Hydrogen process measurement application and safety management

Explosion Protection and Functional Safety in safety applications

Thomas Fritz
Global Process Safety Consultant

Endress+Hauser Group Services (Deutschland) AG+Co. KG

Colmarer Str. 6
79576 Weil am Rhein
Germany

Phone: +49 7621 975 12209
Mobile: +49 151 52 767 193

E-mail: thomas.fritz@endress.com

What we at Endress+Hauser understand of “Safety by Design”

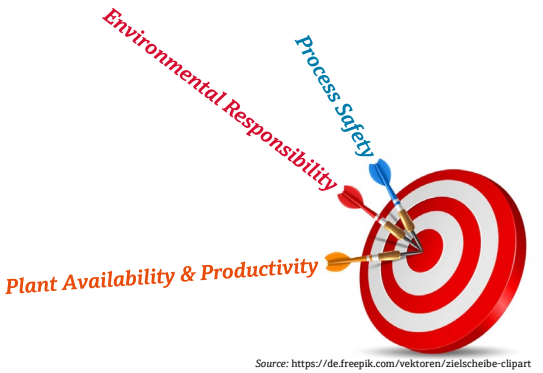
Safety by Design

1. Listen to our customers
2. Following industry standards
3. Using latest technology
4. Treasure employees experience

Explosion Protection + ***Functional Safety*** ⛓ ***Cybersecurity***

Pressure Equipment Directive ***Food Safety***

- Safety through *mechanical integrity* during
  - → the *design phase*
  - → the *manufacturing phase*
  - → the *field operation phase*



Source: https://de.freepik.com/vektoren/zielscheibe-clipart

Endress+Hauser

Leading in plant safety

- Over ***10 million*** devices worldwide in safety applications
- Comprehensive range of measuring instruments with over ***250 certified product lines*** for plant safety
- Leading safety device design
- ***Trend-setting proof test concepts*** reduce the inspection effort with a high proof test coverage or enable the flexibilization of proof test intervals
- Attractive Services and Solutions for more safety

→ *Conclusion*: ***highest*** safety and ***maximum*** availability of the plant

Endress+Hauser

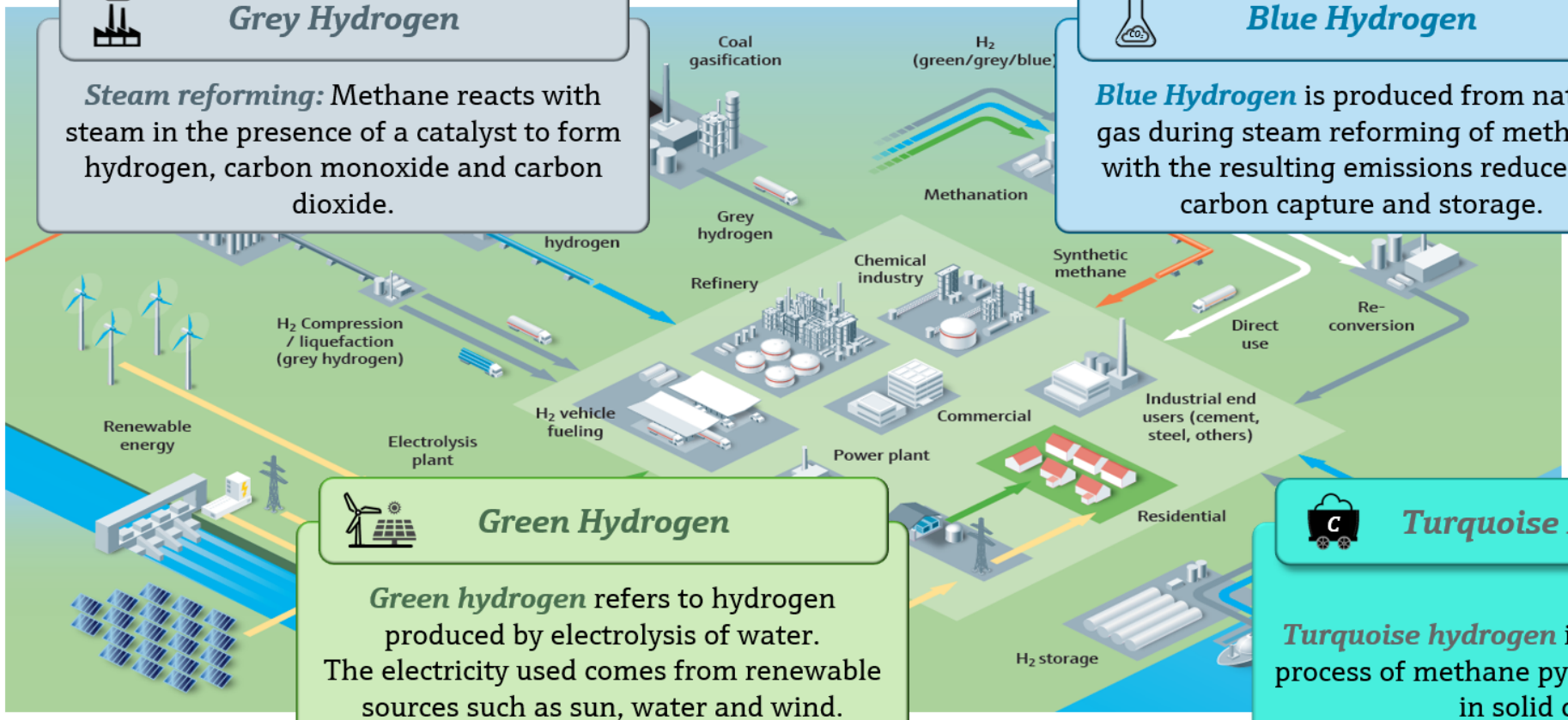
H2: Key element of decarbonization - cross-sectoral

Grey Hydrogen

Steam reforming: Methane reacts with steam in the presence of a catalyst to form hydrogen, carbon monoxide and carbon dioxide.

Blue Hydrogen

Blue Hydrogen is produced from natural gas during steam reforming of methane, with the resulting emissions reduced by carbon capture and storage.



Green Hydrogen

Green hydrogen refers to hydrogen produced by electrolysis of water. The electricity used comes from renewable sources such as sun, water and wind.

Turquoise Hydrogen

Turquoise hydrogen is produced from the process of methane pyrolysis, which results in solid carbon.

Basic requirement for Explosion protection and Functional Safety

Basic requirement for Explosion protection

- An “explosion protection document” explains how explosion hazards are detected and evaluated, safety measures implemented as well as technical and organizational precautions against explosion risks in compliance with national requirements
- The explosion protection document describes:
  - → Relevant substances, regulations and framework conditions that have led to the present assessment
  - → Relevant safety parameters for determining protection measures

Basic requirement for Functional Safety

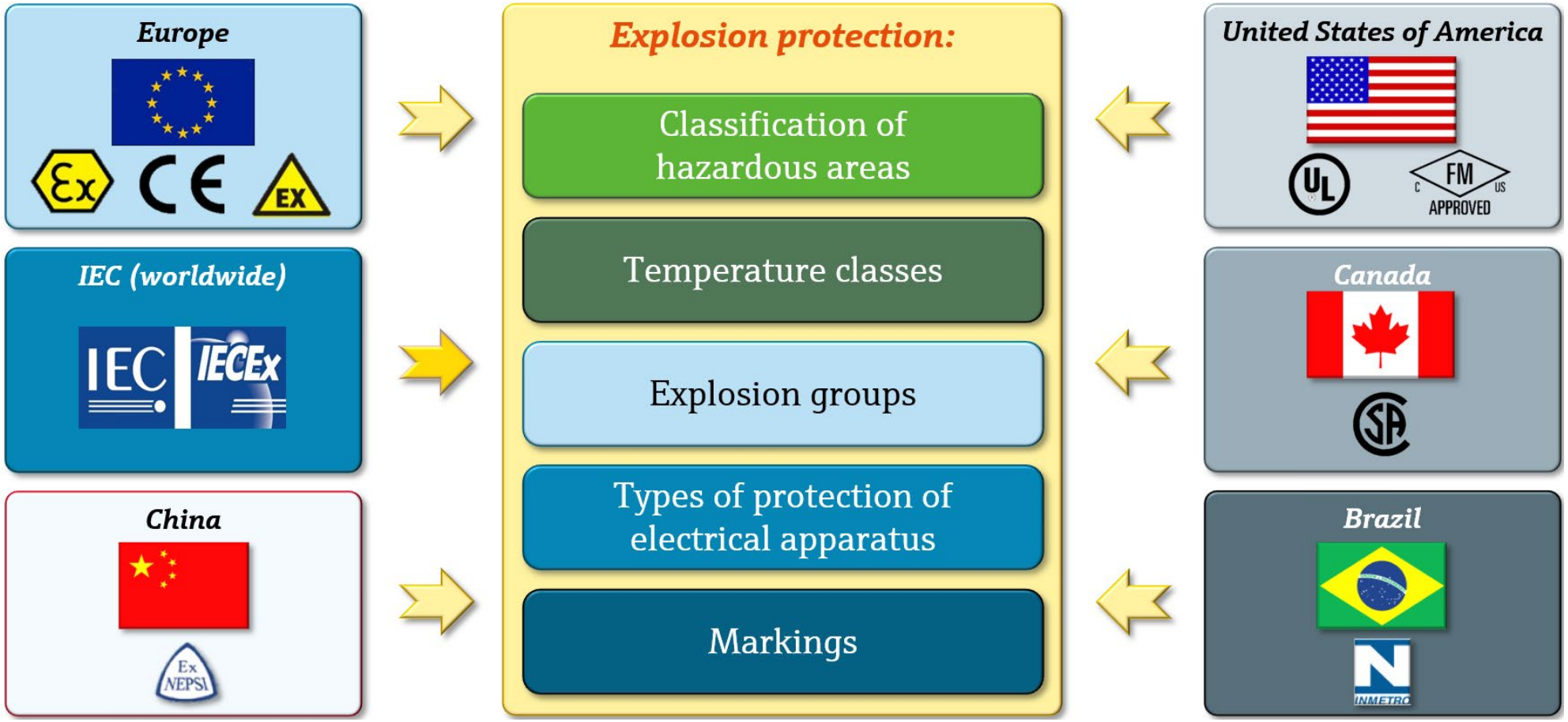
- Safety against hazards resulting from the (faulty) function of a device
  - ➲ Functional safety is achieved when
  - → All parts of a plant or machine function correctly (no dangerous failures) or
  - → In the event of a fault, behave that the plant or machine remains in a safe condition or can be brought into a safe condition
- The requirements for functional safety are based on the avoidance of systematic faults and control of random failures

➲ Use Safety Life-Cycle according IEC 61511-1

Hydrogen process measurement application and safety management

- Explosion protection in the process industry

Commonalities of different global approvals (example selection)



Classification of gases: Hydrogen ▸ Europe (International) vs. North America

Explosion area	International Group acc. to IEC-Norm	EUROPE Group acc. to ATEX 2014/34/EU	Sub- division EN-Norm	Min. ignition energy	Example
Electrical equipment for places with an explosive gas atmosphere	IIA	II	IIA	≥200µJ	Propane
	IIB		IIB	60-200µJ	Ethylene
	IIC		IIC	≤ 20 µJ	Hydrogen, Acetylene

NORTH AMERICA Class	Sub- division	Min. ignition energy	Example
I	D	≥ 160 µJ	Propane
	C	60-160µJ	Ethylene
	B	10-20µJ	Hydrogen
	A	≤ 10 µJ	Acetylene

Explosion limit and ignition temperature of air/gas mixture

Gas	Ignition Temp. [°C]	Flashpoint [°C]	Min. Ignition Energy [mJ]	Lower explosion limit (Vol.% in air)	Upper explosion limit (Vol.% in air)	IEC/ATEX Gas Group	North America Class/Div	Temperature Class
Hydrogen	560	≤ 20	0.017	4.0	78.6	IIC	IB	T1

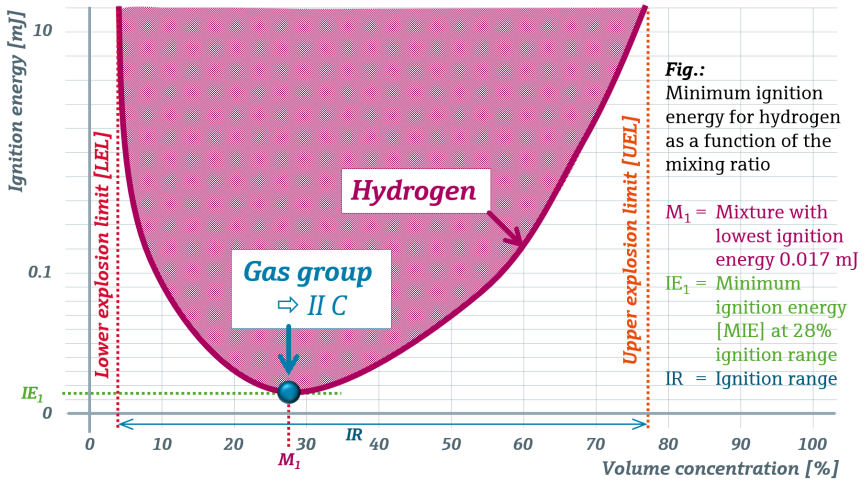


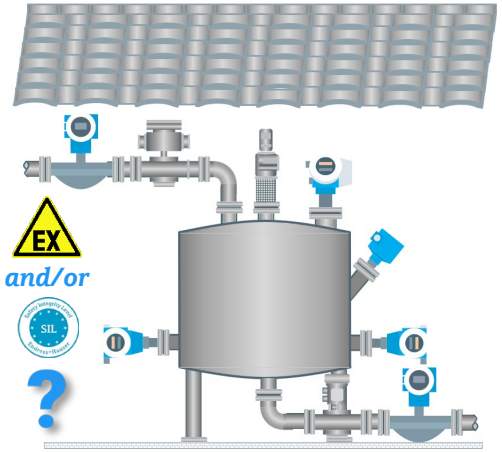
Fig.: Minimum ignition energy for hydrogen as a function of the mixing ratio

M_1 = Mixture with lowest ignition energy 0.017 mJ
IE_1 = Minimum ignition energy [MIE] at 28% ignition range
IR = Ignition range

Endress+Hauser

Handling of hydrogen

- The safe handling of hydrogen requires knowledge of its properties and appropriate safety measures is a prerequisite



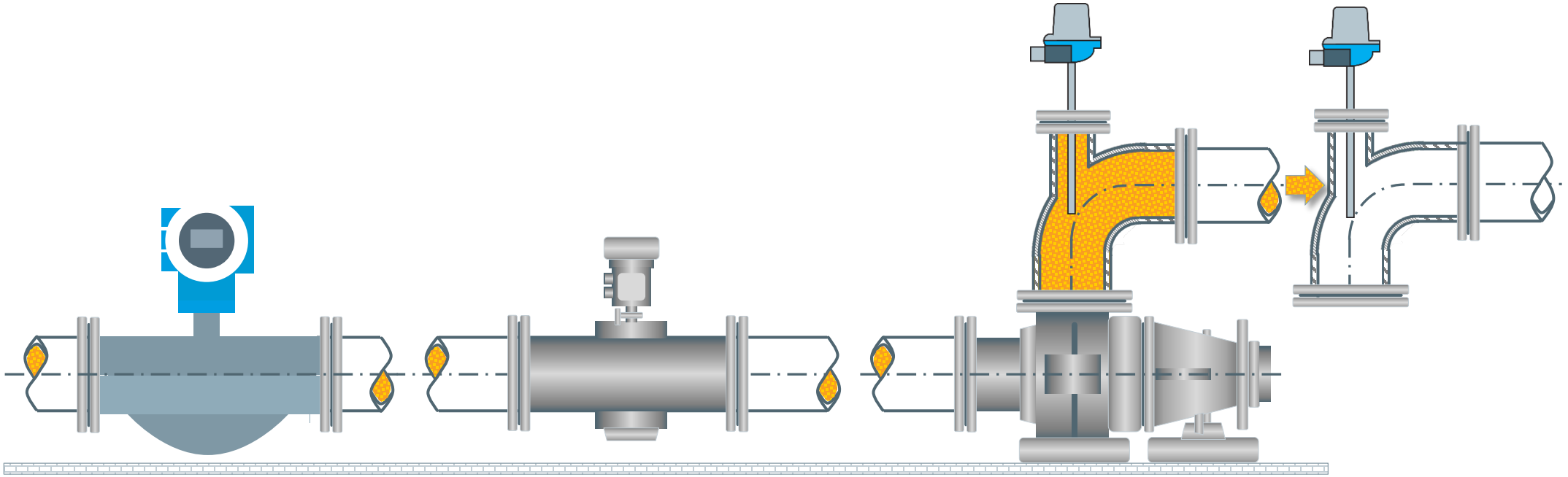
  - The area around hydrogen plants is not considered an explosion hazard zone in all cases

➲ *Avoidance* of *explosive atmospheres* indoors and outdoors

→ The formation of explosive atmospheres in areas around hydrogen plants is prevented by the following conditions:

- Hydrogen plants shall be located in well-ventilated areas
- Hydrogen plants must be tight and remain …

Handling of hydrogen

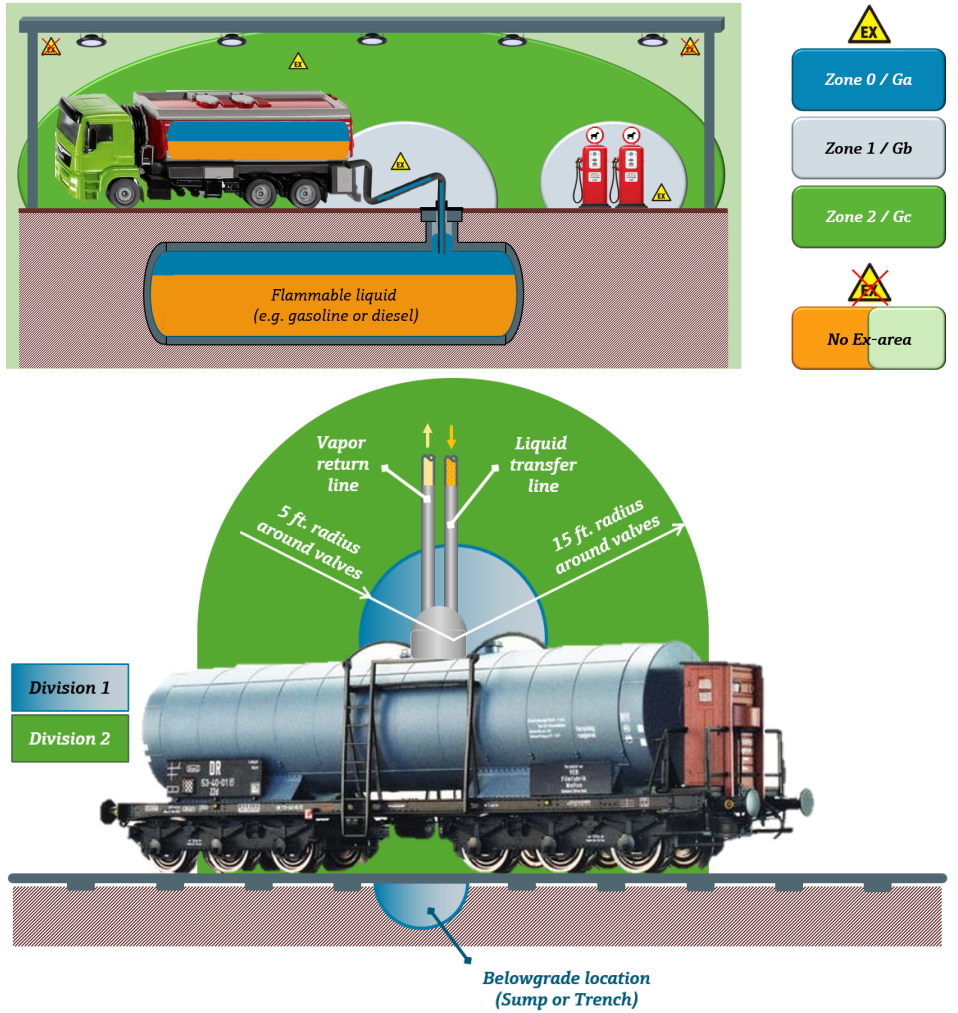


- Before commissioning, the air must be removed from hydrogen systems, e.g. by evacuation or purging with nitrogen (oxygen concentration < 1 vol.%)
- If parts of the plant remain pressurized during decommissioning, the hydrogen must be shut off very carefully against the depressurized part of the plant, e.g. by two closed valves with intermediate depressurization

Hazardous area classification – International (ATEX) vs. North America

	Explosive gas atmosphere		
	Flammable Material Present Continuously	***Flammable*** Material Present Intermittently	***Flammable*** Material Present Abnormally
IEC / EU *(ATEX)*	*Zone 0*	*Zone 1*	*Zone 2*
US (NEC® 505) / ***CA*** (CEC Section 18)	***Zone 0***	***Zone 1***	***Zone 2***
US (NEC® 506) / ***CA*** (CEC Annex J)	***Division 1***		***Division 2***

- IEC (*or EU*) area classification per IEC (*EN*) 60079-10-1
- US area classification per ANSI/NFPA 70 National Electrical Code® (NEC®) Article 500 or Article 505
- CA area classification per CSAC22.1 Canadian Electrical Code (CEC) Section 18 or Annex J



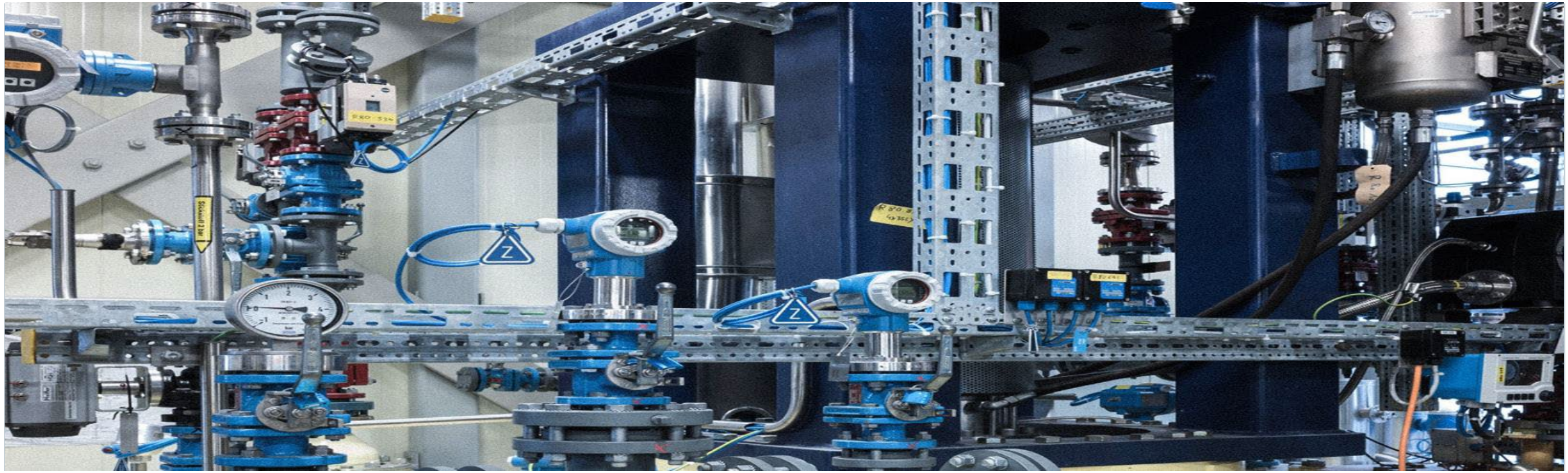
Endress+Hauser

Types of protection of electrical apparatus: International vs. North America

Type of protection	Gas atmosphere (Equipment category / EPL)			Gas Ex / Vapors (Class I)	
	1G / Ga	2G / Gb	3G / Gc	Division 1 + 2	Division 2
Flameproof enclosures	da	db	dc	XP ~ Ex d	
Increased safety		eb	ec		
Intrinsically safe	ia	ib	ic	IS ~ Ex ia	NIFW - Ex ic
Encapsulation	ma	mb	mc		
Oil immersion		ob			o
Powder filling		qb			
Pressurized enclosures		pxb/pyb	pzc	Type X and Y	Type Z
Protection by enclosure					
Non sparking apparatus			nA		NI – Ex nA
Sparking apparatus			nC		
Energy limited apparatus			nL		
Restricted breathing enclosures			nR		

Hydrogen process measurement application and safety management

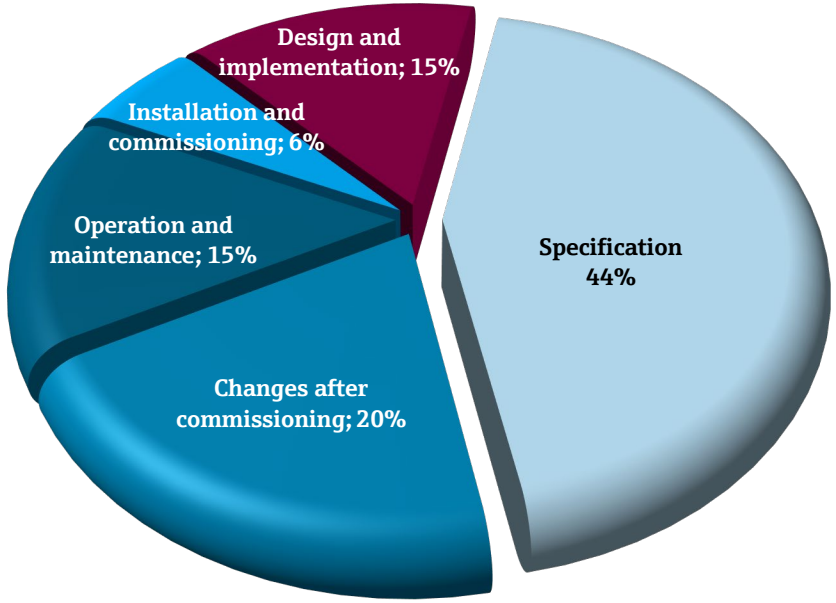
- Functional safety in the process industry



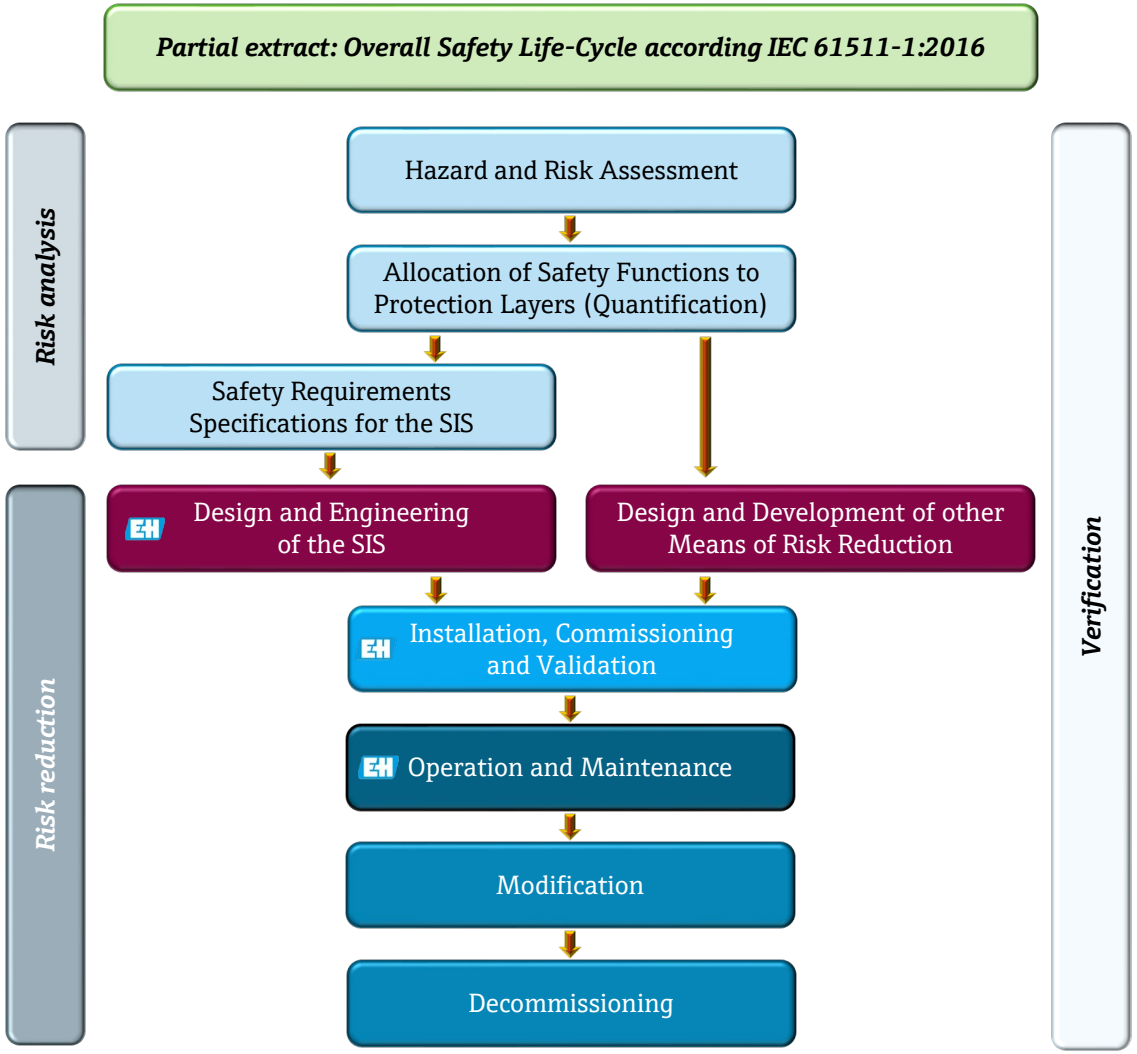
Faults and causes of faults in the life-cycle of Safety Instrumented Systems (SIS)

Something to think about…

- ***90%*** accidents have ***no*** technical background
- ***65%*** failure already exist ***before*** plant put into operation for the first time

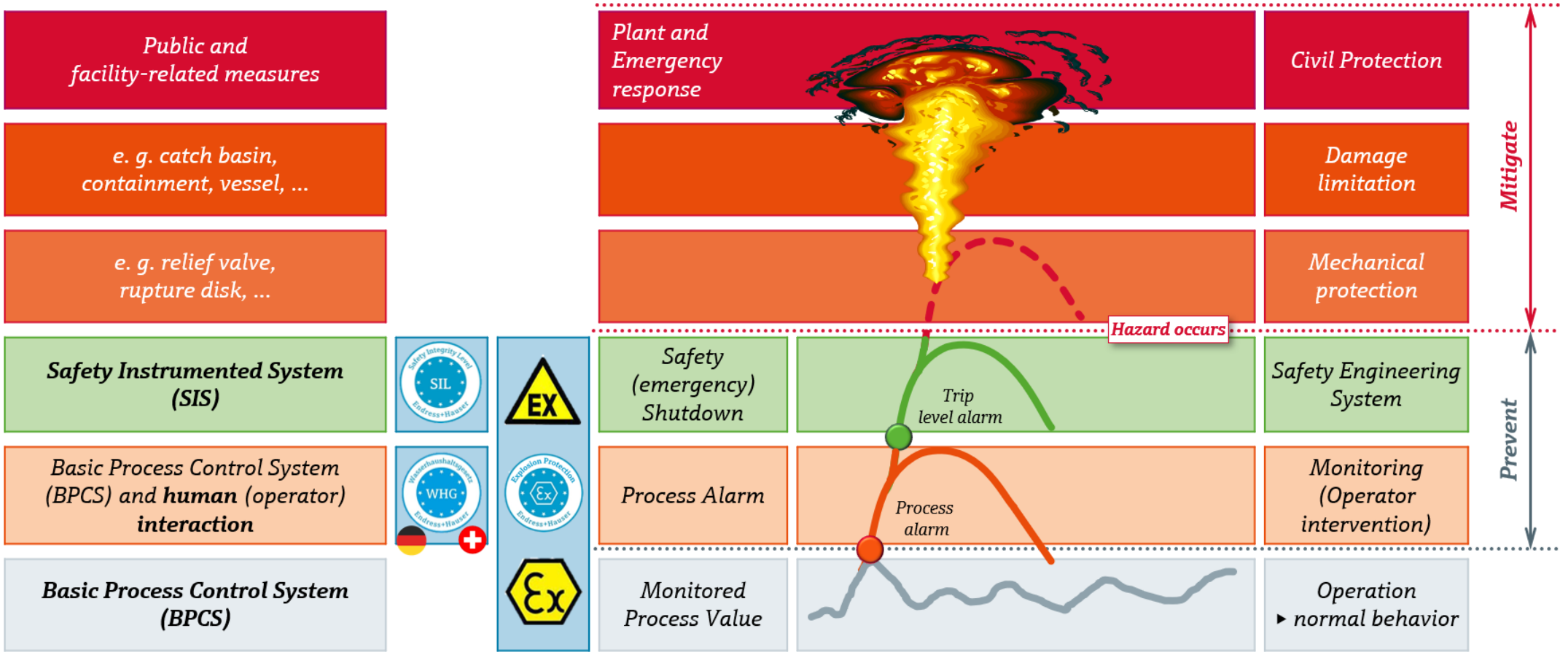


Source: United Kingdom Health Safety and Environmental Committee; HSE (Health and Safety Executive); Out of control: Why control systems go wrong and how to prevent failure, Second Edition 2003



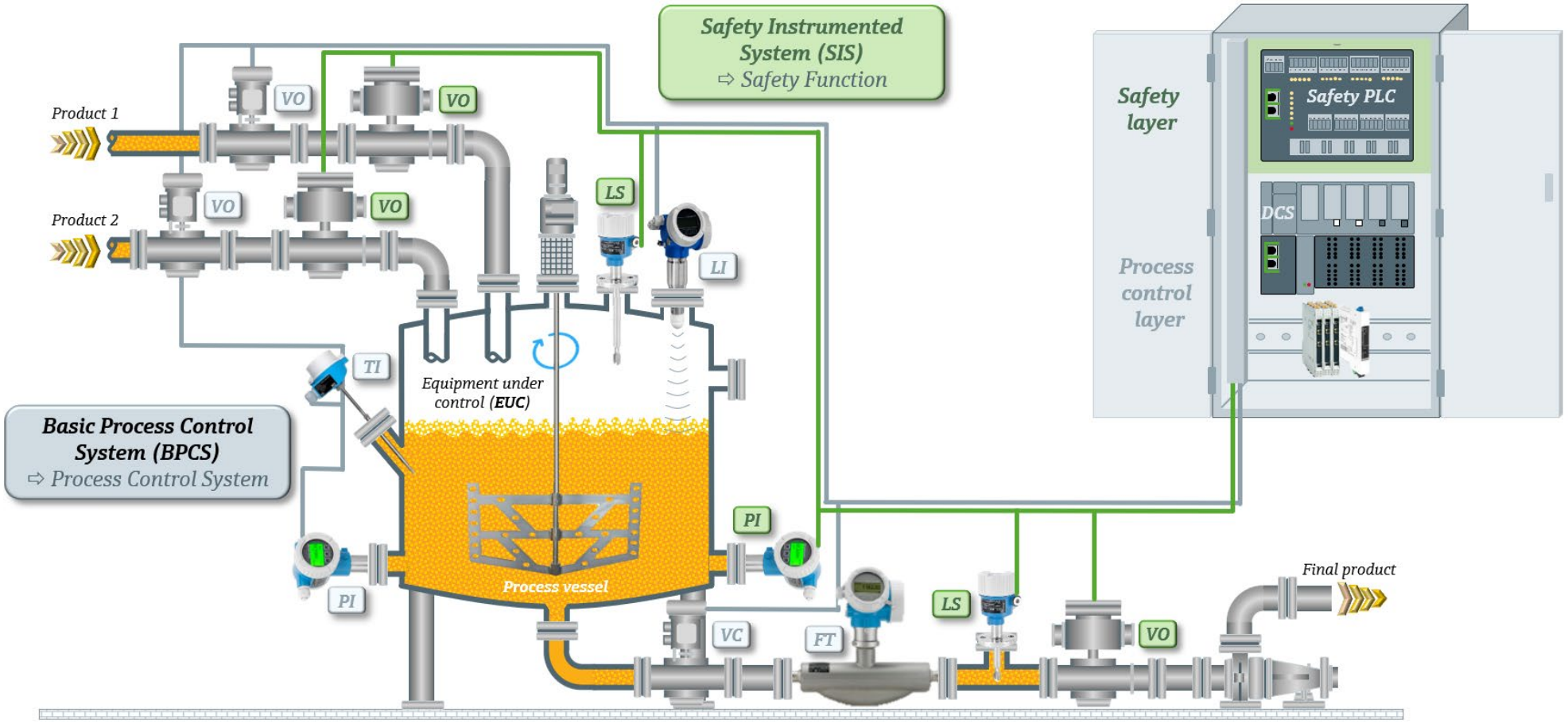
Endress+Hauser

Methods of risk reduction in process plants



Endress+Hauser

Usage and difference of Process Control System (BPCS) to Safety Function (SIS)



DCS = Decentralized Control System (former: Distributed Control System)
PLC = Programmable Logic Controller

Endress+Hauser

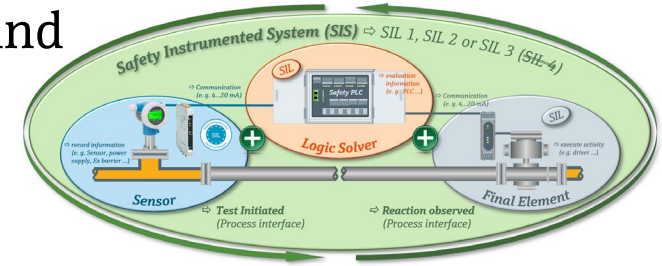
Can a process plant be operated 100% safely?

➲ A ***S***afety ***I***nstrumented ***S***ystem (*SIS*) is ***100%*** functionally safe if ***all*** …

→ *random failures* and

→ *systematic faults*

… *are detected*



do *not lead* to *malfunctioning* of the safety system and do not result in

→ Injury or death of *humans*

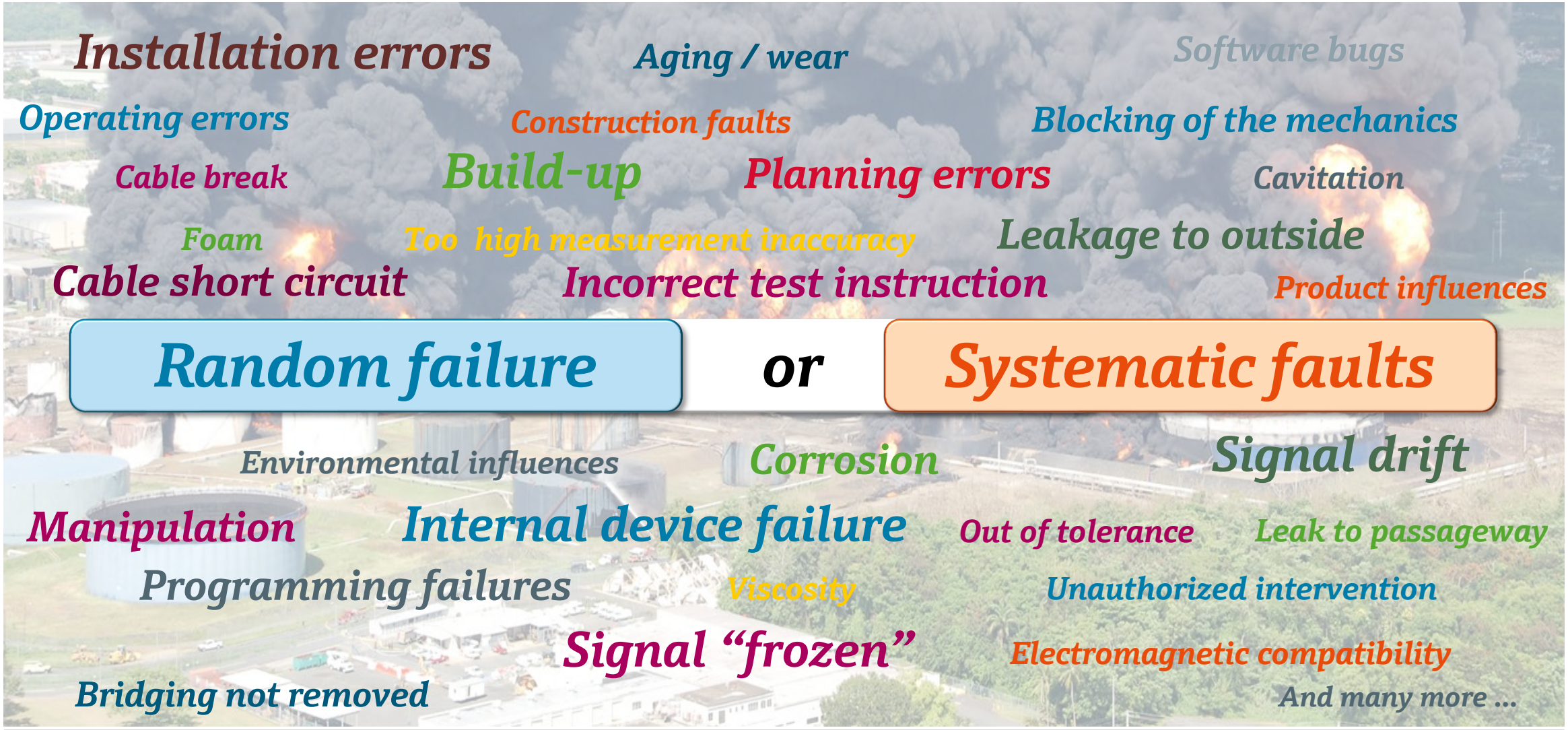
→ Spills to the *environment*

→ Reputational damage, loss of equipment or *production*

⚠ ***100%*** Functional Safety does ***not*** exist ⚠

Endress+Hauser

Typical failures in the process industry

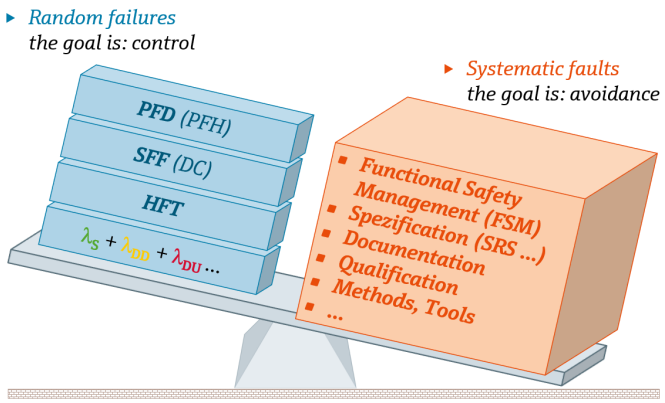


Endress+Hauser

Typical failures in the process industry

Random failures
▸ Internal device failure
▸ Signal “frozen”
▸ “Soft errors”
▸ Other random failures

Systematic faults	
▸ Electromagnetic compatibility	▸ Build-up
▸ Planning errors	▸ Operating errors
▸ Installation errors	▸ Unauthorized intervention
▸ Product influences	▸ Manipulation
▸ Environmental influences	▸ Bridging not removed
▸ Software bugs	▸ Incorrect test instructions
▸ Programming failures	▸ High measurement inaccuracy
▸ Construction faults	▸ Signal drift
▸ Aging / wear	▸ Leak in the passageway
▸ Cable short circuit	▸ Leakage to outside
▸ Corrosion	▸ Blocking of the mechanics ...



Endress+Hauser

What Heartbeat Technology can do for you?

Increase your plant availability and ...

... boost reliability as well as safety levels	*... reduce your verification efforts*	*... improve your process performance*

Heartbeat Technology

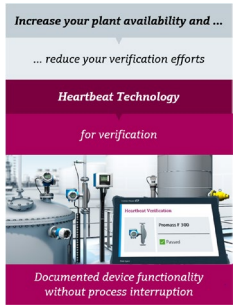
for diagnostics	*for verification*	*for monitoring*
		
Permanent process and device diagnostics	*Documented device functionality without process interruption*	*Information for process optimization and predictive maintenance*

Source: Heartbeat Technology core team presentation 2022-03

SIL sequence for λ_{DU} and Heartbeat Technology for systematic fault detection

Functional Safety

Heartbeat Technology



- *SIL Proof Test*
  - → Un-lock the safety device
  - → Trigger safety function
  - → Confirmation/documentation concept
  - → Lock the safety device …

- *Heartbeat Verification*
  - → Without process interruption
    - ⇒Help to avoid systematic faults with Heartbeat Verification and Heartbeat Monitoring

➲ ***Conclusion:***

- *SIL Proof Test* sequence in combination with *Heartbeat Verification* and *Heartbeat Monitoring* support proof test cycle extension

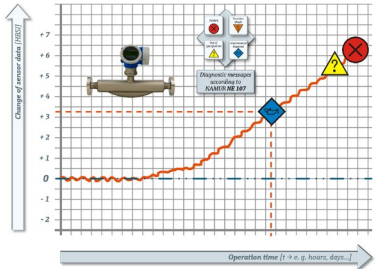
SIL sequence for λ_{DU} and Heartbeat Technology for systematic fault detection

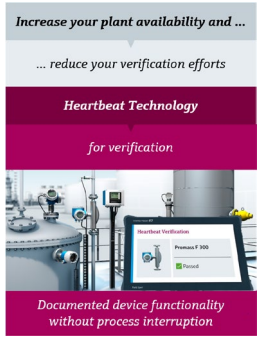
SIL Proof Test

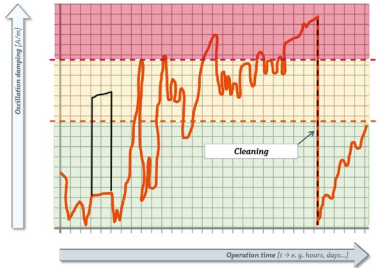
- *Test sequence **C*** *(for details see FY)*
  - → Testing with a secondary standard 1
    - ⇒ PTC = 0.98
- *Test sequence **D*** (with process interruption)
  - → Option BA, BB ⇒ PTC = 76 % or
    Option CA, CB, C ⇒ PTC = 79 %
  - → Proof test procedure (*simplified*)
    - ⇒ Device restart
    - ⇒ Verification of current output 1
    - ⇒ Heartbeat Verification
    - ⇒ Inspection and on-site visual check

Heartbeat Monitoring

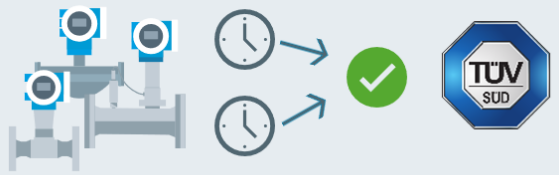
- *E. g. Proline Promass 300/500*
  - → Heartbeat Sensor Integrity (HBSI)
    - ⇒ Abrasion,
    - ⇒ Corrosion
  - → Oscillation damping
    - ⇒ Build-up







Flow – Coriolis, vortex and ultrasonic
Redundant frequency generators
(quartz clocks)



Promass 300/500 ⇒ λ_{DU} = 134 FIT
⇒ SFF = 97.6 %
⇒ DC ~ 94 %

Hint: λ_{DU} = *134 FIT for Option BA, BB*
λ_{DU} = *131 FIT for Option CA, CB, CC*

- *Proof Test Coverage (PTC)*
- Dangerous undetected failure (λ_{DU})
- *Failure in Time* (1 FIT = 10^9 h)
- Safe Failure Fraction (SFF)
- Diagnostic Coverage (DC)

Endress+Hauser

Definition - Functional Proof Test

➲ ***Periodic functional proof test*** performed to *detect dangerous hidden failures* in a *safety-related system* so that, if necessary, a *repair can restore the system to an "as new" condition* or as *close* as practical *to this condition*
(see IEC 61508-1:2010 section 3.8.5 "proof test")

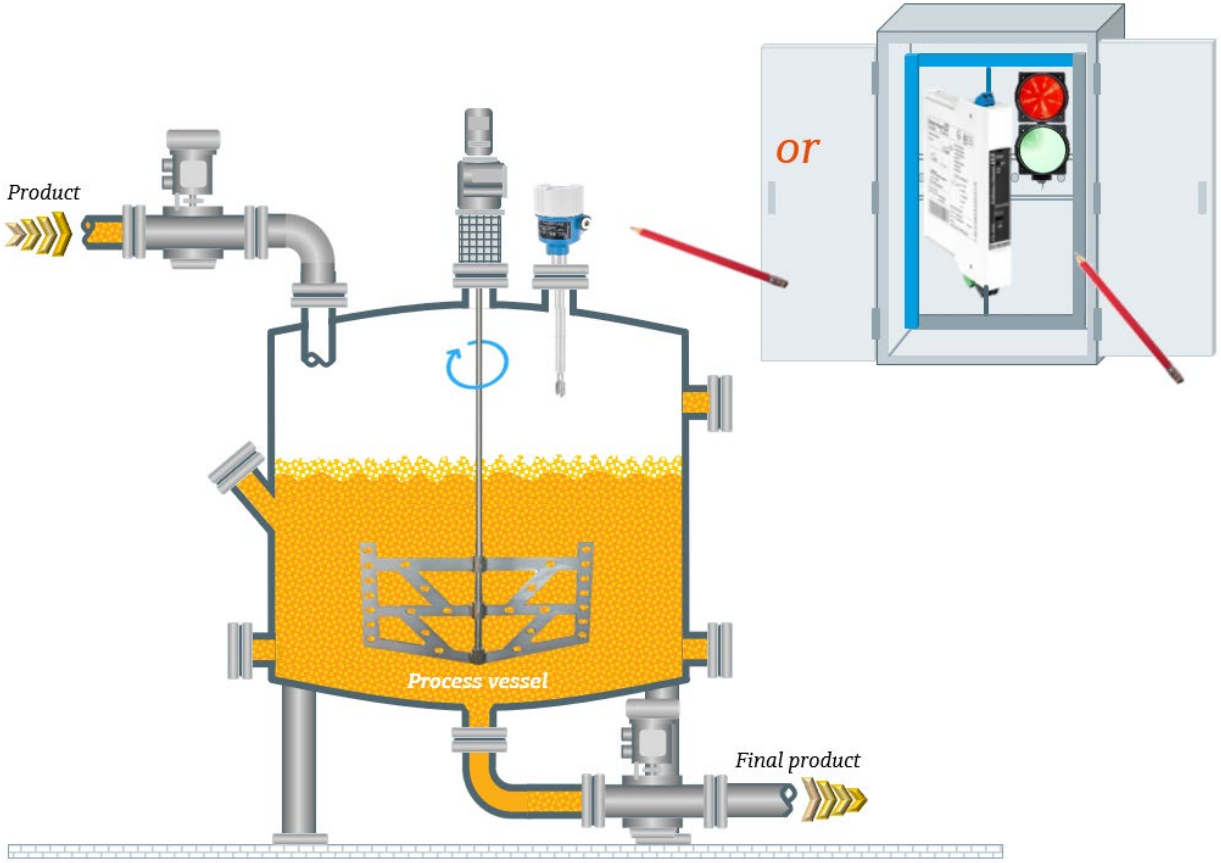
➲ Executed according to a *pre-defined proof test procedure*, it typically consists of:
- → A ***detailed inspection*** of the *instrument* to ***detect*** *potential* problems
- → ***Functional testing*** as *per agreed* test procedure
- → Providing the ***documentary evidence*** of the proper operation of the Safety Instrumented System (SIS)

Practical examples of proof testing the sub-system sensor (e. g. Liquiphant)

Functional proof testing (*full* or *partial*)

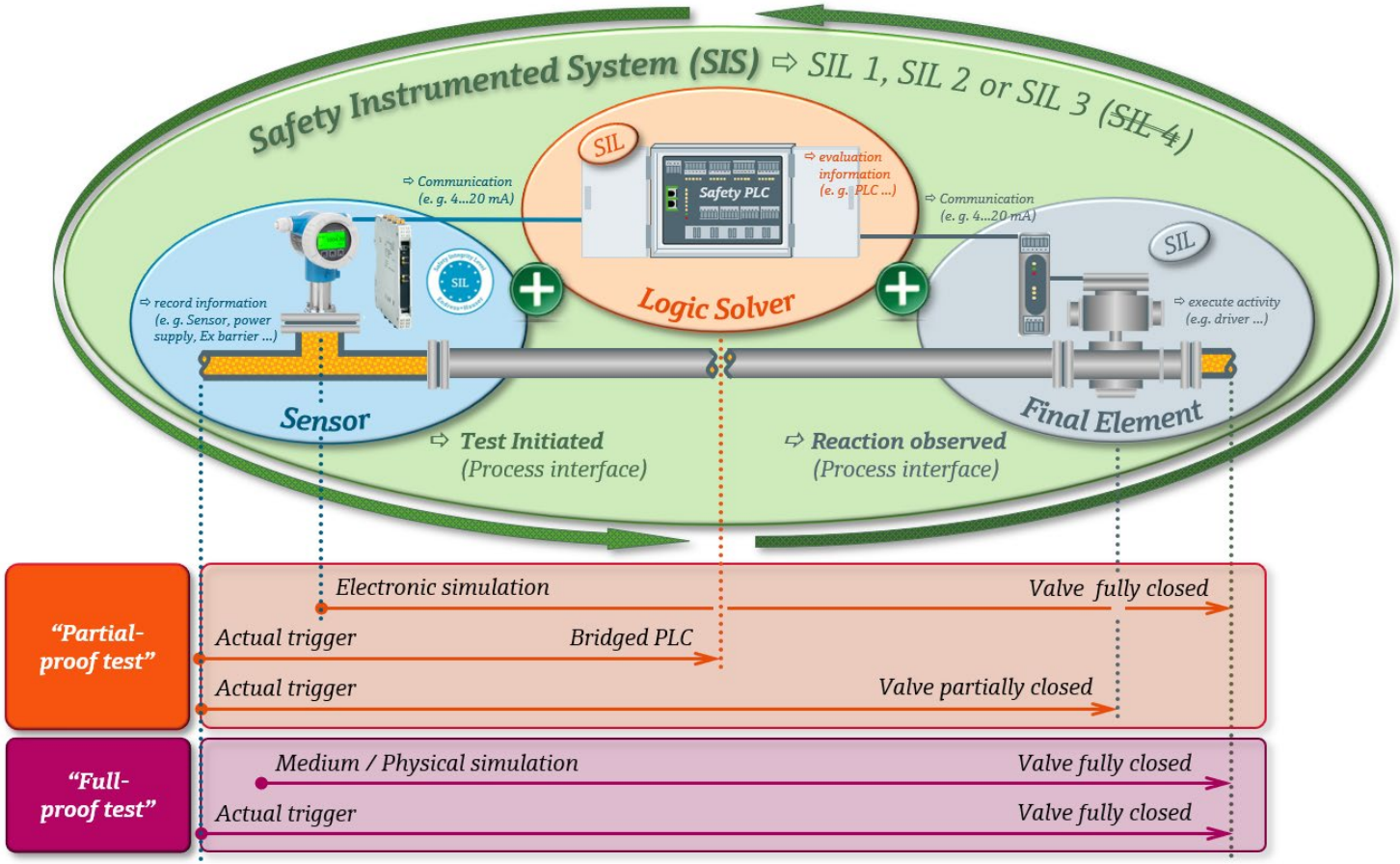
- ***Full-*** *proof test* (PTC ≈ 100%)
  - *Filling* a *reactor* to the max to create a high-level alarm or
  - Alternatively, *removing* the level switch from the tank for a *remote test*

- ***Partial-*** *proof test* (PTC < 100%)
  - *Simulating* the high-level *without filling* the reactor



PTC = **P**roof **T**est **C**overage

Proof Test of a Safety Instrumented System: “Partial”- and / or “full” test?



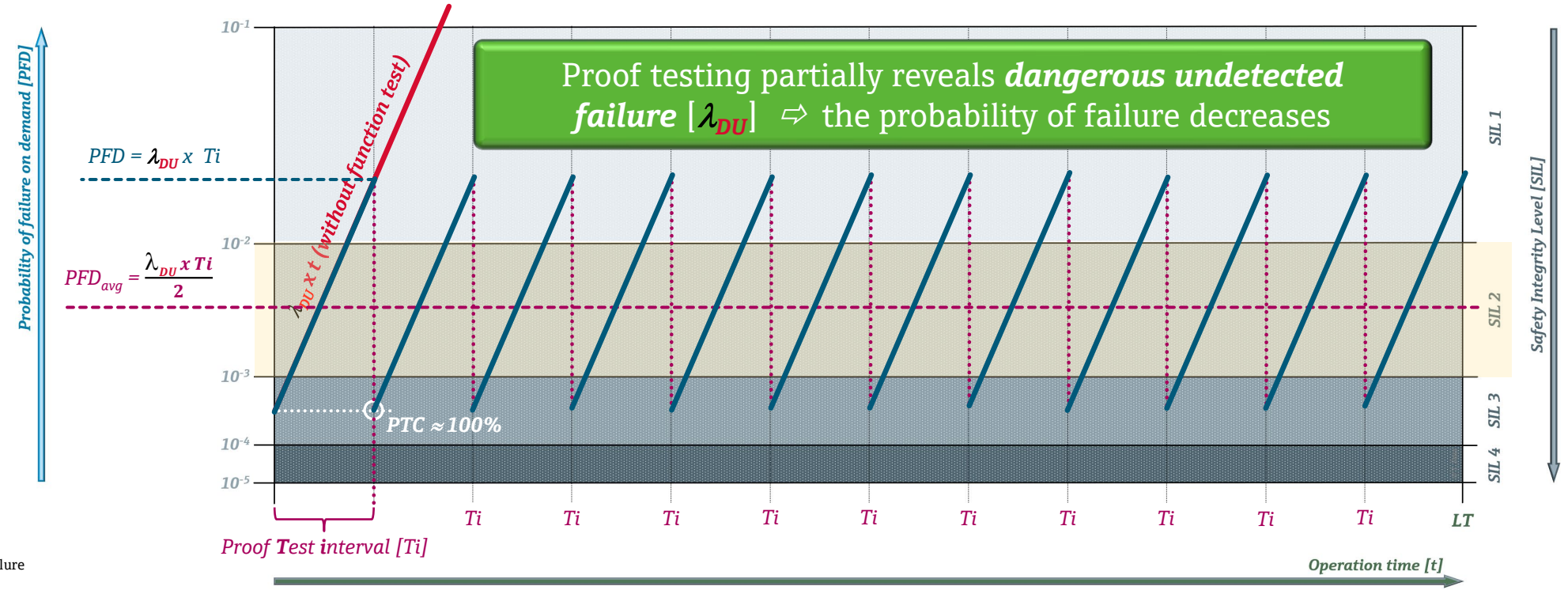
Endress+Hauser

Proof test procedure → Influence of the PTC on the proof test

Example 1): Single channel architecture [**1oo1**] in „ low demand mode“ (~1/a)

PTC ≈ 100%

→ *PTC ≈ 100 %* *(Formula for the calculation:* $PFD_{avg} = \frac{\lambda_{DU} \times Ti}{2}$ *)*



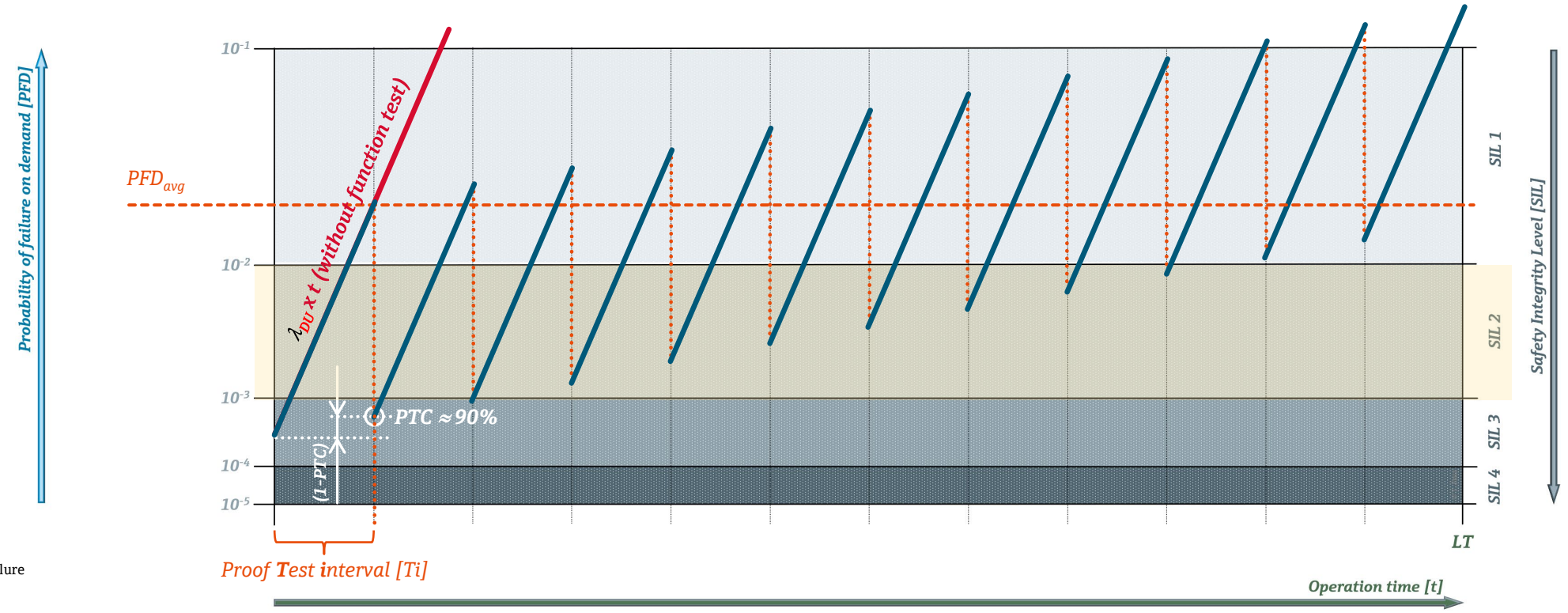
Ti = Proof ***T***est ***i***nterval
PTC = ***P***roof ***T***est ***C***overage
λ_{DU} = ***D***angerous ***U***ndetected failure
LT = ***L***ife ***T***ime

Proof test procedure → Influence of the PTC on the proof test

Example 2): Single channel architecture [***1oo1***] in „ low demand mode“ (~1/a)

PTC < 100%

→ *PTC ≈ 90 %* *(Formula for the calculation:* $PFD_{avg} = \frac{\lambda_{DU} \, x \, Ti \, x \, PTC}{2} \oplus \frac{(1 - PTC) \, x \, \lambda_{DU} \, x \, MT}{2}$ *)*



Ti = Proof ***T***est ***i***nterval
PTC = ***P***roof ***T***est ***C***overage
λ_{DU} = ***D***angerous ***U***ndetected failure
MT = ***M***ission ***T***ime
LT = ***L***ife ***T***ime

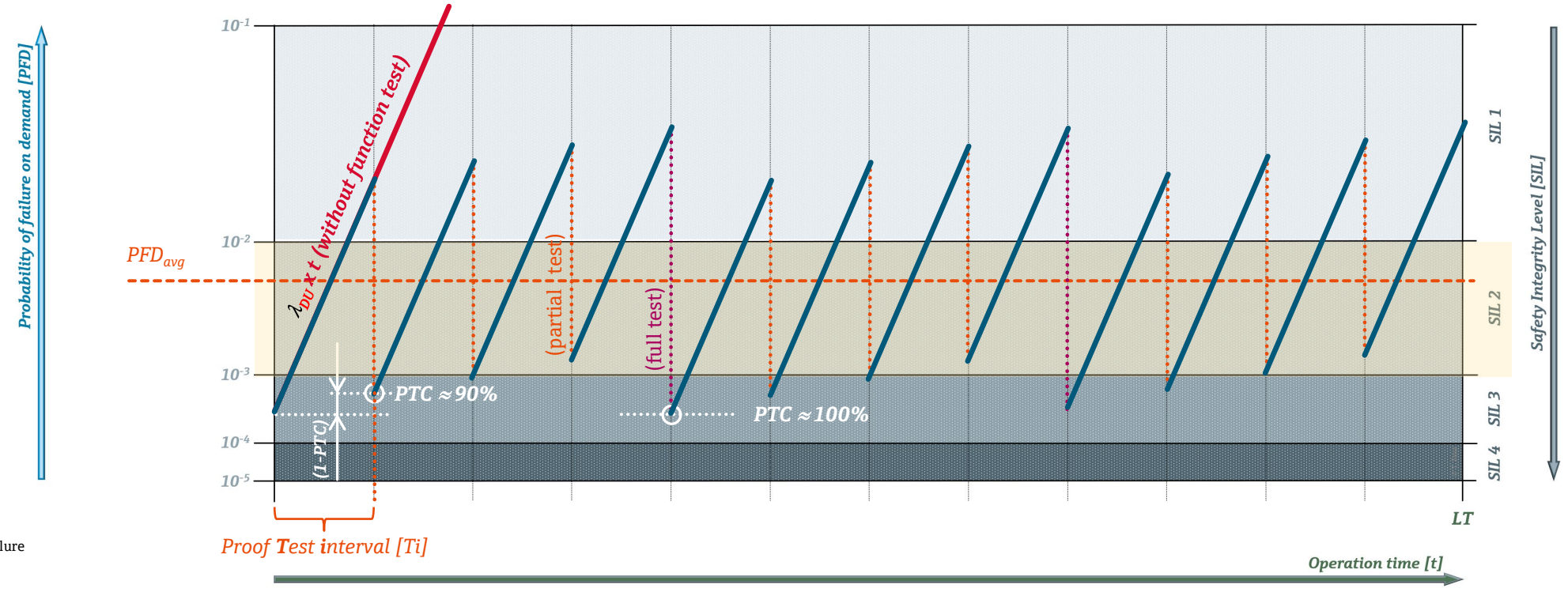
Endress+Hauser

Proof test procedure → Influence of the PTC on the proof test

Solution 2): Single channel architecture [***1oo1***] in „ low demand mode“ (~1/a)

→ *PTC ≈ 90 %* *(Formula for the calculation:* $PFD_{avg} = \frac{\lambda_{DU} \, x \, Ti \, x \, PTC}{2} \oplus \frac{(1 - PTC) \, x \, \lambda_{DU} \, x \, MT}{2}$*)*

→ ***Same*** *device as solution 1) → but every fourth year full proof test*



Ti = Proof ***T***est ***i***nterval
PTC = ***P***roof ***T***est ***C***overage
λ_{DU} = ***D***angerous ***U***ndetected failure
MT = ***M***ission ***T***ime
LT = ***L***ife ***T***ime

Endress+Hauser

How PTC can affect the SIL Rating of your Safety Instrumented Function (SIF)

λ_{DU} = Dangerous undetected failure
1 FIT = 10^9 h

ULT = Useful life time
MT = Mission time

Ti = Proof test interval
PTC = Proof test coverage

➲ *Calculate the PFD_{avg} (1oo1):*

→ $PFD_{avg} = PFD_{avg\ (S)} + PFD_{avg\ (LS)} + PFD_{avg\ (FE)}$

Safety Integrity Level	Probability of Failure on Demand
SIL 1	0.01 ≤ PFD < 0.1
SIL 2	0.001 ≤ PFD < 0.01
SIL 3	0.0001 ≤ PFD < 0.001

Source: IEC 61508-1:2010; Table 2

→ *Full-* proof test (*PTC ≈ 100 %*)

$PFD_{avg} = \frac{\lambda_{DU} \times Ti}{2}\ (S) + \frac{\lambda_{DU} \times Ti}{2}\ (LS) + \frac{\lambda_{DU} \times Ti}{2}\ (FE)$

$8.1906 \times 10^{-4} + 7.74822 \times 10^{-4} + 2.17688 \times 10^{-3}$

3.771×10^{-3} → 3.8×10^{-3} ▸ **SIL 2**

Sensor			Logic Solver				Final Element			
λ_{DU}	121 FIT (*Promass F300*)	66 FIT (Active Barrier)	λ_{DU}	5.54 FIT (Input-Card)	4.9 FIT (CPU)	7.25 FIT (Output-card)	λ_{DU}	9.7 FIT (Valve control)	123 FIT (Actuator)	57 FIT (Limit switch)
PTC *(partial test)*	52 %	99 %	***PTC*** *(partial test)*	99 %	99 %	99 %	***PTC*** *(partial test)*	90 %	95 %	92 %
1-PTC	48 %	1 %	***1-PTC***	1 %	1 %	1 %	***1-PTC***	10 %	5 %	8 %
ULT *(e.g. 12 years)*	105,120 h	105,120 h	***MT*** *(e.g. 20 years)*	175,200 h	175,200 h	175,200 h	***MT*** *(e.g. 20 years)*	175,200 h	175,200 h	175,200 h
Ti *(e.g. 1 year)*	8,760 h	8,760 h	***Ti*** *(e.g. 10 years)*	87,600 h	87,600 h	87,600 h	***Ti*** *(e.g. $^1/_{20}$ year)*	87,600 h	8,760 h	8,760 h

→ *Partial-* proof test (*PTC < 100 %*)

$PFD_{avg} = \frac{\lambda_{DU} \times Ti \times PTC}{2} + \frac{(1-PTC) \times \lambda_{DU} \times ULT}{2}\ (S) + \frac{\lambda_{DU} \times Ti \times PTC}{2} + \frac{(1-PTC) \times \lambda_{DU} \times MT}{2}\ (LS) + \frac{\lambda_{DU} \times Ti \times PTC}{2} + \frac{(1-PTC) \times \lambda_{DU} \times MT}{2}\ (FE)$

$3.6491532 \times 10^{-3} + 7.84364888 \times 10^{-4} + 2.1621662 \times 10^{-3}$

6.595×10^{-3} → 6.6×10^{-3} ▸ **SIL 2**

Endress+Hauser

Any questions?

⇨ Hydrogen process measurement application and safety management

Endress+Hauser