Blowout Preventer Functional Safety Requirements; a discussion on the application of IEC 61508, IEC 61511 and OLF GL 070

Rhodri Morgan, Crystal James
DNV GL

So what is functional safety?

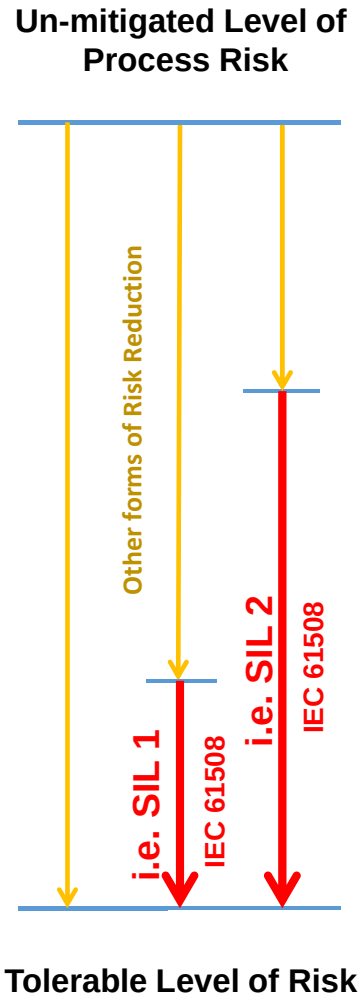
'An Autonomous means of Risk Reduction implemented by an Electrical/Electronic/Programmable Electronic Safety (E/E/PES) Instrumented System which performs a defined Safety Function in order to demonstrate that a risk acceptance criteria is met.'

Safety Instrumented Function (SIF) – A single safety function that protects against a single dangerous event, such as High Pressure.

Safety Instrumented System (SIS) – A system used to implement one or more SIF. A SIS is more than just the PLC, it includes the valves and the instrumentation.

Risk Reduction Factor (RRF)	Probability of failure on demand (PFD) for low demand	Average frequency of dangerous failure, hr^{-1} (PFH) for high/continuous demand	SIL
10^4 to 10^5	10^{-5} to 10^{-4}	10^{-9} to 10^{-8}	4
10^3 to 10^4	10^{-4} to 10^{-3}	10^{-8} to 10^{-7}	3
10^2 to 10^3	10^{-3} to 10^{-2}	10^{-7} to 10^{-6}	2
10^1 to 10^2	10^{-2} to 10^{-1}	10^{-6} to 10^{-5}	1

A process with a SIL 2 SIF will be up to 1,000 times more dangerous if the SIF is not implemented correctly.



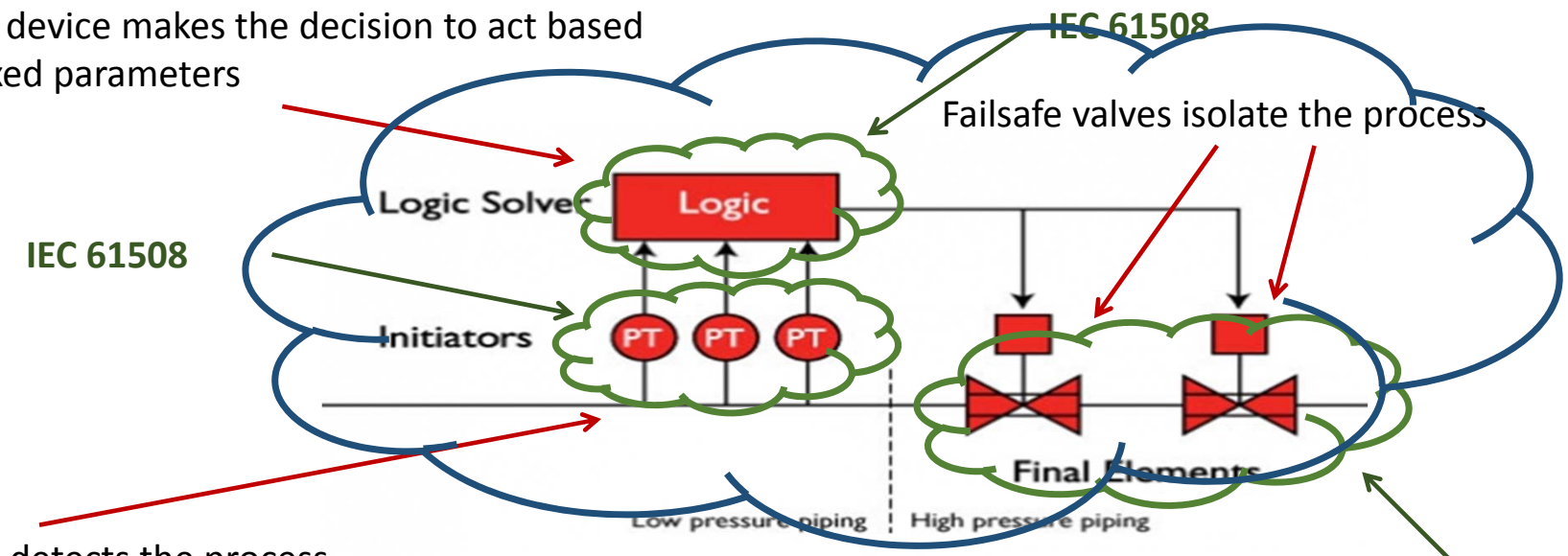
But SIL is more than just a number…

Quantitative Requirements	Semi- Quantitative Requirements	Software Requirements	Qualitative Requirements
Probability of Failure on Demand (PFD)	**Architectural Constraints** • Safe Failure Fractions (SFF) • Hardware Fault Tolerance (HFT) • Type A or Type B subsystems	**Software Safety Functions** • V-Model • Certified blocks • Software assurance processes	**Avoidance and control of Systematic Failures** • Functional Safety Management Plan

SIL

How do the standards fit together?

A typical application of a safety instrumented system for pressure protection:



What standards applies to a BOP?

- Three documents are normally referred to when discussing BOPs

IEC 61508, Functional safety of electrical/electronic/ programmable electronic safety-related systems

Manufacturers' standard

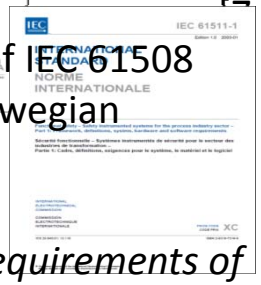
-- Applicable for development of new devices

IEC 61508 (ed.2, 2010)

IEC 61511 Functional safety of safety instrumented systems for the process industry sector

IEC 61511

[7 parts]



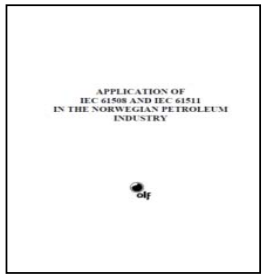
Engineering and end users' standard

-- Applicable for development of systems that are based on IEC 61508 approved or proven in use devices

OLF GL-070 Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry

-- an interpretation the requirements of IEC 61508 and IEC 61511 and guidelines on their implementation on the Norwegian Continental Shelf

OLF GL 070 [3 parts]



[1 part]

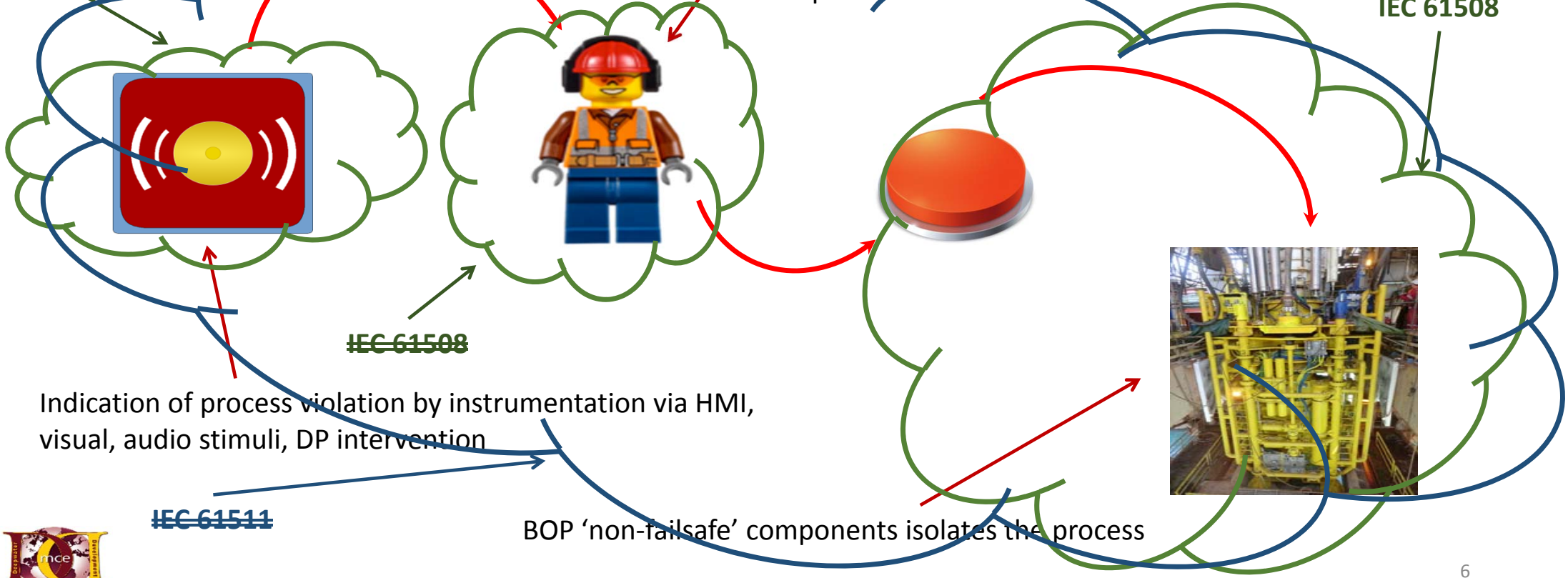
Applying the standards to a BOP

A typical application of a safety instrumented system for blow out preventers?

~~IEC 61508~~

Operator makes the decision based upon training and experience

IEC 61508



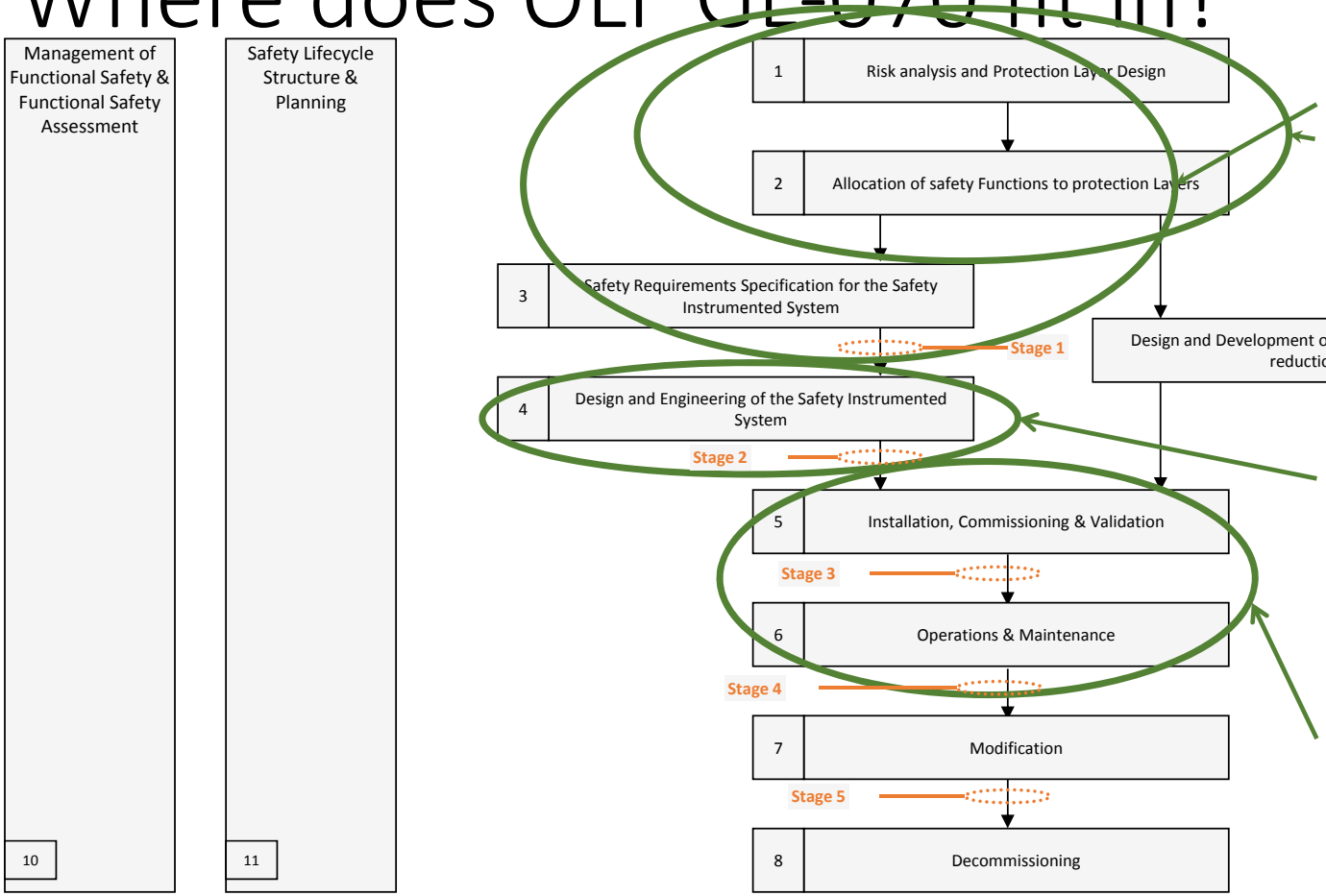
~~IEC 61508~~

Indication of process violation by instrumentation via HMI, visual, audio stimuli, DP intervention

~~IEC 61511~~

BOP 'non-failsafe' components isolates the process

Where does OLF GL-070 fit in?



Stage 1
OLF GL-070
Hazard and Risk Identification
&
Safety Requirement Specification
Removes the need to perform phases 1 and 2. SIL targets are pre-determined

Stage 2
Design of the System

Stage 3
Installation, Commissioning and Validation
&
Operation and Maintenance

OLF GL-070 functional safety requirements

- Drilling related SIFs?
  - **Drilling BOP function**

    Explicit SIL requirements

  - **Well Intervention BOP function**
  - **Kick detection function**
  - **Mud circulation function**
  - **Kill function**
  - **Marine Drilling Riser – Anti Recoil function**
  - **Lifting, Rotation and Pipe Handling**

    Not recommended to set minimum SIL requirement

  - **Marine Drilling Riser – Emergency Disconnect function**

    Minimum SIL level of SIL 2

OLF GL-070 functional safety requirements

- The OLF defines the BOP Safety Functions and defines the safety analysis as a mechanism to demonstrate the achieved SIL:

Table 7.1 cont. Minimum SIL requirements – drilling related safety functions

Safety function	SIL	Functional boundaries for given SIL requirement / comments	Ref. APP. A
Drilling BOP function	2	Annular/pipe ram function [1)]	A.14.2
Closing of relevant BOP valve(s) in order to prevent blowout and/or well leak	2	Blind shear ram function [1)]	A.14.2

1) The total safety functions include activation from the drillers console or the tool pushers console and the remotely operated valves needed to close the BOP sufficiently to prevent blowout and/or well leak.

- Section A.14 describes the drilling related safety functions:
  - **Prevention of blowouts and prevention of well leaks.**
- The SIL is estimated from one method involving the estimated kick frequency and a second involving historic reliability data.

Functions for the BOP

- Safety function typically includes activation from the DCP or TCP and the remote operated valves needed to close the BOP sufficiently so as not to lead to a blowout.
- Functions for the BOP:
  1. Seal around drill pipe
  2. Seal an open hole
  3. Shear drill pipe and seal off well

  2. and 3. are often combined

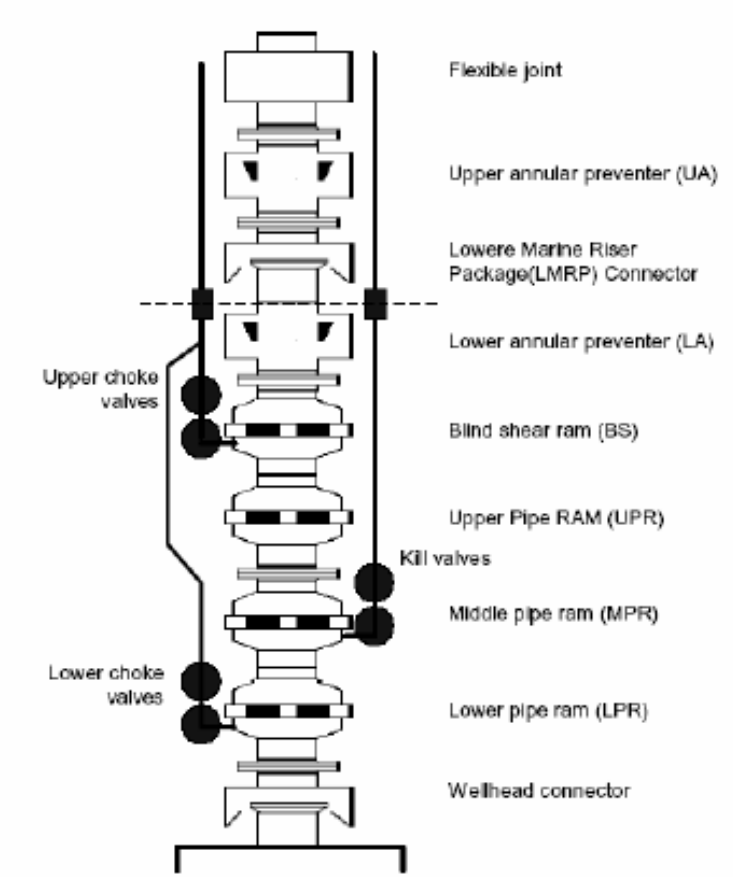
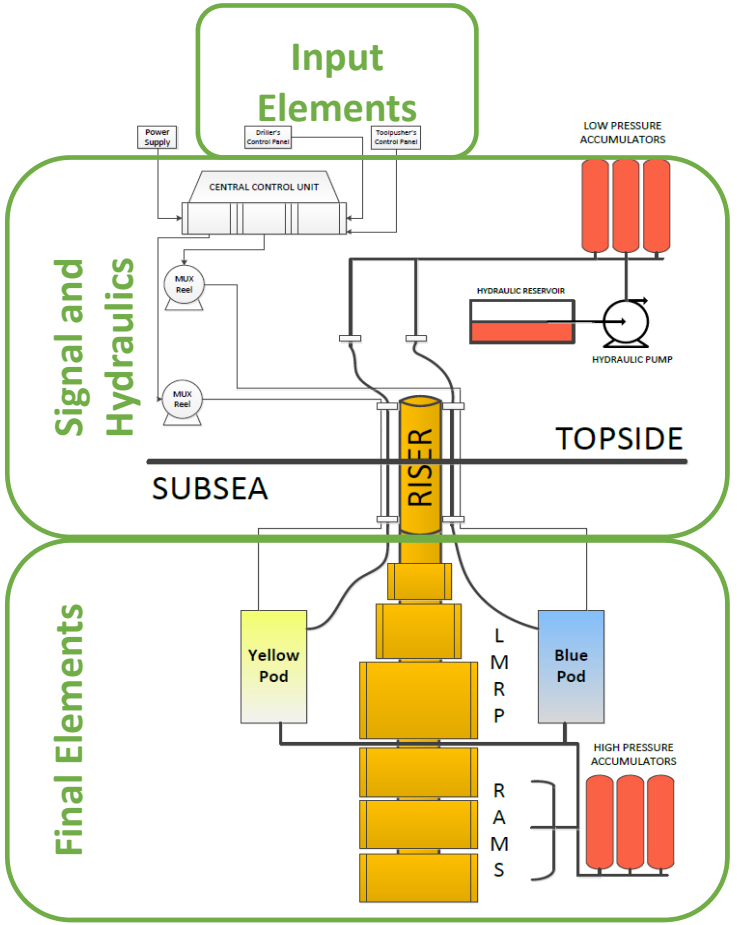


Figure A.22 in OLF

Boundaries for the BOP

- Functional boundaries of the BOP:
  - The panels necessary to activate the function
  - The signal transmission and hydraulics necessary
  - The individual valves and equipment of the BOP



Source unknown

IEC 61508/61511, OLF and actual operations

- IEC 61508/61511 written for autonomous systems.
  - Redundant systems are not able to be considered as part of the analysis.
- OLF allows for operator activation from DCP or TCP.
  - The OLF discusses the operator actions as part of the SIF
- However, operations may not allow activation from various initiation points.
  - The TCP may not be permanently manned.

IEC 61508/61511, OLF and actual operations

- Accepted practice to use HMI based operator stations
  - OLF does not allow activation from a HMI alone.
  - HMIs compliant to IEC 61508 are uncommon.
- Reliability of the operator as an initiating element not included
- IEC 61508/61511 do not allow for operators to be used as diagnostics
  - The blue and yellow pods cannot be considered as redundant
  - No credit can be given for operator intervention in the safety function
- Maintenance and testing requirements are based on prescriptive requirements.
  - D-010 and API 53 are often used as a basis for maintenance activities.
  - IEC 61511/61508 expect maintenance based on test coverage and PFD

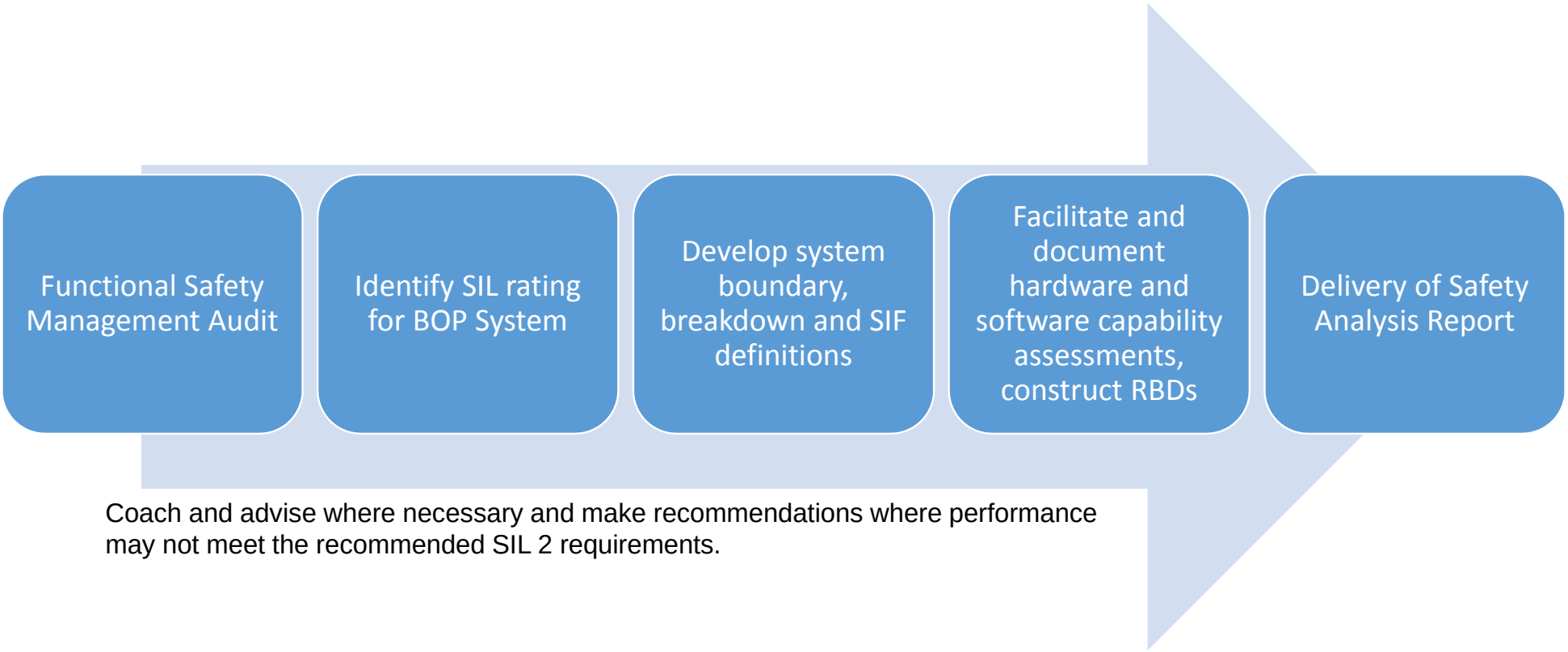
Summary

- Removing the operator as a diagnostic element would improve the SIL achieved by the system.
- Important layers of protection considered are not considered and may lead to an under-estimation of the available level of risk reduction.
  - Manual control.
  - Autoshear/HP Module.
  - Acoustic Safety System.
- However the human plays a critical element in the safety function and as such is a possible common weak line.

Summary

- Current standards are not a perfect fit for BOPs.
- OLF-070 use of a prescriptive requirement is not a bad approach
  - The SIL level prescribed should be based on the risk or consequence and not historical reliability.
  - The requirements should take account of other layers of protection
- A common boundary for the SIF that reflect industry practice should be established.
- A common interpretation of the SIF should be developed.
  - Would a standard Safety Requirements Specification help?
- Reliability data sources.

SAR Methodology



Coach and advise where necessary and make recommendations where performance may not meet the recommended SIL 2 requirements.

SAR definition in the OLF

- Document to show compliance with requirements given in the SRS
  - Any updates after the SAR needs to be documented in the SRS to ensure compliance with SRS requirements
- SAR Example:

I Abbreviations
II References
III Summary

1. Introduction
2. System Description
3. System Topology and Block Diagram
4. Operational description of the system (including modes of operation)
5. List of all assumptions
6. Failure rate of the components
7. Common Cause failures
8. Diagnostic Coverage & Safe Failure Fraction
9. Behaviour of system/components on detection of a fault
10. Factory testing
11. Operational testing (incl. test procedures and recommended functional test interval)
12. Architectural Constraints
13. Avoidance and Control of Systematic Failures
14. Software documentation
15. Results

Appendices
E.g. Certificates, test documentation, FMECA, Failure reports.