NTNU | Kunnskap for en bedre verden

What can we learn from others? Introducing GL 070

Oil and gas industry

PiperAlpha 1988

Professor Mary Ann Lundteigen | institutt for teknisk kybernetikk
E-mail: Mary.a.lundteigen@ntnu.no

SFI• AUTOSHIP
Autonomous ships

Topics covered

- Overview of GL 070 (Norwegian Oil and Gas)
- Meaning of SIL – safety integrity level
- Meaning of Minimum SIL requirements
    - How they are established
    - How they are used
- Thoughts on the relevance for autonomous waterbuses

Background: Guideline NOROG 070

070 – NORWEGIAN OIL AND GAS

APPLICATION OF
IEC 61508 AND IEC 61511
IN THE NORWEGIAN PETROLEUM
INDUSTRY
(Recommended SIL requirements)

Norsk olje&gass

1. Edition 2001
2. Edition 2004
3. Edition 2016
4. Edition 2020

- Developed as joint industry project
- Aim: Simplify the adaption key standards on design and operation of electronic and programmable safety systems.
- Agree on best practices for the standards' requirements on:
  - Planning and life cycle activities
  - Risk-based analyses
  - Documentation
  - Follow-up in operational phase
  - Interpretation of independence
- Preserve well established safety design philosophies with minimum SIL requirements ("equivalence principle")
- Referenced by Petroleum Safety Authority

What is safety integrity level (SIL)?

- Safety performance measure for safety functions that rely on sensors, controllers, actuators,…
- Introduced in IEC 61508
- Four levels (SIL 1 to SIL 4)

SIL has two implications:

- Defines range for failure measures (makes the link to risk acceptance)
- Defines rules that frame design and operation/maintenance
  - Work processes
  - Competences and roles
  - Safe design principles
  - Software program development
  - Data collection and analysis
  - ….

SIL	PFD - failure probability
4	≤ 0.01%
3	≤ 0.1%
2	≤ 1%
1	≤ 10%

SIL table in IEC 61508

Minimum SIL requirements

- Benchmark concept coined by GL 070
- Predefined SIL requirements (1-4) for typical/ commonly used safety functions (“achieving functional goals”)
- Why?
  - A wish to preserve good engineering practice – despite the use of risk-based approaches (“standardize where possible“)
  - Avoid that risk-based approaches are used to justify lower safety levels than in the past

Focus of next slides

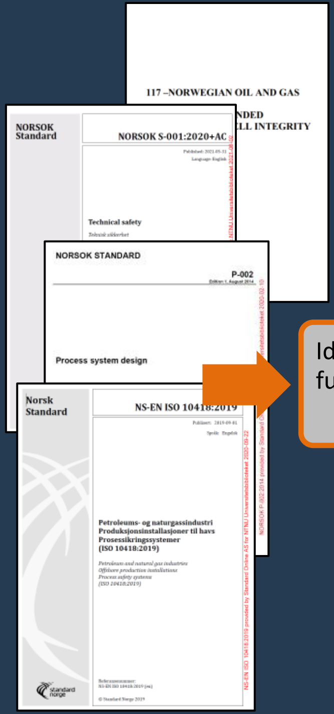
1. Explain how minimum SIL requirements have been *developed*

   (“As benchmarks in GL 070”)

2. Explain how minimum SIL requirements are *used*

   («When designing a new system»)

Developing minimum SIL requirements



117 –NORWEGIAN OIL AND GAS

NDED
LL INTEGRITY

NORSOK Standard

NORSOK S-001:2020+AC

Technical safety

Teknisk sikkerhet

NORSOK STANDARD

P-002

Process system design

Norsk Standard

NS-EN ISO 10418:2019

Petroleums- og naturgassindustri
Produksjonsinstallasjoner til havs
Prosessikringssystemer
(ISO 10418:2019)

Petroleum and natural gas industries
Offshore production installations
Process safety systems
(ISO 10418:2019)

Identify typical safety functions

- Standards
- Regulations
- Best practices

PDS DATA HANDBOOK – 2021 EDITION

Reliability Data
for Safety Equipment

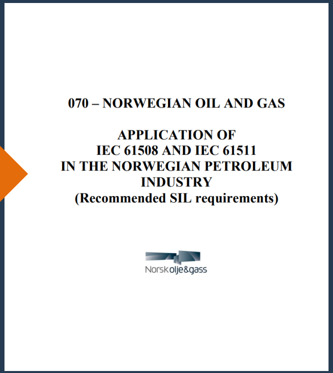
SINTEF

Estimation of historical safety level

- Reliability data
- Failure statistics
- Assumptions

Agree on safety level → minimum SIL req.

- Uncertainty
- Continuous improvement



070 – NORWEGIAN OIL AND GAS

APPLICATION OF
IEC 61508 AND IEC 61511
IN THE NORWEGIAN PETROLEUM
INDUSTRY
(Recommended SIL requirements)

Norsk olje&gass

Steps leading up to requirements in GL 070

Minimum SIL requirements

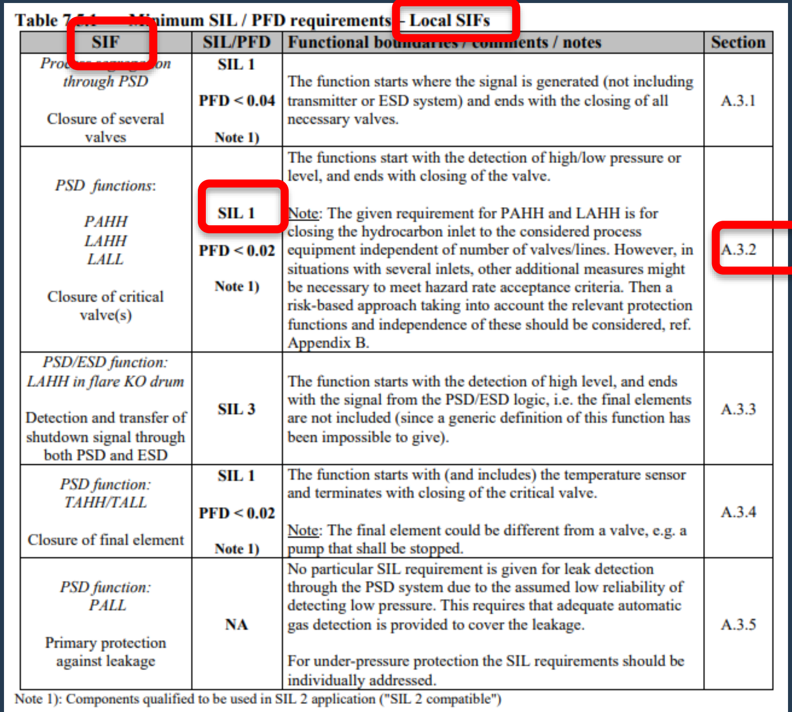


Table 7.5.1 Minimum SIL / PFD requirements - Local SIFs

SIF	SIL/PFD	Functional boundaries / comments / notes	Section
Process segregation through PSD Closure of several valves	**SIL 1** **PFD < 0.04** **Note 1)**	The function starts where the signal is generated (not including transmitter or ESD system) and ends with the closing of all necessary valves.	A.3.1
PSD functions: *PAHH* *LAHH* *LALL* Closure of critical valve(s)	**SIL 1** **PFD < 0.02** **Note 1)**	The functions start with the detection of high/low pressure or level, and ends with closing of the valve. Note: The given requirement for PAHH and LAHH is for closing the hydrocarbon inlet to the considered process equipment independent of number of valves/lines. However, in situations with several inlets, other additional measures might be necessary to meet hazard rate acceptance criteria. Then a risk-based approach taking into account the relevant protection functions and independence of these should be considered, ref. Appendix B.	A.3.2
PSD/ESD function: *LAHH in flare KO drum* Detection and transfer of shutdown signal through both PSD and ESD	**SIL 3**	The function starts with the detection of high level, and ends with the signal from the PSD/ESD logic, i.e. the final elements are not included (since a generic definition of this function has been impossible to give).	A.3.3
PSD function: *TAHH/TALL* Closure of final element	**SIL 1** **PFD < 0.02** **Note 1)**	The function starts with (and includes) the temperature sensor and terminates with closing of the critical valve. Note: The final element could be different from a valve, e.g. a pump that shall be stopped.	A.3.4
PSD function: *PALL* Primary protection against leakage	**NA**	No particular SIL requirement is given for leak detection through the PSD system due to the assumed low reliability of detecting low pressure. This requires that adequate automatic gas detection is provided to cover the leakage. For under-pressure protection the SIL requirements should be individually addressed.	A.3.5

Note 1): Components qualified to be used in SIL 2 application ("SIL 2 compatible")

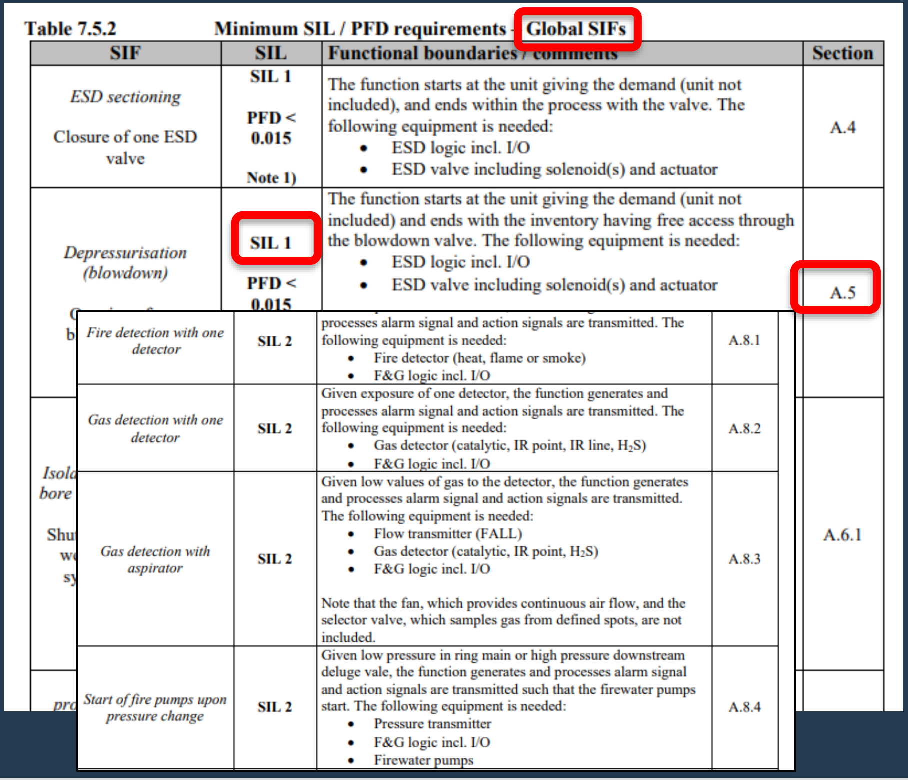


Table 7.5.2 Minimum SIL / PFD requirements - Global SIFs

SIF	SIL	Functional boundaries / comments	Section
ESD sectioning Closure of one ESD valve	**SIL 1** **PFD < 0.015** **Note 1)**	The function starts at the unit giving the demand (unit not included), and ends within the process with the valve. The following equipment is needed: • ESD logic incl. I/O • ESD valve including solenoid(s) and actuator	A.4
Depressurisation (blowdown)	**SIL 1** **PFD < 0.015**	The function starts at the unit giving the demand (unit not included) and ends with the inventory having free access through the blowdown valve. The following equipment is needed: • ESD logic incl. I/O • ESD valve including solenoid(s) and actuator	A.5
			A.6.1

Fire detection with one detector	**SIL 2**	processes alarm signal and action signals are transmitted. The following equipment is needed: • Fire detector (heat, flame or smoke) • F&G logic incl. I/O	A.8.1
Gas detection with one detector	**SIL 2**	Given exposure of one detector, the function generates and processes alarm signal and action signals are transmitted. The following equipment is needed: • Gas detector (catalytic, IR point, IR line, H_2S) • F&G logic incl. I/O	A.8.2
Gas detection with aspirator	**SIL 2**	Given low values of gas to the detector, the function generates and processes alarm signal and action signals are transmitted. The following equipment is needed: • Flow transmitter (FALL) • Gas detector (catalytic, IR point, H_2S) • F&G logic incl. I/O Note that the fan, which provides continuous air flow, and the selector valve, which samples gas from defined spots, are not included.	A.8.3
Start of fire pumps upon pressure change	**SIL 2**	Given low pressure in ring main or high pressure downstream deluge vale, the function generates and processes alarm signal and action signals are transmitted such that the firewater pumps start. The following equipment is needed: • Pressure transmitter • F&G logic incl. I/O • Firewater pumps	A.8.4

Example

Safety function: **Isolation of subsea well**

Estimation of historical safety level

SIL 3 level required for closure of specific critical valves

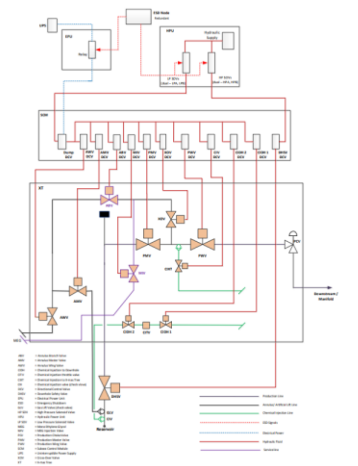


Figure A.13.1 Typical sketch of an XT for isolation of one subsea well.

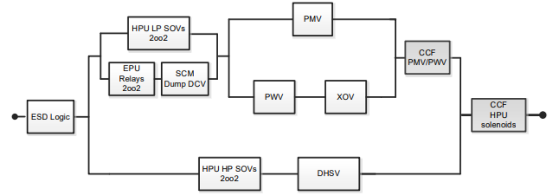


Figure A.13.2 RBD for the SIF "Primary and secondary barrier isolation of production/injection bore in one subsea well".

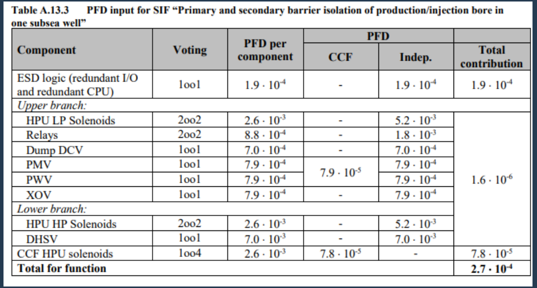


Table A.13.3 PFD input for SIF "Primary and secondary barrier isolation of production/injection bore in one subsea well"

Component	**Voting**	**PFD per component**	**PFD**		**Total contribution**
			CCF	**Indep.**	
ESD logic (redundant I/O and redundant CPU)	1oo1	$1.9 \cdot 10^{-4}$	-	$1.9 \cdot 10^{-4}$	$1.9 \cdot 10^{-4}$
Upper branch:					
HPU LP Solenoids	2oo2	$2.6 \cdot 10^{-3}$	-	$5.2 \cdot 10^{-3}$	$1.6 \cdot 10^{-6}$
Relays	2oo2	$8.8 \cdot 10^{-4}$	-	$1.8 \cdot 10^{-3}$	
Dump DCV	1oo1	$7.0 \cdot 10^{-4}$	-	$7.0 \cdot 10^{-4}$	
PMV	1oo1	$7.9 \cdot 10^{-4}$	$7.9 \cdot 10^{-5}$	$7.9 \cdot 10^{-4}$	
PWV	1oo1	$7.9 \cdot 10^{-4}$		$7.9 \cdot 10^{-4}$	
XOV	1oo1	$7.9 \cdot 10^{-4}$	-	$7.9 \cdot 10^{-4}$	
Lower branch:					
HPU HP Solenoids	2oo2	$2.6 \cdot 10^{-3}$	-	$5.2 \cdot 10^{-3}$	
DHSV	1oo1	$7.0 \cdot 10^{-3}$	-	$7.0 \cdot 10^{-3}$	
CCF HPU solenoids	1oo4	$2.6 \cdot 10^{-3}$	$7.8 \cdot 10^{-5}$	-	$7.8 \cdot 10^{-5}$
Total for function					$\mathbf{2.7 \cdot 10^{-4}}$

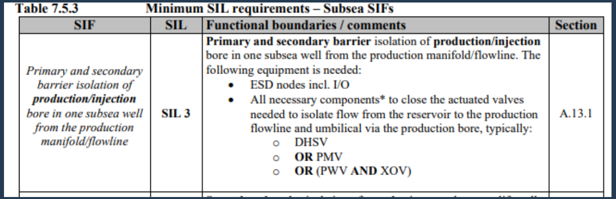
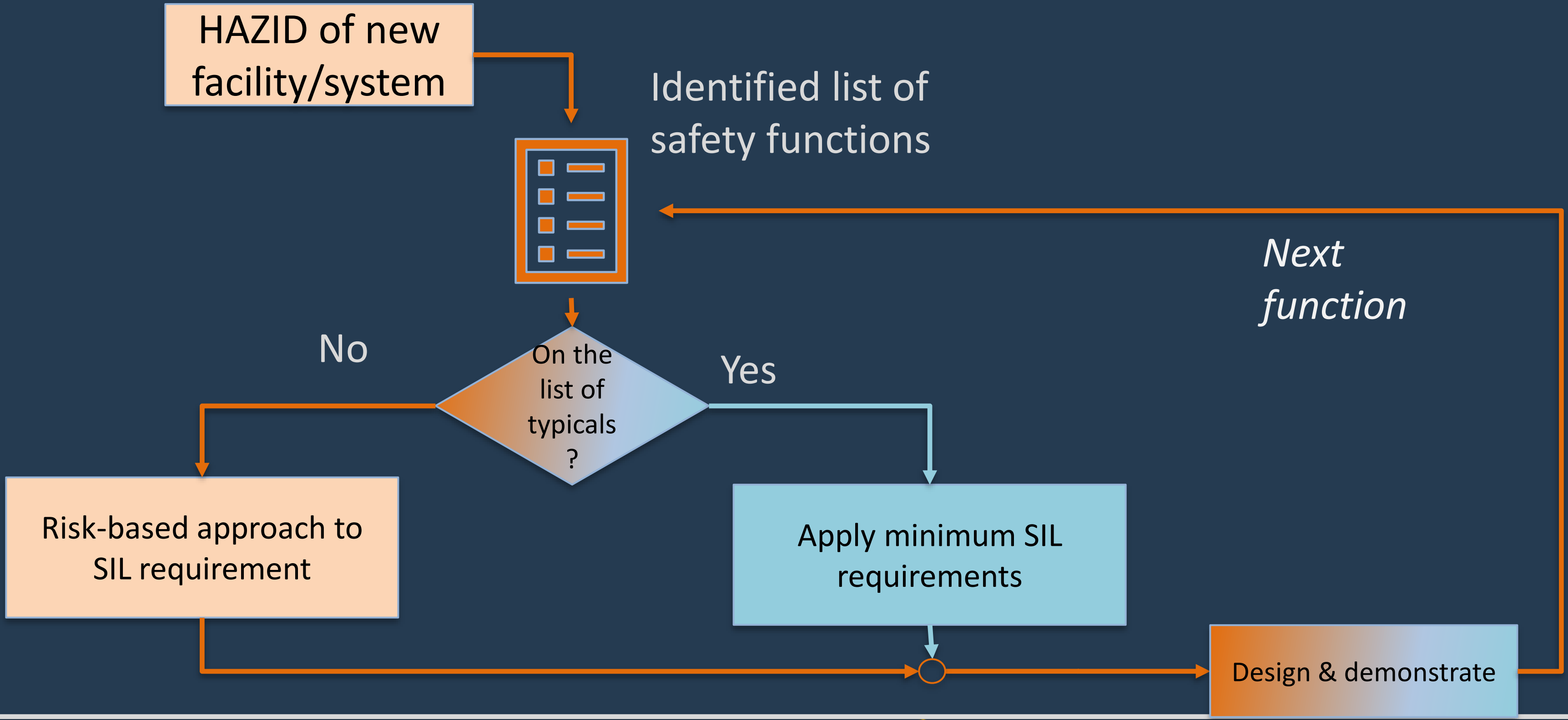


Table 7.5.3 Minimum SIL requirements – Subsea SIFs

SIF	**SIL**	**Functional boundaries / comments**	**Section**
*Primary and secondary barrier isolation of **production/injection** bore in one subsea well from the production manifold/flowline*	**SIL 3**	**Primary and secondary barrier** isolation of **production/injection** bore in one subsea well from the production manifold/flowline. The following equipment is needed: • ESD nodes incl. I/O • All necessary components* to close the actuated valves needed to isolate flow from the reservoir to the production flowline and umbilical via the production bore, typically: ○ DHSV ○ **OR** PMV ○ **OR** (PWV **AND** XOV)	A.13.1

Application of minimum SIL



HAZID of new facility/system

Identified list of safety functions

Next function

On the list of typicals ?

No

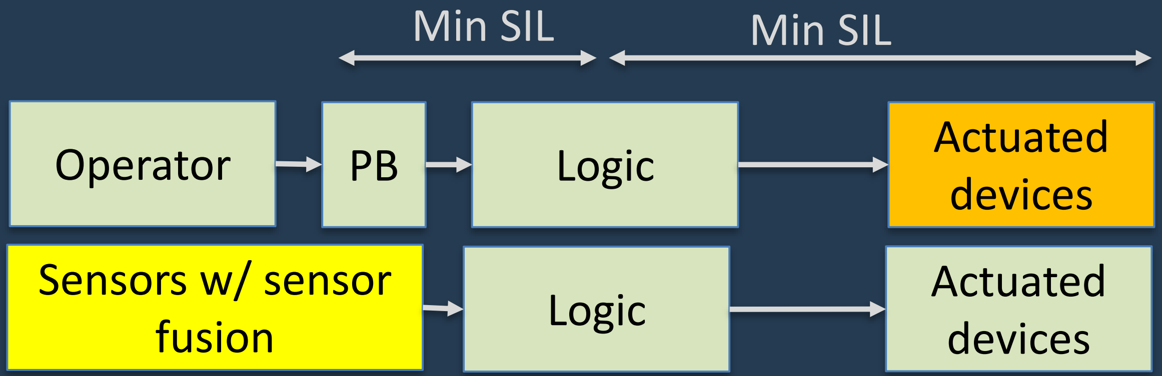
Yes

Risk-based approach to SIL requirement

Apply minimum SIL requirements

Design & demonstrate

What if…



---

1. Replacing electro-hydraulic valves with all-electric & battery assisted fail-safe closure

Existing minimum SIL requirement applies. It must be demonstrated that the new realization still meets the minimum SIL requirement

---

2. A situation awareness system is replacing operator

A new minimum SIL requirement is needed. New potential risks? Human-machine interfaces for remote monitoring? For the technical part: Should the new system be at least as reliable as operator under best scenario («trained» and “low complex situations”) (e.g. < 0.01)

Relevance to autonomous waterbuses?

- Benefit from developing a common recommended practice?

Some thoughts:

- A standardization opportunity (cost-efficient, consistent safety target)
  - Possible to establish a conceptual (Semi) autonomous waterbus system as basis? (Common assumptions)
  - *Name* typical safety functions?
- Benefit from establishing a set of well communicated safety functions and performance criteria to achieve public acceptance?

Performance level?

NTNU | Kunnskap for en bedre verden

Comments? Questions?

GL 070 is found here:
https://norskoljeoggass.no/en/working-conditions/retningslinjer/health-working-environment-safety/technical-safety/070-guidelines/

Professor Mary Ann Lundteigen | institutt for teknisk kybernetikk
E-mail: Mary.a.lundteigen@ntnu.no & https://www.ntnu.edu/sfi-autoship