NTNU

Norwegian University of Science and Technology

Application of STPA to Subsea Systems

Opportunities and Challenges

29.3.2018

Dr. Kim, Hyungju
Prof. Lundteigen, Mary Ann

hyung-ju.kim@ntnu.no

NTNU

Background

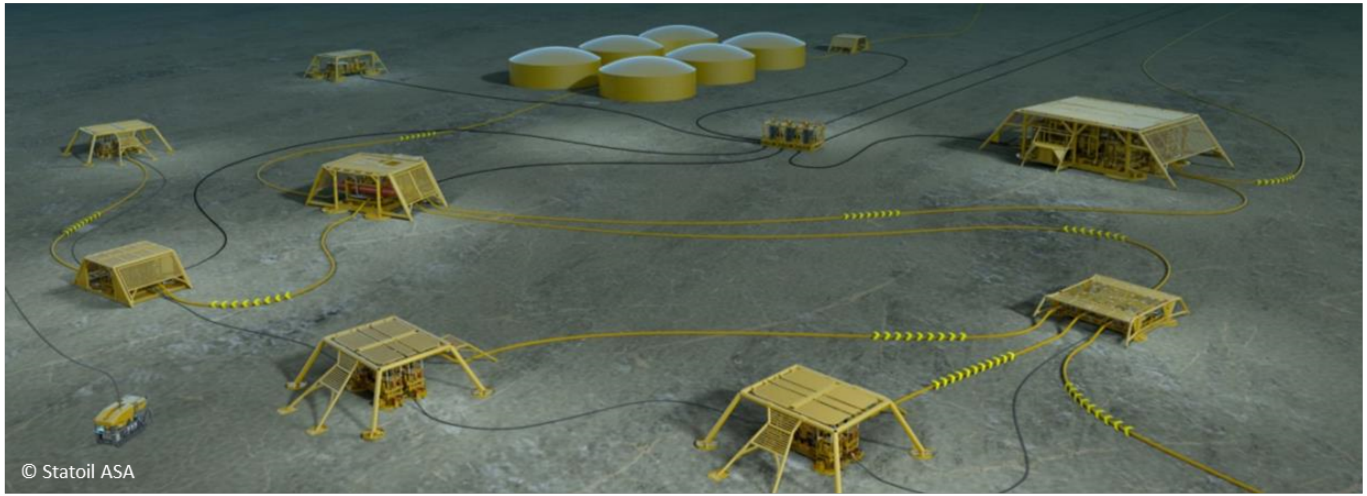
NTNU

NTNU
Norwegian University of Science and Technology

SUBPRO
SUBSEA PRODUCTION AND PROCESSING

SUBPRO

- Innovating subsea systems, integration, and decision-making



SUBPRO's objective & goals

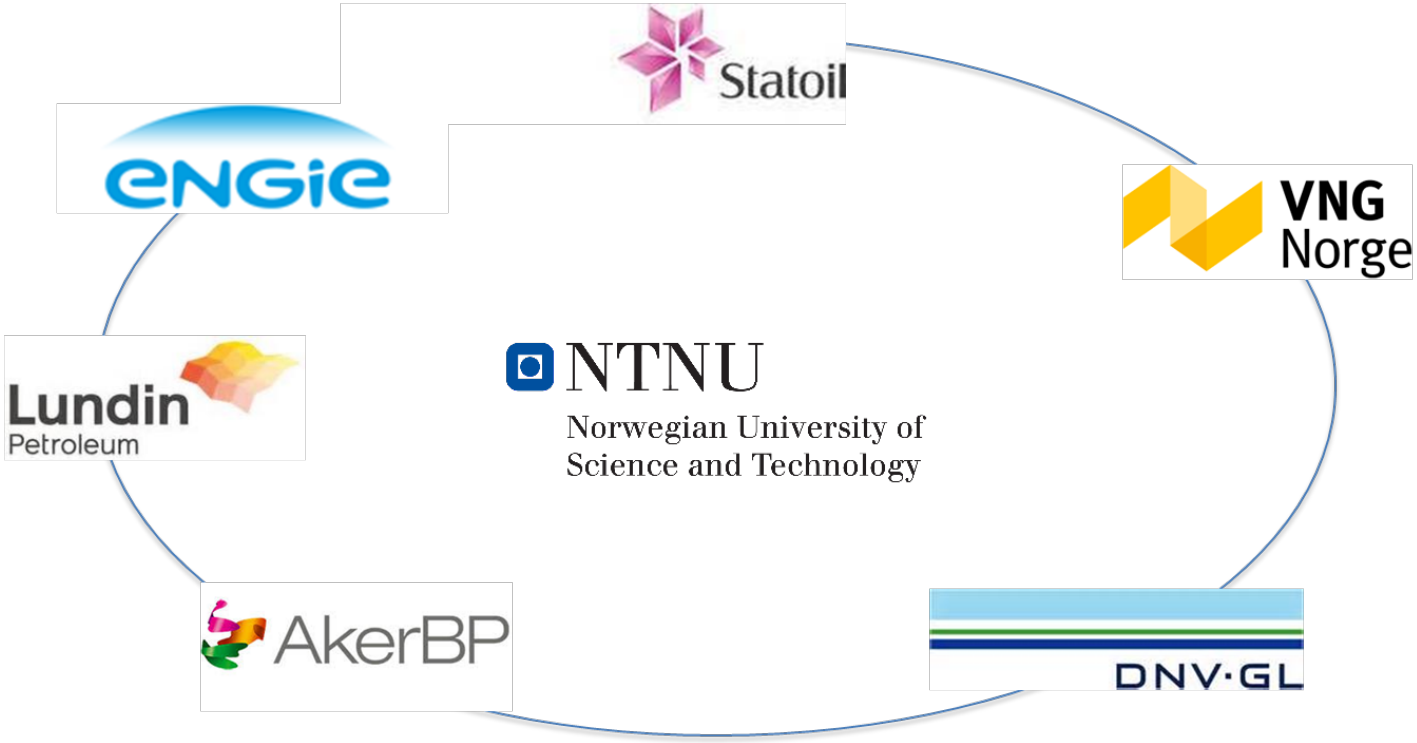
The primary objective of the center is to become a

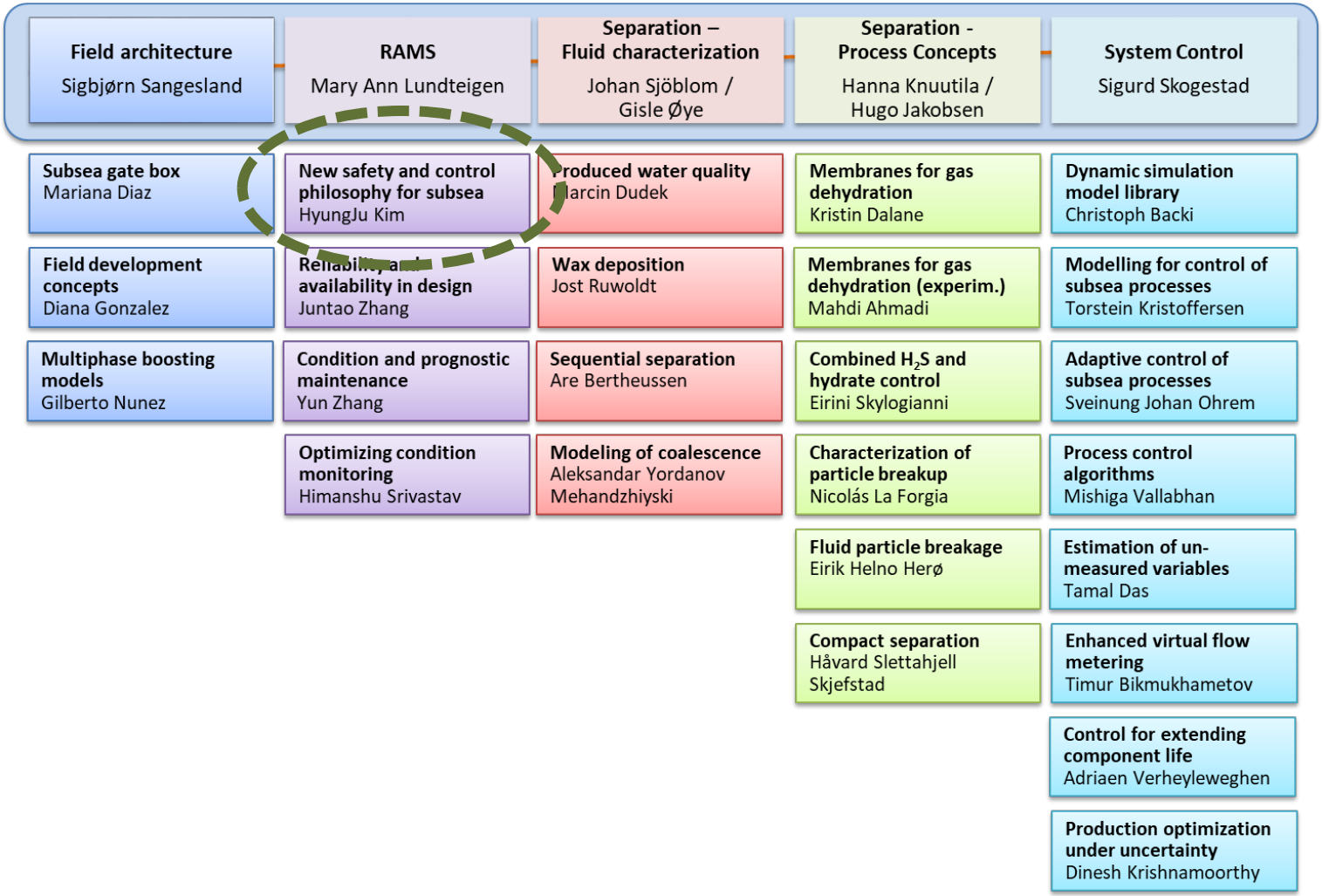
global leader for research based innovation

within subsea production and processing, providing:

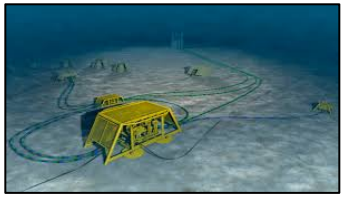
- *International excellence* in fundamental and applied research
- Knowledge, methods, technology and system understanding – as basis for industrial innovation
- Internationally high level of graduated master and PhD candidates

Partners


Statoil
ENGIE
VNG Norge
Lundin Petroleum
NTNU
Norwegian University of Science and Technology
AkerBP
DNV·GL


Field architecture
Sigbjørn Sangesland
RAMS
Mary Ann Lundteigen
Separation – Fluid characterization
Johan Sjöblom / Gisle Øye
Separation - Process Concepts
Hanna Knuutila / Hugo Jakobsen
System Control
Sigurd Skogestad
Subsea gate box
Mariana Diaz
New safety and control philosophy for subsea
HyungJu Kim
Produced water quality
Marcin Dudek
Membranes for gas dehydration
Kristin Dalane
Dynamic simulation model library
Christoph Backi
Field development concepts
Diana Gonzalez
availability in design
Juntao Zhang
Wax deposition
Jost Ruwoldt
Membranes for gas dehydration (experim.)
Mahdi Ahmadi
Modelling for control of subsea processes
Torstein Kristoffersen
Multiphase boosting models
Gilberto Nunez
Condition and prognostic maintenance
Yun Zhang
Sequential separation
Are Bertheussen
Combined H2S and hydrate control
Eirini Skylogianni
Adaptive control of subsea processes
Sveinung Johan Ohrem
Optimizing condition monitoring
Himanshu Srivastav
Modeling of coalescence
Aleksandar Yordanov Mehandzhiyski
Characterization of particle breakup
Nicolás La Forgia
Process control algorithms
Mishiga Vallabhan
Fluid particle breakage
Eirik Helno Herø
Estimation of un-measured variables
Tamal Das
Compact separation
Håvard Slettahjell Skjefstad
Enhanced virtual flow metering
Timur Bikmukhametov
Control for extending component life
Adriaen Verheyleweghen
Production optimization under uncertainty
Dinesh Krishnamoorthy

STPA Studies in RAMS Group, NTNU



- Subsea Gatebox – Master thesis
- Subsea Gatebox – Journal paper
- Isolation of subsea wells – OTC 2018
- Subsea gas compression – ESREL 2018
- To be continued…



- Autonomous ship – Master thesis
- Dynamic positioning system in Arctic condition – ESREL 2018 (with KRISO)



- Securing maintenance area – Master thesis

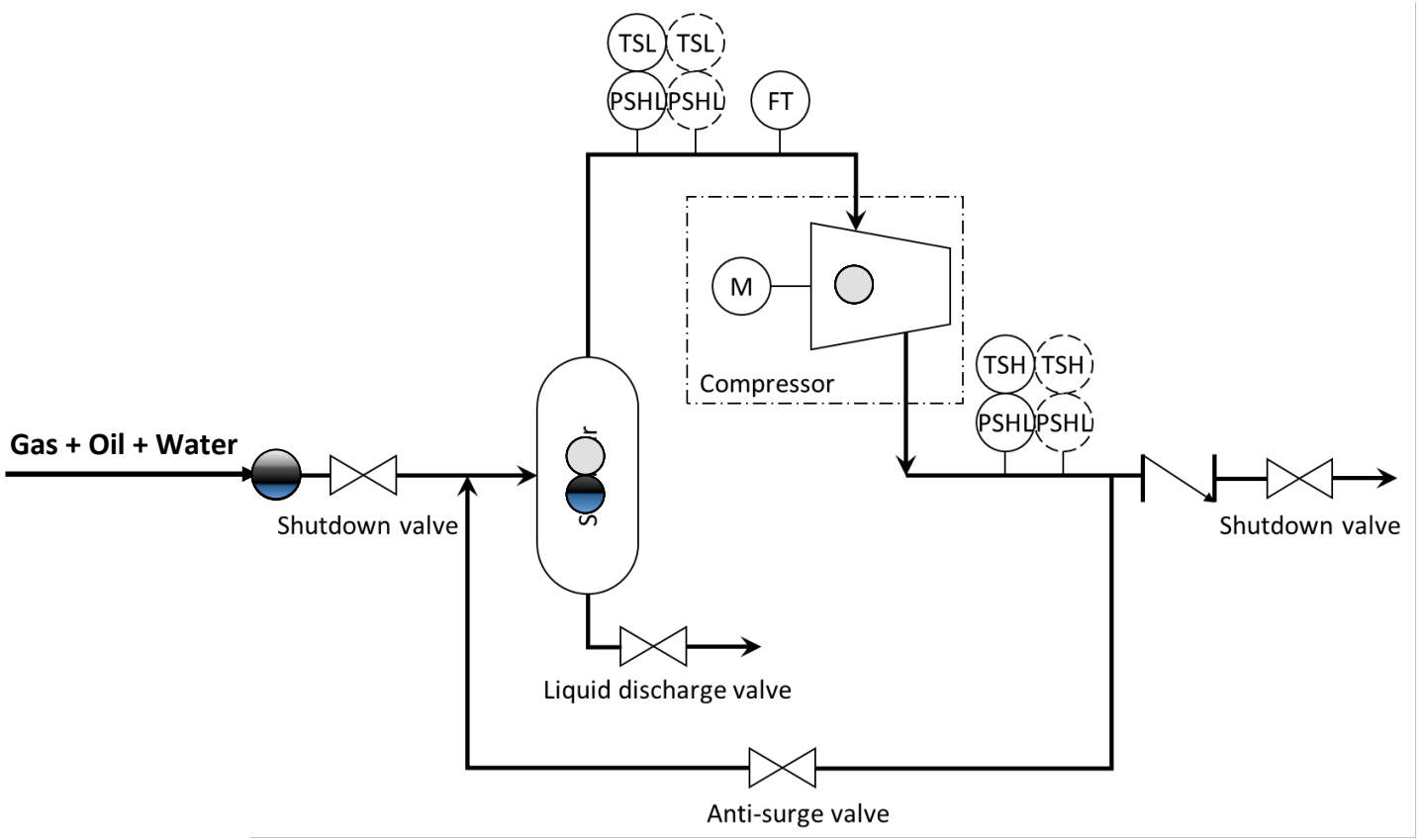
NTNU

STPA to Subsea Gas Compression

Subsea System

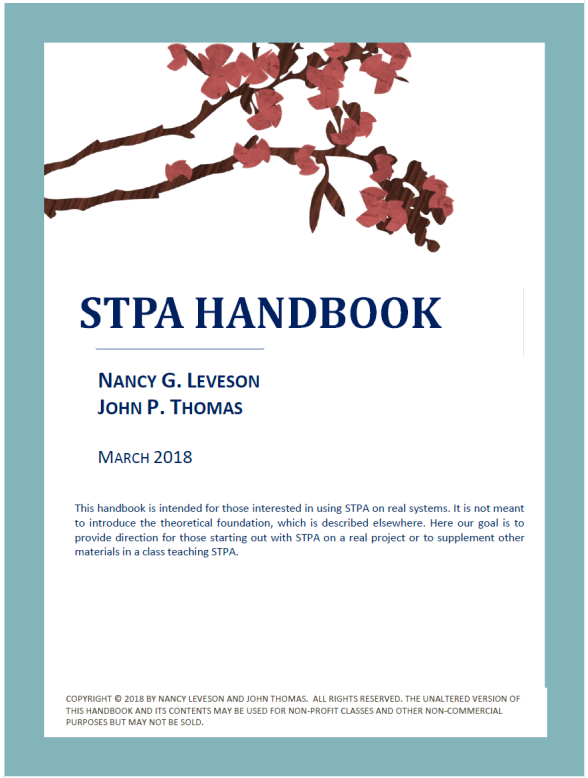


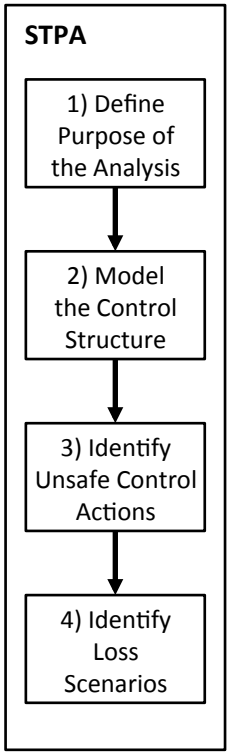
System Configuration



Ref: API RP 17V (2015), Recommended Practice for Analysis, Design, Installation, and Testing of Safety Systems for Subsea Applications

STPA Procedure





System	Losses
Subsea Gas Compression System	L-1: Loss of life or injury to people
	L-2: Environmental loss
	L-3: Damage to valuable SGC components
	L-4: Reduced gas production

1) Define Purpose of the Analysis → 2) Model the Control Structure → 3) Identify Unsafe Control Actions → 4) Identify Loss Scenarios

- a) Identifying losses
- b) Identifying system-level hazards

System	Losses	System-Level Hazards
Subsea Gas Compression System	L-1: Loss of life or injury to people	H-1: SGC system continues to supply gas when gas leaks to the environment
	L-2: Environmental loss	
	L-3: Damage to valuable SGC components	H-2: SGC system operates under abnormal conditions
	L-4: Reduced gas production	H-3: SGC system cannot produce gas with maximum capacity

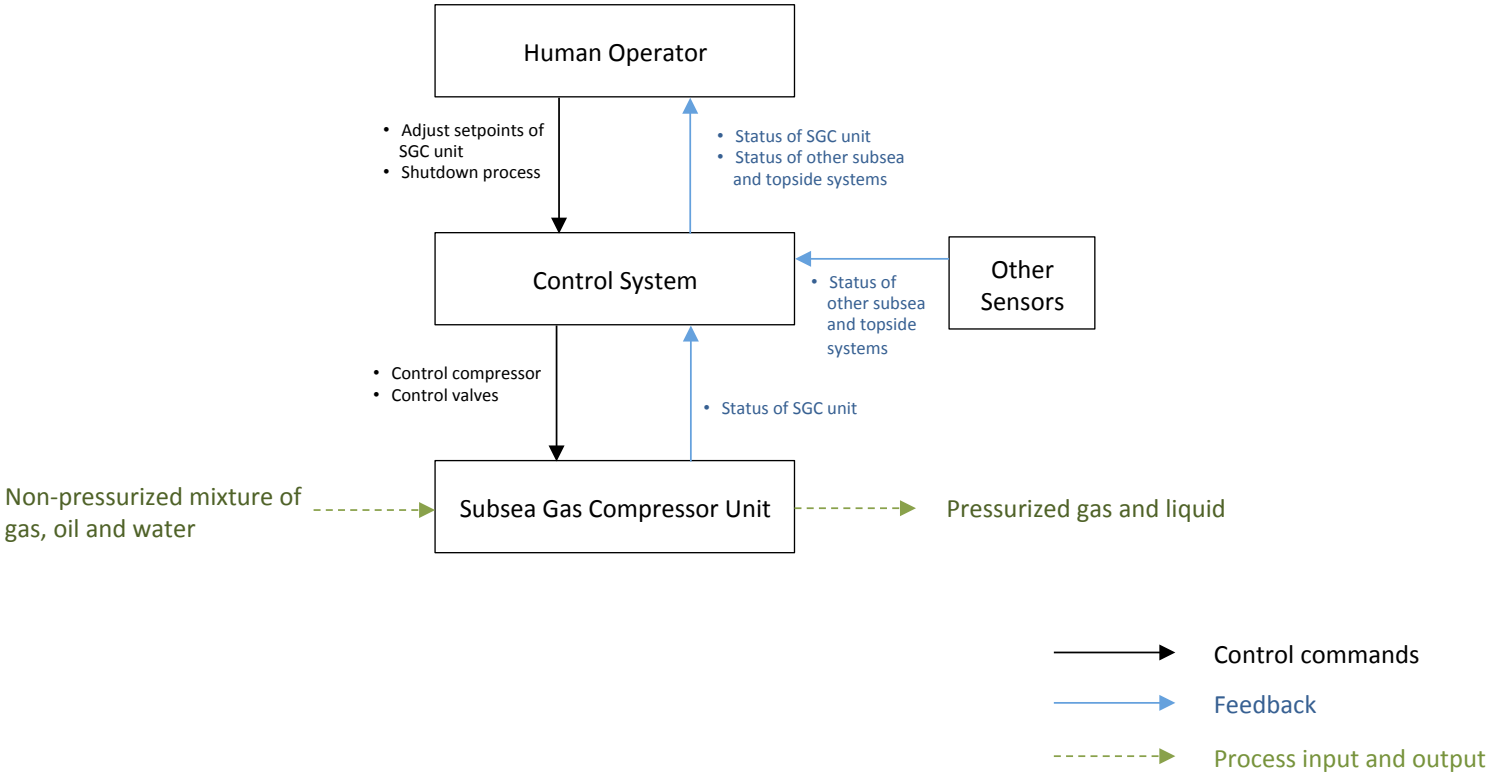
System	Losses	System-Level Hazards	System-Level Constraints
Subsea Gas Compression System	L-1: Loss of life or injury to people	H-1: SGC system continues to supply gas when gas leaks to the environment	SC-1: SGC system must stop compressing gas when gas leaks to the environment
	L-2: Environmental loss		
	L-3: Damage to valuable SGC components	H-2: SGC system operates under abnormal conditions	SC-2: SGC system must be protected from abnormal operating conditions that can damage valuable components
	L-4: Reduced gas production	H-3: SGC system cannot produce gas with maximum capacity	SC-3: SGC system must always produce gas with maximum capacity

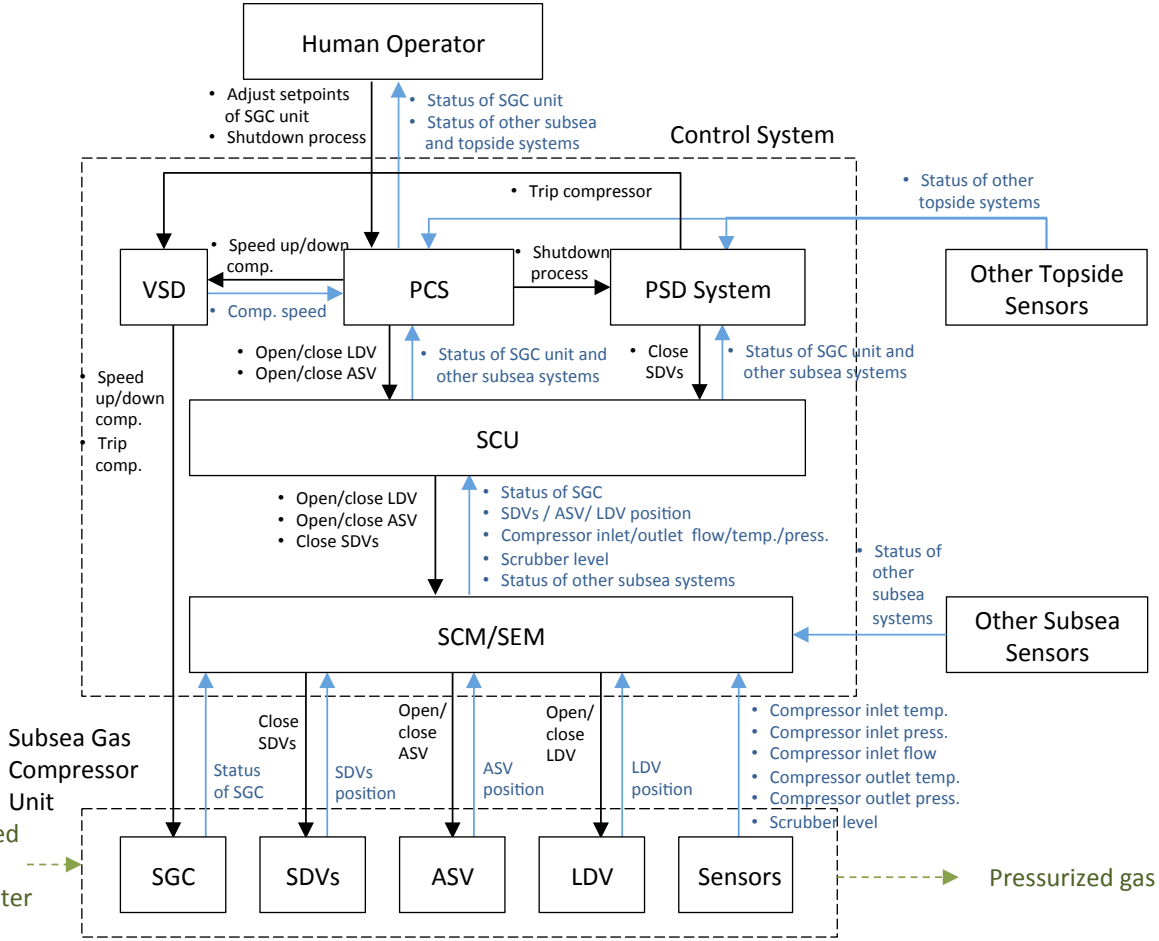
NTNU

1) Define Purpose of the Analysis → 2) Model the Control Structure → 3) Identify Unsafe Control Actions → 4) Identify Loss Scenarios

- a) Identifying losses
- b) Identifying system-level hazards
- c) Defining system-level constraints
- d) Refining the system-level hazards

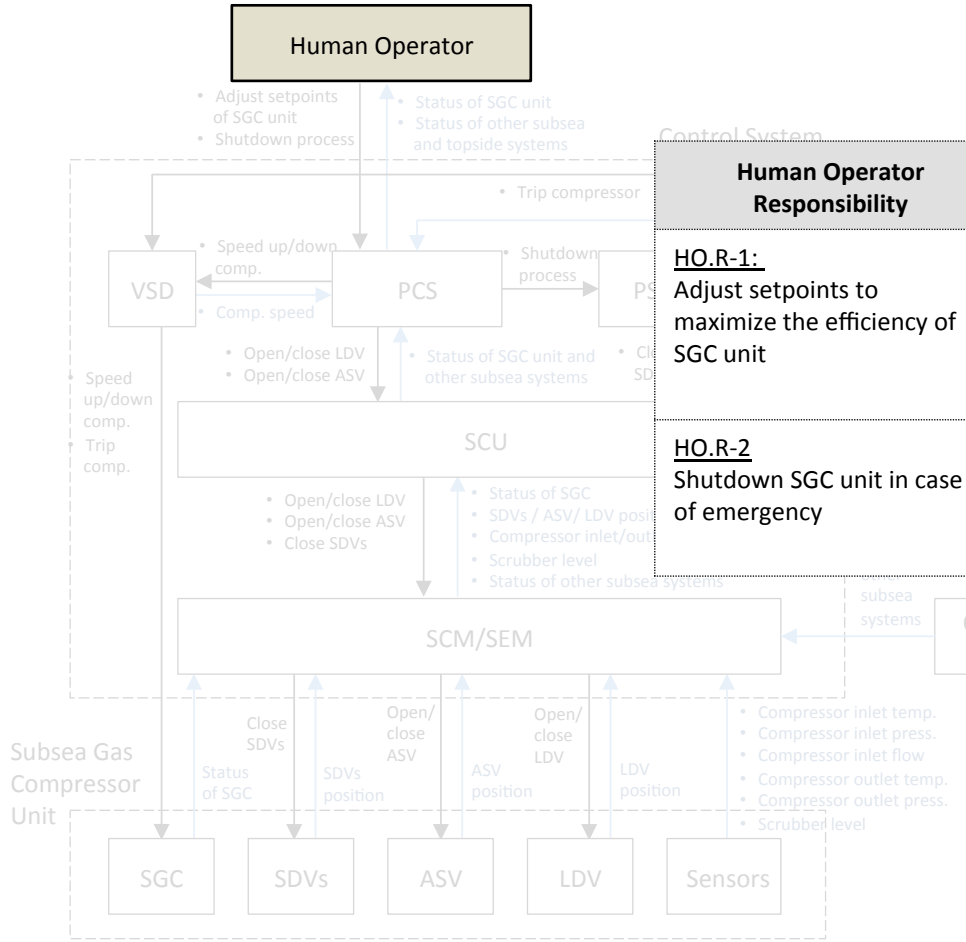
System-level hazard	Sub-hazards derived from system-level hazards	Sub-constraints
H-2: SGC system operates under abnormal conditions	H-2.1: Liquid flows into the gas compressor	SC-2.1: Liquid must never flow into gas compressor
	H-2.2: Gas flows into the liquid pump	SC-2.2: Gas must never flow into liquid pump
H-3: SGC system cannot produce gas with maximum capacity	H-3.1: SGC system stops compressing gas when compression is needed	SC-2.1: SGC system must never stop compressing gas when gas compression is needed
	H-3.2: SGC system operates under non-optimal operating conditions	SC-2.2: SGC system must be operated under optimal operating conditions


Human Operator
• Adjust setpoints of SGC unit
• Shutdown process
• Status of SGC unit
• Status of other subsea and topside systems
Control System
Other Sensors
• Status of other subsea and topside systems
• Control compressor
• Control valves
• Status of SGC unit
Non-pressurized mixture of gas, oil and water
Subsea Gas Compressor Unit
Pressurized gas and liquid
Control commands
Feedback
Process input and output

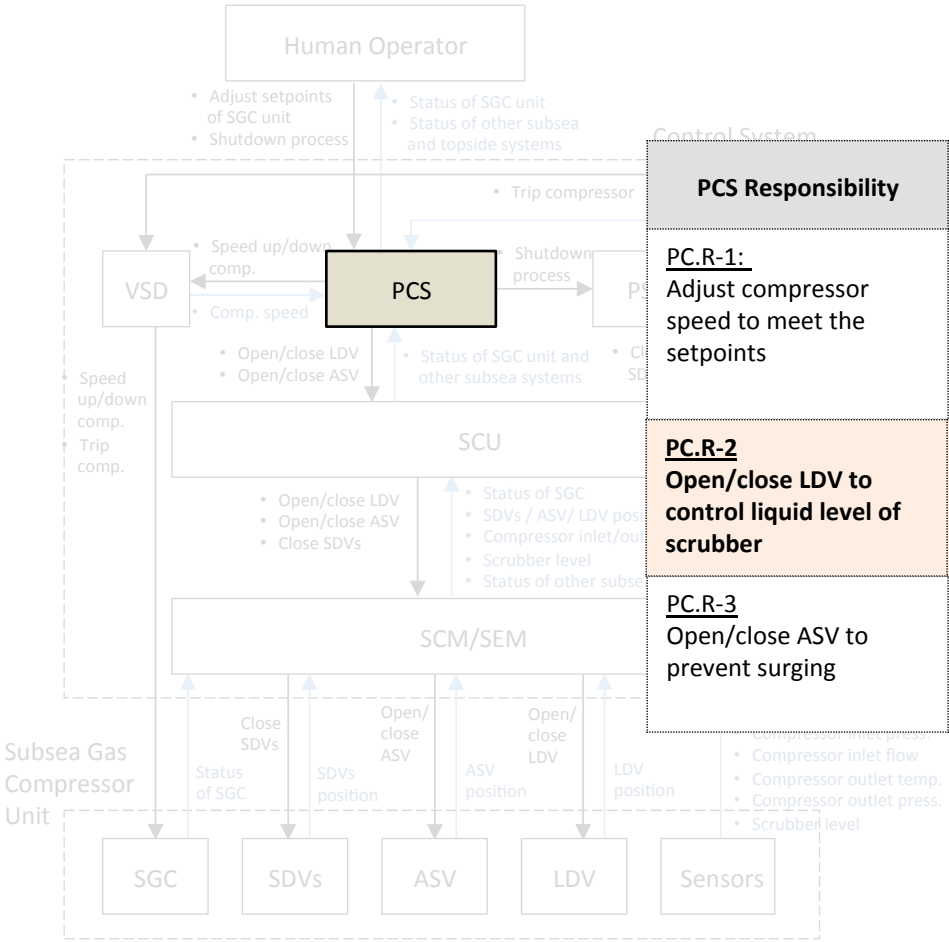


Abbreviation

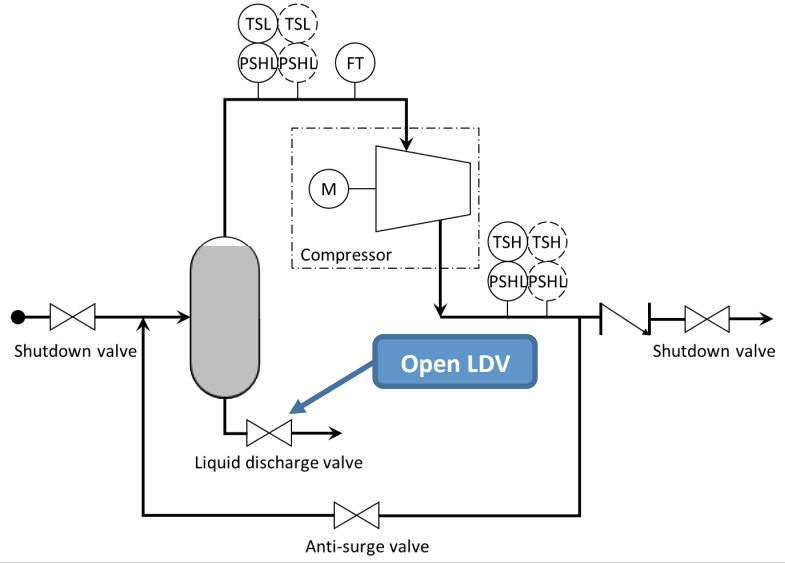
- VSD: Variable Speed Drive
- PCS: Process Control System
- PSD: Process Shutdown
- SCU: Subsea Control Unit
- SCM: Subsea Control Module
- SEM: Subsea Electronic Module
- SGC: Subsea Gas Compressor
- SDV: Shutdown Valve
- ASV: Anti-Surge Valve
- LDV: Liquid Discharge Valve



Human Operator Responsibility	Process Model	Feedback
HO.R-1: Adjust setpoints to maximize the efficiency of SGC unit	HO.P-1 Setpoints of subsea gas compressor is not optimal	• Compressor inlet/outlet pressure • Compressor inlet/outlet flow
HO.R-2 Shutdown SGC unit in case of emergency	HO.P-2 Hydrocarbons leak to the environment	• Status of subsea systems (normal/leak) • Status of topside systems (normal/leak)



PCS Responsibility	Process Model	Feedback
PC.R-1: Adjust compressor speed to meet the setpoints	HO.P-1 Compressor speed is not aligned with the setpoints	• Compressor inlet/outlet pressure • Compressor inlet/outlet flow • Compressor speed
PC.R-2 Open/close LDV to control liquid level of scrubber	**HO.P-2 Scrubber level is too high or too low**	• **Liquid level of scrubber**
PC.R-3 Open/close ASV to prevent surging	HO.P-3 Surging is about to happen	• Compressor inlet/outlet pressure



Controller : PCS								
No	Control Action	Process Model	Unsafe Control Actions?					
		Scrubber level	Not provided	Provided	Too early	Too late	Too short	Too long
1	Open LDV	High	Unsafe	Safe	Safe	Unsafe	Unsafe	Safe
2		Normal	Safe	Safe	Safe	Safe	Safe	Safe
3		Low	Safe	Unsafe	N/A	N/A	N/A	N/A
4	Close LDV	High						
5		Normal						
6		Low						

Controller : PCS								
No	Control Action	Process Model	Unsafe Control Actions?					
		Scrubber level	Not provided	Provided	Too early	Too late	Too short	Too long
1	Open LDV	High	Unsafe [H2]	Safe	Safe	Unsafe [H2]	Unsafe [H2]	Safe
2		Normal	Safe	Safe	Safe	Safe	Safe	Safe
3		Low	Safe	Unsafe [H2]	N/A	N/A	N/A	N/A
4	Close LDV	High	Safe	Unsafe [H2]	N/A	N/A	N/A	N/A
5		Normal	Safe	Safe	Safe	Safe	Safe	Safe
6		Low	Unsafe [H2]	Safe	Safe	Unsafe [H2]	Unsafe [H2]	Safe

UCA.PCS.LDV.001: PCS does not provide *open LDV* command when scrubber level is high [H-2.1]

UCA.PCS.LDV.002: PCS provides *open LDV* command too late when scrubber level is high [H-2.1]

UCA.PCS.LDV.003: PCS provides *open LDV* command too short (before the level drops to normal) when scrubber level is high [H-2.1]

UCA.PCS.LDV.004: PCS provides *open LDV* command when scrubber level is low [H-2.2]

UCA.PCS.LDV.005: PCS provides *close LDV* command when scrubber level is high [H-2.1]

.
.
.

Unsafe Control Actions	Controller Constraints
UCA.PCS.LDV.001 PCS does not provide *open LDV* command when scrubber level is high [H-2.1]	CC.PCS.LDV.001 PCS must provide *open LDV* command when scrubber level is high [UCA.PCS.LDV.001]
UCA.PCS.LDV.002 PCS provides *open LDV* command too late when scrubber level is high [H-2.1]	CC.PCS.LDV.002 PCS must provide *open LDV* command within XX seconds when scrubber level is high [UCA.PCS.LDV.002]
UCA.PCS.LDV.003 PCS provides *open LDV* command too short (before the level drops to normal) when scrubber level is high [H-2.1]	CC.PCS.LDV.003 PCS must not stop providing *open LDV* command before the scrubber level drops to normal when scrubber level is high [UCA.PCS.LDV.003]
UCA.PCS.LDV.004 PCS provides *open LDV* command when scrubber level is low [H-2.2]	CC.PCS.LDV.004 PCS must not provide *open LDV* command when scrubber level is low [UCA.PCS.LDV.004]

UCA.PCS.LDV.001

PCS does not provide *open LDV* command when scrubber level is high [H-2.1]

- Scenario 1: The PCS physical controller fails when scrubber level is high, causing the valve open command not to be provided [UCA.PCS.LDV.001]. As a result, liquid may flow into the gas compressor [H-2.1]. (physical controller)
- Scenario 2: The liquid in the scrubber reaches high level, but processing failures within the PCS result in the valve open command being not provided [UCA.PCS.LDV.001]. As a result, liquid may flow into the gas compressor [H-2.1]. (inadequate control algorithm)
- Scenario 3: The liquid in the scrubber reaches high level, but the PCS does not provide the valve open command [UCA.PCS.LDV.001] because the PCS incorrectly believes the liquid level is normal or low. This flawed process model will occur if the level transmitter drifts and provides wrong measurement. As a result, liquid may flow into the gas compressor [H-2.1]. (inadequate process models)
- Scenario 4: The liquid in the scrubber reaches high level, but the PCS does not provide the valve open command [UCA.PCS.LDV.001] because the PCS is not aware of this situation. This flawed process model will occur if the level transmitter fails, if power is not supplied to the transmitter, or if the signal cable from the transmitter is disconnected. As a result, liquid may flow into the gas compressor [H-2.1]. (inadequate process models)

UCA.PCS.LDV.001

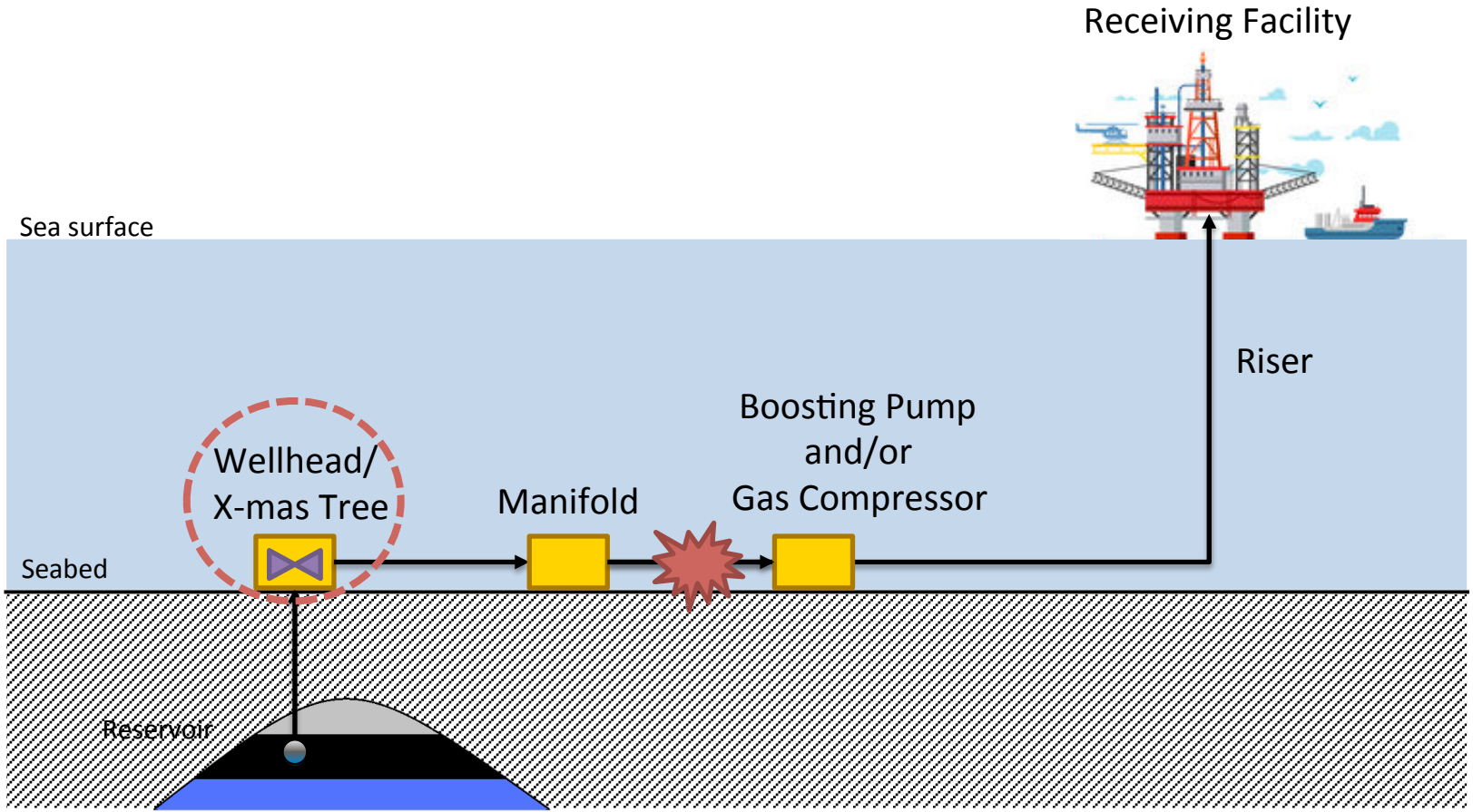
PCS does not provide *open LDV* command when scrubber level is high [H-2.1]

- Scenario 5: PCS provides valve open command when scrubber level is high, but the valve actuator does not receive the control command due to a wiring error between PCS and the valve actuator. As a result, liquid may flow into the gas compressor [H-2.1]. (scenario involving the control path)
- Scenario 6: PCS provides valve open command, and the actuator receives the command when scrubber level is high, but the valve is not opened due no response from the valve actuator. This flawed response will occur if the actuator fails, if power is not supplied to the actuator, or if the valve is stuck. As a result, liquid may flow into the gas compressor [H-2.1]. (scenario involving the control path)
- Scenario 7: PCS provides valve open command when scrubber level is high, and the valve is open, but the liquid level does not drop because liquid supply rate is larger than discharge rate. This flawed process will occur if the calculation of supply and discharge rate was wrong in the design phase. As a result, liquid may flow into the gas compressor [H-2.1]. (scenario related to the controlled process)

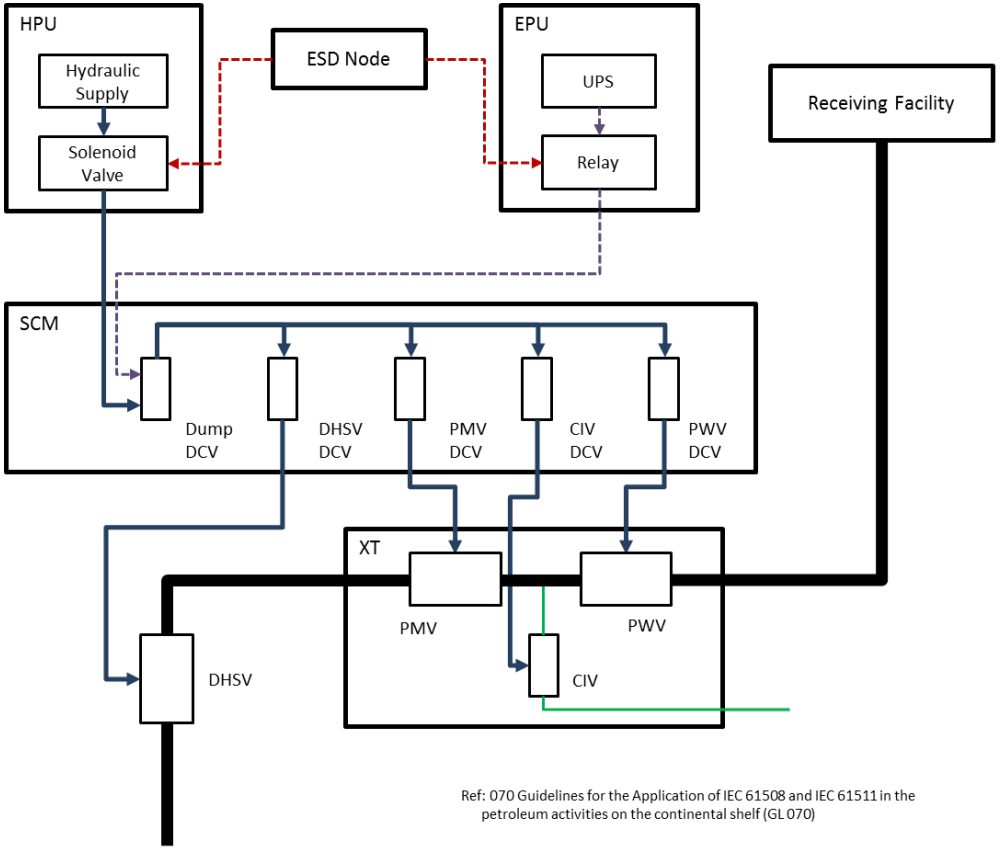
NTNU

STPA to Isolation of Subsea Wells

System Description



System Configuration

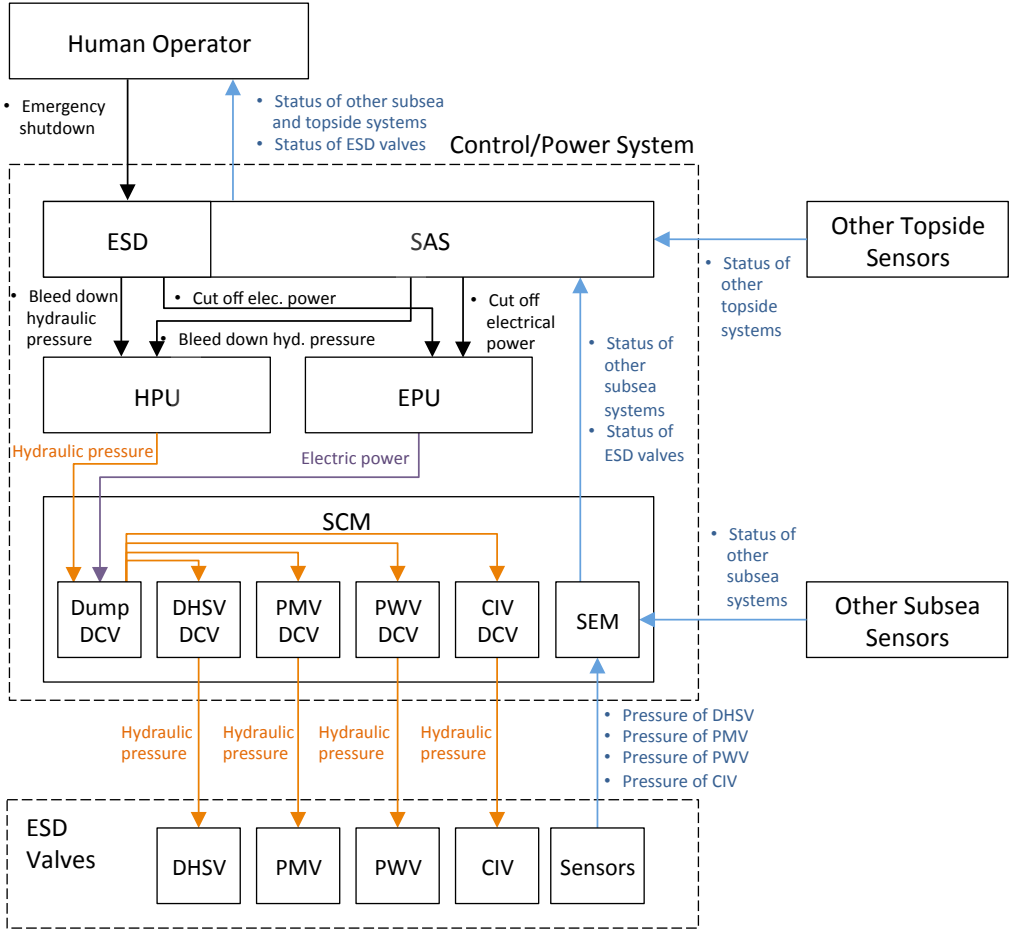


Abbreviation

- CIV: Chemical Injection Valve
- DCV: Directional Control Valve
- DHSV: Down Hole Safety Valve
- EPU: Electrical Power Unit
- ESD: Emergency Shut Down
- HPU: Hydraulic Power Unit
- PMV: Production Master Valve
- PWV: Production Wing Valve
- SCM: Subsea Control Module
- UPS: Uninterruptible Power Supply
- XT: X-mas Tree

Production Flow
Injection Line
ESD Signals
Electrical Power
Hydraulic Fluid

Ref: 070 Guidelines for the Application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf (GL 070)



Abbreviation

- SAS: Safety Automation System
- HPU: Hydraulic Power Unit
- EPU: Electric Power Unit
- SCM: Subsea Control Module
- DCV: Direction Control Valve
- ESD: Emergency Shutdown
- DHSV: Down Hole Safety Valve
- PMW: Production Master Valve
- PWV: Production Wing Valve
- CIV: Chemical Injection Valve
- SEM: Subsea Electronic Module

Control commands
Feedback
Hydraulic pressure
Hydraulic pressure

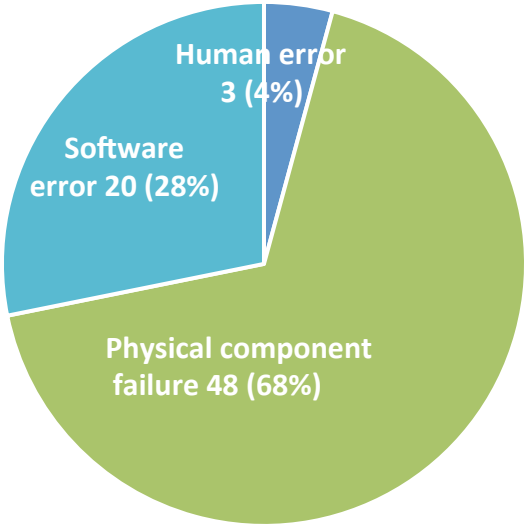
NTNU

Discussions

Opportunities

1. Advantages of STPA – Wider scope

- STPA can cover human errors, software flaws, and physical component failures
- 71 scenarios were identified from Isolation of subsea wells



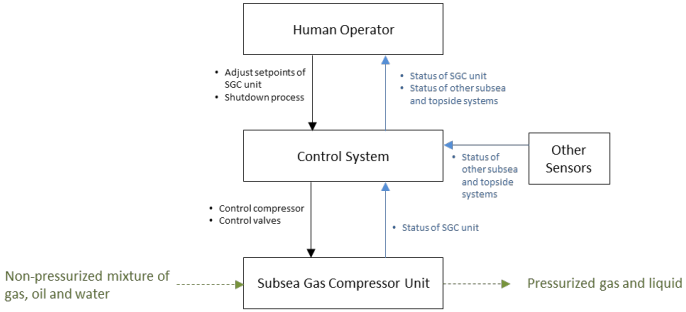


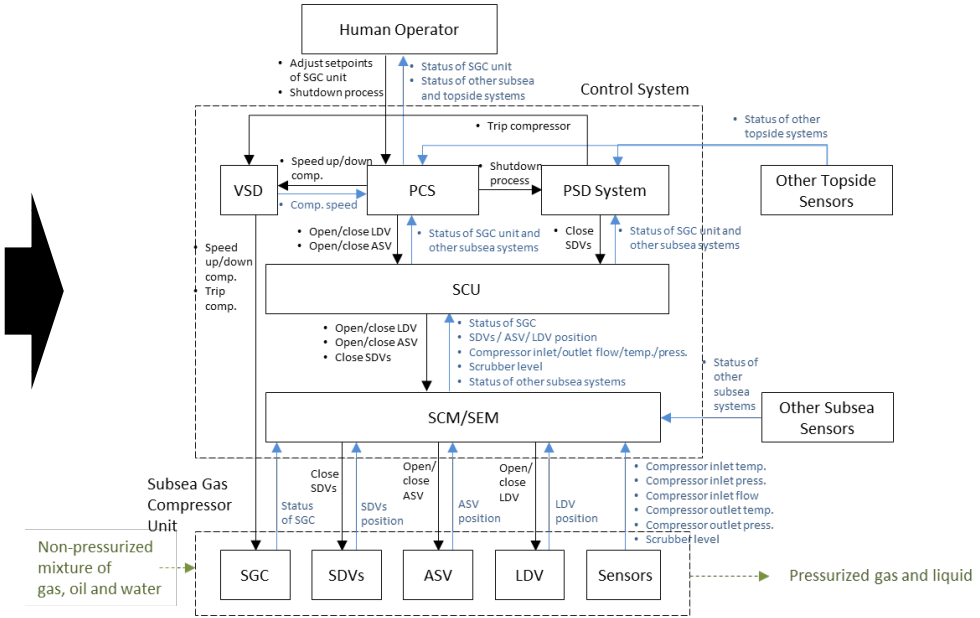
No	Contents
UCA:HOP:001	Human Operator does not provide emergency shutdown command when an emergency occurs [H1,H2]
	SNR:HOP:001.01 Human Operator receives wrong feedback from SAS due to sensor failure
	SNR:HOP:001.02 Human Operator receives no feedback from SAS due to sensor failure
	SNR:HOP:001.03 Human Operator receives no feedback from SAS due to communication cable failure
	SNR:HOP:001.04 Human Operator receives no feedback from SAS due to loss of power supply
	SNR:HOP:001.05 Human Operator receives wrong feedback from SAS due to software error inside SAS
	SNR:HOP:001.06 Human Operator receives no feedback from SAS due to software error inside SAS
	SNR:HOP:001.07 Human Operator receives no feedback from SAS due to HMI failure
	SNR:HOP:001.08 Human Operator receives correct feedback from SAS, but does not provide command
UCA:HOP:002	Human Operator provides emergency shutdown command too late when an emergency occurs [H1,H2]
	SNR:HOP:002.01 Human Operator receives feedback from SAS too late due to sensor failure
	SNR:HOP:002.02 Human Operator receives feedback from SAS too late due to software error inside SAS
	SNR:HOP:002.03 Human Operator receives feedback from SAS in time, but provides control command too late
UCA:HOP:003	Human Operator provides emergency shutdown command when an emergency does not occur [H3]
	SNR:HOP:003.01 Human Operator receives wrong feedback from SAS due to sensor failure
	SNR:HOP:003.02 Human Operator receives wrong feedback from SAS due to software error inside SAS
	SNR:HOP:003.03 Human Operator receives correct feedback from SAS, but provides command
UCA:ESD:001	ESD does not provide bleed down hydraulic pressure command when Human Operator provides emergency shutdown command [H1,H2]
	SNR:ESD:001.01 ESD does not receive control command from Human Operator due to cable failure
	SNR:ESD:001.02 ESD does not receive control command from Human Operator due to loss of power supply
	SNR:ESD:001.03 ESD receives control command from Human Operator, but does not provide control command due to ESD system failure
	n Human Operator provides emergency shutdown command [H1,H2]
	en Human Operator provides emergency shutdown command [H1,H2]
	Operator does not provide emergency shutdown command [H3]
	[
	ESD does not provide cut off electrical power command when Human Operator provides emergency shutdown command [H1,H2]
	SNR:ESD:005.01 ESD does not receive control command from Human Operator due to cable failure
	SNR:ESD:005.02 ESD does not receive control command from Human Operator due loss of power supply
	SNR:ESD:005.03 ESD receives control command from Human Operator, but does not provide control command due to ESD system failure
UCA:ESD:006	ESD provides cut off electrical power command too late when Human Operator provides emergency shutdown command [H1,H2]
	SNR:ESD:006.01 No possible scenario
UCA:ESD:007	ESD provides cut off electrical power command too short when Human Operator provides emergency shutdown command [H1,H2]
	SNR:ESD:007.01 No possible scenario
UCA:ESD:008	ESD provides cut off electrical power command when Human Operator does not provide emergency shutdown command [H3]
	SNR:ESD:008.01 ESD provides control command due to short circuit
UCA:SAS:001	SAS does not provide bleed down hydraulic pressure command when pre-defined abnormal conditions are detected [H1,H2]
	SNR:SAS:001.01 SAS receives wrong feedback from sensors due to sensor failure
	SNR:SAS:001.02 SAS receives no feedback from sensors due to sensor failure
	SNR:SAS:001.03 SAS receives no feedback from sensors due to signal cable failure
	SNR:SAS:001.04 SAS receives no feedback from sensors due to loss of power supply
	SNR:SAS:001.05 SAS receives correct feedback from sensors, but does not provide command due to software error inside SAS
UCA:SAS:002	SAS provides bleed down hydraulic pressure command too late when pre-defined abnormal conditions are detected [H1,H2]
	SNR:SAS:002.01 SAS receives feedback from sensors too late due to sensor failure
	SNR:SAS:002.02 SAS receives feedback from sensors in time, but provides control command too late due to software error inside SAS
UCA:SAS:003	SAS provides bleed down hydraulic pressure command too short when pre-defined abnormal conditions are detected [H1,H2]
	SNR:SAS:003.01 SAS stops providing bleed down command too soon due to software error inside SAS
UCA:SAS:004	SAS provides bleed down hydraulic pressure command when pre-defined abnormal conditions are not detected [H3]
	SNR:SAS:004.01 SAS receives wrong feedback from sensors due to sensor failure
	SNR:SAS:004.02 SAS receives correct feedback from sensors, but provides command due to software error inside SAS
UCA:SAS:005	SAS does not provide cut off electrical power command when pre-defined abnormal conditions are detected [H1,H2]
	SNR:SAS:005.01 SAS receives wrong feedback from sensors due to sensor failure
	SNR:SAS:005.02 SAS receives no feedback from sensors due to sensor failure
	SNR:SAS:005.03 SAS receives no feedback from sensors due to signal cable failure
	SNR:SAS:005.04 SAS receives no feedback from sensors due to loss of power supply
	SNR:SAS:005.05 SAS receives correct feedback from sensors, but does not provide command due to software error inside SAS
UCA:SAS:006	SAS provides cut off electrical power command too late when pre-defined abnormal conditions are detected [H1,H2]
	SNR:SAS:006.01 SAS receives feedback from sensors too late due to sensor failure
	SNR:SAS:006.02 SAS receives feedback from sensors in time, but provides control command too late due to software error inside SAS
UCA:SAS:007	SAS provides cut off electrical power command too short when pre-defined abnormal conditions are detected [H1,H2]
	SNR:SAS:007.01 SAS stops providing bleed down command too soon due to software error inside SAS
UCA:SAS:008	SAS provides cut off electrical power command when pre-defined abnormal conditions are not detected [H3]
	SNR:SAS:008.01 SAS receives wrong feedback from sensors due to sensor failure
	SNR:SAS:008.02 SAS receives correct feedback from sensors, but provides command due to software error inside SAS
UCA:HPU:001	HPU provides hydraulic pressure when ESD or SAS provides bleed down hydraulic pressure command [H1,H2]
	SNR:HPU:001.01 HPU receives wrong command from ESD or SAS due to communication cable failire
	SNR:HPU:001.02 HPU receives no command from ESD or SAS due to communication cable failure
	SNR:HPU:001.03 HPU receives no command from ESD or SAS due to loss of power supply
	SNR:HPU:001.04 HPU receives command from ESD or SAS, but provides hydraulic pressure due to software error inside HPU
	SNR:HPU:001.05 HPU receives command from ESD or SAS, but provides hydraulic pressure due to solenoid valve failure
UCA:HPU:002	HPU does not provide hydraulic pressure too late when ESD or SAS provides bleed down hydraulic pressure command [H1,H2]
	SNR:HPU:002.01 HPU receives command from ESD or SAS too late due to communication cable failure
	SNR:HPU:002.02 HPU receives command in time, but stop providing hydraulic pressure too late due to software error inside HPU
	SNR:HPU:002.03 HPU receives command in time, but stop providing hydraulic pressure too late due to solenoid valve failure
UCA:HPU:003	HPU does not provide hydraulic pressure too short when ESD or SAS provides bleed down hydraulic pressure command [H1,H2]
	SNR:HPU:003.01 HPU starts providing hydraulic pressure again due to software error inside HPU
	SNR:HPU:003.02 HPU starts providing hydraulic pressure again due to solenoid valve failure
UCA:HPU:004	HPU does not provide hydraulic pressure when ESD or SAS does not provide bleed down hydraulic pressure command [H3]
	SNR:HPU:004.01 HPU receives wrong command from ESD or SAS due to communication cable failire
	SNR:HPU:004.02 HPU does not receive command from ESD or SAS, but provides hydraulic pressure due to software error inside HPU
	SNR:HPU:004.03 HPU does not receive command from ESD or SAS, but provides hydraulic pressure due to solenoid valve failure
UCA:EPU:001	EPU provides electric power when ESD or SAS provides cut off electrical power command [H1,H2]
	SNR:EPU:001.01 EPU receives wrong command from ESD or SAS due to communication cable failire
	SNR:EPU:001.02 EPU receives no command from ESD or SAS due to communication cable failure
	SNR:EPU:001.03 EPU receives no command from ESD or SAS due to loss of power supply
	SNR:EPU:001.04 EPU receives command from ESD or SAS, but provides electric power due to software error inside EPU
	SNR:EPU:001.05 EPU receives command from ESD or SAS, but provides electric power due to relay failure
UCA:EPU:002	EPU does not provide electric power too late when ESD or SAS provides cut off electrical power command [H1,H2]
	SNR:EPU:002.01 EPU receives command from ESD or SAS too late due to communication cable failure
	SNR:EPU:002.02 EPU receives command in time, but stop providing electric power too late due to software error inside EPU
	SNR:EPU:002.03 EPU receives command in time, but stop providing electric power too late due to relay failure
UCA:EPU:003	EPU does not provide electric power too short when ESD or SAS provides cut off electrical power command [H1,H2]
	SNR:EPU:003.01 EPU starts providing hydraulic pressure again due to software error inside EPU
	SNR:EPU:003.02 EPU starts providing hydraulic pressure again due to relay failure
UCA:EPU:004	EPU does not provide electric power when ESD or SAS does not provide cut off electrical power command [H3]
	SNR:EPU:004.01 EPU receives wrong command from ESD or SAS due to communication cable failire
	SNR:EPU:004.02 EPU does not receive command from ESD or SAS, but provides electric power due to software error inside EPU
	SNR:EPU:004.03 EPU does not receive command from ESD or SAS, but provides electric power due to relay failure
UCA:SCM:001	SCM does not distribute hydraulic pressure when hydraulic pressure or electric power is supplied [H3]
	SNR:SCM:001.01 Hydraulic leak
	SNR:SCM:001.02 DCVs are clogged
UCA:SCM:002	SCM distributes hydraulic pressure when hydraulic pressure or electric power is not supplied [H1,H2]
	SNR:SCM:002.01 No possible scenario
UCA:SCM:003	SCM does not distribute hydraulic pressure too late when hydraulic pressure or electric power is not supplied [H1,H2]
	SNR:SCM:003.01 Due to long distance between HPU and SCM

Opportunities

2. Advantages of STPA – Top-down approach

- Analysis can be refined with more details





Opportunities

2. Advantages of STPA – Top-down approach

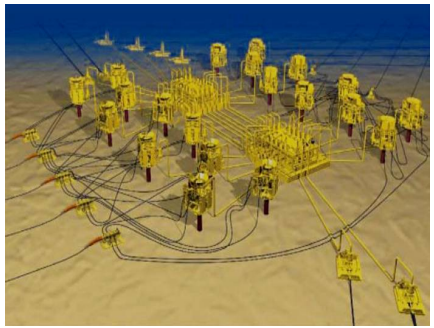
- Analysis can be refined with more details

- Gas leak at HVAC inlet
- Gas leak in non-hazardous area
- Gas leak in hazardous area
- Fire in hazardous area
- Gas/water heat exchanger tube

Controller : SAS								
No	Control Action	Process model: Pre-defined emergency conditions	Unsafe Control Actions? Not provided	Provided	Too early	Too late	Too short	Too long
1	Bleed down hydraulic pressure	Occurred	Unsafe [H1,H2]	Safe	N/A	Unsafe [H1,H2]	Unsafe [H1,H2]	N/A
2		Not occurred	Safe	Unsafe [H3]	N/A	N/A	N/A	N/A
3	Cut off electrical power	Occurred	Unsafe [H1,H2]	Safe	N/A	Unsafe [H1,H2]	Unsafe [H1,H2]	N/A
4		Not occurred	Safe	Unsafe [H3]	N/A	N/A	N/A	N/A


Subsea Compression Station
Åsgard Subsea Compression Project
Compressor Module
Client tag: 17XK116
Scrubber Module
Client tag: 17XL113
Inlet Cooler module
Client tag: 17XH114
Discharge Cooler Module
Client tag: 17XH117
In operation since 2015
Cassette Base Frame
Client tag: 17XC103
Pump Module
Client tag: 17XP113
Spool Interface module
Client tag: 17XL204
VS
CPDU module
Client tag: 17XE112
Subsea Compressor Station Template
Client tag: 17XC002
CPDU Transformer module
Client tag: 17XE165
PumpTransformer module
Client tag: 17XE161
Train 1
Train 2
Pump and Control UTA
Client tag: 17XE196
Statoil
AkerSolutions

Opportunities





Subsea systems are suddenly getting more complex and software-intensive

⬇

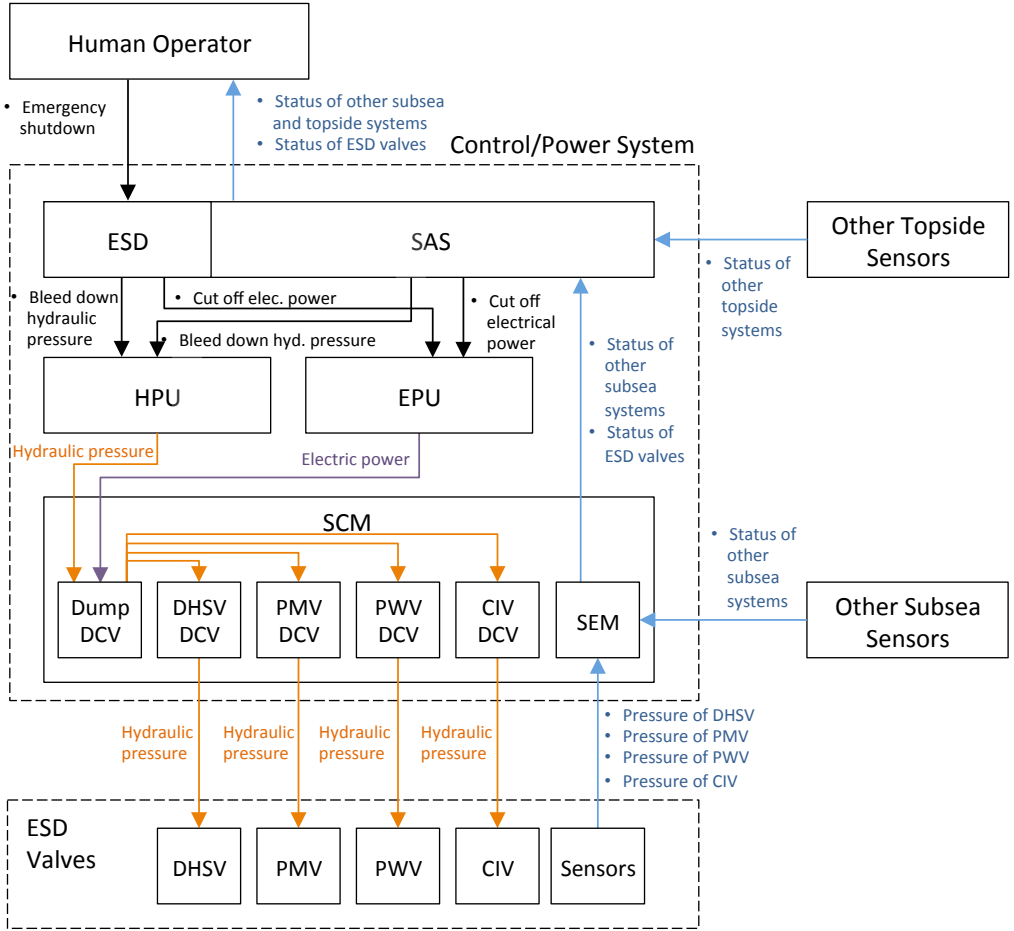
Traditional hazard identification methods (FMECA or HAZOP) are not suitable to identify software flaws, human errors, or interactions of complex system components

⬇

STPA can do it!
(with systematic and top-down approach)

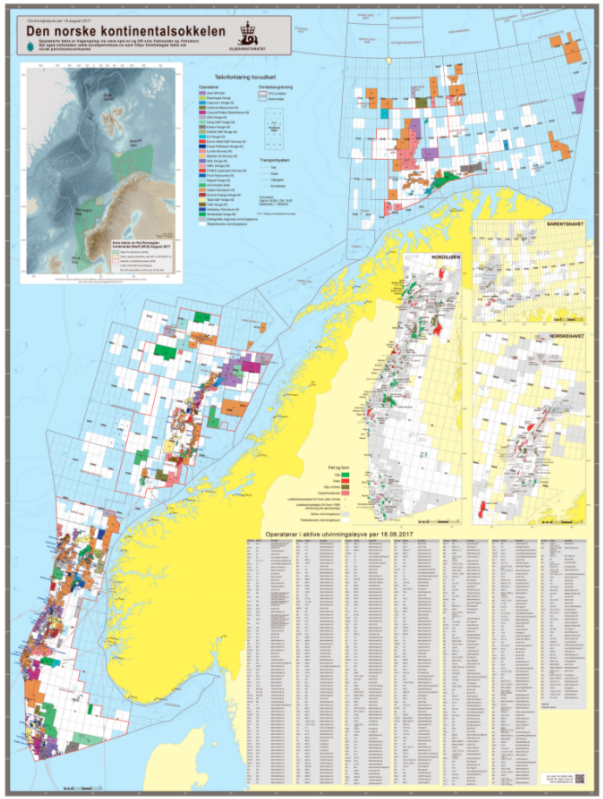
Challenges

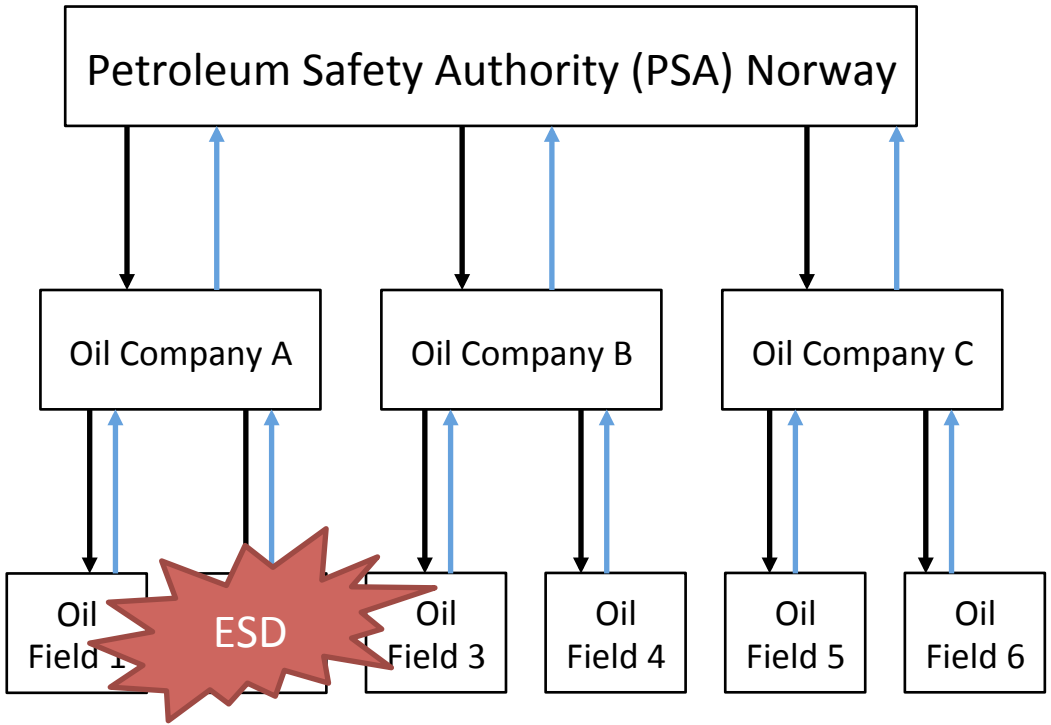
1. Dynamic control structure



Challenges

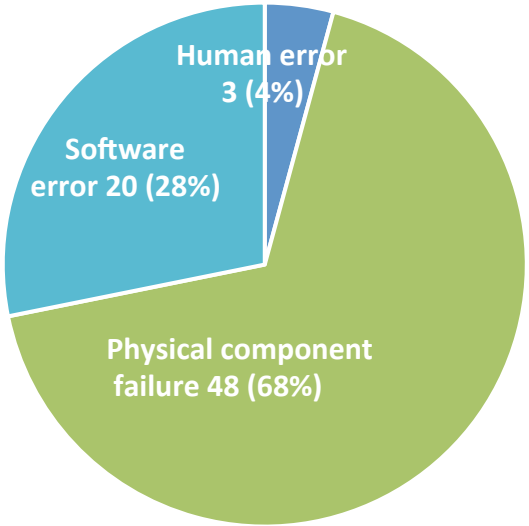
1. Dynamic control structure





Challenges

2. Physical component plays an important role in subsea systems



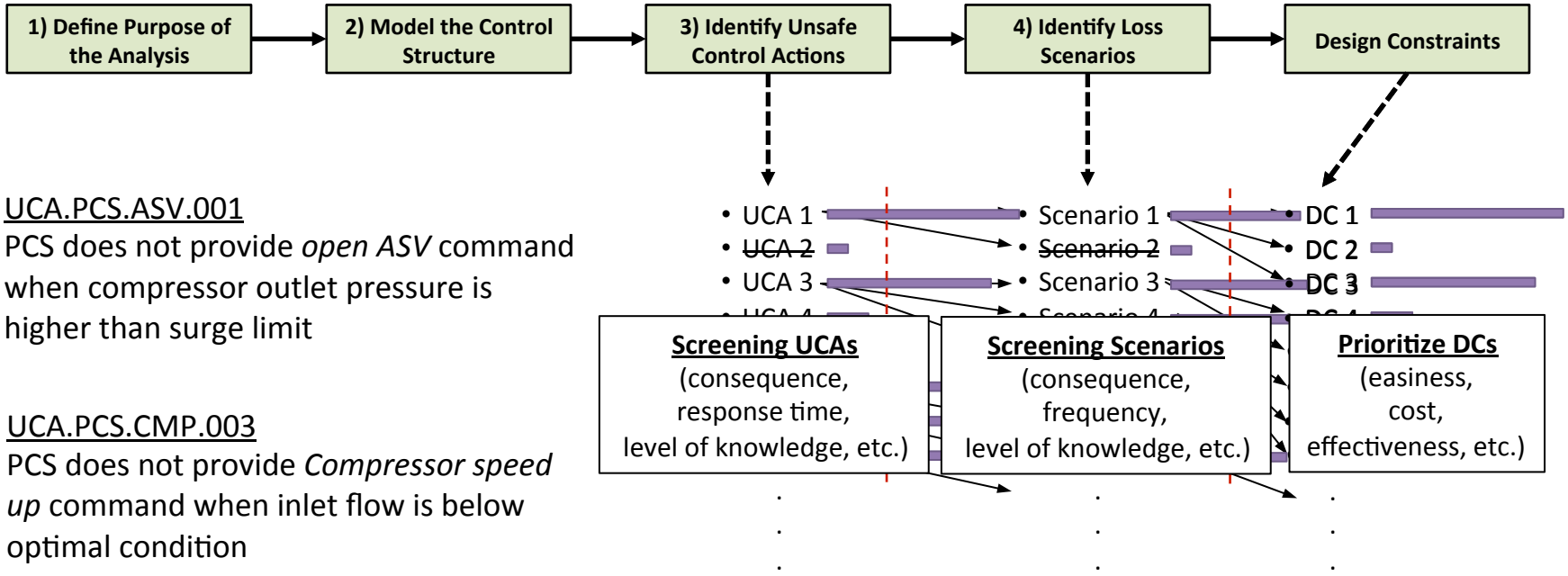
Hardware-oriented design constraints, like

- Gas leakage detector must have redundancy (2oo3 configuration)
- Gas leakage detector must be connected to redundant power supply or UPS

Need to classify and prioritize design constraints

- Some constraints are cheap, easy and very effective, while others are expensive, difficult and less effective
- Some scenarios can never be completely prevented, while others can be

Screening and Prioritization

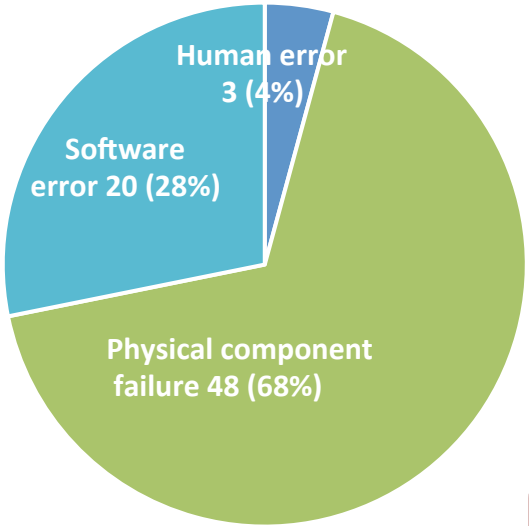


UCA.PCS.ASV.001
PCS does not provide *open ASV* command when compressor outlet pressure is higher than surge limit

UCA.PCS.CMP.003
PCS does not provide *Compressor speed up* command when inlet flow is below optimal condition

Challenges

3. Iterations of STPA



Hardware-oriented design constraints, like

- Gas leakage detector must have redundancy (2oo3 configuration)
- Gas leakage detector must be connected to redundant power supply of UPS

Design constraints that increase system complexity, like

- SAS must generate an alarm when no signal is received from gas leakage detector

Do we need to conduct STPA again?
- if not, what can we do for additional hazards?
- if so, when can we stop?

Future Work

- Subsea Processing System
- Subsea Safety System
- Subsea Production System

→ Summarize overall STPA challenges in subsea application and provide solutions

→ Apply STPA to Subsea safety standards in Norway

NTNU



NTNU

