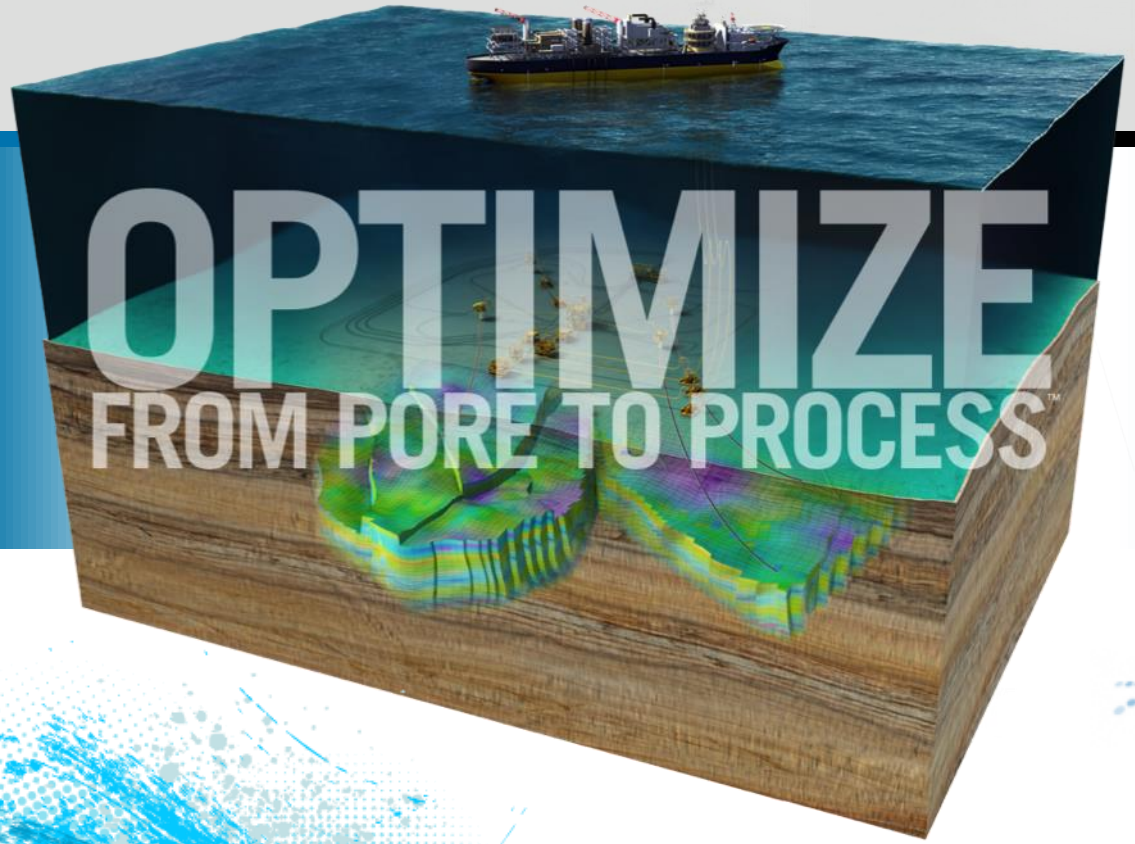


Application of Functional Safety in All-Electric Control Systems

Dr. Carsten Mahler
Prof. Dr. Markus Glaser

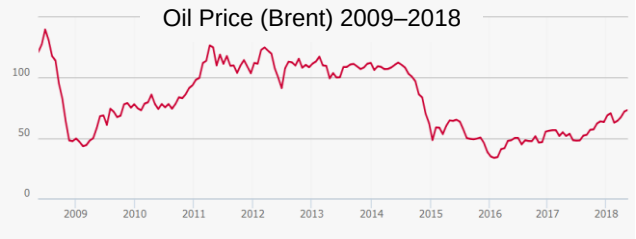
Aalen University

OneSubsea
A Schlumberger Company

Introduction

Current market situation

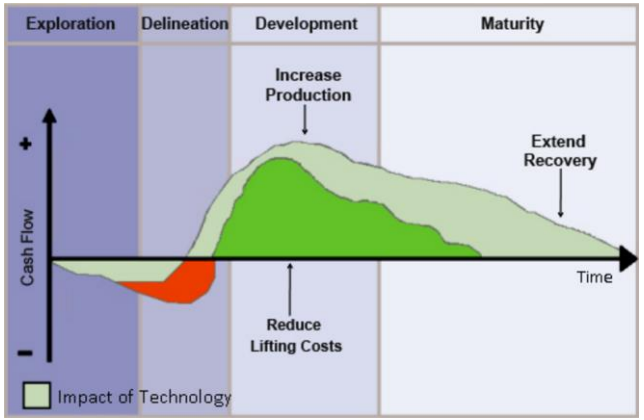
- Most severe downturn in decades
- Slow recovery; prices as before 2015 will not be reached in the near future



Source: boerse-online.de.

OG21 recommendations to cut costs and enhance recovery

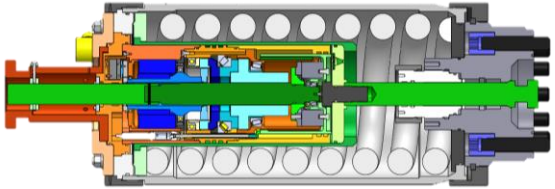
- Standardization
- Simplification
- All-electric technology



Source: The Digital Oil Field. Oil & Gas Investor.

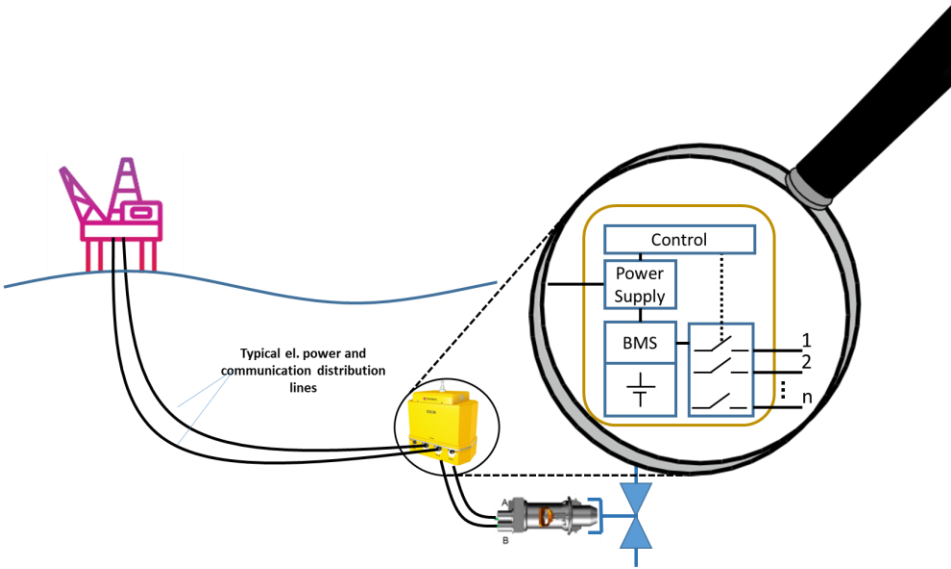
Fail-Safe Concepts for All-Electric Systems

Mechanical Spring and Clutch



5-in actuator.

All-electric tree with spring-return actuators.



Suitable Applications

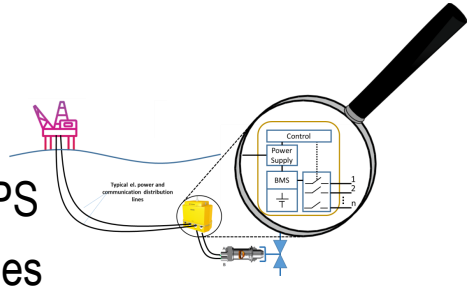
Mechanical spring and clutch

- Trees
- Subsea separation
- Greenfield
- When enough power is available
- Wherever batteries are not acceptable

Well known

Battery concept

- Trees
- Electric HIPPS
- Pump modules
- Greenfields and tie-backs with limited power



New to industry

Joint Industry Project

OneSubsea
A Schlumberger Company

Aalen University

WITTENSTEIN

Federal Ministry
for Economic Affairs
and Energy

Challenges

Technical:

- Safety and availability
- Novel architecture of fail-safe system
- Design life of energy storage

Non-Technical:

- Step change approach
- No AE standards available
- System target costs

Elisha Graves Otis demonstrates his first elevator in the Crystal Palace, New York Exhibition
Source: Wikipedia

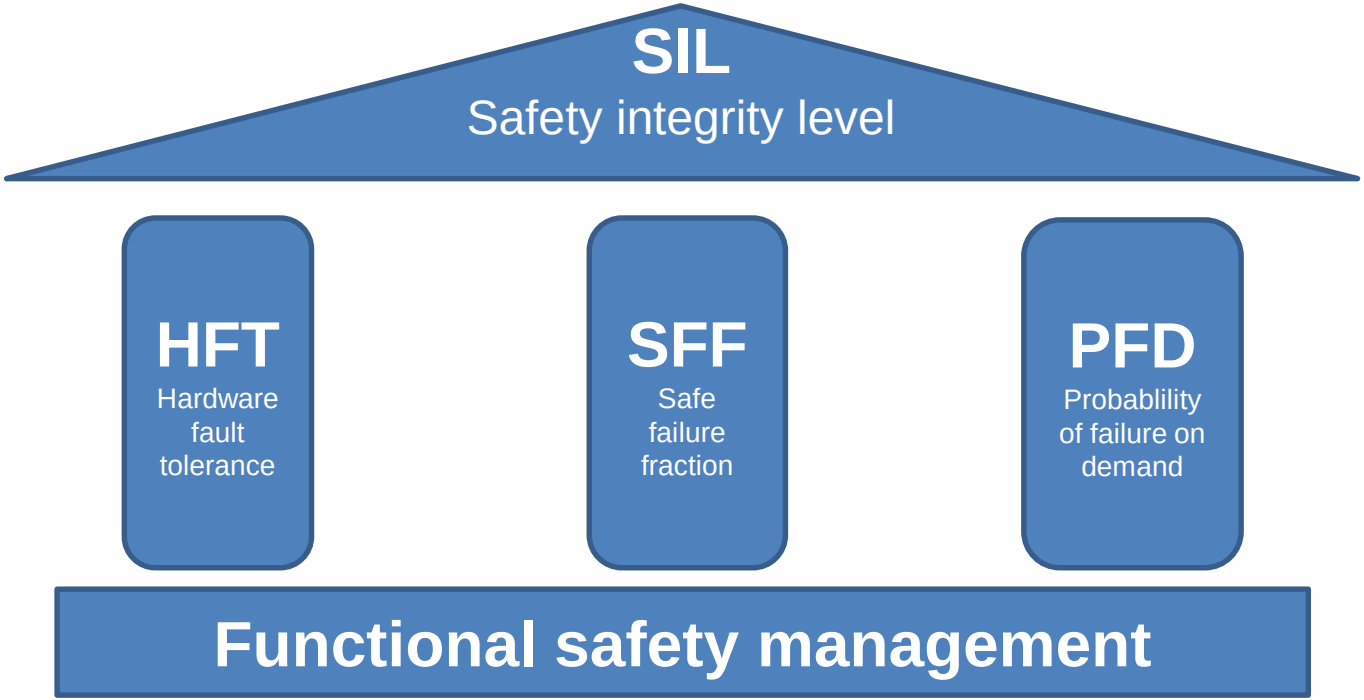
Approach: Application of Functional Safety

Any **random, systematic, and common-cause failure** will not lead to a failure of the safety system, which could result in

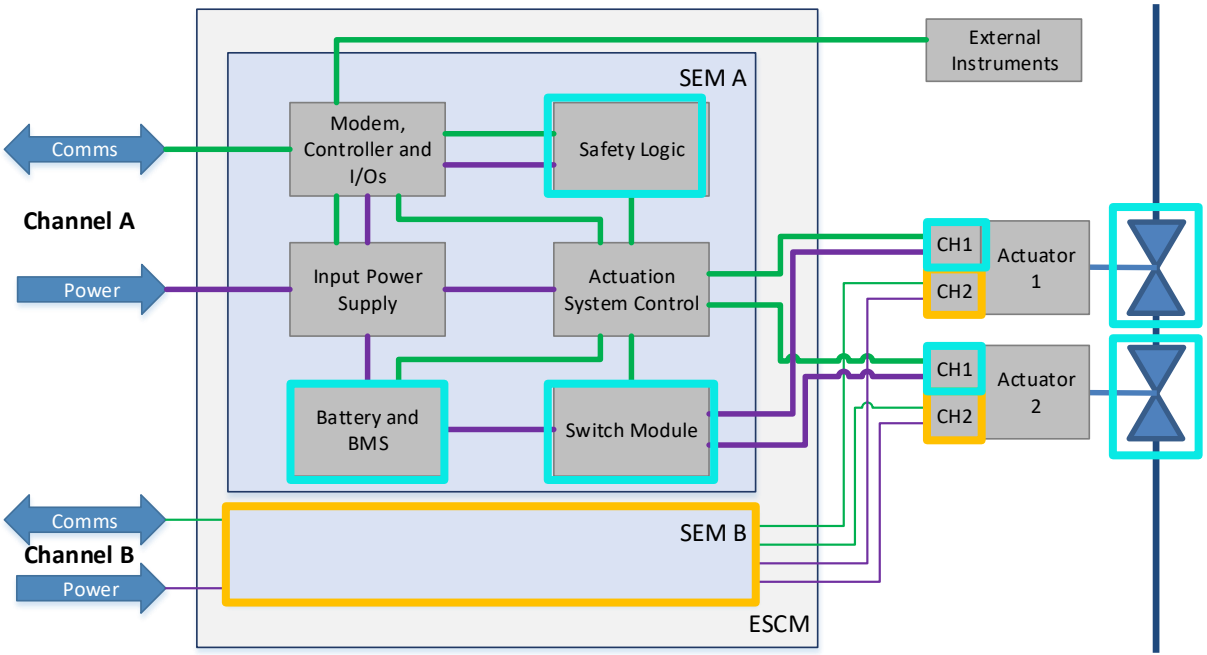
- loss of asset or facility
- pollution
- injury or death.

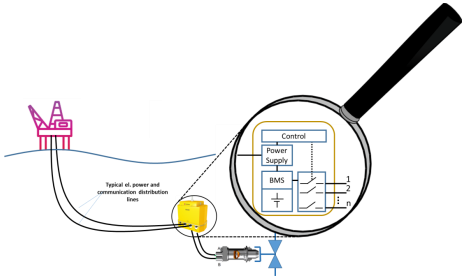
SIL	*Risk Reduction*	Allowed Probability of Event
1	>10	Once in 10 years
2	>100	Once in 100 years
3	>1,000	Once in 1,000 years
4	>10,000	Once in 10,000 years

Functional Safety Principles



System Architecture with redundancy (HFT) for Availability and Safety

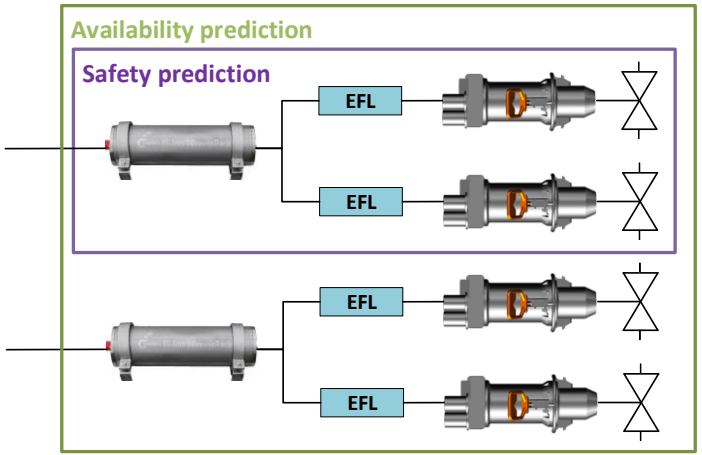
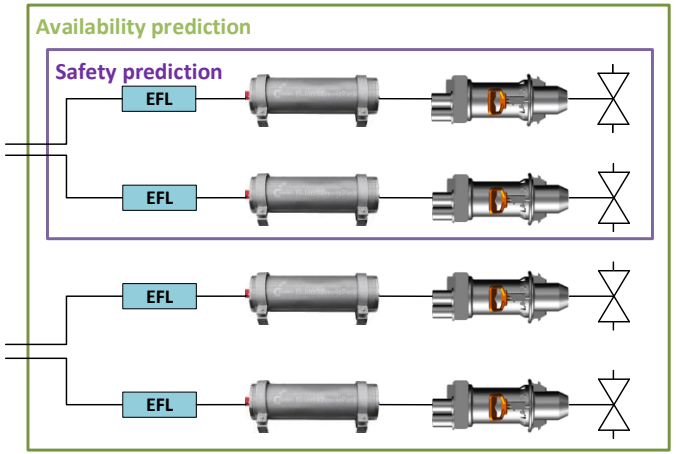




HFT for Availability

HFT for Safety

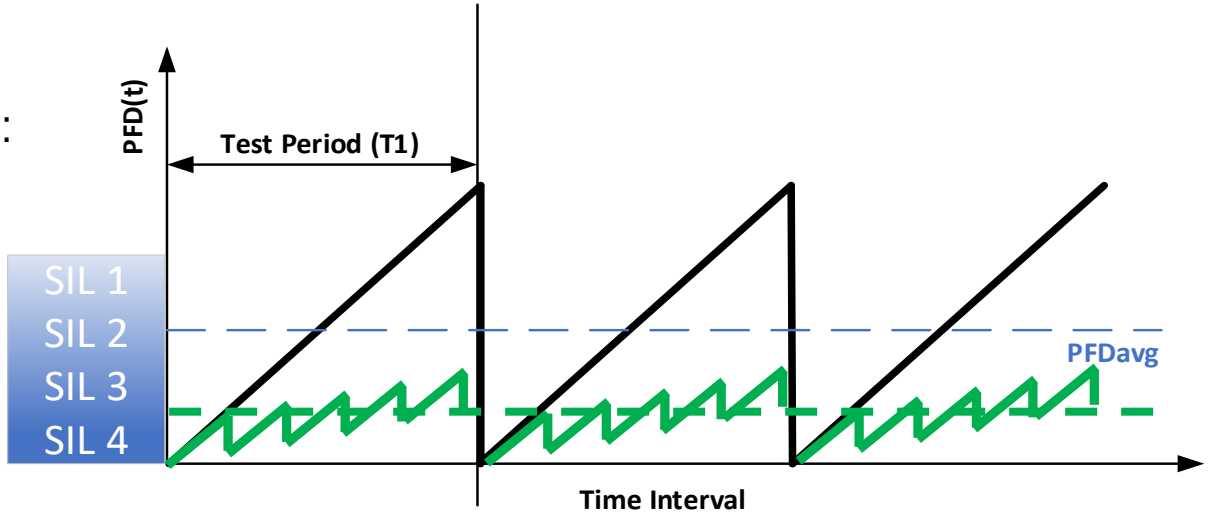
System Architectural Design Trades

Configuration	central	integrated in actuator
Layout / RBD		
Safety (PFD)	SIL 2 (1/500)	SIL 2 (1/500)
Relative Downtime	**70 %**	100%
Cost	**70..90 %** (depending on number of actuators)	100%

Probability of Failure on Demand

Lower PFD by development and introduction of enhanced diagnosis:

- Cross Checks
- Sweep Test
- Partial Stroke Test
- …



➔ **Immediate detection of failures without additional components!**

Systematic Capability: Hardware Fault Tolerance

SFF	Hardware Fault Tolerance					
	0		1		2	
	Complex	Simple	Complex	Simple	Complex	Simple
<60%	Not allowed	SIL 1	SIL 1	SIL 2	SIL 2	SIL 3
≥60%	SIL 1	SIL 2	SIL 2	SIL 3	SIL 3	SIL 4
≥90%	SIL 2	SIL 3	SIL 3	SIL 4	SIL 4	SIL 4
≥99%	SIL 3	SIL 3	SIL 4	SIL 4	SIL 4	SIL 4

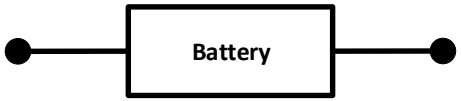
Due to high SFF (Diagnosis) the Systematic Capability is SIL 2 or SIL 3

Improved HFT (and PFD) by SMART redundancies

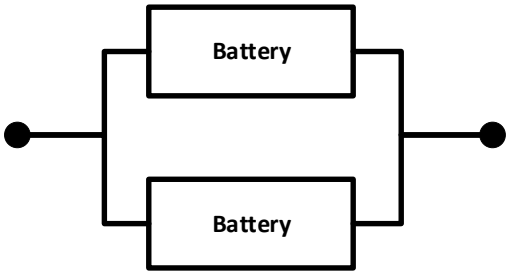
System Architecture: Battery

Battery Data	
λ_{DU}[10e-6]	0.98
λ_{DD}[10E-6]	8.82
λ_{SU}[10E-6]	0
λ_{SD}[10E-6]	0
SFF [%]	90%
T_1 [h]	720 h
MTTR[h]	1 h

Single Battery



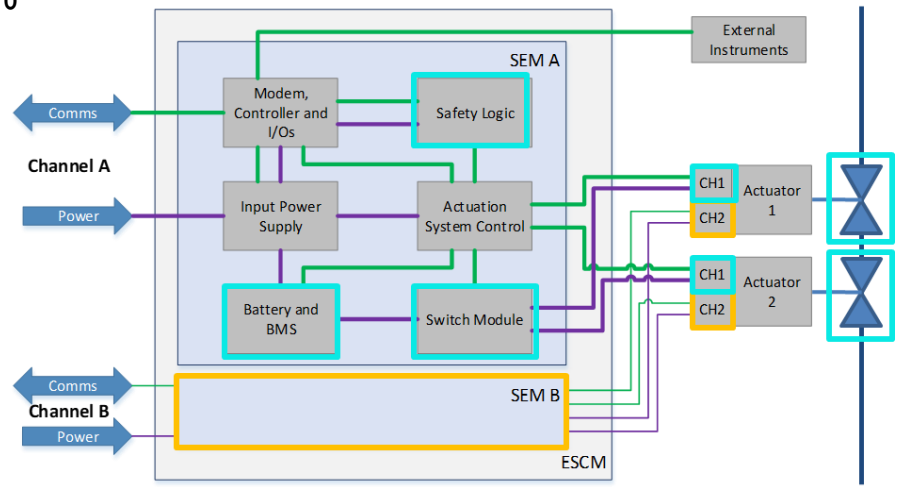
Dual Battery



Comparison		
	Single Battery	Dual Battery
HFT	0	1
Type	Complex	Complex
SC	SIL 2	SIL 3
PFD	3.63**E-04**	3.64**E-05**
Av	99,67180%	99,99892%
Statistical Downtime	28.75 h/year	57 min/year
Volume	100%	130%

All-Electric Actuation System Summary

- SIL 2 (risk reduction of 100) with continued production at single fault
- System diagnostic coverage >90%
- Valve diagnostic coverage increases to >90%
- High SFF and Safety
- High Availability



Thank you.

Dr. Carsten Mahler, OneSubsea, a Schlumberger company
Prof. Dr. Markus Glaser, Aalen University

Aalen University

OneSubsea
A Schlumberger Company