Functional Safety at the European process Industry

Peter Sieber, VP Norms & Standards

VP Region China

HIMA

SMART SAFETY.

About Peter Sieber

About me

- Peter Sieber, Vice President Norms & Standards
  Vice President Region China
  of HIMA Group.
- Working in safety automation since 1989.
- Participating on steering committees working on functional safety (IEC 61508/11, ISO 13849), Automation security (IEC 62443) and engineering processes since 1998.

About HIMA

- HIMA is the world's leading specialist for safety-related automation with more than 45 years of Domain experience.
- Headquartered in Brühl (Mannheim), Germany.
- Family-owned company founded in 1908.

Legislative framework in Europe

Guiding Principle

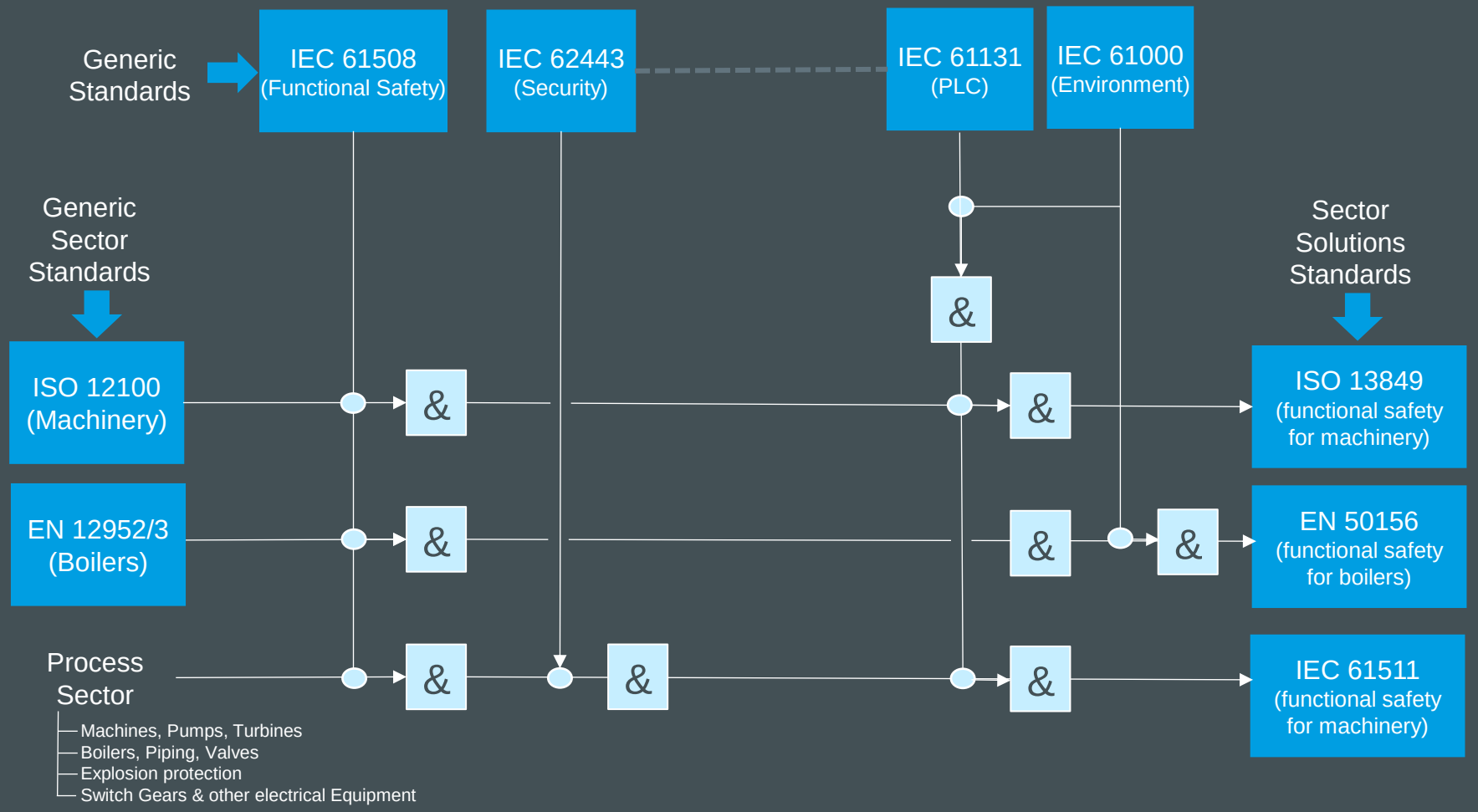
- EU Directive (European Law)
  (e.g. Seveso Directive, Machinery directive, pressurized equipment directive
  Low voltage directive, EMC directive etc.)

- Definition of underlying Standards (attachment to EU Directive)
  (e.g. EN 50156, EN 61000, EN 298, EN 746, EN 12952, EN/ISO 13849 …. EN(IEC) 61511

- Local Implementation
  (e.g. in Germany “Arbeitssicherheitsgesetz”, “Bundes-Immissionsschutzgesetz”)

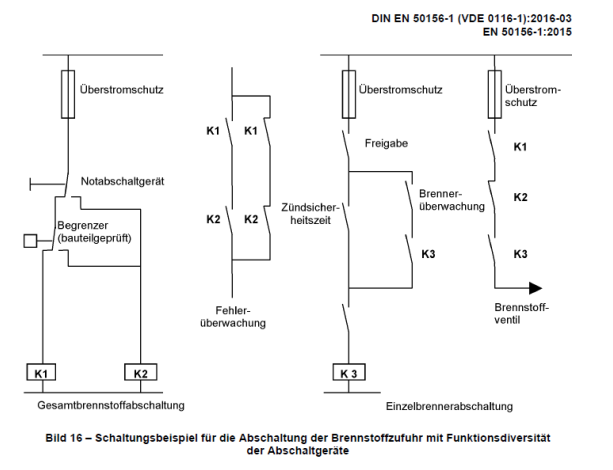
- Local Implementation rules
  (e.g. in Germany VDI/VDE 2180 being the implementation rule for IEC 61511)

Norms, Standards, correlations & Challenges



Descriptive vs. non descriptive

Descriptive



Pro:
Clear recommendations
Con:
Technology depending
Inflexible when combining with others

Non Descriptive

5.2.7SIS configuration management

5.2.7.1Requirements

5.2.7.1.1 Procedures for configuration management of the SIS during any safety life-cycle phase shall be available. In particular, the following should be specified:

- the stage at which formal configuration management is to be implemented;
- the procedures to be used for uniquely identifying all components of a device (hardware and software);
- the procedures for preventing unauthorized devices from entering service.

5.2.7.1.2 The SIS application program, embedded software and utility software (tools) procedures and related SIS hardware used to develop and execute the application program shall be subject to configuration management and shall be maintained under revision control.

Pro:
Not technology depending
Flexible when combining with others
Con:
Always having room for interpretation

EN 61511: Why this standard?

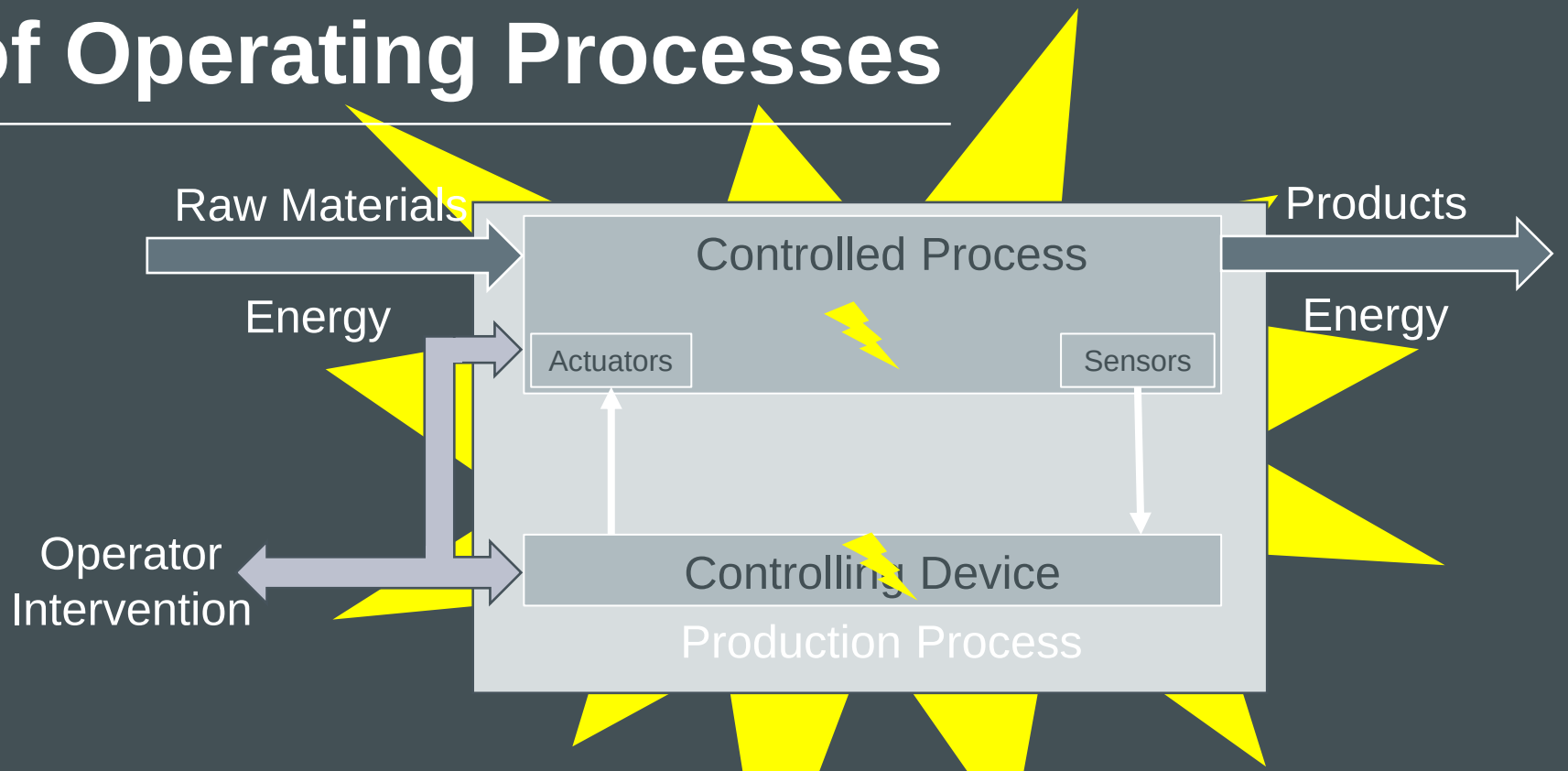
Process plant

	Pipes	Tanks/Reactors/Vessels	Rotating Equipment	Support Equipment
Risk	Rupture Leaking Fire	Rupture Leaking Fire/Explosion	Rupture Leaking Fire/Explosion Mechanical risks	2. deg. Fire/Explosion electrical risks EMC Malfunctioning

Conceptual Risk reduction based on instrumented functions: IEC 61511

Sector Standards	Yes multiple	Yes multiple	Yes multiple	Yes multiple

Risk of Operating Processes

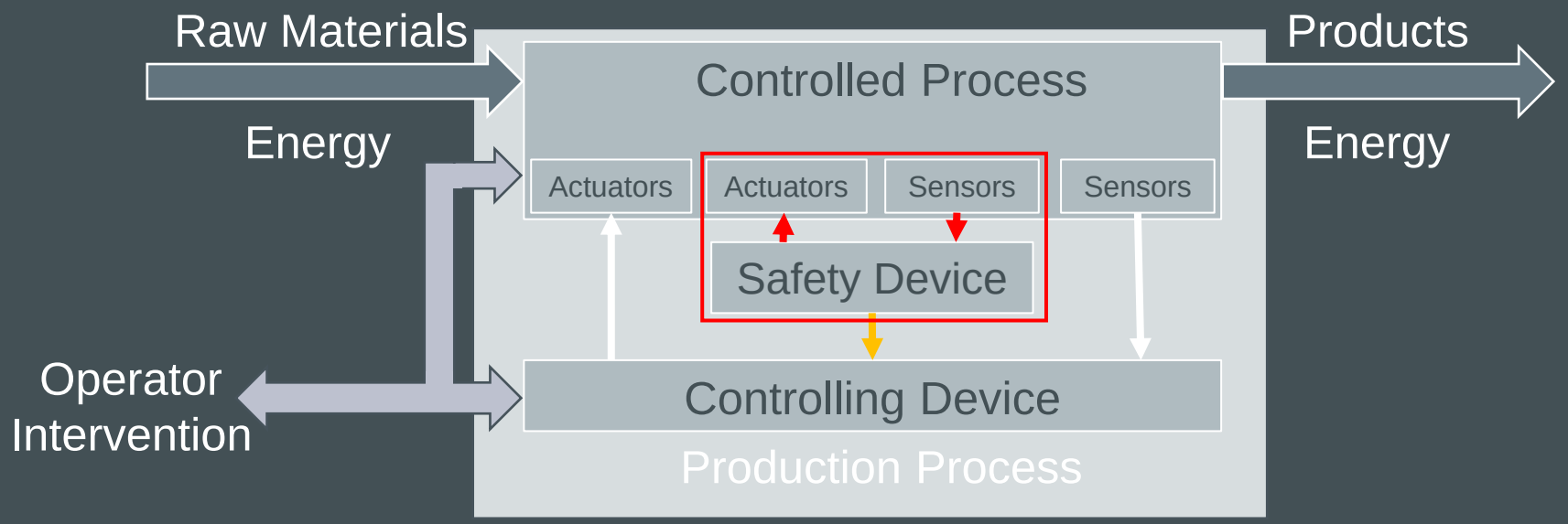


Take Away:

The risk born by a dedicated production process need to be mitigated to an acceptable level

- A hazard and risk analysis is required to understand the process
- Adequate counter measures need to be defined, implemented and maintained
- A part of such counter measures may be using control functions

Functional Safety Solution

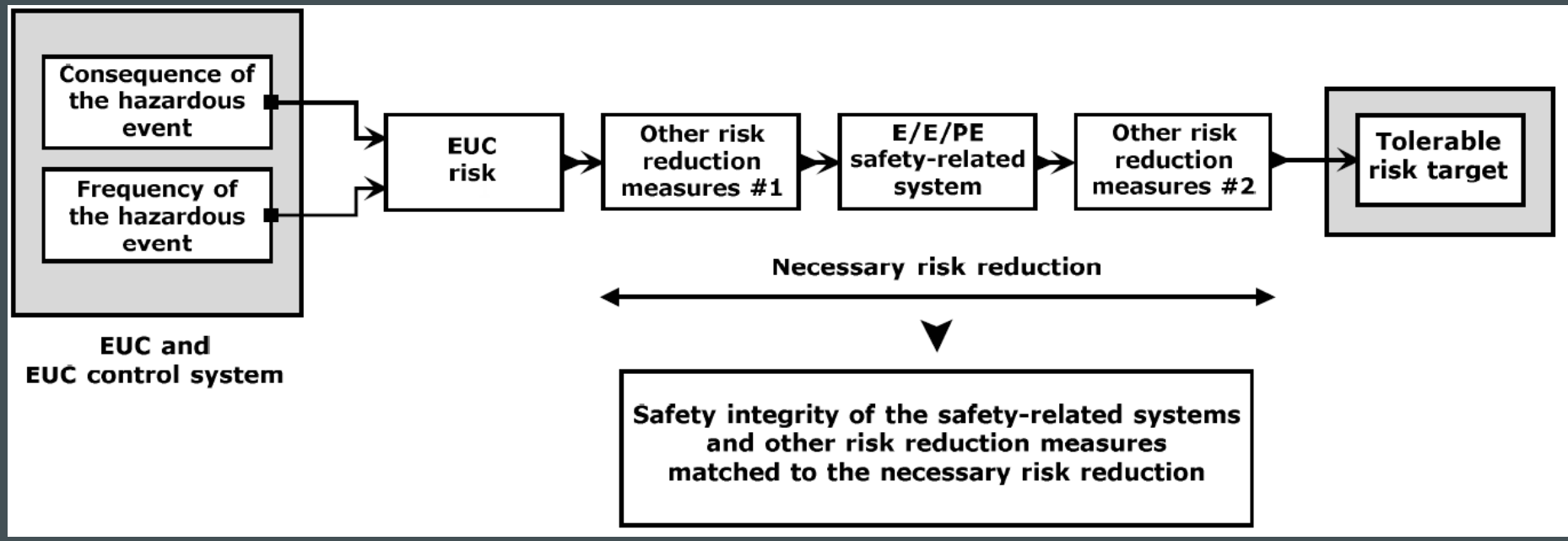


Take Away:

Adding an additional, reliable level of control can help, but

- The functional design requires a specific process to be followed
- Design, implementation and maintenance requires special attention
- Separation from BPCS is key to prevent common cause failures

Concept of Risk Reduction

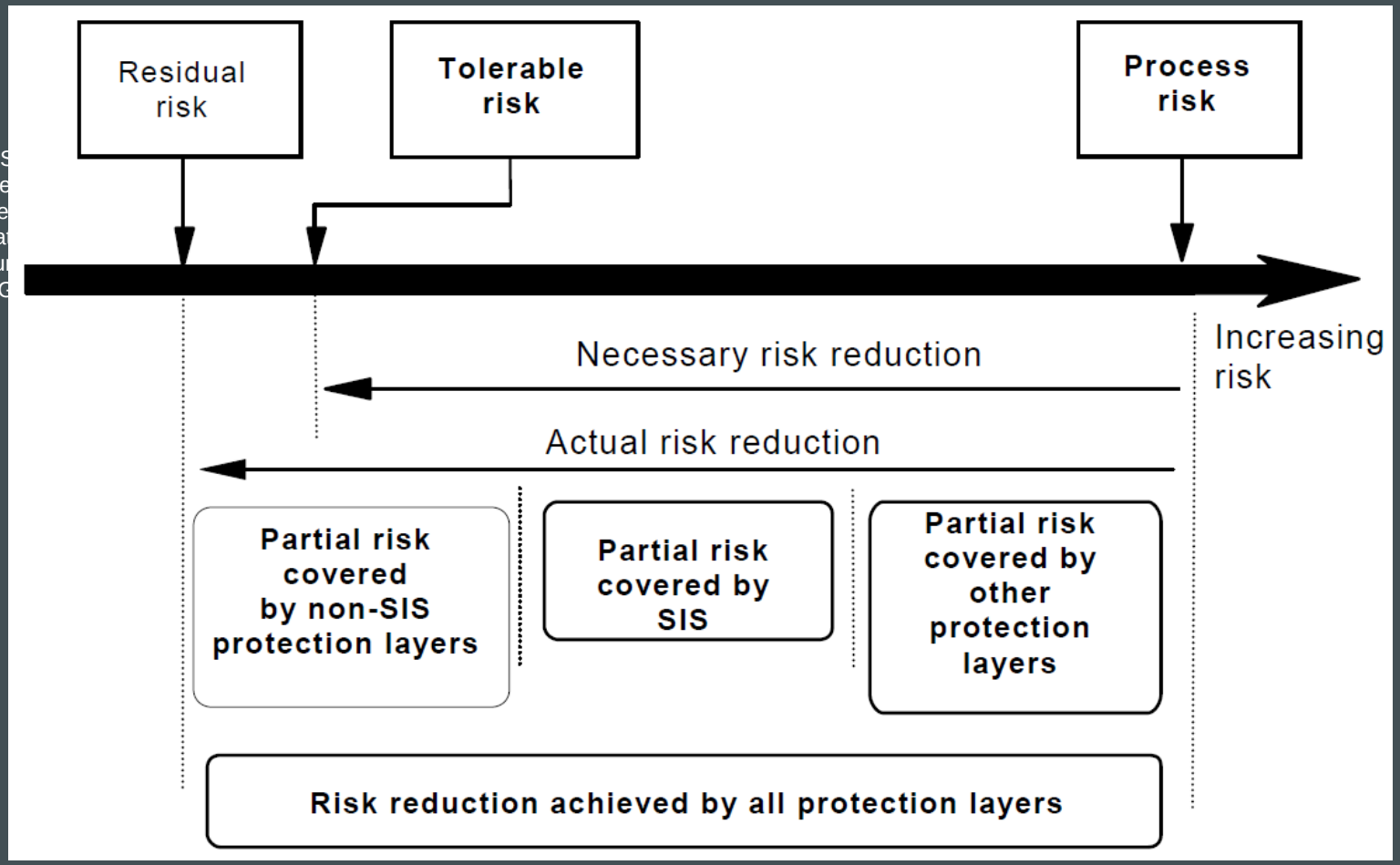


Measures # 1: e.g. BPCS; $R_R < 10$
E/E/PES: $10 \geq R_R < 10.000$
Measures # 2: Mitigation Systems (e.g. F&G Systems, Leakage monitoring etc.)

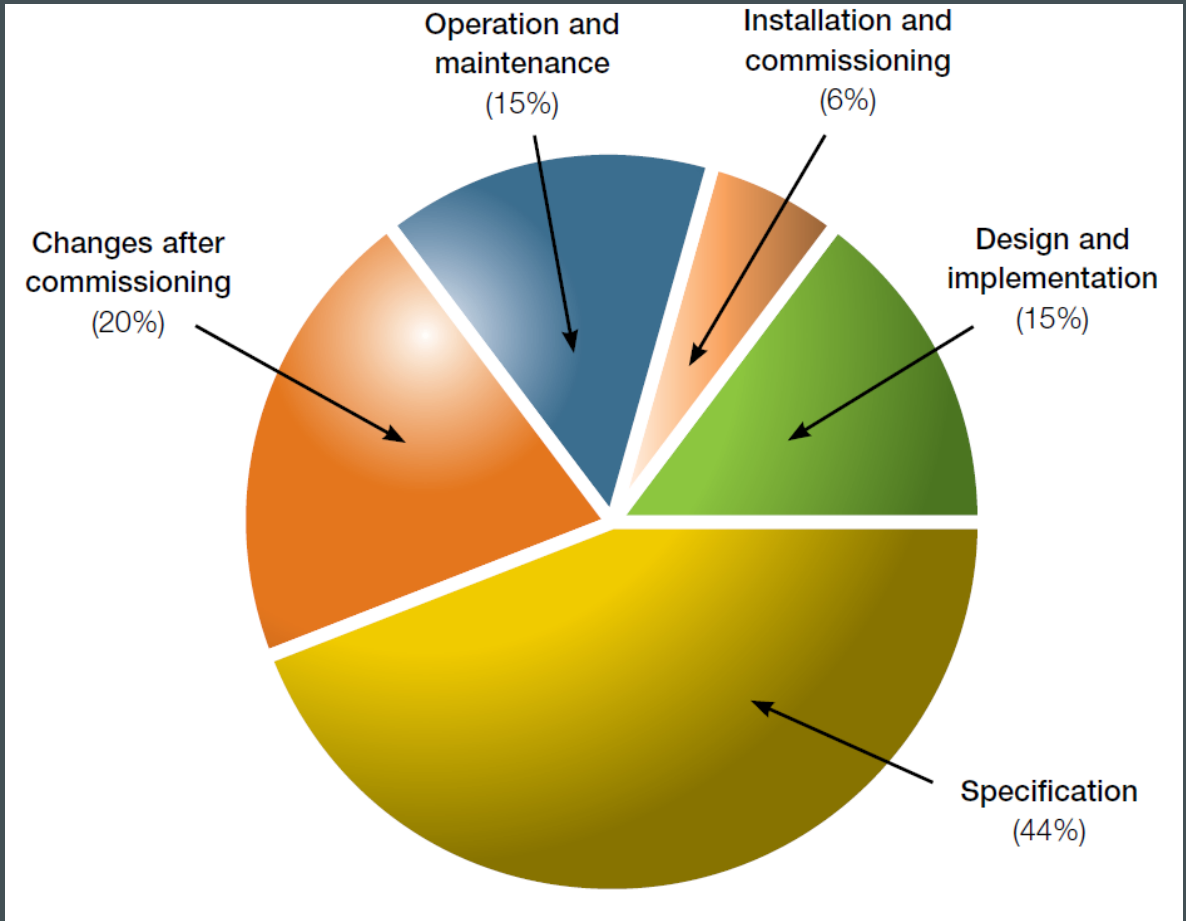
Independent Layer of Protection Concept

Mitigation

- Mechanical S
  (e.g. Rupture
- Civil enginee
  (e.g. Dikes a
- Safety instru
  (e.g. Fire & G



Causes of Accidents



Points to ponder:

- Specification, Design and Implementation
- Changes after Commissioning

Source: Out of Control; Why control systems go wrong and how to prevent failures
ISBN:978071762192 7

Concept of IEC 61511

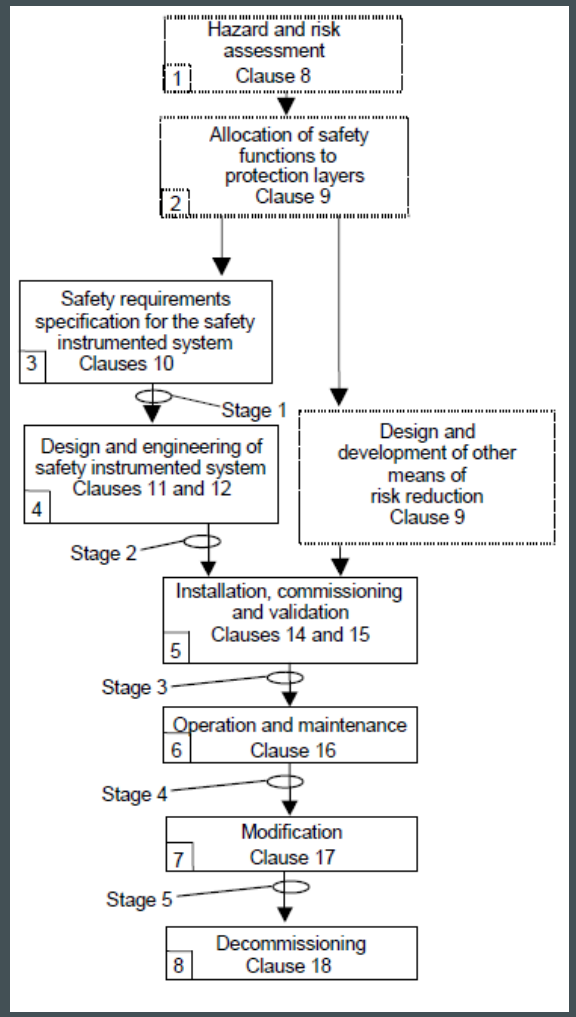
IEC 61511 provides guidance and recommendations for

- Management of functional Safety (Chapter 5)
- Functional Safety Lifecycle (Chapter 6)
- Verification (Chapter 7)
- Risk evaluation and Management (Chapter 8)
- Layering of solutions (Chapter 9)
- Functional Design specifications (Chapter 10)
- Design and Engineering (Chapter 11)
- Assessment Procedures
- Commissioning
- Maintenance and Retrofit

Structured Approach Acc. to IEC 61511 ed. 2

Management of Functional Safety

1. Hazard & Risk Assessment
   (Chapter 8)
2. Allocation of Safety functions to protection layers
   (Chapter 9)
3. Safety Requirement Specification
   (Chapter 10)
4. A compliant engineering & Design process
   (Chapters 11, 12)
5. A compliant build, installation, commissioning & validation
   (Chapters 14, 15)
6. A compliant maintenance concept,
   maintaining the anticipated reliability of the SIS
   (Chapter 16)



Source: IEC 61511 ed. 2

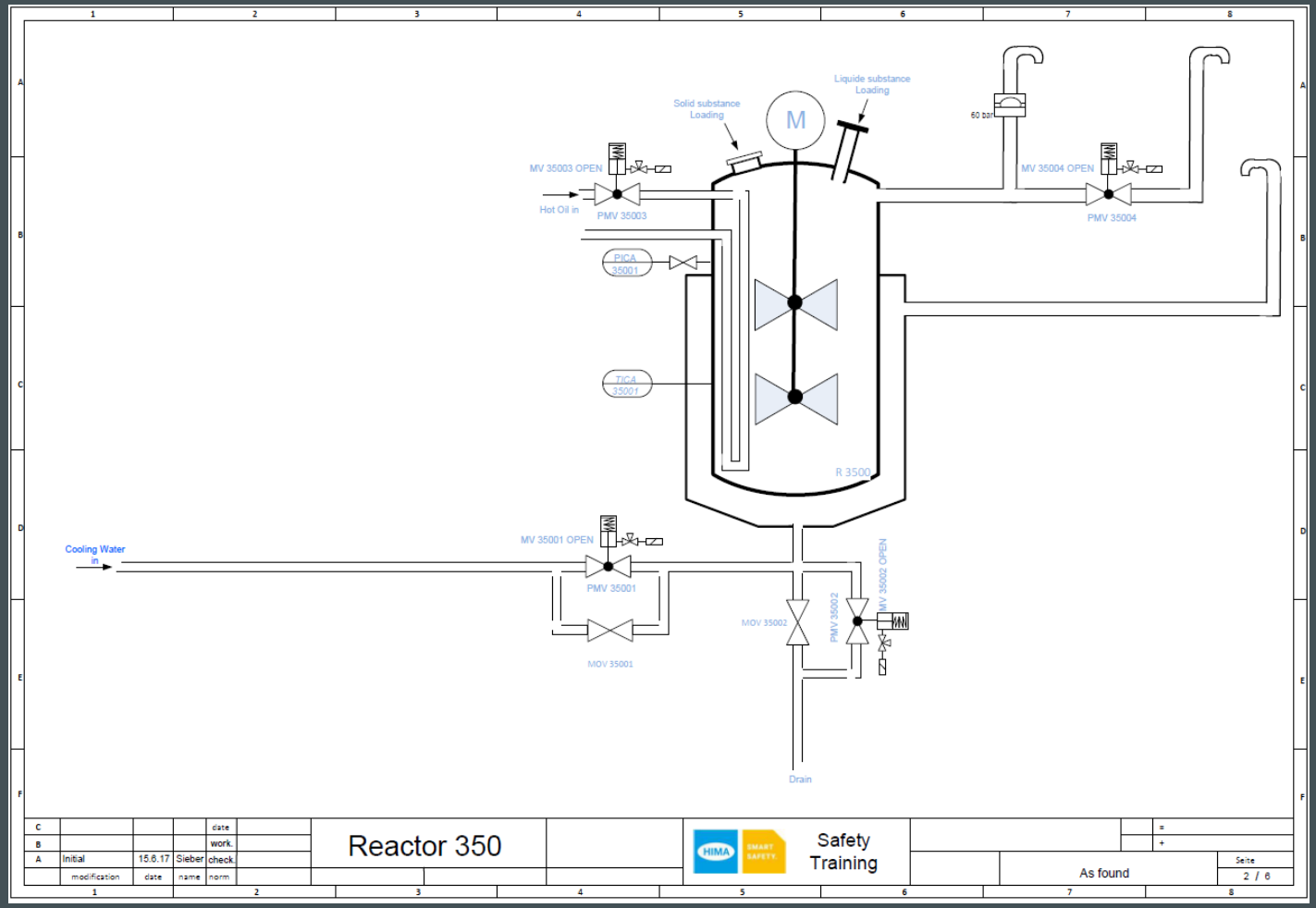
Practical Example: Chemical Reactor

Description

- Hosting exothermal reaction
- Reaction started by heating
- Pressure controlled by cooling
- Reaction Gas vented

Question:

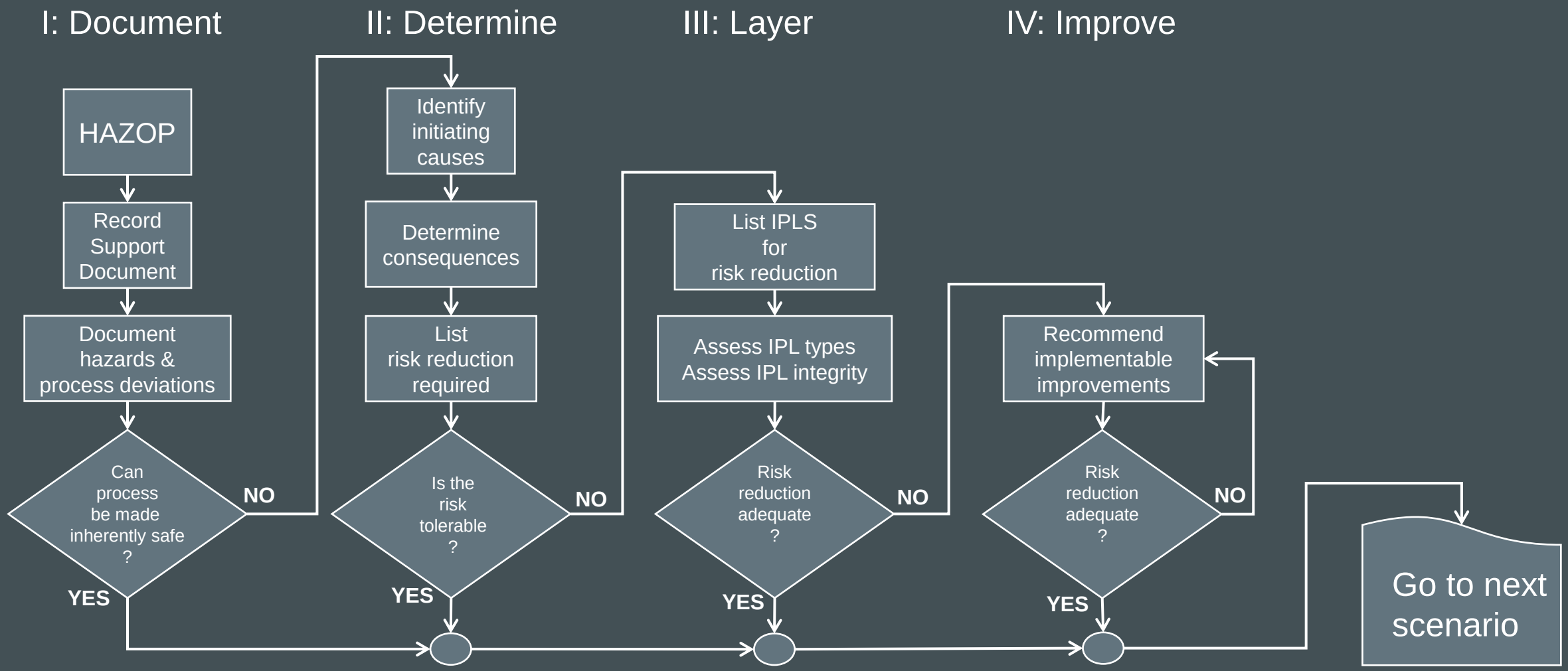
How to Safeguard such cases?



Reference:

CSB Safety Video
https://www.youtube.com/watch?v=C561PCq5E1g

A Structured Approach on how to …



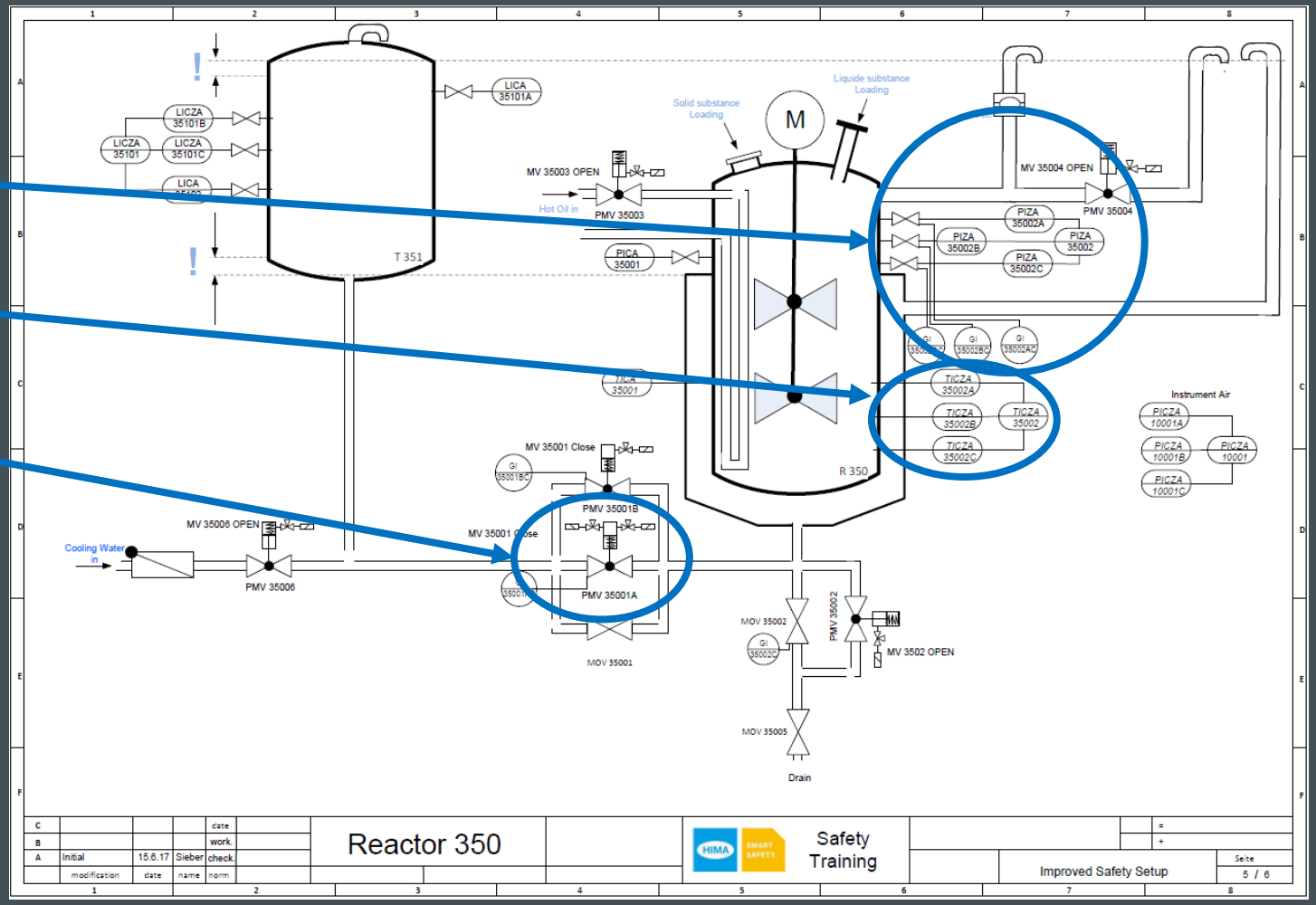
LOPA , Phase III Review Layered Solution

	Impact Event Description	Severity Level M/S/E	Initiating Cause	Initiation Likelyhood	General Process Design	BPCS Function	Alarms independend to BPCS	Additinal Mitigation Access rest.	IPL Additional Mitigation	Intermediate Failure Rate	Target Failure Rate	SIF Integrity Level	Final Failure Rate
1	High Pressure	E	Lack of cooling water due to stack close of Valve	0,1	0,1	0,1	1	0,1	0,1	1,E-05	1,E-08	3	1,E-08
2	High Pressure	S	Lack of cooling water due to Stack open of drain	0,1	0,1	0,1	1	0,1	0,1	1,E-05	1,E-07	2	1,E-07
3	High Pressure	E	No Cooling Water	0,1	0,1	0,1	1	0,1	0,1	1,E-05	1,E-08	2	1,E-07
4	High Pressure	M	Stack of pressure control valve	0,1	0,1	0,1	1	0,1	1	1,E-04	1,E-06	2	1,E-06
5	Temperatur High	M	Stack of Hot Oil valve	0,1	0,1	0,1	1	0,1	0,01	1,E-06	1,E-06		1,E-06
7	Temperature High	M	Process failure	1	0,1	0,1	0,1	0,1	0,1	1,E-05	1,E-06	2	1,E-07
10	Loss of Valve functions	E	Lack of Intstrument air	0,1	0,1	0,1	0,1	0,1	0,1	1,E-06	1,E-08	2	1,E-08

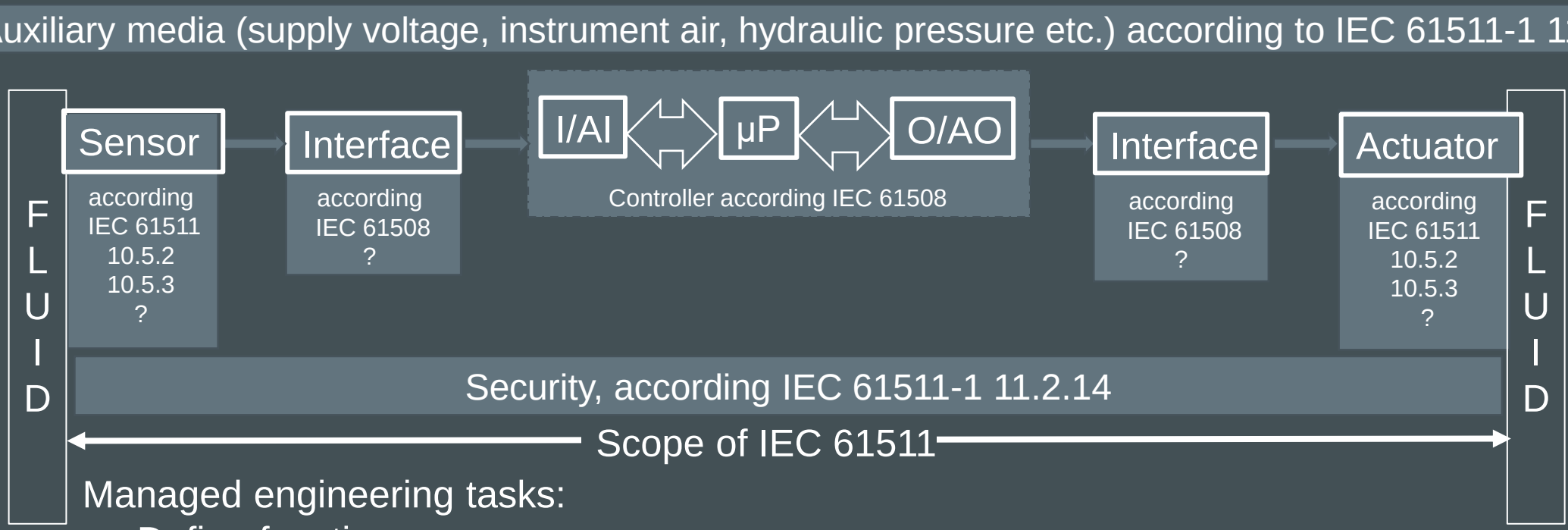
Practical Example: Incl. Safety Functions

Safety Functions needed

- Pressure monitoring
- Temperature monitoring
- Cooling water flow



Safety Engineering as per IEC 61511 ed. 2

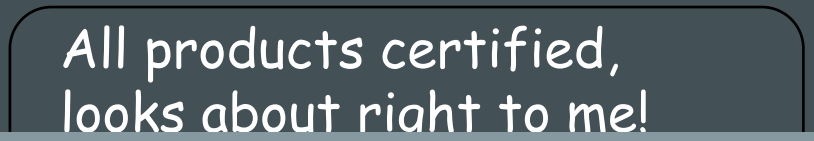


Managed engineering tasks:

- Define function
- Select & qualify equipment
- Select, implement & qualify functions

IEC 61511-1 10.5.2: Selection of devices
IEC 61511-1 10.5.3: Selection of devices based on prior use

Compliant plants by certified products?

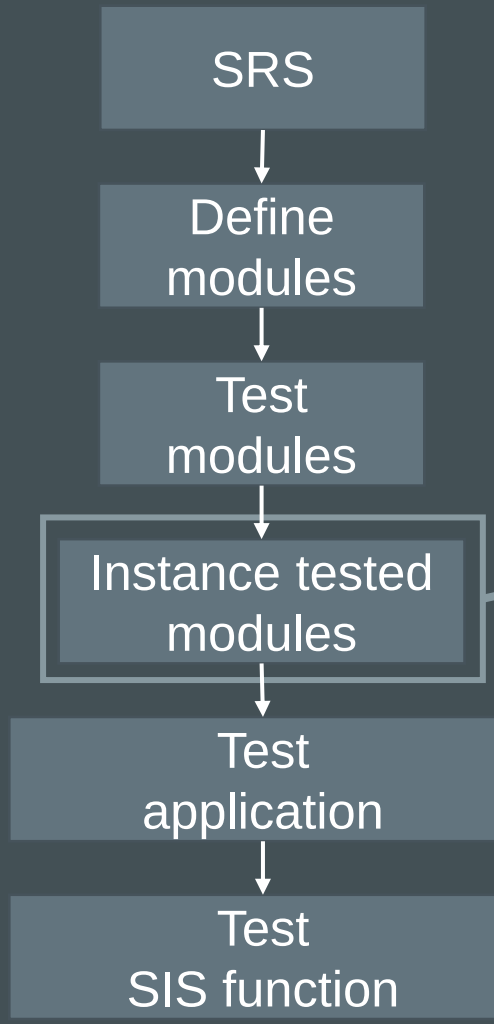


In order to be compliant you need to:

1. Analyze the risk to be mitigated
2. Apply a compliant Design & Engineering process including all recommendations in competency, independence of people involved
3. Test the installation (not just switch it on after installation)
4. Maintain it properly (reliability will drop during operation)
5. Apply an adequate management of change
6. When using certified products, make sure

Thesis: Even if you can prove to use certified products only, You are not compliant nor safe by definition!

Application Software



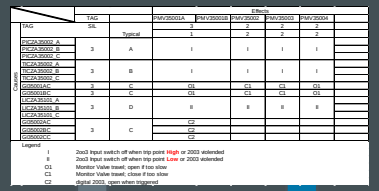
				Effects					
	TAG			PMV35001A	PMV35001B	PMV35002	PMV35003	PMV35004	
Causes	TAG	SIL	Typical	3		2	2	2	
				1		2	2	2	
	PICZA35002_A	3	A	I		I	I	I	
	PICZA35002_B								
	PICZA35002_C								
	TICZA35002_A	3	B	I		I	I	I	
	TICZA35002_B								
	TICZA35002_C								
	GI35001AC	3	C	O1		C1	C1	O1	
	GI35001BC	3	C	O1		C1	C1	O1	
	LICZA35101_A	3	D	II		II	II	II	
	LICZA35101_B								
	LICZA35101_C								
	GI35002AC	3	C	C2					
	GI35002BC			C2					
	GI35002CC			C2					

Legend

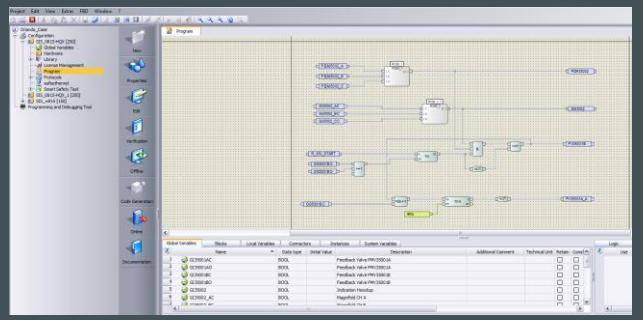
I	2oo3 Input switch off when trip point **High** or 2003 violended
II	2oo3 Input switch off when trip point **Low** or 2003 violended
O1	Monitor Valve travel; open if too slow
C1	Monitor Valve travel; close if too slow
C2	digital 2003, open when triggered

How to Validate Applications

SRS
(IEC 61511-1 10.3.2)

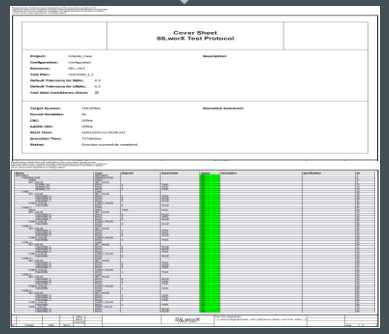


Application Program
(IEC 61511-1 12.1 to 12.3)

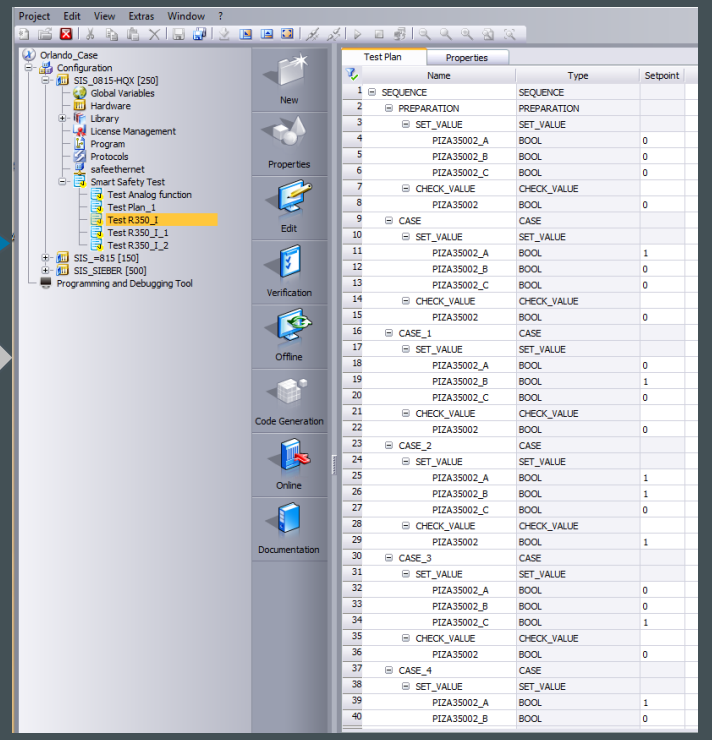


SILworX®

Engineering Tool



Validation Planning
(IEC 61511-1 15.2.2)



Validation Evidence
IEC 61511-1 15.2.4

Performance Monitoring

Chapter 16

Consequences of deviating from designed behavior

More frequent demand of the process

than estimated in the risk analysis

Low demand rate

changes to

high demand rate

Design

e.g. other measures relating to fault tolerance

Operation

e.g. shorter testing intervals

More device failures

than estimated when selecting device

Low reliability

leads to higher

likelihood of failures

Design

e.g. other devices, automated diagnostics

Operation

e.g. shorter testing intervals

IEC 61511 5.2.6.1.9

In cases where a FSA is carried out on a *modification* the assessment shall consider the impact analysis carried out on the proposed modification and confirm that the modification work performed is in compliance with the requirements of IEC 61511.

Thank You.

Peter Sieber
VP Norms and Standards
VP Region China

Phone +49 6202 709-830
+86 21 2051 6308
Mobile +49 172 62 61 518
E-Mail p.sieber@hima.com

HIMA Group
Albert-Bassermann-Str. 28
68782 Brühl, Germany

Phone: +49 (0) 6202 / 709-145
Fax: +49 (0) 6202 / 709-6145

Website: www.hima.com