Functional Safety workshop
Slovnaft a.s.
IEC61508 & IEC61511

Ladislav Nagy

Operations and Functional Safety Manager
FS Engineer (TÜV Rheinland; #3520/11; SIS)
FS Trainer (TÜV Rheinland; #58/2020; SIS)

Version 2023-05-16

Ladislav Nagy

Digitally signed by Ladislav Nagy
Date: 2023.05.16 20:51:26 +02'00'

Purpose

Purpose of this workshop

- To get a basic understanding of functional safety
- For everybody involved in safety projects
- It is a requirement of safety standards: IEC 61508 and IEC 61511
- It is a requirement of Slovnaft a.s. : PROD_PD_SN8

IEC 61508 Ed. 2 part 1, section 6

6.2.3 All persons, departments and organizations responsible for carrying out activities in the applicable overall, E/E/PE system or software safety lifecycle phases (including persons responsible for verification and functional safety assessment and, where relevant, licensing authorities or safety regulatory bodies) shall be identified, and their responsibilities shall be fully and clearly communicated to them.

6.2.12 Those individuals who have responsibility for one or more phases of the overall, E/E/PE system or software safety lifecycles shall, in respect of those phases for which they have responsibility and in accordance with the procedures defined in 6.2.1 to 6.2.11, specify all management and technical activities that are necessary to ensure the achievement, demonstration and maintenance of functional safety of the E/E/PE safety-related systems.

6.2.13 Procedures shall be developed to ensure that all persons with responsibilities defined in accordance with 6.2.1 and 6.2.3 (i.e. including all persons involved in any overall, E/E/PE system or software lifecycle activity, including activities for verification, management of functional safety and functional safety assessment), shall have the appropriate competence (i.e. training, technical knowledge, experience and qualifications) relevant to the specific duties that they have to perform. Such procedures shall include requirements for the refreshing, updating and continued assessment of competence.

6.2.14 The appropriateness of competence shall be considered in relation to the particular application, taking into account all relevant factors.

6.2.15 The competence of all persons with responsibilities defined in accordance with 6.2.1 and 6.2.3 shall be documented.

6.2.16 The activities specified as a result of 6.2.2 to 6.2.15 shall be implemented and monitored.

IEC 61508 Ed. 2 part 1, section 6

6.2.3. All people working in safety must be informed of their responsibility.

6.2.12. Management shall specify all the necessary activities for safety.

6.2.13. Management shall make procedures to make sure all people are competent (including the refreshing and assessing).

6.2.14. Consider responsibility, supervision, failure consequences, SIL, novelty of design and/or application, experience, engineering knowledge, legal knowledge.

6.2.15. People's competence shall be documented.

6.2.16. All the above to be implemented and monitored.

What is safety?

Safety:

"Freedom from risk which is not tolerable"

(IEC 61508 / IEC 61511)

Risk:

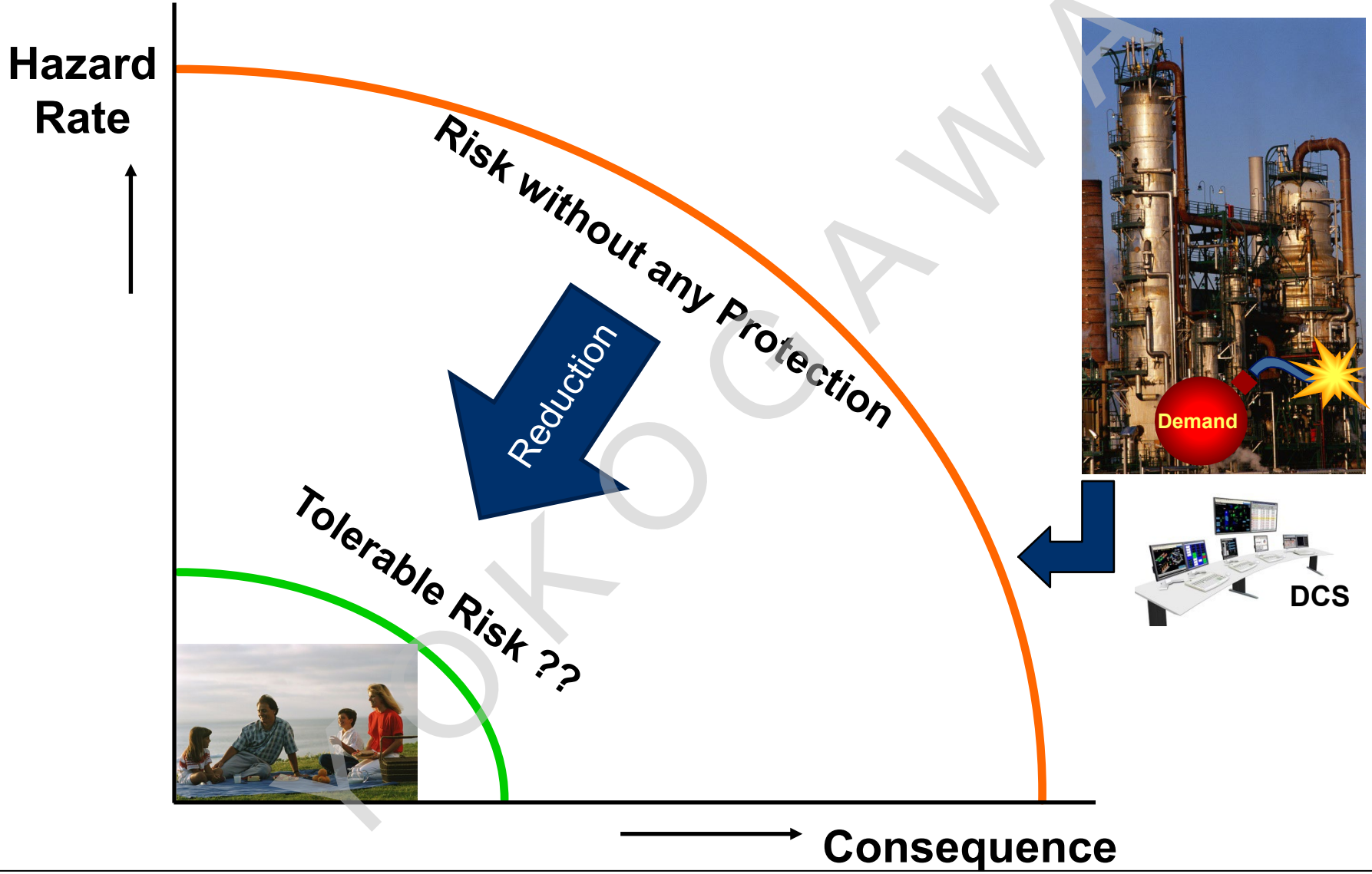
"Combination of the frequency of occurrence of harm and the severity of that harm"

(IEC 61508 / IEC 61511)

Functional Safety :

"part of safety that depends on safety functions implemented in a safety system"

Safety = Risk Reduction



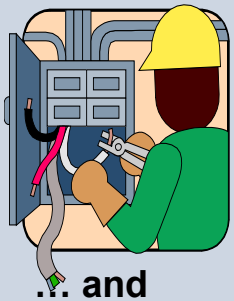
What has to be protected ?

Society

Safety first!

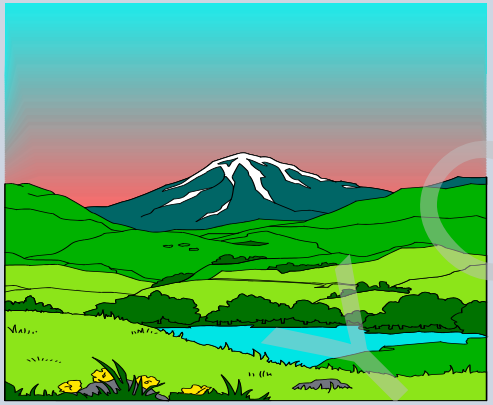
People

Outside plant



... and inside plant

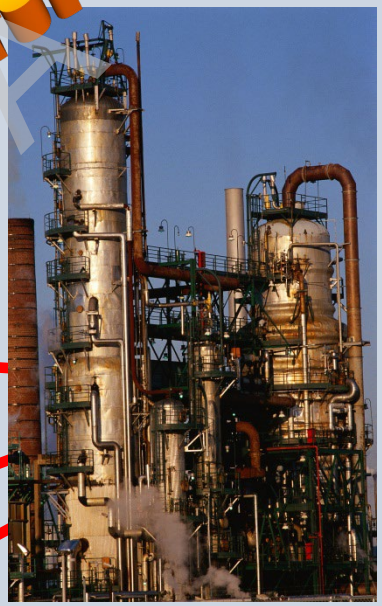
Environment



Plant owner

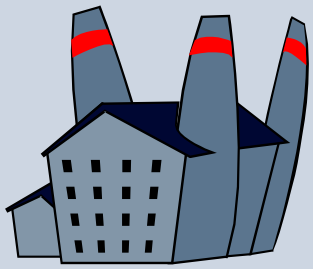
Availability first!

RISK

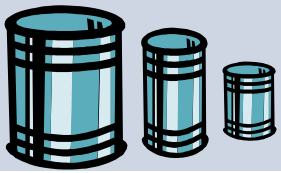


RISK

Assets

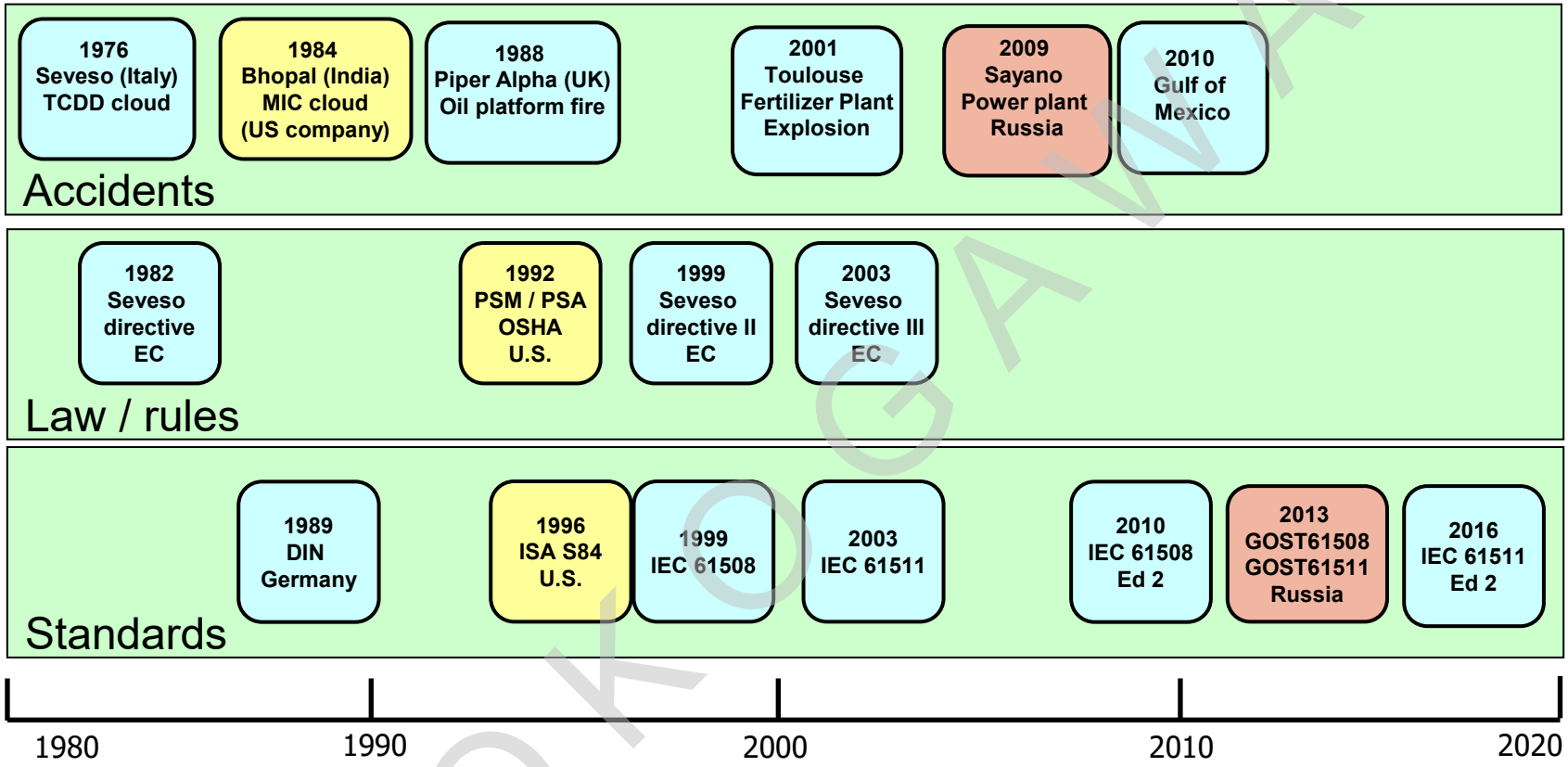


Off-spec production



Corporate image

Evolution of functional safety standards



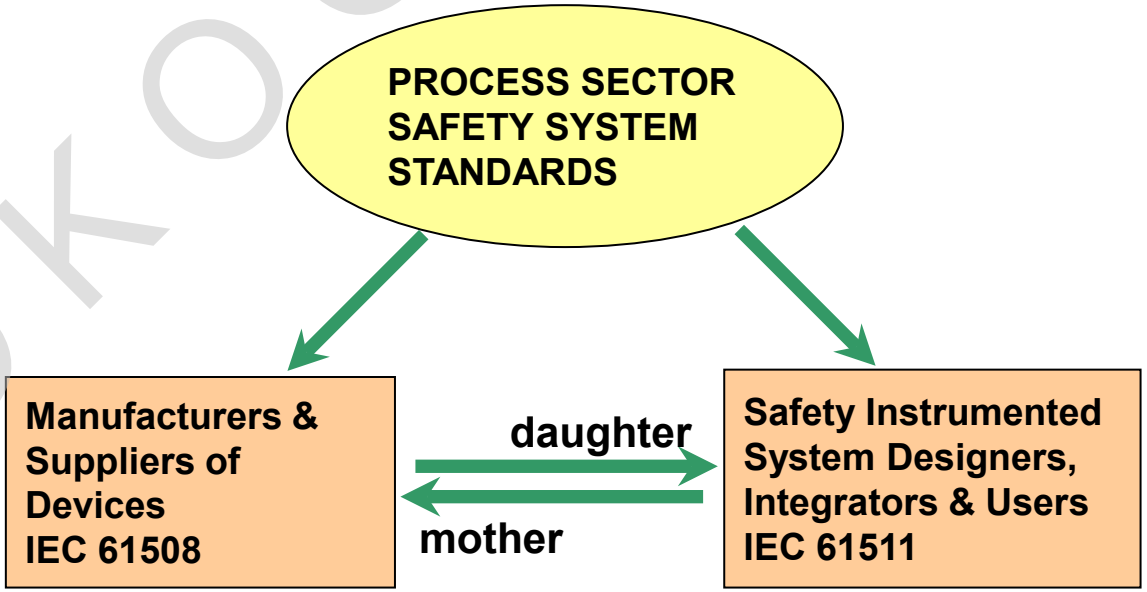
The IEC 61508 / 61511 Standard

IEC 61508 Ed.2 part 1 – 7 (May 2010) : functional safety of electrical / electronic / programmable electronic safety-related systems.

- a generic standard (much attention for development)

IEC 61511 Ed.2 part 1 – 3 (2016) : (ISA 84.00.01 is identical)
functional safety for the process industry

- for the process industry (much attention for the application)



6 most significant aspects of IEC 61508 / 61511

The Safety Lifecycle

The “pipe-to-pipe” approach

The safety calculations

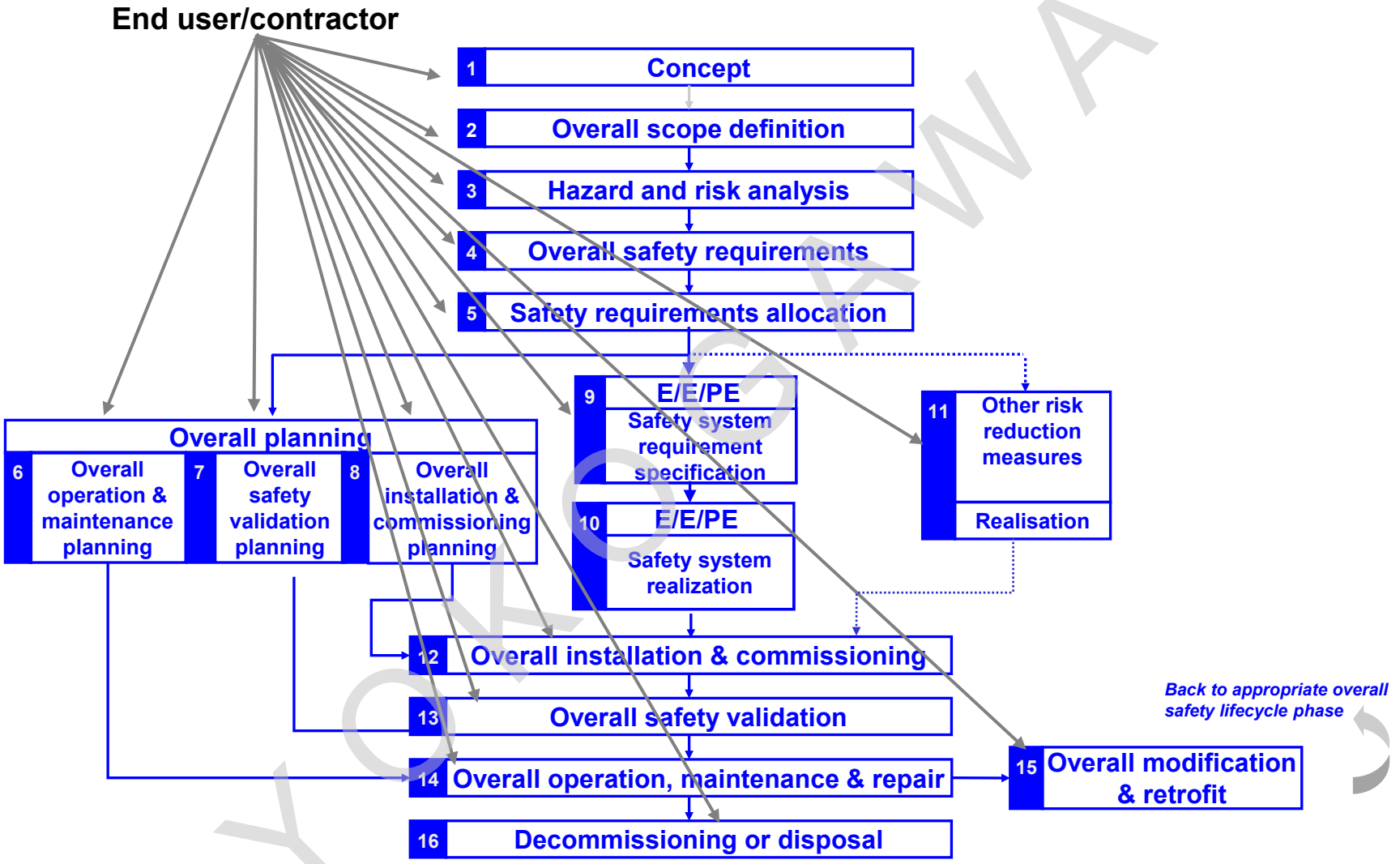
The hardware fault tolerance

The systematic capability

The Functional Safety Management System

All these subjects will be discussed in the next slides.

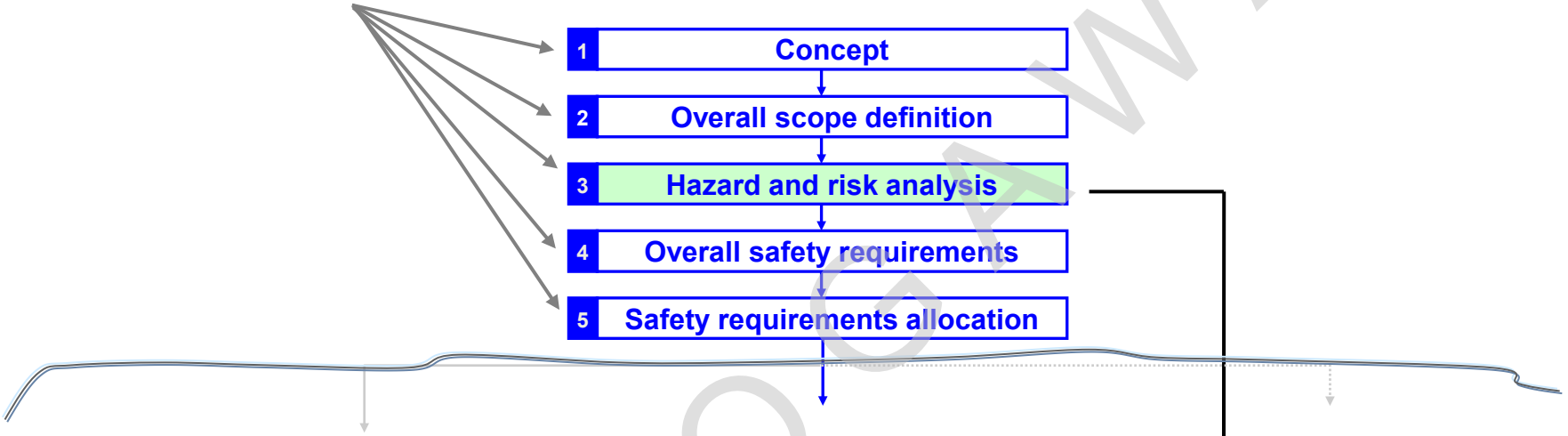
IEC 61508 Overall Safety Lifecycle



The responsibility is split between the designers, integrators and the end user

Hazard Identification

End user/contractor



No method prescribed

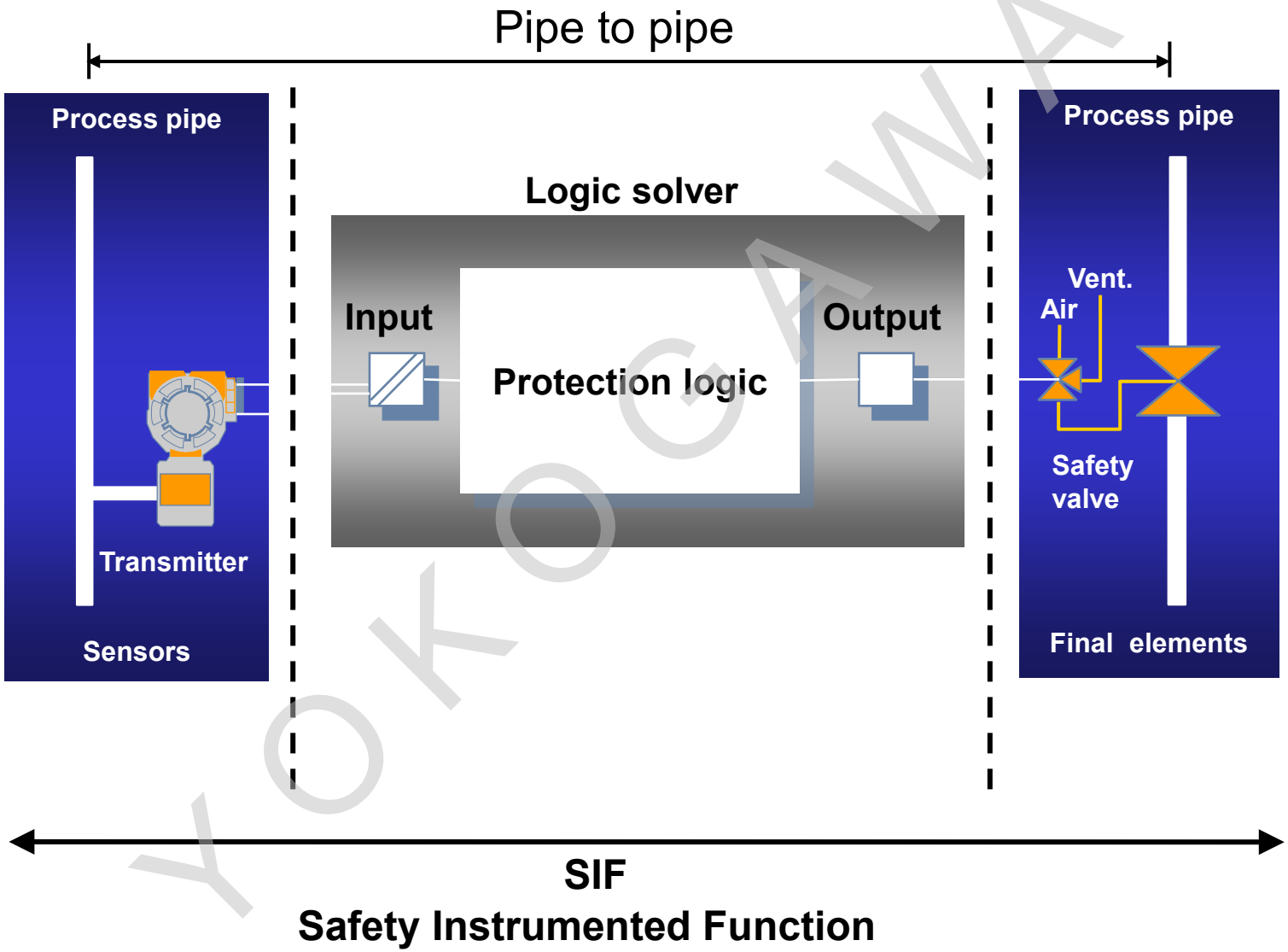
General method : HAZOP
HAZard and OPerability study

Determine target SIL

IEC61508 : part 5 and IEC61511 : part 3

- As Low As Reasonably Practical (ALARP)
- Risk Graph
- Risk Matrix
- Event Tree Analysis (ETA)
- Layers Of Protection Analysis (LOPA)

Pipe to pipe



SIL level definition and the 3 criteria for a SIF to reach a SIL level

- Safety Integrity Level (SIL) : discrete level (one out of a possible four), corresponding to a range of safety integrity values. The highest is 4.

- The safety requirements are specified for each SIF and are expressed in a Safety Integrity Level (SIL), a figure that defines the risk reduction.
  The end-user must determine the SIFs.

- The target SIL indicates
  - the maximum average Probability of Failure on Demand (PFDavg) that the SIF may have.
  - the minimum Hardware Fault Tolerance (HFT)
  - the minimum Systematic Capability (SC)

- **Note:** PFDavg is for low demand mode (demand rate less than once per year). This is the case for Emergency Shutdown Systems, Emergency brake of a train, Airbag…

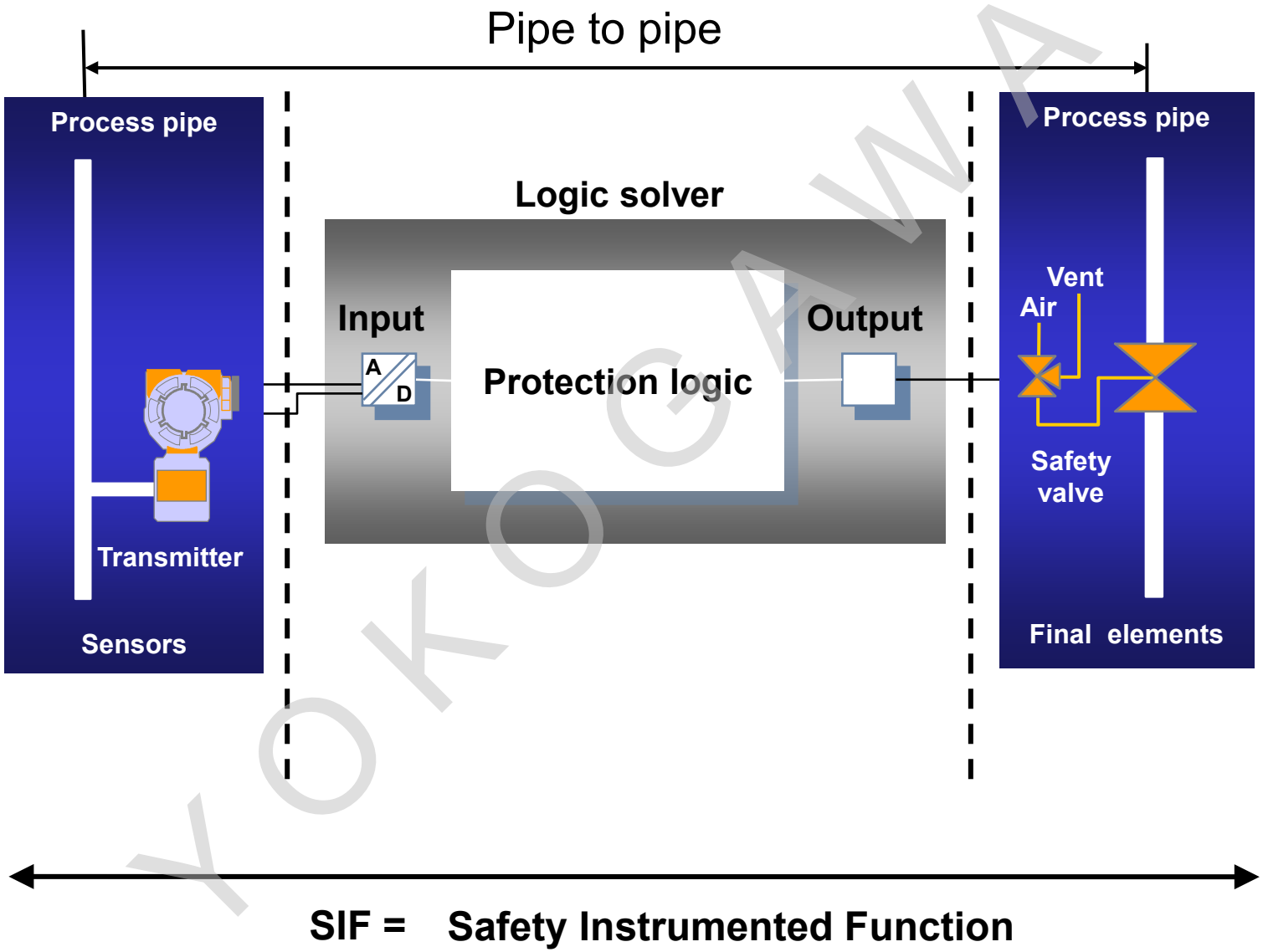
SIL, PFDavg and Risk Reduction

- The target SIL indicates the maximum average Probability of Failure on Demand (PFDavg) that the SIF may have.

- We need to calculate and demonstrate that each SIF meets its target SIL.
  (SIL achieved ≥ SIL target)

Safety Integrity Level	Average Probability of Failure on Demand (PFD_{AVG})	Risk Reduction Factor (RRF) ($=1/PFD_{AVG}$)
4	$\geq 10^{-5}$ to $< 10^{-4}$	>10 000 to ≤ 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	>1 000 to ≤ 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	>100 to ≤ 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	>10 to ≤ 100
	IEC 61508-1 table 2	IEC 61511-1 table 4

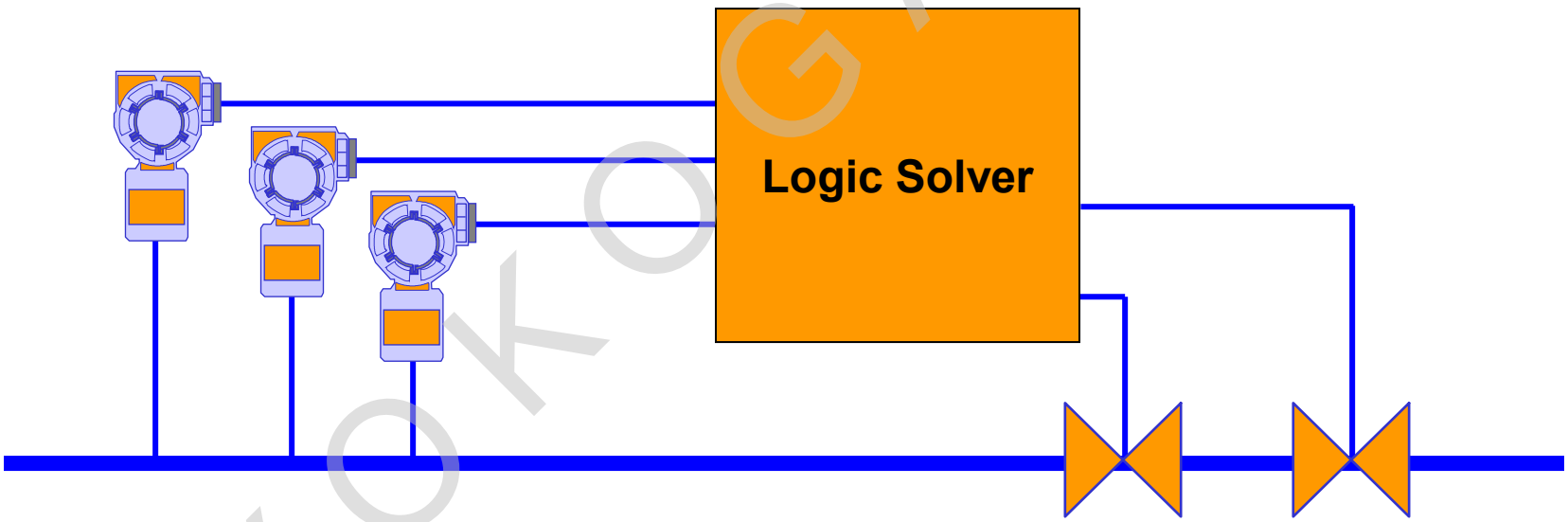
Pipe to pipe



SIF = Safety Instrumented Function

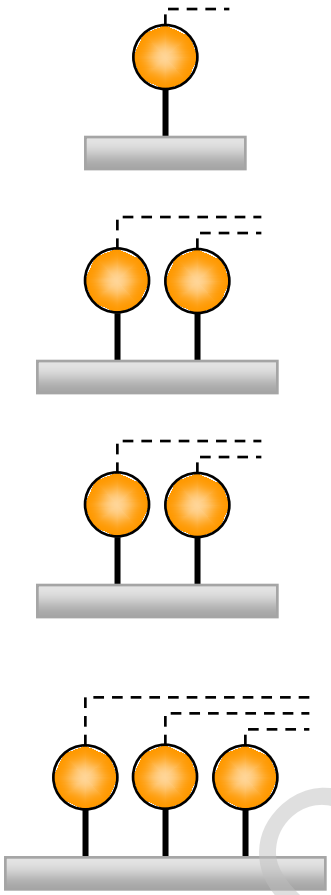
Hardware fault tolerance

The target SIL indicates the maximum PFD_{AVG} but also depending on type and quality of the used device double / triple devices (1oo2, 1oo3) might be required



There are tables in both standards

Redundancy for sensors



1oo1

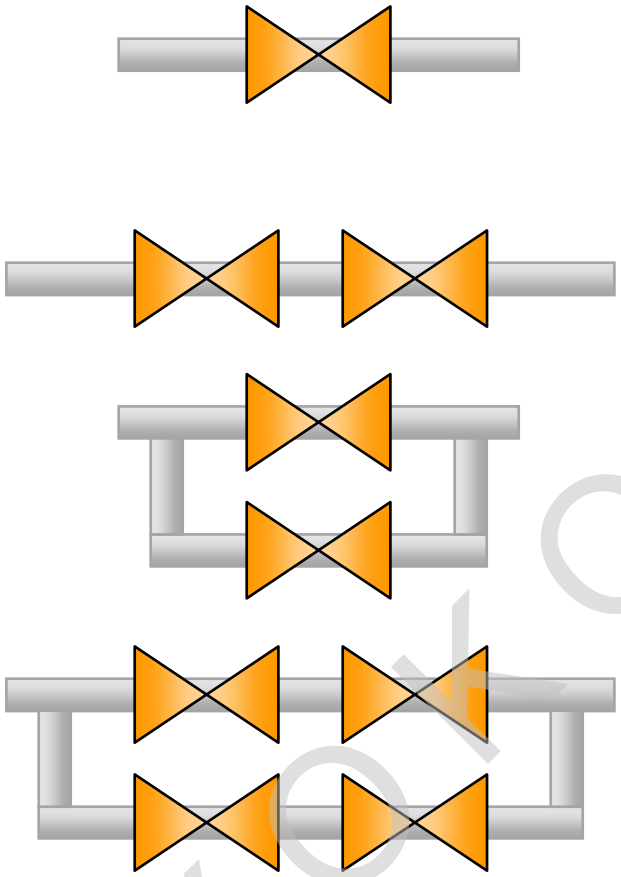
1oo2 — ***Better Safety***

2oo2 — ***Better Availability***

1oo3 — ***Even better Safety (but higher false trip rate)***

2oo3 — ***Good combination : better Safety AND better Availability***

Redundancy for final elements (DTS)



1oo1

1oo2

Better Safety

2oo2

Better Availability

2 x 1oo2

Good combination :
better Safety AND better Availability
(but very expensive)

Systematic Capability

Measure of the quality of the manufacturer's organization and Functional Safety Management system.

It is expressed as SC1 to SC4

The Systematic Capability must correspond with the target SIL.

1. For all procured devices in the SIF:

   Declaration of manufacturer is needed
   (or from certification body)

2. For the realisation in Yokogawa offices (design, implementation, test, project management):

   Systematic Capability is SC3 because FSM is applied

Functional Safety Management System

Functional Safety Management aims to reduce or avoid systematic failures.

Most important for Safety Projects is to make sure that all steps of the lifecycle are really executed.
For this there is a special quality system, the Functional Safety Management (FSM). You may think of it as a “super ISO 9001”.

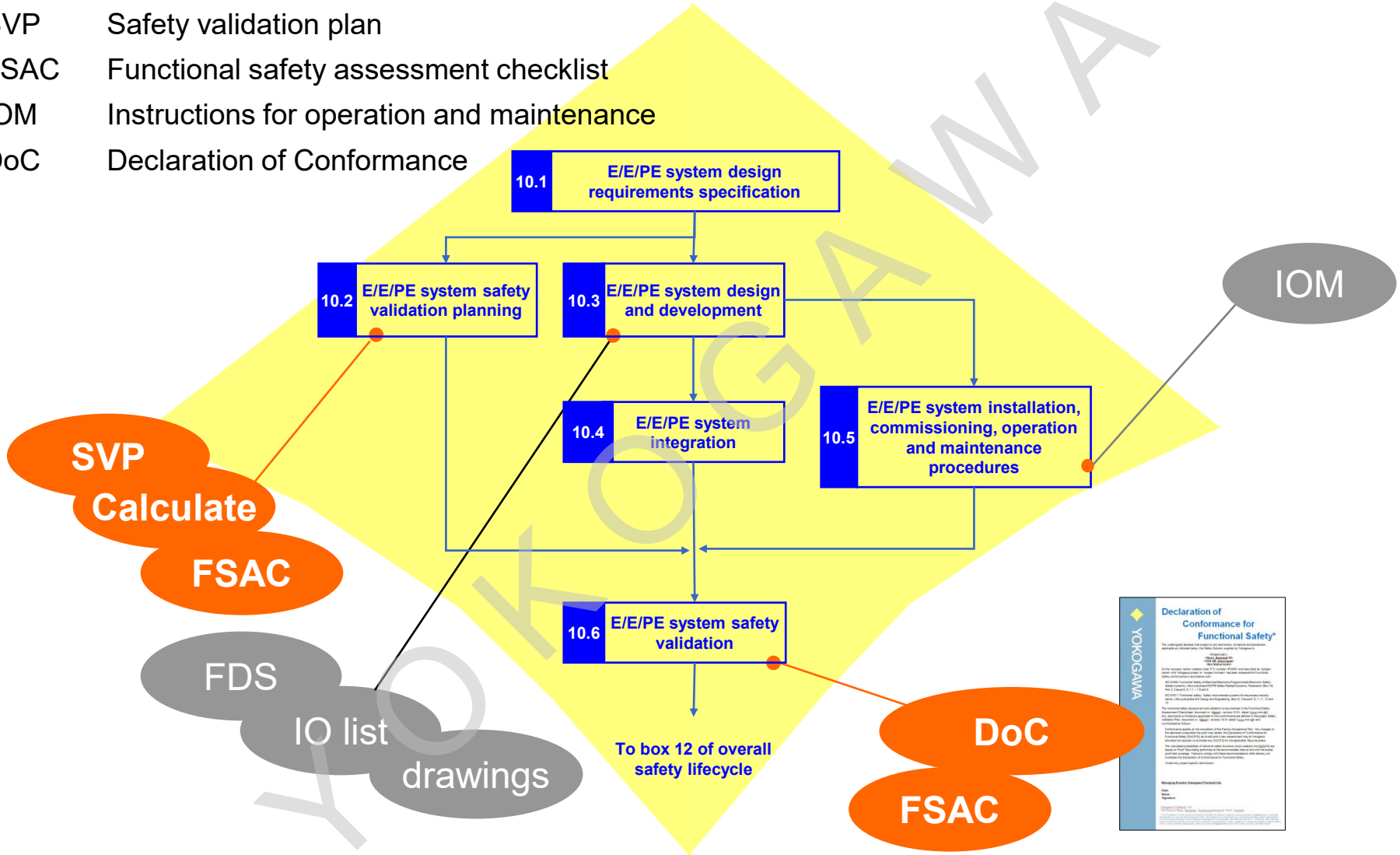
WHY ? Functional Safety Management aims to reduce or avoid systematic failures and consequently increase the systematic safety integrity.

HOW ?
Employ competent personnel
Plan the actions and execute them
Use adequate procedures, tools and templates
Verify / review thoroughly by another person
Verify / test thoroughly by another person
Record and document the plan and the execution of all steps
Validate

WHO ? End-user, Contractor, SIS supplier

Project Management in the SIS Realisation phase

SVP	Safety validation plan
FSAC	Functional safety assessment checklist
IOM	Instructions for operation and maintenance
DoC	Declaration of Conformance



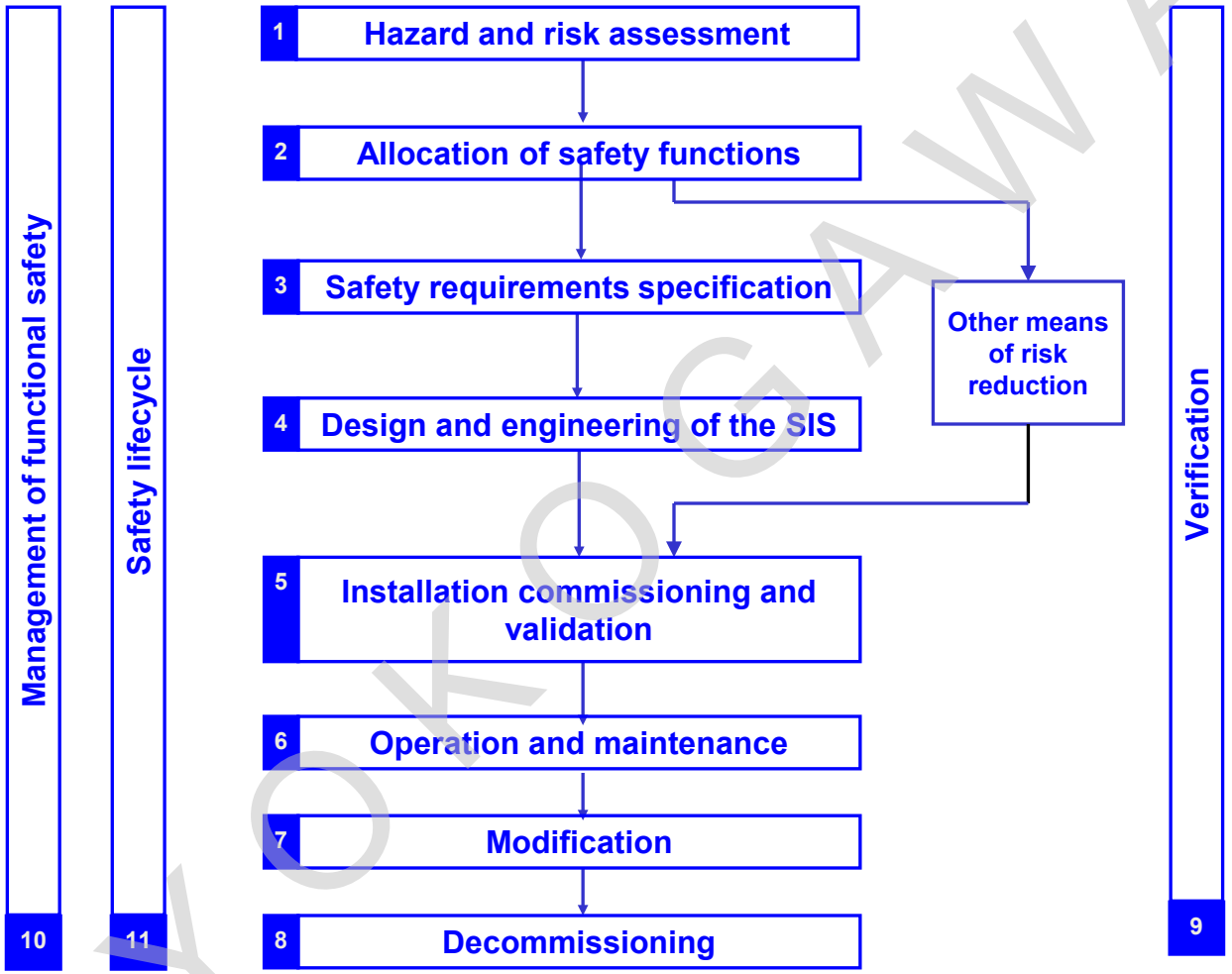
End-User Safety training program

- Functional Safety for Engineering (a.k.a. TÜV Rheinland FS Engineer)
  - Certificate: TÜV Rheinland - FS Engineer SIS
  - 3 days training + 4 hours examination

- Functional Safety for Operations (a.k.a. TÜV Rheinland FS Technician)
  - Certificate: TÜV Rheinland - FS Technician SIS
  - 2 days training + 3 hours examination

- Functional Safety for End-Users
  - Introduction on functional safety (IEC 61508 / IEC 61511)
  - For End-users
  - 2 days

IEC 61511 Overall Safety Lifecycle



source: IEC 61511-1 fig. 8

Co-innovating tomorrow™