Functional Safety Activities (1)

ALBA – CERN workshop

Borja Fernández Adiego BE/ICS

Functional safety in ICS

- 2 different teams performing Functional Safety solutions:
  - **Process control & safety** (*Thursday afternoon module of the workshop*)

    Agenda
    - Introduction: standards and SIL (just some tips)
    - Examples of SISs
    - SIS specification and development
    - SIL compliance

  - **Personnel safety, access control** (*Friday morning module of the workshop*)

Process control and safety

- Functional safety activities following the IEC 61508 and IEC 61511 standards *(a bit of IEC 62061)*
- **IEC 61508**: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems
- **IEC 61511**: specific for the process industry
- *IEC 62061: specific for the machinery industry*
- SIL (Safety Integrity Level) concept:
  - **Not only about hardware random failures** (PFD or PFH)
  - Hardware safety integrity (random failures & Architectural constrains)
  - Systematic safety integrity

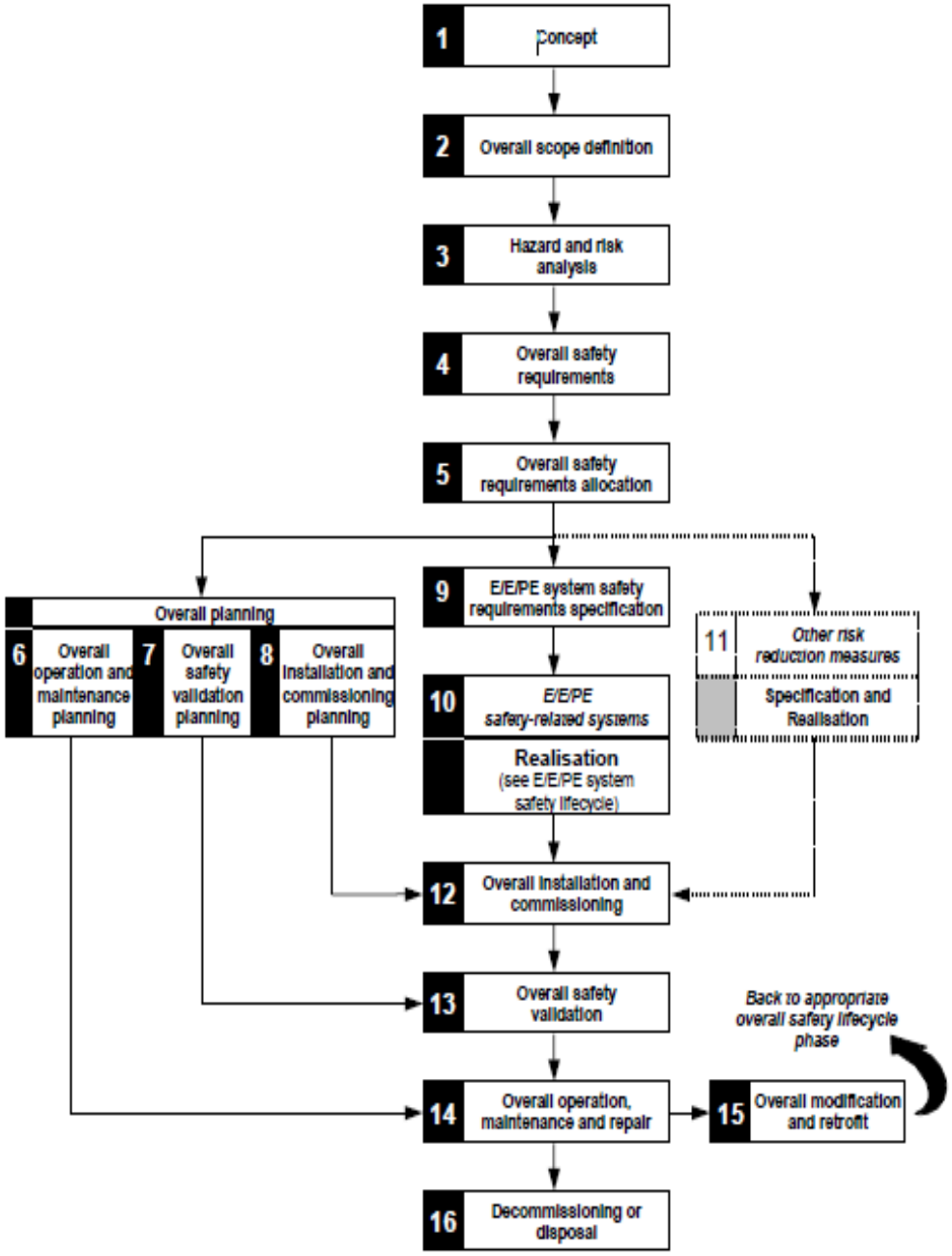
Safety Integrity Level	Demand Mode of Operation (average probability of failure to perform its design function on demand - PFD)	Continuous / High Demand Mode of Operation (probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

IEC 61508 safety lifecycle

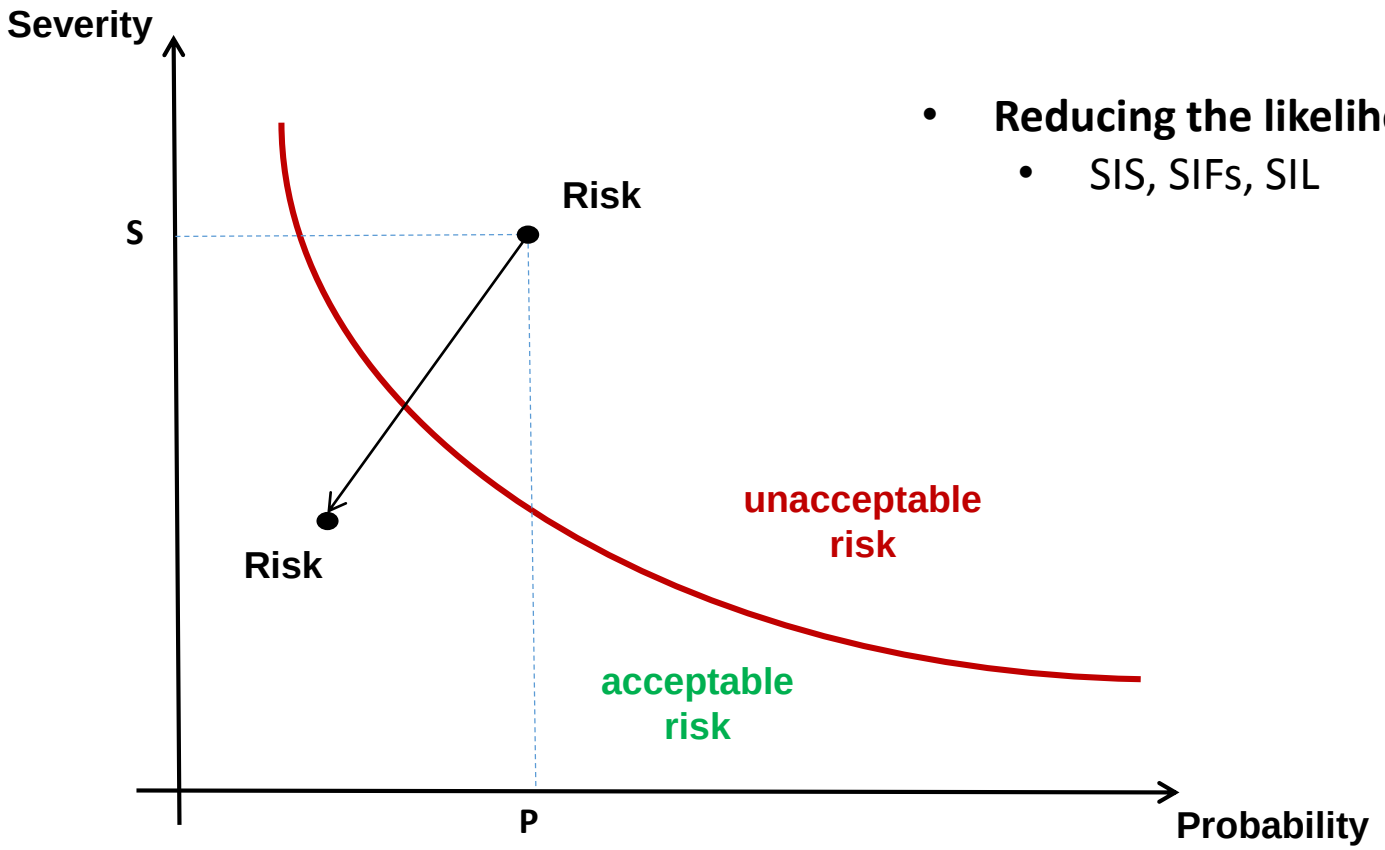
1. **Analysis**
   - Risk analysis
   - Safety Instrumented Functions definitions

2. **Realization**
   - Implementation of the Safety Instrumented System
   - Steps to prove the SIL of one SIF

3. Commissioning, operation and management of the SISs

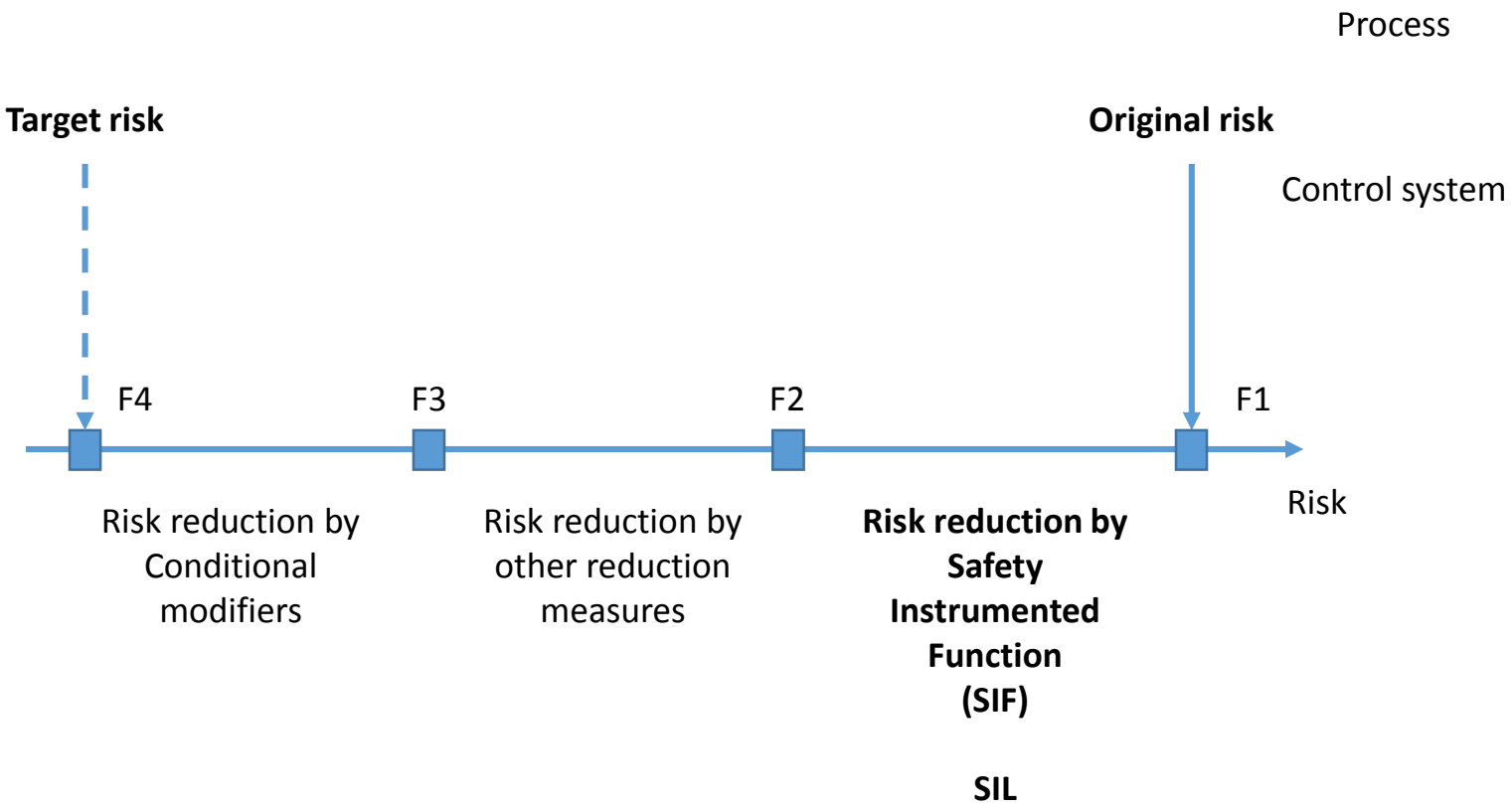


How can we reduce the risk?



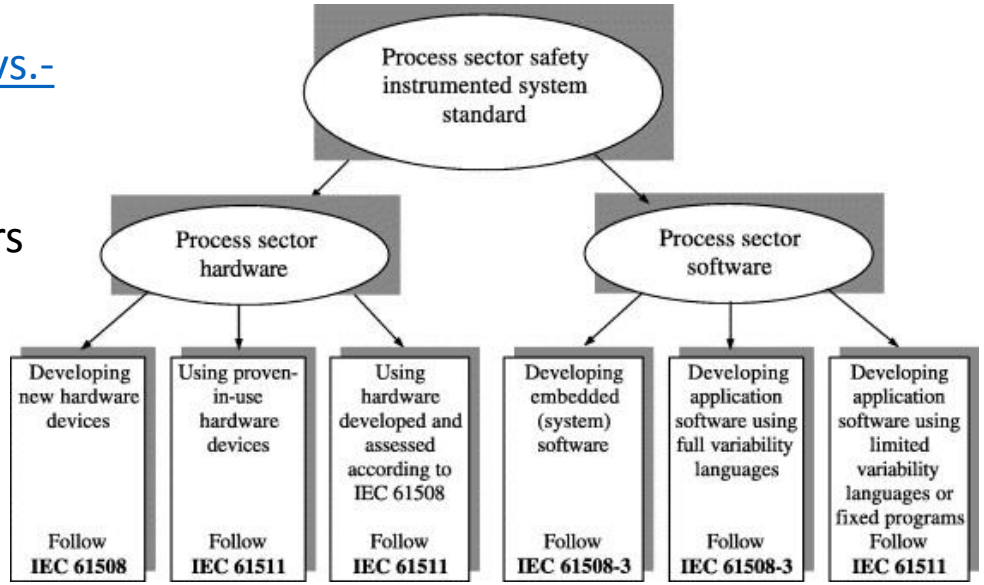
- Reducing the severity of the consequence
- **Reducing the likelihood** of the consequence
  - SIS, SIFs, SIL

How can we reduce **the likelihood** of the risk?



Differences between IEC 61508 and IEC 61511

- http://www.exida.com/Blog/functional-safety-standards-iec-61508-vs.-iec-61511
- IEC 61508 is a generic standard and useful for various industry sectors
- But some parts of the realization phase are applicable to equipment manufacturers
- IEC 61511 is user focused
- **They both have same lifecycle and SIL concepts**, but 61511 has a more specific language and context



IEC 61508	IEC 61511
Safety-related system	Safety Instrumented system (SIS)
Safety Function	Safety Instrumented Function (SIF)
EUC	Process
EUC control system	BPCS