

Uncertainty of SIL determination

György Baradits sr. SIL4S

dr. János Madár SIL4S

György Baradits jr. SIL4S

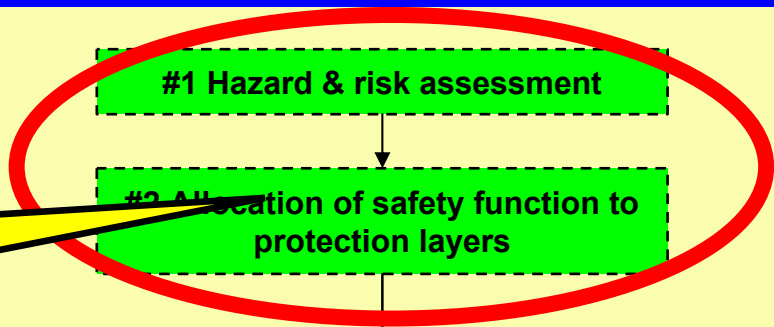
- **SIL determination**
- **Risk matrix**
- **Risk graph**
- **Independent Protection Layers & LOPA**
- **PFD values of IPLs**
- **Cumulative LOPA**
- **Comparison of different methods**

SIL Determination

SIL Calculation

#10 Management of functional safety and functional safety assessment and auditing

#11 Safety life-cycle Structure and planning



#3 Safety requirements specification (SRS) for SIS

#4 Design and engineering of SIS

Design and development of NON SIS

#5 Installation, commissioning and validation

#6 Operation & Maintenance

#7 Modification

#8 Decommissioning

Analysis
End User/Licensor/Consultant

Realization
Vendor/Contractor/End User

Operation
End User/Contractor

No detailed requirements

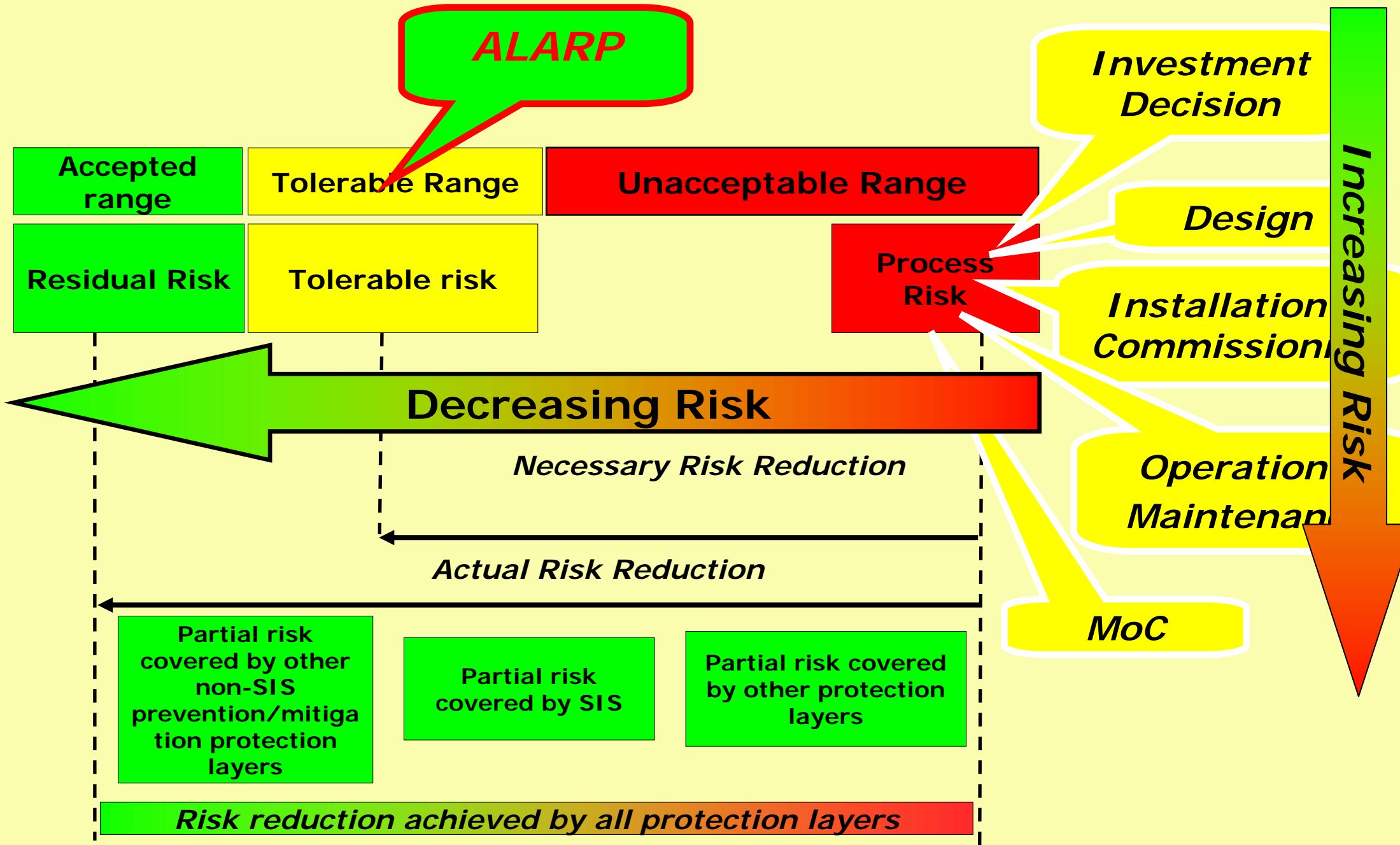
Whole life cycle

#9 Verification



- There are two steps in the safety lifecycle when we determine/calculate SIL values!
- We say “**SIL determination**” when
 - *The goal is to determine the **required SIL** and **RRF** values of SIFs.*
 - *It is done after Process Hazard Analysis and before SRS.*
 - *Methods: Risk matrix, Risk graph, LOPA*
- We say “**SIL calculation**” when
 - *The goal is to calculate the **achieved SIL** and **RRF** values of SIFs.*
 - *It is done during Validation or Pre-validation*
 - *Methods: Reliability Analysis, PFD equations*

- To achieve the **functional safety** we must reduce the risk of the process. The risk reduction may be
 - *Too small* ➡ *The safety will be not achieved (under engineering)*
 - *Too big* ➡ *The cost will be too high (over engineering)*
- **So we should determine:**
 - *Process risk*
 - *Risk reduction* achieved by different protection functions (protection layers)
- **The risk reduction must be enough to decreases the process risk to the **tolerable risk level (ALARP value)**.**



- **Why is there uncertainty in the SIL determination?**
 - *Methodology (qualitative problems)*
 - *Numerical values (quantitative problems)*
- **Methodology**
 - *Risk Matrix*
 - *Risk Graph*
 - *LOPA*

Risk matrix from ExSILentia software:

Increasing Demand Rate

Tolerable Risk Calibration Wizard - Hazard Matrix

Demand Frequency

Safety Integrity Level

D5	< 0.1 years	2	3	4	b	b
D4	0.1 to 0.5 years	1	2	3	4	b
D3	0.5 to 4 years	a	1	2	3	4
D2	4 to 20 years	--	a	1	2	3
D1	> 20 years	--	--	a	1	2

Health and Safety Slight Injury Minor Injury Major Injury Single Fatality Multiple Fatalities

Environment Slight Effect Minor Effect Localized Effect Major Effect Massive Effect

Economics Slight Damage (< \$10K) Minor Damage (\$10 to \$100K) Local Damage (\$100K to \$1M) Major Damage (\$1M to \$10M) Extensive Damage (> \$10M)

Consequence Category

C1	C2	C3	C4	C5
----	----	----	----	----

Load Defaults Cancel << Back Next >> Finish

SIL 2

Increasing Severity

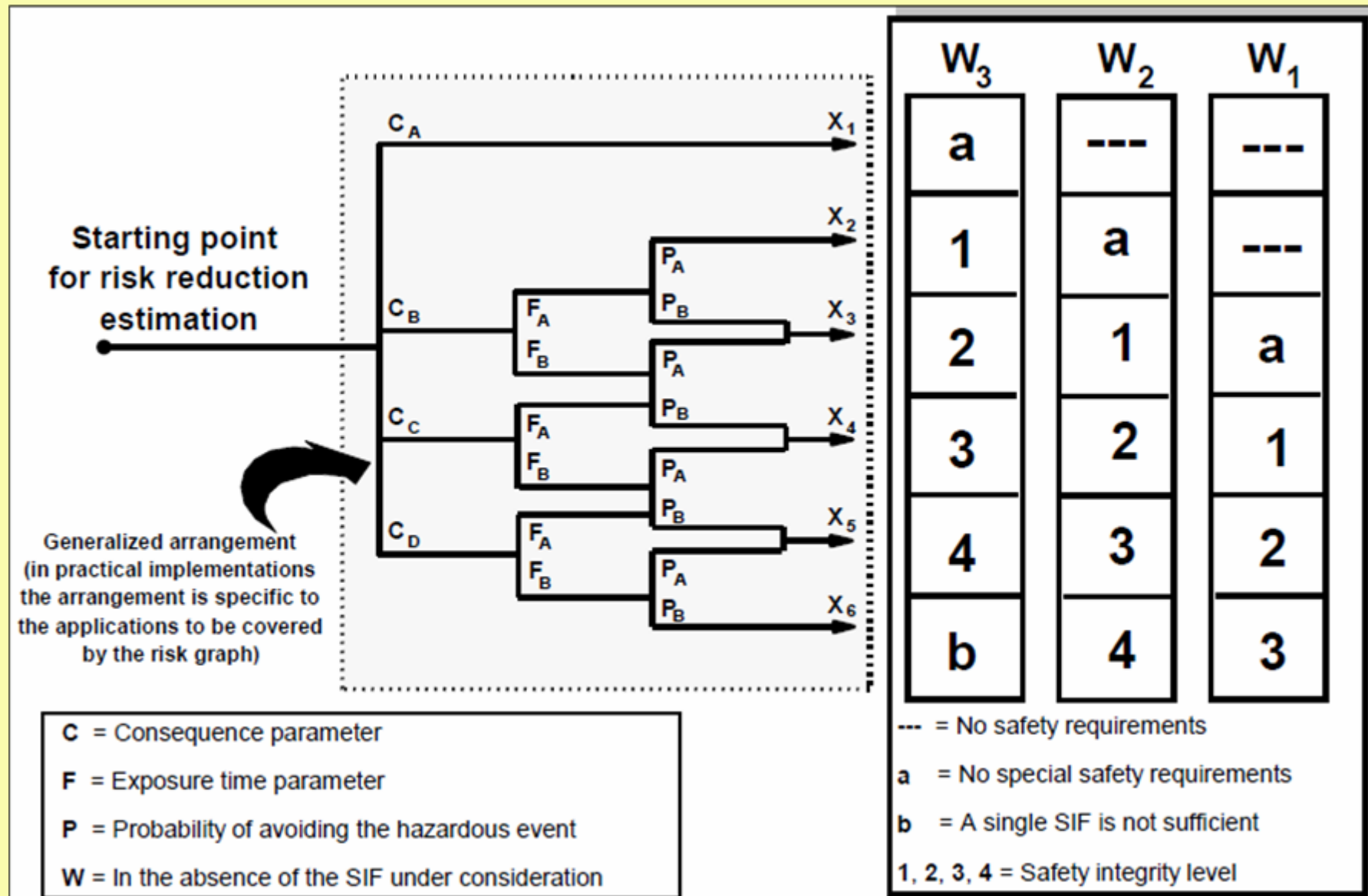
■ Advantages:

- *Very simple and fast*

■ Uncertainty in Risk matrix:

- *Cannot calculate with the possibility of avoiding of hazardous event (human exposure, etc.)*
- *What about if there are other independent layers (e.g. alarm, relief valve)?*
 - *Shall we decrease the frequency category? How?*
- *What about if there are several causes of an hazardous event with mixed IPLs?*
 - *Shall we increase the frequency category? How?*

Risk graph from IEC 61511 Part 3:



(W) Demand rate

W1 = Very low (10 - 100 year)

W2 = Low (1 - 10 year)

W3 = High (< 1 year)

(C) Consequence if the effect is not avoided

CA = Small injury

CB = Several injury / single fatality

CC = Several fatality

CD = Catastrophic

(F) Exposure in the hazardous zone

FA = Rare to more frequent

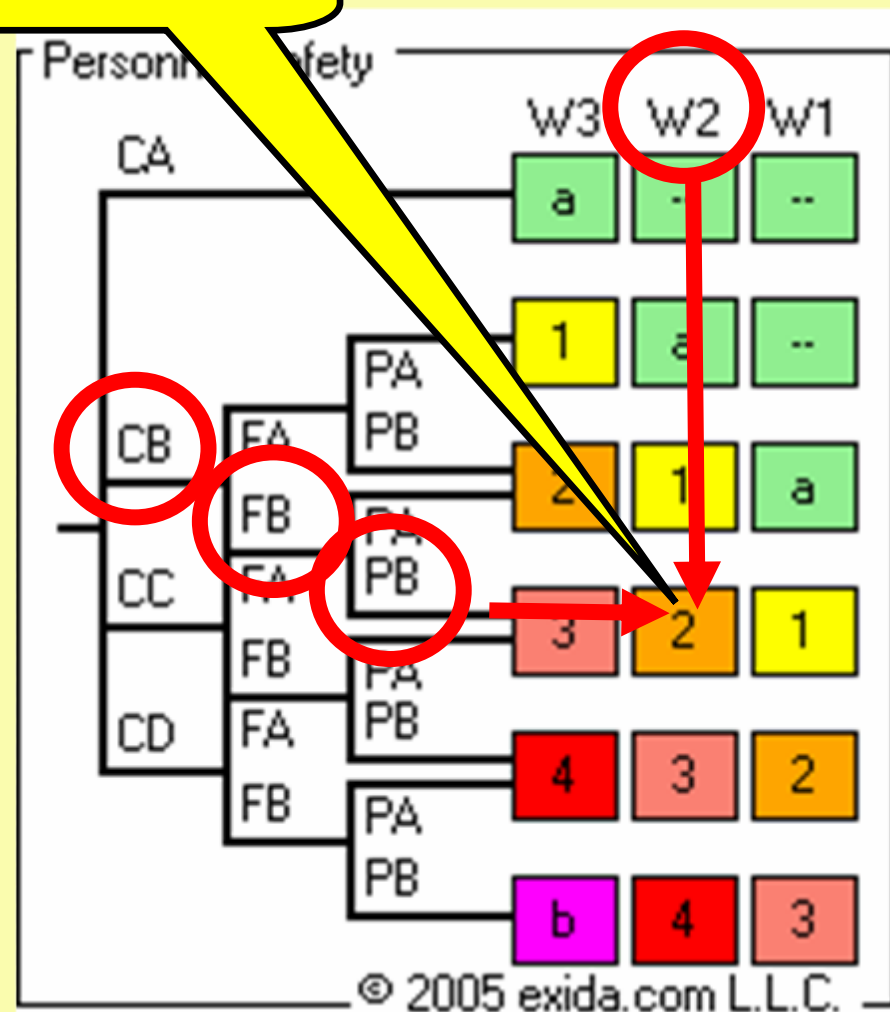
FB = Frequent to permanent

(P) Probability of avoiding the hazardous event

PA = Possible (see the standard)

PB = Not possible

SIL 2



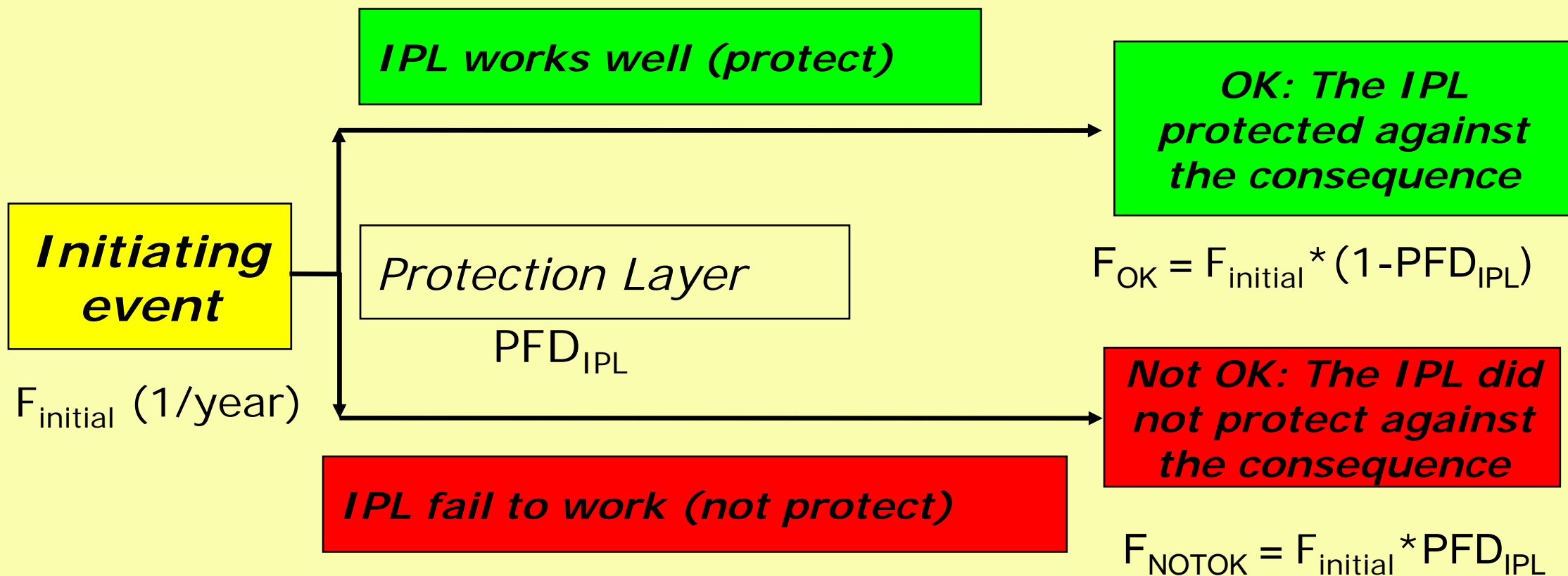
■ Advantages:

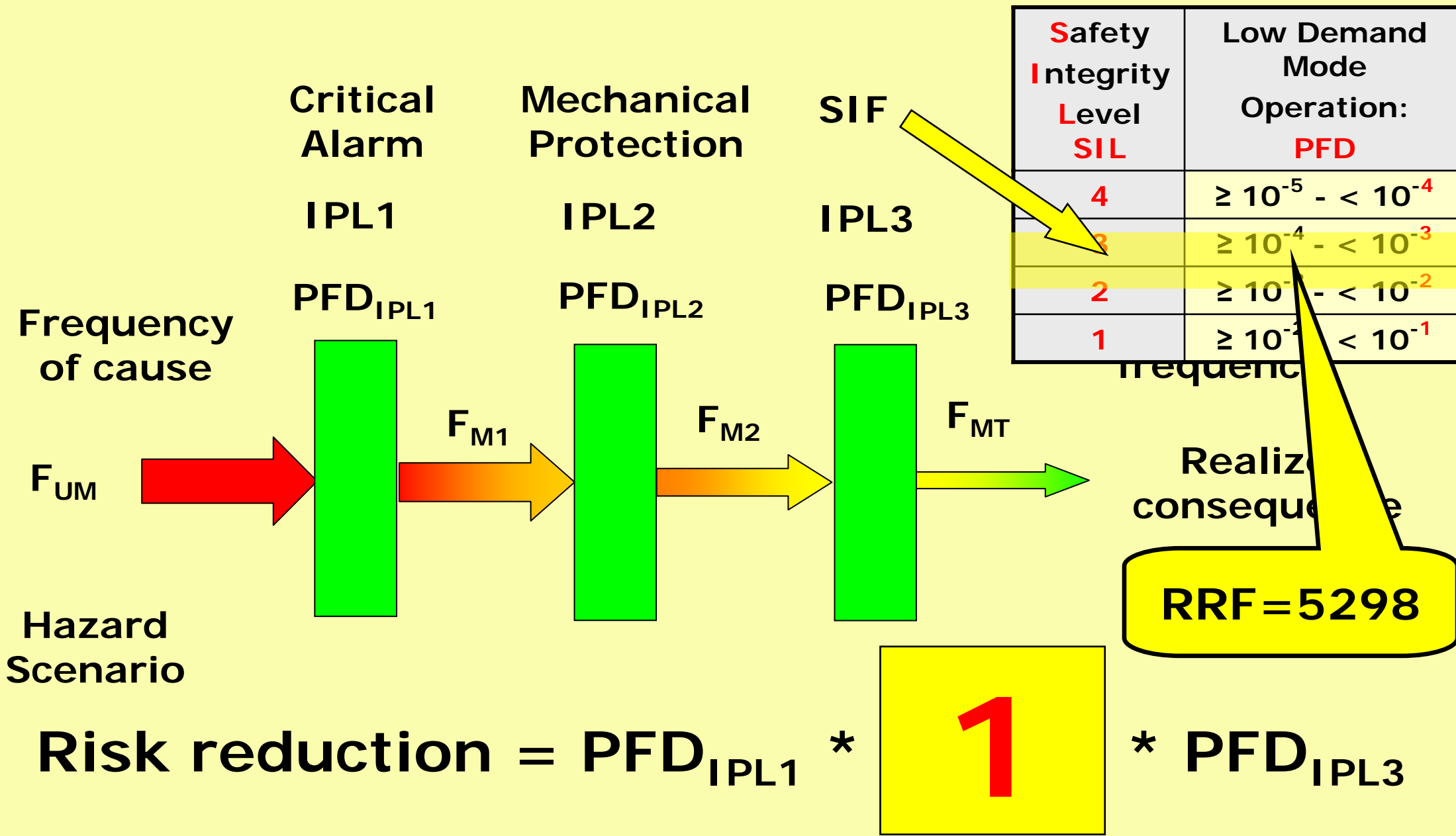
- *Simple*
- *It can calculate with the probability of avoiding the hazardous event*

■ Uncertainty in Risk Graph:

- *What about if there are several independent layers (e.g. alarm and relief valve)?*
 - *Shall we decrease the frequency category? Or rather the consequence category?*
- *What about if there are several causes of an hazardous event with mixed IPLs?*
 - *Shall we increase the frequency category?*

- **The LOPA main objectives are the followings:**
 - *Identify all independent protection layers (IPLs).*
 - *Determine if SIF is required.*
 - *Determine required SIL and RRF values of SIFs.*
- **Main steps of LOPA procedure are the followings:**
 - *Develop each impact event scenario based on PHA (typically HAZOP).*
 - *Evaluate the frequency of initiating event(s) and the severity of consequence(s).*
 - *Add independent protection layers (IPLs) to mitigate the impact event scenario.*
 - *Set the probability of failure on demand (PFD) values of IPLs.*
 - *Determine the SIL&RRF for SIF if SIF is necessary.*





Advantages of LOPA

- *The most accurate method*
- *Prevents against over engineering*
- *Prevents against under engineering*

Disadvantages of LOPA

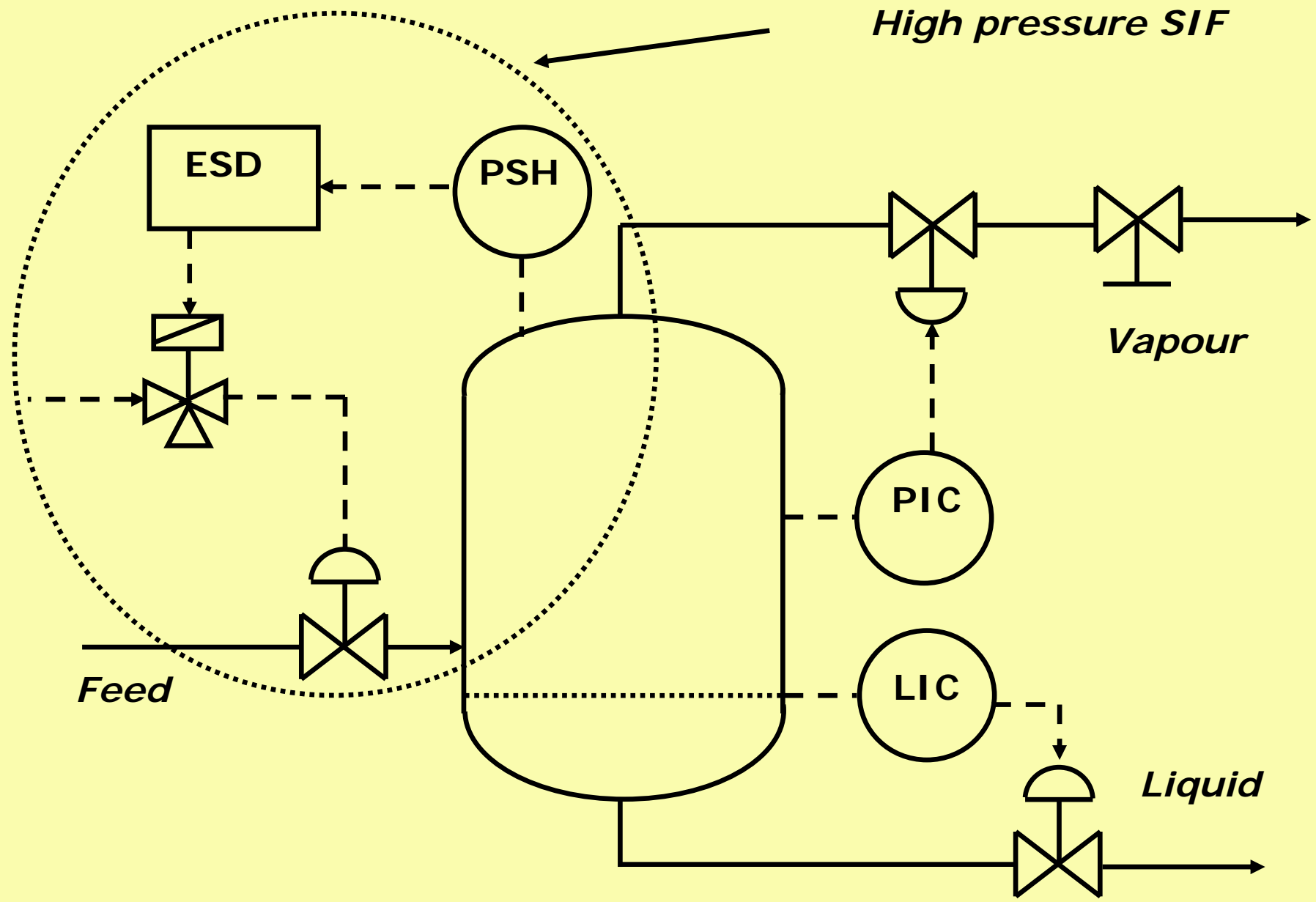
- *Time consuming. But it can be handled by a good software (e.g. Tool4S)*
- *It needs Quantitative Tolerable Risk Matrix. Some company do not want to give a QTRM.*

For SIL-3 loops the LOPA is highly recommended!

- **Uncertainty in LOPA:**
 - *How would we calculate the mitigated risk frequency if there are more causes or even more hazard scenarios with mixed IPLs?*
 - *How would we select the PFD values for different IPLs?*
- **The first problem can be handled by Cumulative LOPA.**

- In everyday practice, the mitigated risk is calculated separately for every scenario (“Per-scenario” method).
- But it cannot take into consideration that a hazard may contain several scenarios with the same consequence and partly or completely same protection layers (e.g. a SIF).
- The IEC 65111-3 standard says about the SIL&RRF determination the following:

“The last step is to add up all the mitigated event likelihood for serious and extensive impact events that present the same hazard”



■ HAZOP of the system:

Cause	Cause freq.	Consequence	Tol. freq.	IPL
The pressure control loop fails (PV close)	0.05	Overpressure of the vessel	0.001	SIF_1: PSH high trip closes the feed valve
Vapour line is blocked	0.1	<i>same as above</i>	<i>same as above</i>	SIF_1: PSH high trip closes the feed valve

$$RRF_1 = 0.05 / 0.001 = 50, RRF_2 = 0.001 / 0.1 = 100$$

"Per-scenario" LOPA: $RRF = \max(RRF_1, RRF_2) = 100$

"Cumulative" LOPA: $RRF = RRF_1 + RRF_2 = 150$

- LOPA uses several quantified parameters, such as initiating event frequency, PFD values of IPLs.
- Example PFD values from different sources:

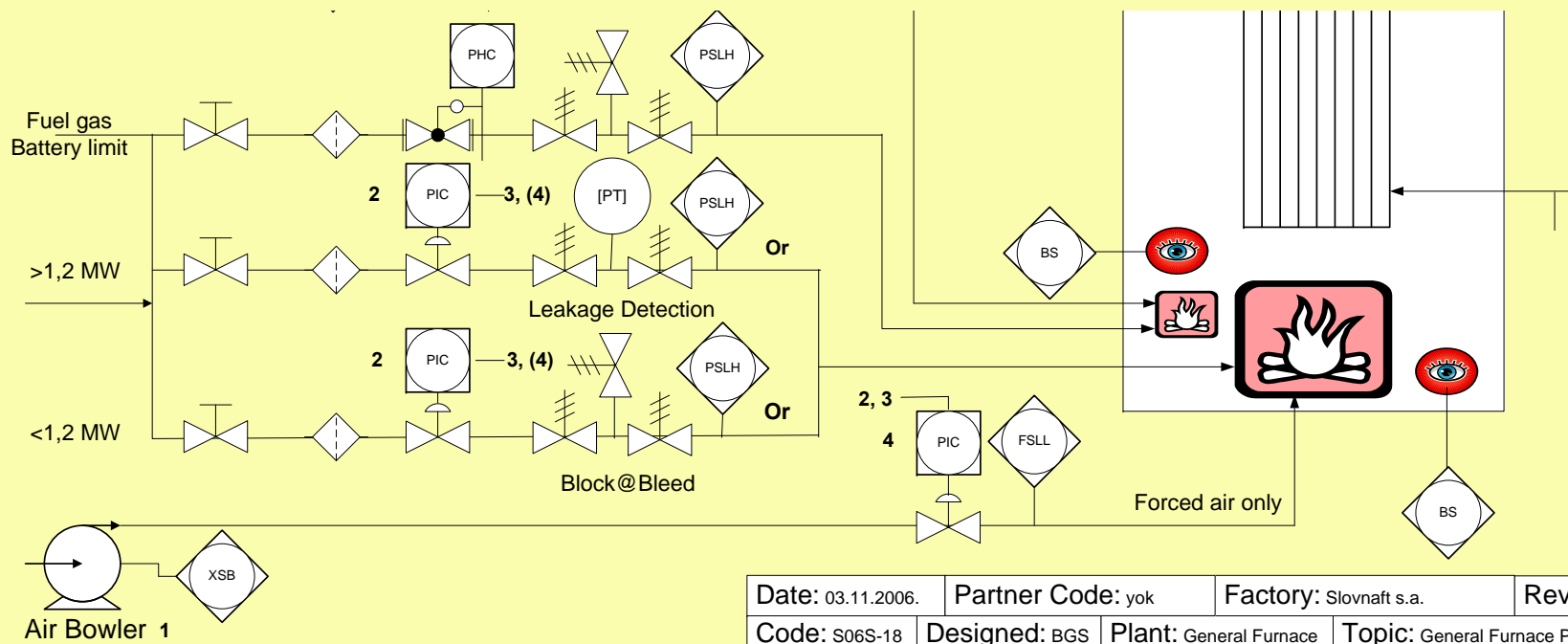
IPL	PFD (source 1)	PFD (source 2)
Control loop	10^{-2}	$10^{-1} - 10^{-2}$ ($> 10^{-1}$ by IEC)
Alarm + operator	10^{-2} (trained, no stress) 10^{-1} (alarm response)	10^{-1}
Relief valve	10^{-2}	$10^{-1} - 10^{-5}$
Dike	N.A.	$10^{-2} - 10^{-3}$

Source 1: A. M. Dowell, "Layer of protection analysis for determining safety integrity level", ISA Transaction 37 (1998)

Source 2: "Layer of Protection Analysis – Simplified Process Risk Assessment", CCPS, AIChE, N.Y., ISBN 0-81690811-7

Let's investigate an example:

- The system is a boiler.
- Now focus only on the "low fuel gas pressure" hazard.



■ The example HAZOP of the hazard

Hazard: Low fuel gas pressure into the boiler		
Causes	Consequences	Safeguards
1. Fuel gas supply failure	1.1 Flame extinguish, fuel gas accumulates in the furnace, explosion risk	1.1.1 SIF_01: Fuel gas pressure low-low trip 1.1.2 Explosion door
2. Fuel gas pressure control failure	2.1 Flame extinguish, fuel gas accumulates in the furnace, explosion risk	2.1.1 SIF_01: Fuel gas pressure low-low trip 2.1.2 Explosion door
3. Plugging of fuel gas filter	3.1 Flame extinguish, fuel gas accumulates in the furnace, explosion risk	3.1.1 Filter DP high alarm 3.1.2 SIF_01: Fuel gas pressure low-low trip 3.1.3 Explosion door

- Before the risk assessment we need to define the probability of causes, the severity of consequences:
 - For simplicity the probability of every cause is *0.1 / year*.
 - The consequence of the hazard is the same for every scenario: explosion which can cause a *single fatality* and *more than 1 M€ damage*.

- Using the default Risk Matrix of Exida software:

SIL 2

Tolerable Risk Calibration Wizard - Hazard Matrix

Demand Frequency

Safety Integrity Level

D5	< 0.1 years	2	3	4	b	b
D4	0.1 to 0.5 years	1	2	3	4	b
D3	0.5 to 4 years	a	1	2	3	4
D2	4 to 20 years	a	1	2	3	4
D1	> 20 years	--	--	a	1	2

Health and Safety
 Environment
 Economics

Slight Injury	Minor Injury	Major Injury	Single Fatality	Multiple Fatalities
Slight Effect	Minor Effect	Localized Effect	Major Effect	Massive Effect
Slight Damage (< \$10K)	Minor Damage (\$10 to \$100K)	Local Damage (\$100K to \$1M)	Major Damage (\$1M to \$10M)	Extensive Damage (> \$10M)
C1	C2	C3	C4	C5

- **Apply the Risk matrix:**
 - *The demand frequency category is **D2** (4 – 20 years)*
 - *The consequence category is **C4** for person and **C4** for economy*
 - *So the safety integrity level: **SIL 2***
- **Here is the question is how we shall calculate with the “Explosion door” safeguard?**
 - *If there was not “explosion door” the Risk matrix would give the same result: **SIL 2***
 - *So maybe we should decrease the SIL level with one saying that the demand frequency is lower because the explosion door **???***
 - *If yes, the result is **SIL 1***

➤ Using the default Risk Graph of Exida software (same as IEC 61511) for human:

Tolerable Risk Calibration Wizard - Risk Graph

Personnel Safety Environmental Loss

Classification

(C) Consequences if Fail on Demand
 CA=Minor Injury
 CB=Severe Injury/Death
 CC=Severe Burns
 CD=Minor Deaths/Catastrophe

(F) Frequency in the Danger Zone
 FA=Seldom to Frequently
 FB=Frequently to Continuously

(P) Probability to avert Hazard
 PA=Under Certain Circumstances
 PB=Almost Impossible

(W) Demand Rate
 W1=Very Low (10 to 100 years)
 W2=Low (1 to 10 years)
 W3=High (<1 year)

(M) Monetary Loss
 M1=Minor \$10K to \$100K, < 1 day
 M2=Moderate \$100K to \$1M, 1-5 days
 M3=Major \$1M to \$6M, 5 - 15 days
 M4=Extensive \$6M to \$12M, 15 - 30 days
 M5=Catastrophic >\$12M, > 30 days

Buttons: Load Defaults, Cancel, << Back, Next >>, Finish

SIL 1

- **Apply the Risk graph:**
 - *For person: W2, CB, FA, PB: SIL 1*
 - *The economy: W2, M3: SIL 1*
 - *So the safety integrity level: SIL 1*
- **Here is the question is how we shall calculate with the “Explosion door” safeguard?**
 - *Shall we change the PB to PA ???*
 - *Or maybe we should decrease the SIL level with one saying that the demand frequency is lower because the explosion door ???*
- **If yes, the result is SIL 0**

- **Let's define the tolerable frequency for the consequence:**
 - *Possible fatality of a personnel: $10^{-5}/\text{year}$*
 - *Major economical damage: $10^{-4}/\text{year}$*
- **So the tolerable freq.: $10^{-5}/\text{year}$**
- **PFD values of IPLs:**
 - *Explosion door: PFD = 0.1 (or other source: 0.01)*
 - *DP high alarm+operator response: PFD = 0.1*
- **Presence in dangerous zone:**
 - *Rare: $P_{\text{presence}} = 0.1$*

- $$RRF_1 = F_{\text{cause1}} / F_{\text{tol}} * PFD_{\text{ex.door}} * P_{\text{presence}} = 10^{-1} / 10^{-5} * 0.1 * 0.1 = 100$$

- $$RRF_2 = F_{\text{cause2}} / F_{\text{tol}} * PFD_{\text{ex.door}} * P_{\text{presence}} = 10^{-1} / 10^{-5} * 0.1 * 0.1 = 100$$

- $$RRF_3 = F_{\text{cause3}} / F_{\text{tol}} * PFD_{\text{ex.door}} * PFD_{\text{alarm}} * P_{\text{presence}} = 10^{-1} / 10^{-5} * 0.1 * 0.1 * 0.1 = 10$$

- Results:**

- Per-scenario LOPA: $RRF = 100, SIL = 2$ (border of SIL 1 – SIL 2)

- Cumulative LOPA: $RRF = 220, SIL = 2$

- If the $PFD_{\text{ex.door}}$ was be 0.01, the results would be:**

- Per-scenario LOPA: $RRF = 10, SIL = 1$ (border of SIL 0 – SIL 1)

- Cumulative LOPA: $RRF = 22, SIL = 1$

- The results show that the uncertainty of SIL can be 1. (SIL 2 or SIL 1)
- Even if the LOPA has uncertainty, we claim that LOPA is more accurate than the other methods because:
 1. *It is the only the LOPA method which calculates the RRF. It is not the same if we have a SIL 1 SIF with $RRF = 10$ or if we have a SIL 1 SIF with $RRF = 90$ (also do not forget about the ALARP!).*
 2. *Only the cumulative LOPA can adds up the hazard scenarios. If there are several scenarios, the RRF may be multiplied (which may increase the SIL).*

■ Cont.:

3. *However even if the PFD values are not exact, at least the LOPA is coherent as the same PFD values are used for the same IPLs. So the resulted RRF and SIL values of the different SIFs of a plant has a logical and coherent relation with each other.*
4. *The risk graph and especially the risk matrix may result in illogical SIL values because they cannot take into consideration of multiple hazardous scenarios with multiple IPLs. The LOPA is more logical.*
5. *Finally, the reliability analysis (SIL calculation) also has some uncertainty. The quantitative uncertainty of the LOPA is likely not bigger than the uncertainty of reliability analysis.*

	Risk Matrix	Risk Graph	LOPA	Cumulative LOPA
SIL	± 0.5	± 0.5	*	*
RRF	NO	NO	YES	YES
IPL	NO	NO	YES	YES
Multiple Hazard Scenarios	NO	NO	NO	YES

* Depends on the PFD Figures

Thank you for your attention

Any Question?