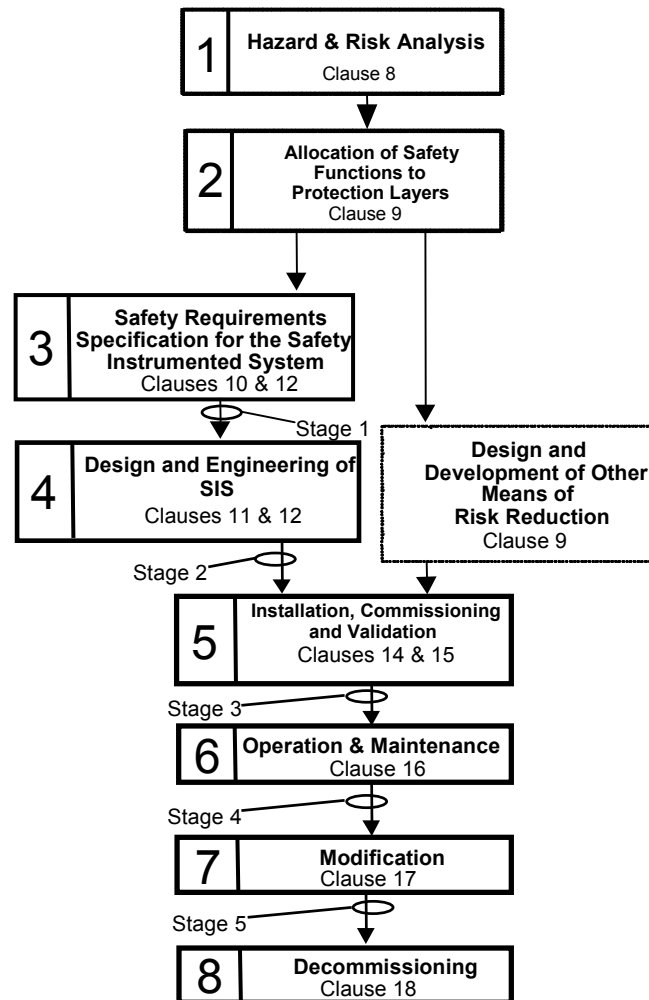


# **CASE STUDY**

## **INSTRUMENT SAFETY FUNCTION FOR A STORAGE TANK WITH A LIQUIFIED HYDROCARBON according to IEC-61508 and IEC-61511**

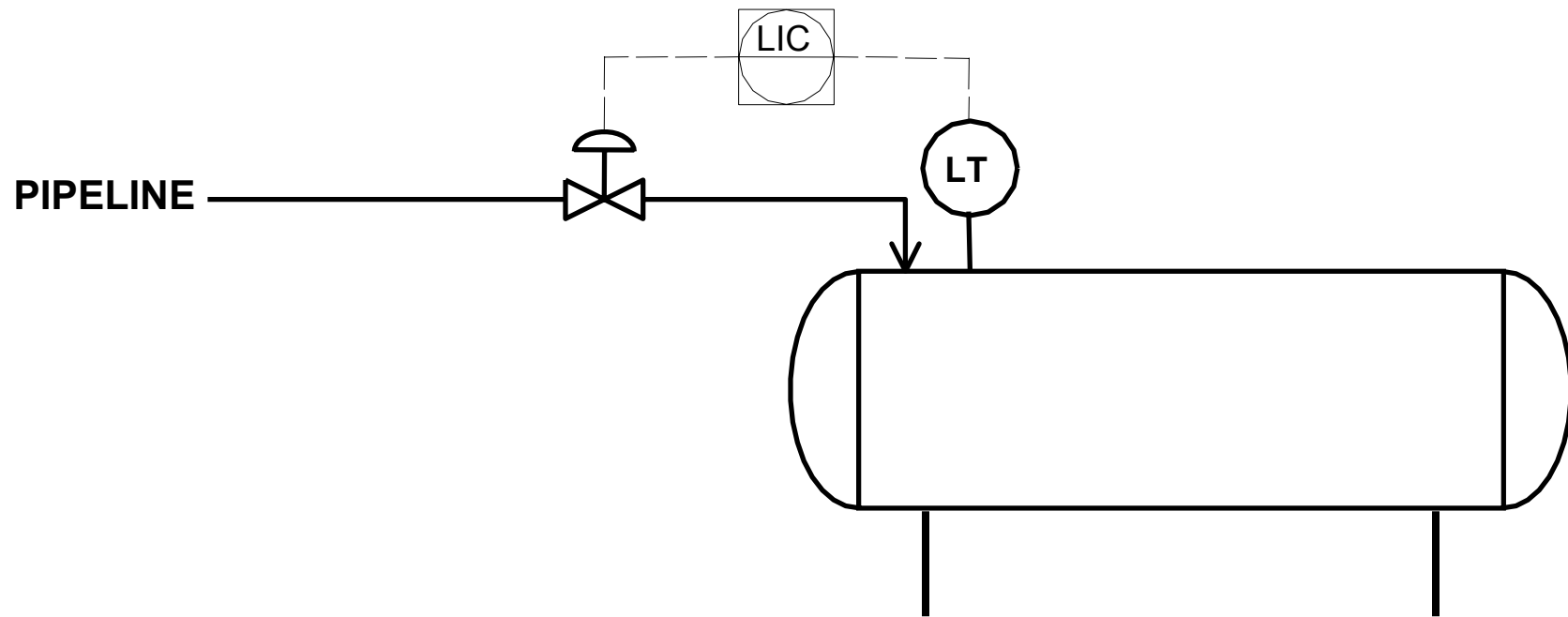
**Erik Dom  
Nero Engineering**

# IEC-61511 lifecycle model



# Concept & Scope (IEC-61508)

Define EUC (“Equipment Under Control” – IEC-61508) or Process (IEC-61511).  
In this case: storage tank for a “liquified gas” with a level control loop, alarming included, on DCS.



# Risk analysis

Possible methods: HAZOP (see below), What if?, PLANOP,...

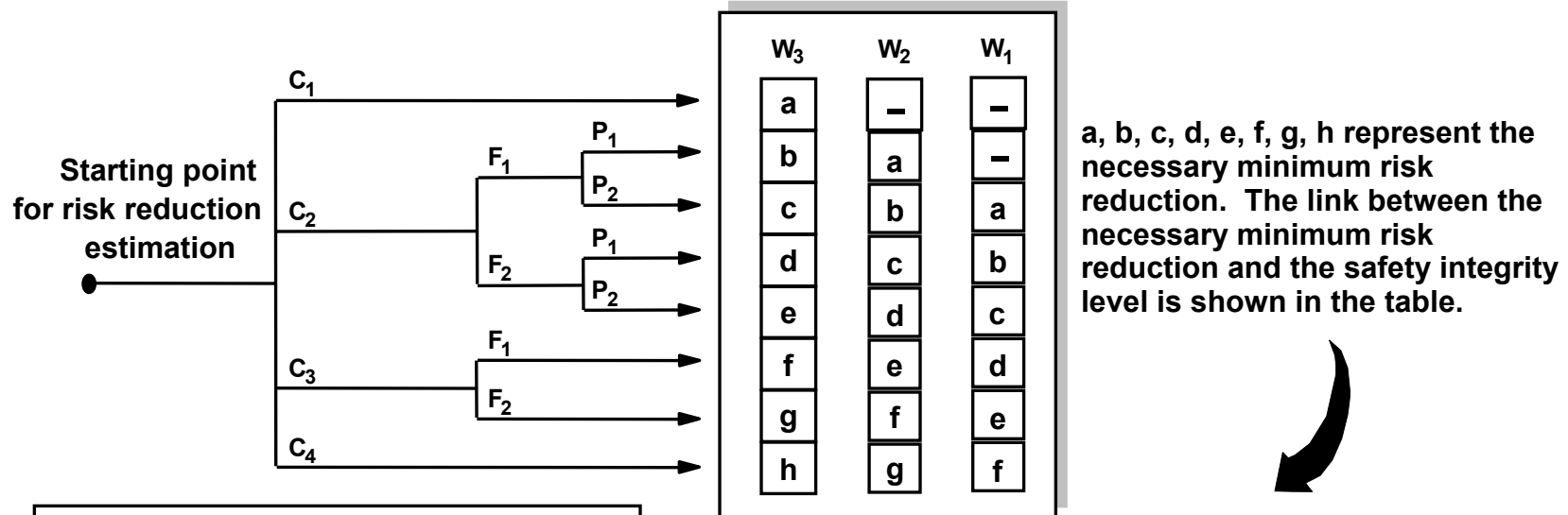
Item	Deviation	Causes	Consequences	Safeguards	Action
Tank	Hoog niveau	<ol style="list-style-type: none"> <li>1. Faling DCS</li> <li>2. Faling klep</li> <li>3. Faling meting</li> <li>4. Faling operator (DCS controller op manueel en verkeerde output)</li> </ol>	Vrijzetting ontvlambaar product naar atmosfeer.	Geen, alleen mitigerende maatregelen (sprinklers, gasdetectie,...)	Voorzie een instrumentele beveiliging + bepaal benodigde SIL

# SIL evaluation

---

- Risk graph  
(safety/environment/economics)
- LOPA
- Quantitative analyse (not treated in this presentation)

# Risk graph (used as example in IEC)



**C** = Consequence risk parameter

**F** = Frequency and exposure time risk parameter

**P** = Possibility of avoiding hazard risk parameter

**W** = Probability of the unwanted occurrence

**a, b, c ... h** = Estimates of the required risk reduction for the SRSs

Necessary minimum risk reduction	Safety integrity level
-	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An E/E/PE SRS is not sufficient

# Result risk graph

- Scenario 1

(consequence max. 1 dead person)

- Scenario 2

(consequence more dead persons)

C2:

F1:

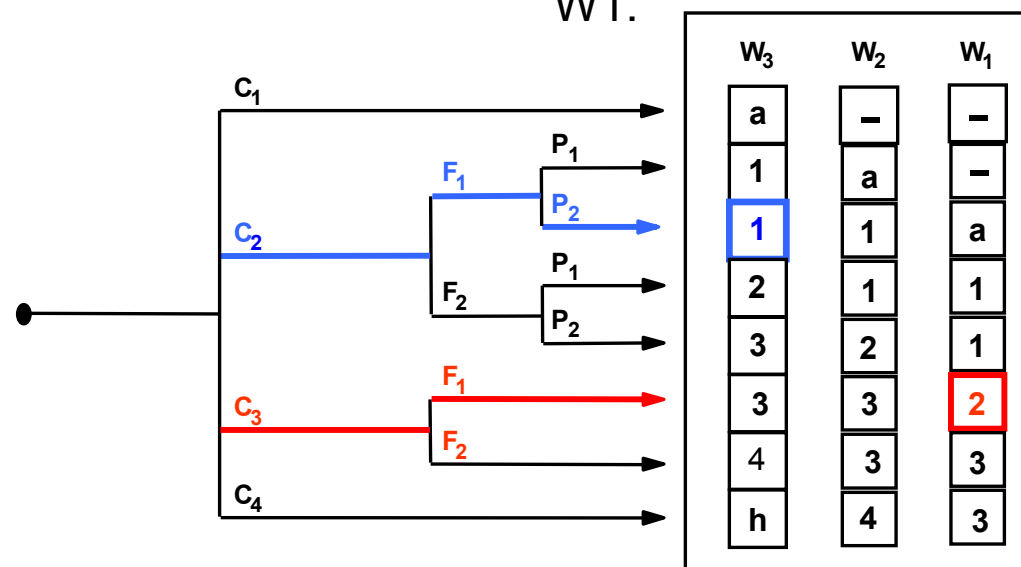
P2:

W3:

C3:

F1:

W1:

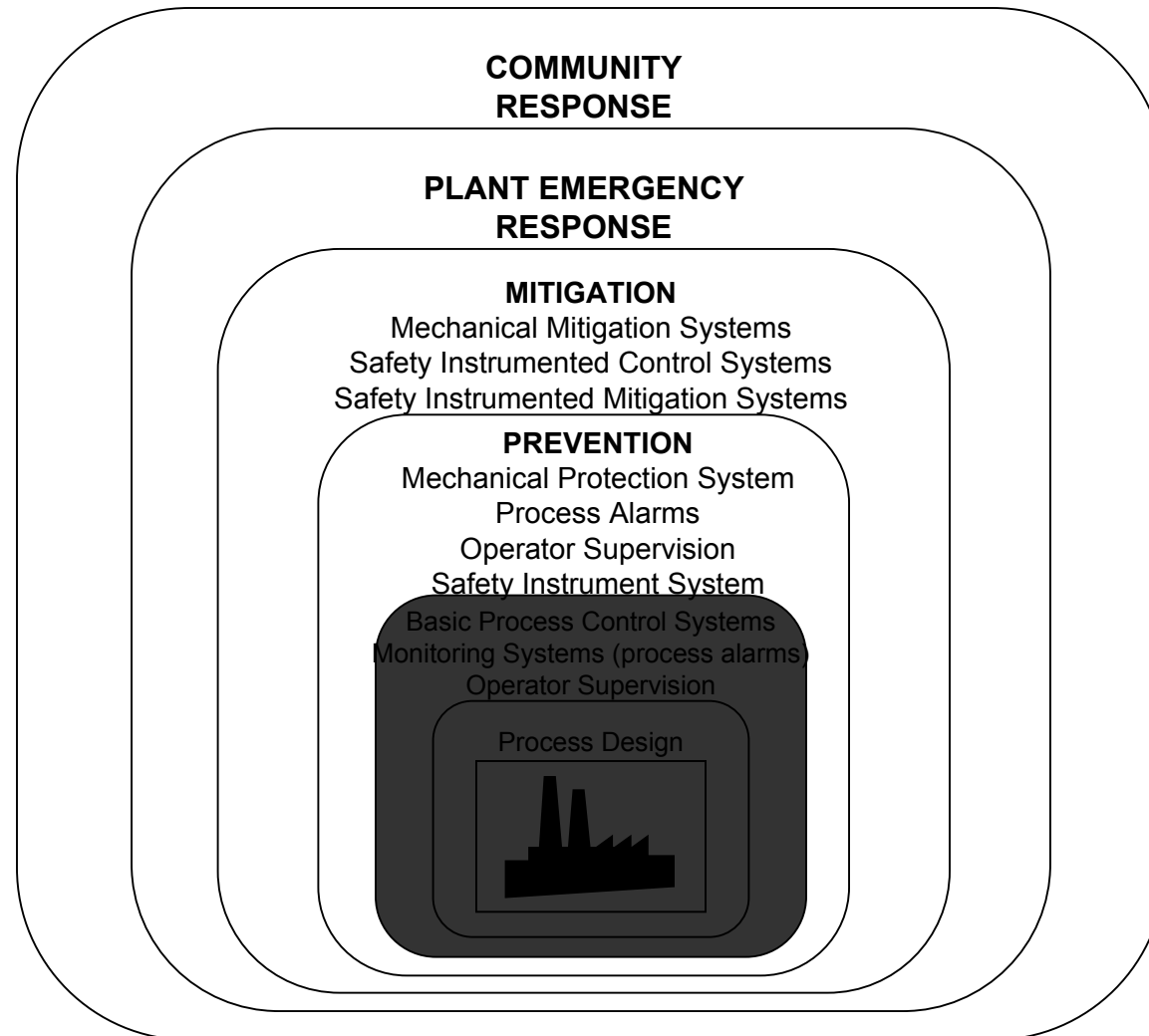


# What is LOPA?

---

- A simplified form of risk assessment
- Verifies if sufficient layers of protection are present
- Limited to evaluating a single cause-consequence pair as scenario
- Represents typically one path (worst case) through an event tree

# Principles of LOPA



Concept of layers of protection acc. to IEC-61511-1

# A practical approach

	Description	Probability	Frequency (per year)
<b>Consequence</b>			
<b>Risk tolerance criteria</b>	Maximum tolerance for serious fire Maximum tolerance for fatal injury		$< 1 \times 10^{-4}$ $< 1 \times 10^{-5}$
<b>Initiating event</b>	Failure of DCS		$1 \times 10^{-1}$
<b>Enabling event</b>		N/A	
<b>Conditional Modifiers</b>	Probability of ignition	0.1	
	Probability of personnel in affected area	0.1	
	Probability of fatal injury	0.5	
	Others	N/A	
<b>Frequency of unmitigated consequence</b>			$5 \times 10^{-4}$
<b>Independent Protection layers</b>	SIF (not yet existing, to be added)	$1 \times 10^{-2}$	
	Human action upon DCS alarm cannot be taken into account since DCS failure is the initiating event!		
<b>Total PFD for all IPL's</b>		$1 \times 10^{-2}$	
<b>Frequency of Mitigated Consequence</b>			$5 \times 10^{-6}$
<b>Actions required to meet required risk reduction</b>	Install SIF with a PFD of $1 \times 10^{-2}$		

# Design in acc. to IEC

- General requirements:
  - Detection of hazard
  - Avert hazardous events
  - Architectural constraints / fault tolerance
  - Low demand mode – High demand mode
  - Response time
  - Functional logics
  - Documentation and specification
  - Safety management plan (realisation, integration, commissioning, operation, maintenance, testing/inspection, modification,...)
  - .....

# Architectural constraints – fault tolerance

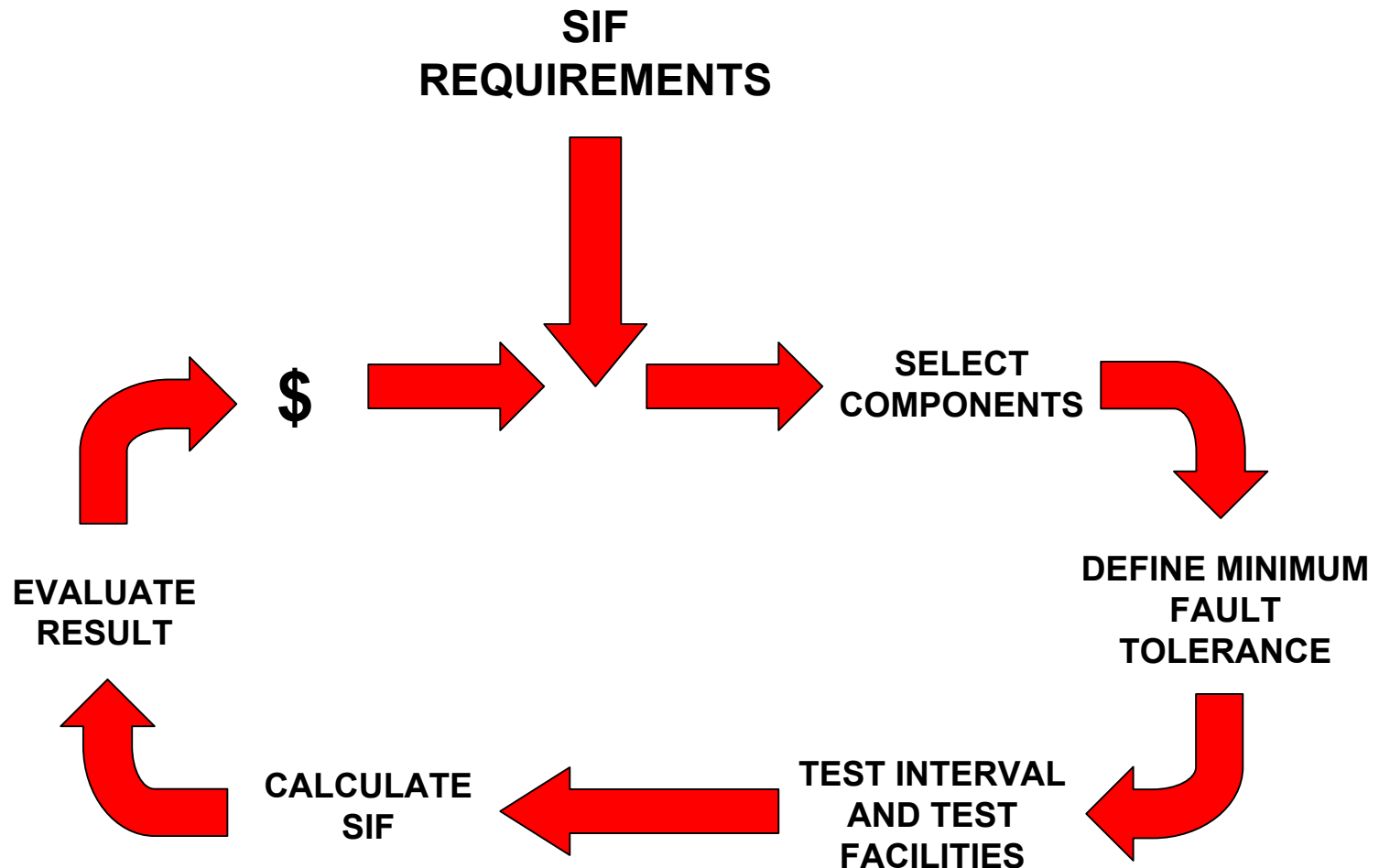
Table 3 from IEC-61508 – Architectural constraints for Type A			
Safe failure fraction	Hardware fault tolerance		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60% to <90%	SIL 2	SIL 3	SIL 4
90% to <99%	SIL 3	SIL 4	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

Table 3 from IEC-61508 – Architectural constraints for Type B			
Safe failure fraction	Hardware fault tolerance		
	0	1	2
<60%	Not Allowed	SIL 1	SIL 2
60% to <90%	SIL 1	SIL 2	SIL 3
90% to <99%	SIL 2	SIL 3	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

IEC-61511 – Minimum hardware fault tolerance					
Table 5 – Logic Solvers				Table 6 – other devices	
SIL	Minimum hardware fault tolerance			SIL	
	SFF<60%	SFF 60% to 90%	SFF >90%		
1	1	0	0	1	0
2	2	1	0	2	1
3	3	2	1	3	2
4	See IEC-61508			4	See IEC-61508

Impact on min. fault tolerance of table 5		
	yes	no
Prior use	- 1	0
Fail safe	0	+ 1

# Flow chart for design of SIF



# Reliability data

---

- Oreda
- Vendor data (uncertified)
- Vendor data (certified)
- MIL (for electric/electronic components)
- Commercial databases
- Owner's database
- Industry's average

# Components and calculation data

- **Level sensor – float**
  - Diagnostic coverage = 0%
  - $\lambda = 4E-6$  (% safe = 25%)
  - Type “A” component
  - SFF = 25% → fault tolerance = 0 for SIL 1 and 1 for SIL 2
- **Level sensor – transmitter**
  - Diagnostic coverage = 60% if monitored on DCS
  - $\lambda = 4E-6$  (% safe = 50%)
  - Type “B” component
  - SFF = 80% → fault tolerance = 0 for SIL 1 and 1 for SIL 2
- **Ball valve**
  - Diagnostic coverage = 0%
  - $\lambda = 6E-6$  (% safe = 50%)
  - SFF = 50% → fault tolerance = 0 for SIL 1 and 1 for SIL 2

# Calculation results

Component	Type	Voting	$\lambda$	% <sub>safe</sub>	SFF %	DC Dang.	MTTR (days)	Test Int. (months)	PFD <sub>avg</sub>
Level	Float	1001	4E-6	25	25	0	1	24	2.6E-2
	Radar	1001	4E-6	50	80	60	1	24	7E-3
	Float	1002	4E-6	25	25	0	1	24	1.4E-3
	Radar	1002	4E-6	50	80	60	1	24	2E-4

Component	Type	Voting	$\lambda$	% <sub>safe</sub>	SFF	DC Dang.	MTTR (days)	Test Int. (months)	PFD <sub>avg</sub>
Valve	Ball	1001	6E-6	50	50	0	1	24	2.6E-2
	Ball	1002	6E-6	50	50	0	1	24	3.4E-3
	Ball	1002	6E-6	50	50	0	1	24	8.3E-4
	Globe		6E-6	50	75	50	1	24	

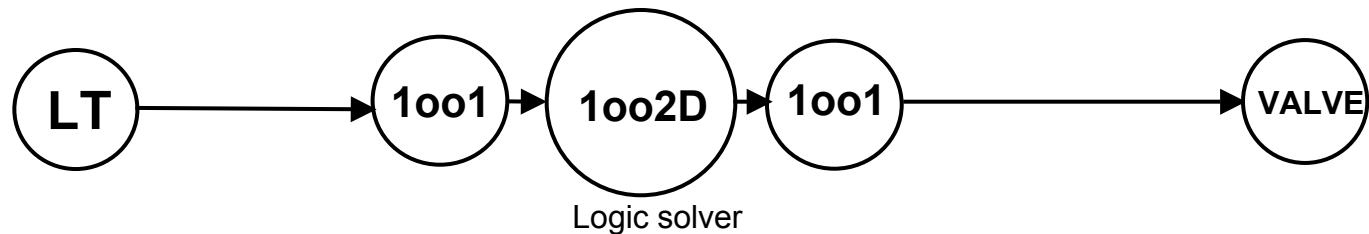
# Calculation results total SIF

$$PFD_{avg}^{SIF} = PFD_{avg}^{sensor} + PFD_{avg}^{logic\ solver} + PFD_{avg}^{valves}$$

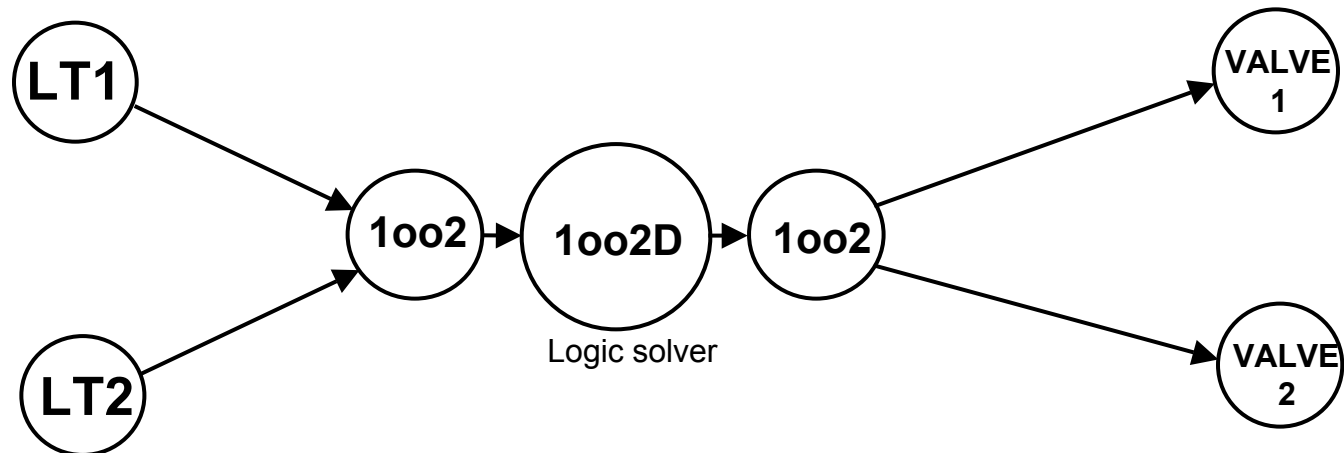
	$PFD_{avg}^{sensor}$	$PFD_{avg}^{logicsolver}$	$PFD_{avg}^{valves}$	$PFD_{avg}^{SIF}$	SIL
LT <sub>FLOAT</sub> + BALL VALVE	2.6E-2	<<	2.6E-2	5.2E-2	1
LT <sub>RADAR</sub> + BALL VALVE	7E-3	<<	2.6E-2	3.3E-2	1
2 x LT <sub>FLOAT</sub> + 2x BALL VALVE	1.4E-3	<<	3.4E-3	4.8E-3	2
2 x LT <sub>RADAR</sub> + 2x BALL VALVE	2E-4	<<	3.4E-3	3.6E-3	2
2 x LT <sub>FLOAT</sub> + BALL + GLOBE	1.4E-3	<<	8.3E-4	2.2E-3	2
2 x LT <sub>RADAR</sub> + BALL + GLOBE	2E-4	<<	8.3E-4	1.3E-3	2

# Architectural structure

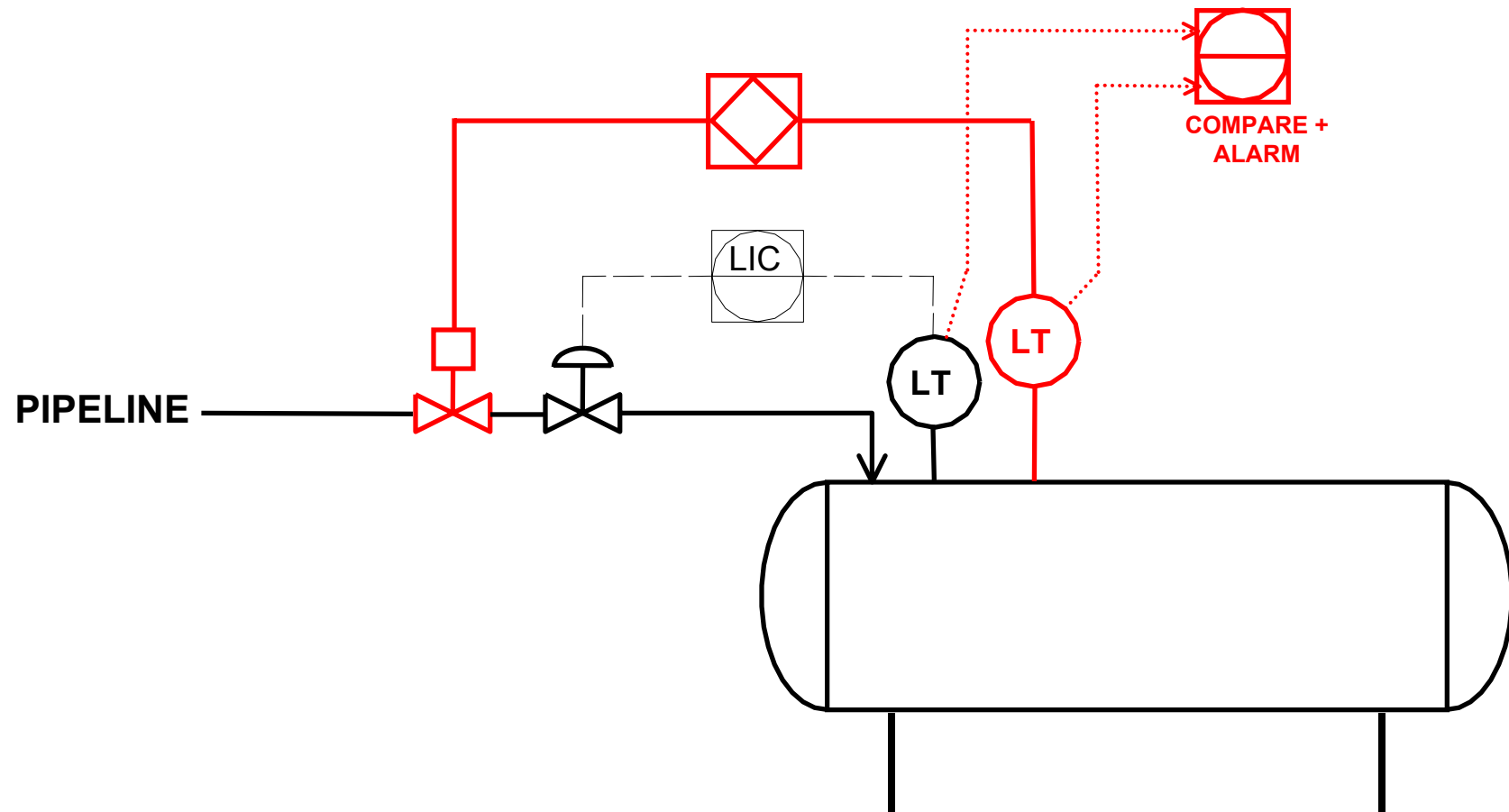
- SIL 1 scenario



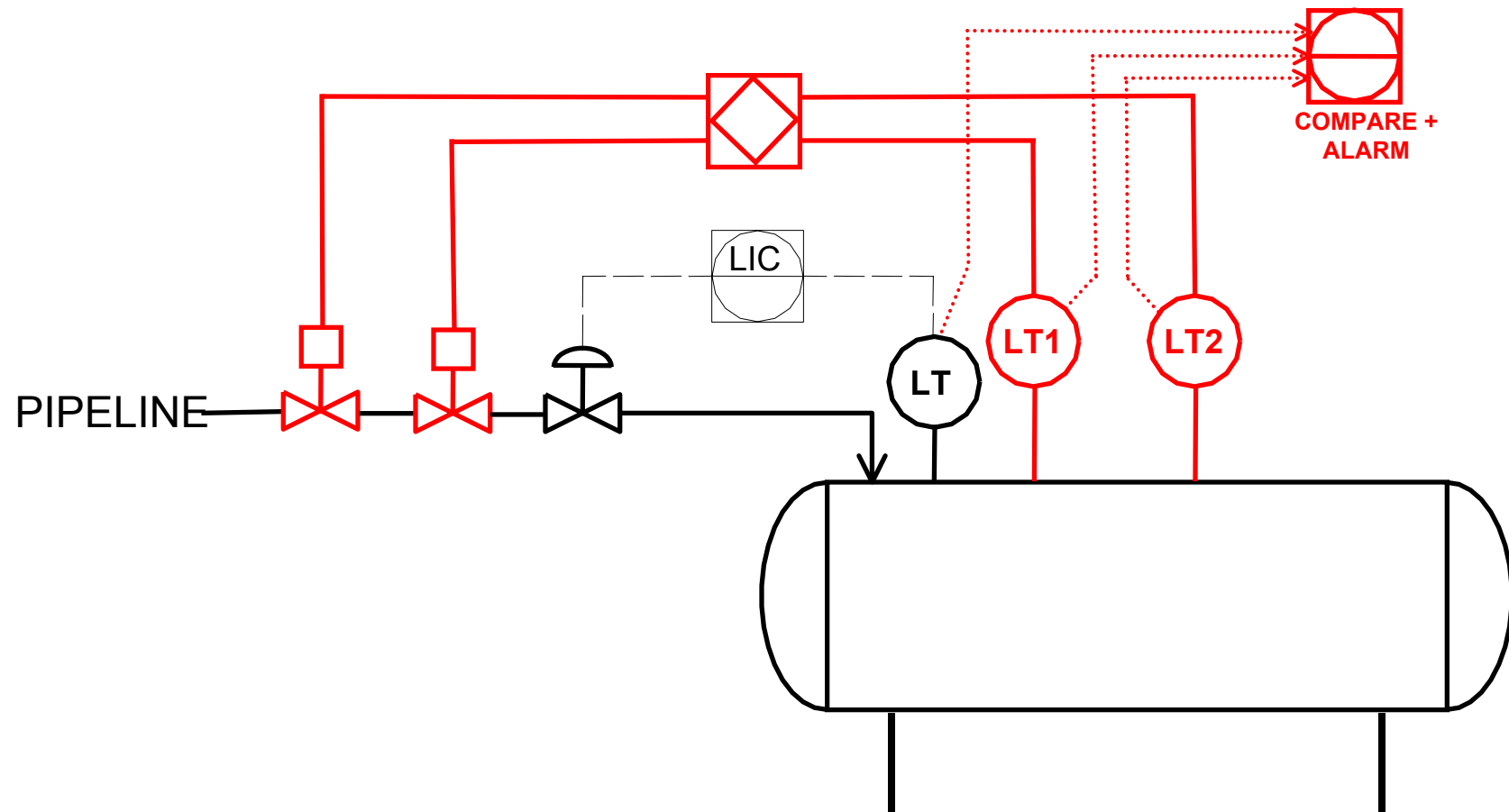
- SIL 2 scenario



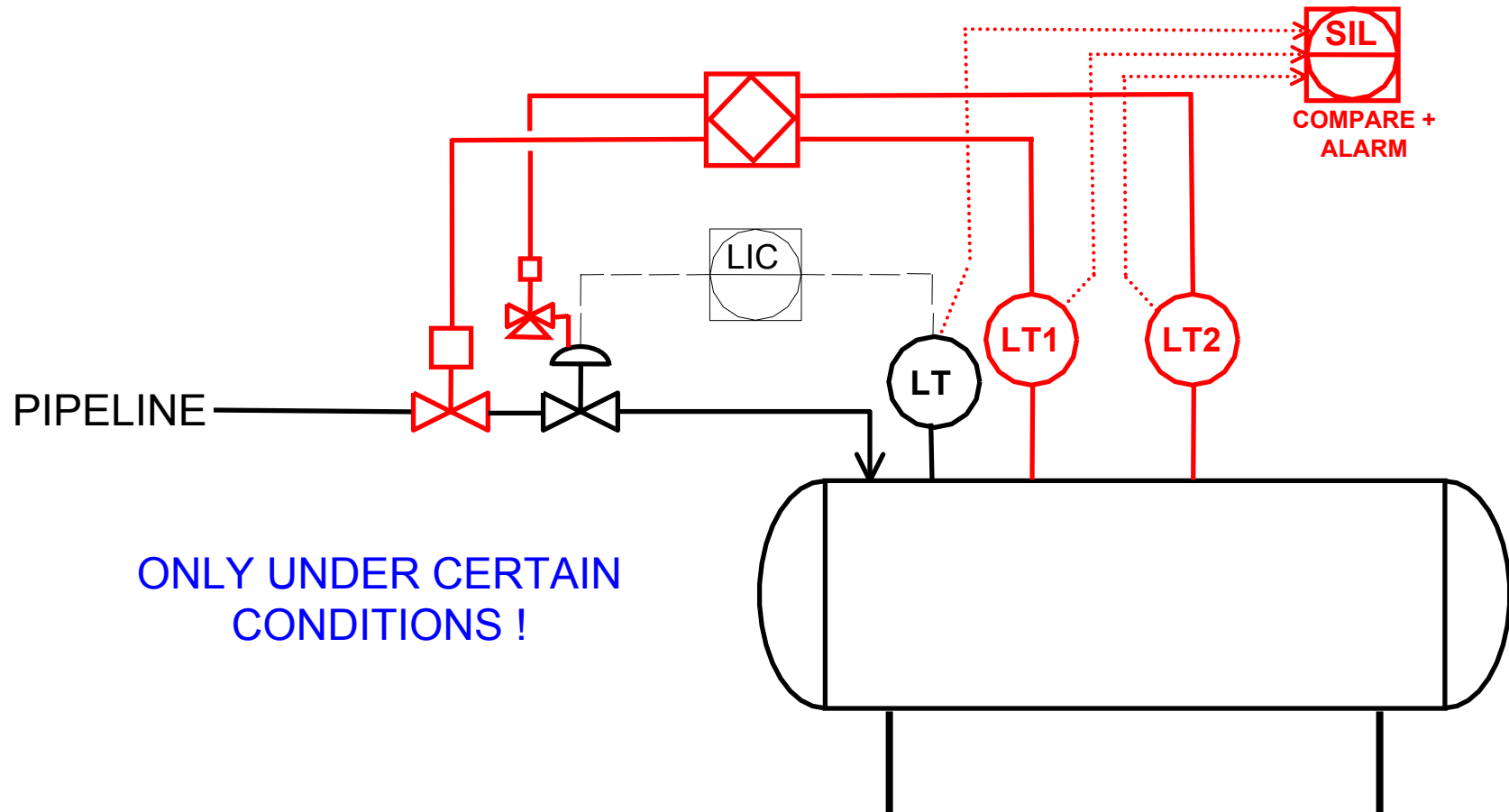
# Possible design for SIL 1



# Possible design for SIL 2



# Alternative design for SIL 2



# Reduce fault tolerance

---

- Increased diagnostic coverage → higher SFF

→ Possible solutions:

- Valves: partial stroke testing (DC ~ 60%)
- Sensors: smart transmitters with very high diagnostic coverage

- Proven in use - Prior use

→ See presentation Bert Knegtering

# Safety valves - approaches

- **Approach 1:  $SIL_{OVERALL} = SIL_{PSV} + SIL_{SIF}$**

Concerns:

- What is the risk reduction of a safety valve? How guarantee that this is obtained? Lifecycle?
- Risk reduction is dependent on application (dirty fluids, influence of installation, impact of rupture discs,...)
- In case of atmospheric release, SIL evaluation to be done for extra scenario
- Vendor reliability data is not available
- How to define test interval?
- Existing tests (pre-test) only verify limited number of possible errors

- **Approach 2: safety valves not taken into account**

Concerns:

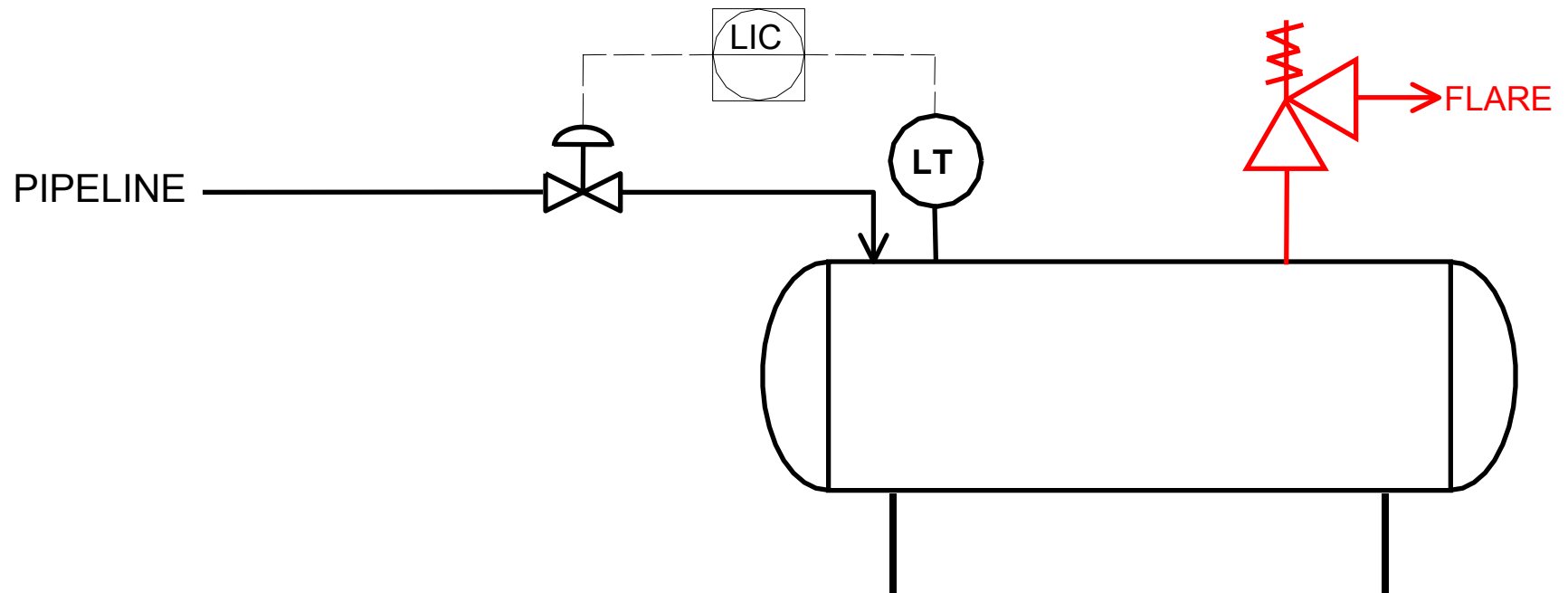
- Important economical impact (more pressure SIF required)

Advantages:

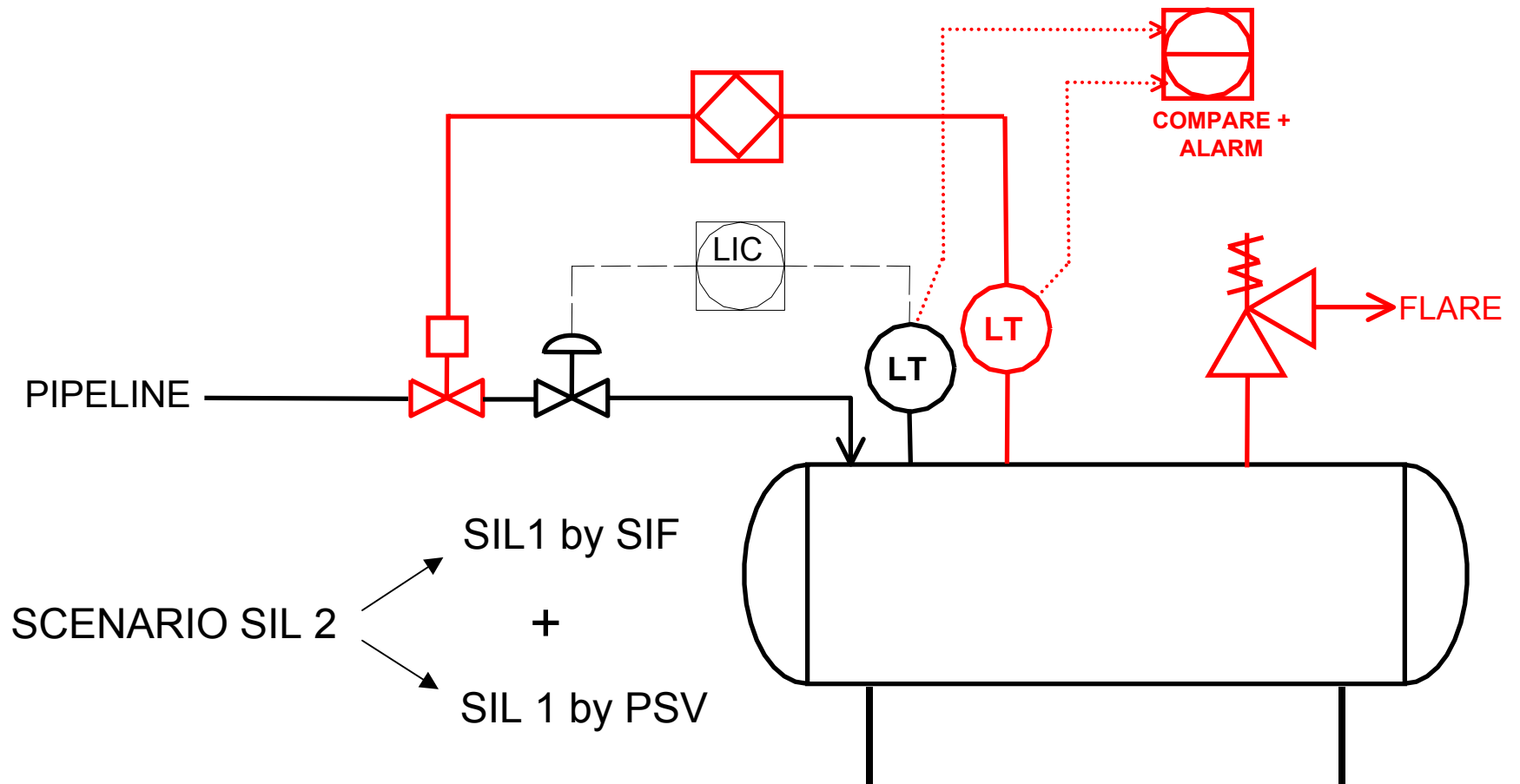
- Dual layer of protection will be always present → higher safety level

# Design for SIL 1 with PSV

Assume SIL 1 risk reduction by PSV

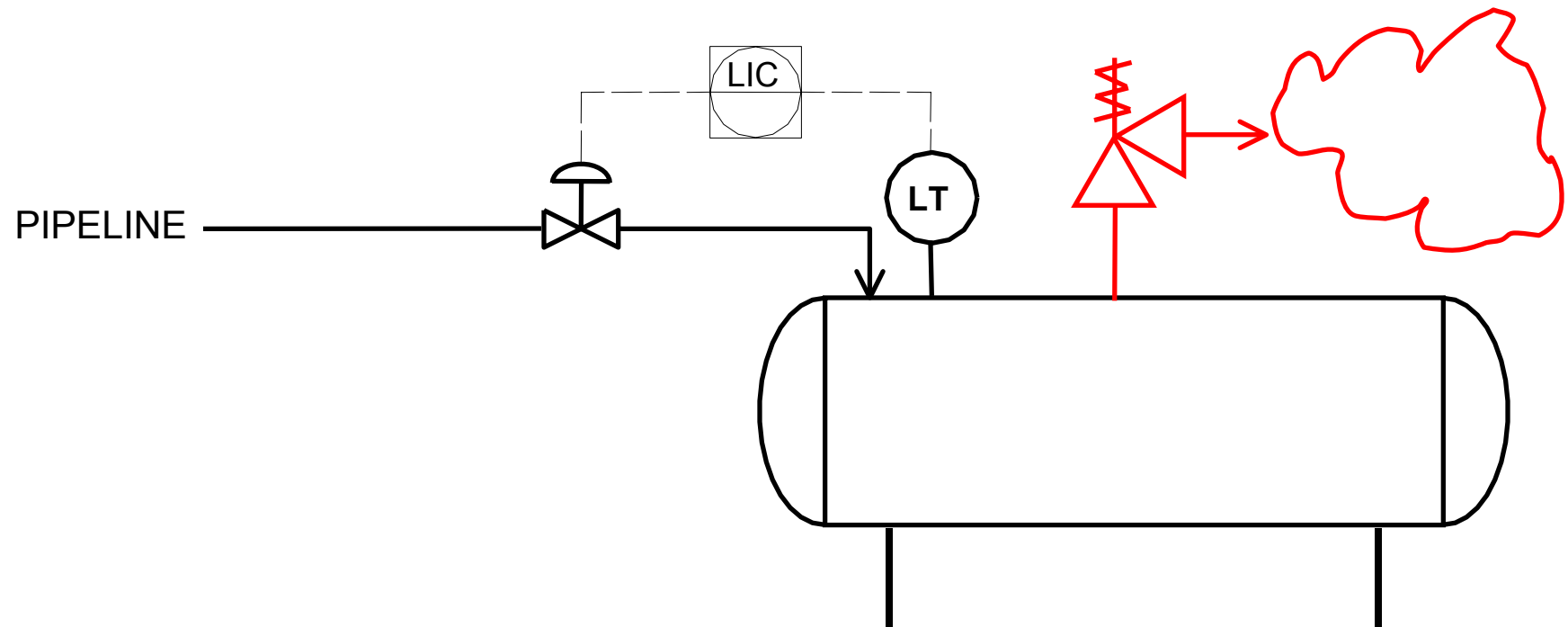


# Design for SIL 2 with PSV



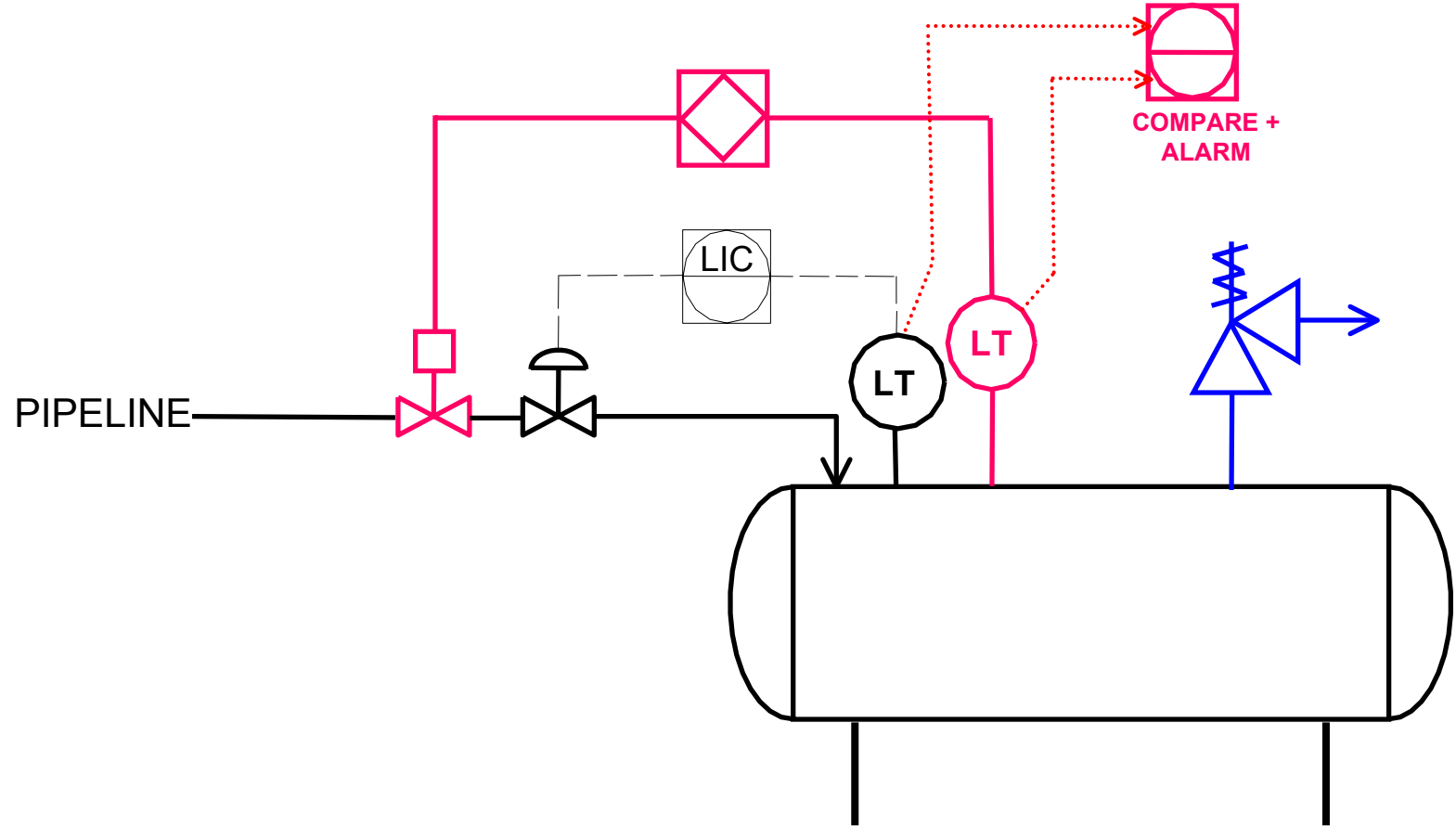
# Release via PSV → additional scenario

RELEASE TO ATMOSPHERE LEADS TO ADDITIONAL RISKS → RISK ANALYSIS → SIL EVALUATION → POSSIBLE INSTALLATION OF SIF



# Design with PSV outlet to atmosphere

- Avoid damage of vessel → PSV (SIL 1)
- Avoid opening of PSV → SIF (SIL1)



# LOPA for SIL 2 with PSV

	Description.	Probability	Frequency (per year)
<b>Consequence</b>			
Risk tolerance criteria	Maximum tolerance for serious fire Maximum tolerance for fatal injury		< 1 x 10 <sup>-4</sup> < 1 x 10 <sup>-5</sup>
Initiating event	Failure of DCS		1 x 10 <sup>-1</sup>
Enabling event		N/A	
Conditional Modifiers	Probability of ignition	0.1	
	Probability of personnel in affected area	0.1	
	Probability of fatal injury	0.5	
	Others	N/A	
Frequency of unmitigated consequence			5 x 10 <sup>-4</sup>
Independent Protection layers	PSV (installed)	<del>1 x 10<sup>-1</sup></del>	
	SIF (not yet existing, to be added)	<del>1 x 10<sup>-1</sup></del>	
	Human action upon DCS alarm cannot be taken into account since DCS failure is the initiating event!		
Total PFD for all IPL's		1 x 10 <sup>-2</sup>	
Frequency of Mitigated Consequence			5 x 10 <sup>-6</sup>
Actions required to meet required risk reduction	Install SIF with a PFD of 1 x 10 <sup>-1</sup>		

# Installation, commissioning & validation

---

## Installation & commissioning

- Need for specifications (installation) and procedures (commissioning)
- Documentation!

## Validation

- IEC-61511 gives details!

# Validation

**15.2.4 The validation of the safety instrumented system and its associated safety instrumented functions shall be carried out in accordance with the safety instrumented system validation planning. Validation activities shall include, but not be limited to, the following:**

- the safety instrumented system performs under normal and abnormal operating modes (e.g., startup, shutdown) as identified in the safety requirement specification;
- confirmation that adverse interaction of the basic process control system and other connected systems do not affect the proper operation of the safety instrumented system;
- the safety instrumented system properly communicates (where required) with the basic process control system or any other system or network;
- sensors, logic solver, and final elements perform in accordance with the safety requirement specification, including all redundant channels;
- NOTE If a factory acceptance test (FAT) was performed on the logic solver as described in clause 13, credit may be taken for validation of the logic solver by the FAT.
- safety instrumented system documentation is consistent with the installed system;
- confirmation that the safety instrumented function performs as specified on invalid process variable values (e.g., out of range);
- the proper shutdown sequence is activated;
- the safety instrumented system provides the proper annunciation and proper operation display;
- computations that are included in the safety instrumented system are correct;
- the safety instrumented system reset functions perform as defined in the safety requirement specification;
- bypass functions operate correctly;
- start-up overrides operate correctly;
- manual shutdown systems operate correctly;
- the proof test intervals are documented in the maintenance procedures;
- diagnostic alarm functions perform as required;
- confirmation that the safety instrumented system performs as required on loss of utilities (e.g., electrical power, air, hydraulics) and confirmation that, when the utilities are restored, the safety instrumented system returns to the desired state;
- confirmation that the EMC- immunity, as specified in the safety requirements specification (see clause 10.3), has been achieved.

# Maintenance & operations

- Objective: maintain integrity of SIS
- How?
  - Inspection (normal maintenance & proof testing)
  - Data collection
  - Data and event analysis, root cause analysis
  - Procedures and planning covering:
    - Responsibilities
    - Frequency of actions
    - Detailed procedures
    - Details on documentation and document flow
    - Action plans
- Continuous improvement in safety and availability!

# Maintenance & operations

		Radar level transmitter	Ball valve
<b>Normal maintenance</b>			
Maintenance	Job description		
	Execution time / action by		
Operations	Plant condition requirement		
	Estimated frequency of availability		
	Required precautions (field, MOS, bypasses)		
	Special measures to maintain safety levels.		
<b>Proof Testing</b>			
Maintenance	Job description		
	Execution time / action by		
Operations	Plant condition requirement		
	Estimated frequency of availability		
	Required precautions (field, MOS, bypasses)		
	Special measures to maintain safety levels.		
<b>Component failure (safe)</b>			
Maintenance	Failure description		
	Job description		
	Execution time / action by		
Operations	Actions to be taken		
<b>Component failure (dangerous)</b>			
Maintenance	Failure description		
	Job description		
	Execution time / action by		
Operations	Actions to be taken		