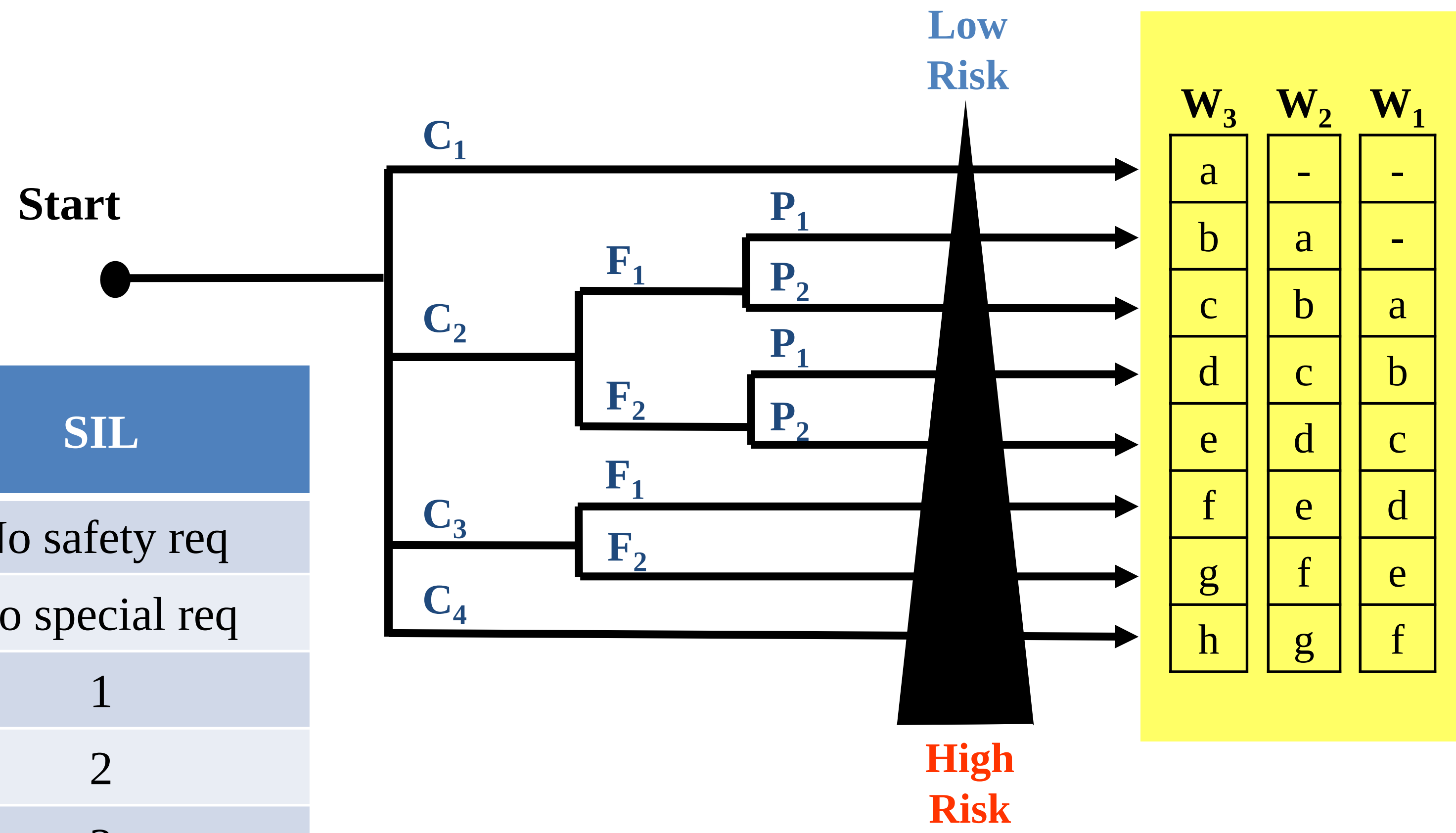
Risk Parameter		Classifications	Comments
Possibility of avoiding hazardous event (P)	P_1	Possible under certain condition	This parameter takes into account • operation of a process (supervised or not) • rate of development of the hazardous event • ease of recognition of danger • actual safety experience (similar MCS)
	P_2	Almost Impossible	
Probability of unwanted occurrence (W)	W_1	Very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely	The purpose of the W factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any MCS, but including any external risk reduction facilities
	W_2	Slight probability that occurrences will come to pass and few occurrences are likely	
	W_3	probability that occurrences will come to pass and frequent occurrences are likely	

Risk Analysis – Hazard Identification

- Electronically controlled powershift transmission

Hazard to operator	**Risk parameter**			
	C	F	P	W
Unexpected gearing down (eg 4th to 1st)	C_2 Operator could be seriously injured	F_2 Operator permanently exposed	P_1 Operator able to use safety belt	W_1 Experience shows – probability of such incidents can be estimated as W_1
Hazard to other people				
Unexpected gearing down (eg 4th to 1st) on public road	C_2 Possibility of collision with sudden stopping of machine	F_1 Travelling on public roads is limited	P_1 Possible to use brakes, or other vehicles may be able to swerve	W_1 Experience shows – probability of such incidents can be estimated as W_1

Risk Graph - Example



Min Risk Reduction	SIL
-	No safety req
a	No special req
b, c	1
d	2
e, f	3
g	4
h	MCS not sufficient

Conclusion

– develop according to SIL

END SUMMARY – QUALITATIVE RISK

- ✓ Risk Assessment Methods – Logic trees
- ✓ Risk Analysis on Safety Instrumented Systems
- ✓ Risk Analysis with Risk Graphs