NTNU

Norwegian University of Science and Technology

Application of STPA to Subsea Systems

Opportunities and Challenges

2.2.2018

Hyungju Kim
Mary Ann Lundteigen

Contents

Introduction to STPA

What is STPA?

- Systems-Theoretic Process Analysis (STPA)
- A hazard identification technique based on control and systems theory
- Accidents are not “Failure Problem”, but “Control Problem”
- The main objective is to identify unsafe control actions and derive safety constraints
- Used in many different sectors and domains, but have not yet been tested for subsea systems

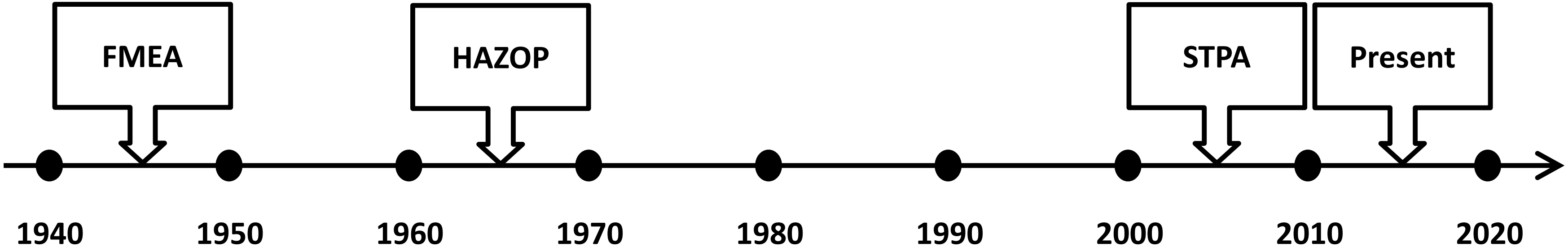
Why STPA?

- We already have widely used Hazard Identification Methods
  - Preliminary Hazard Analysis (PHA)
  - Failure Modes and Effects Analysis (FMEA)
  - HAZard and OPerability analysis (HAZOP)

  .
  .
  .

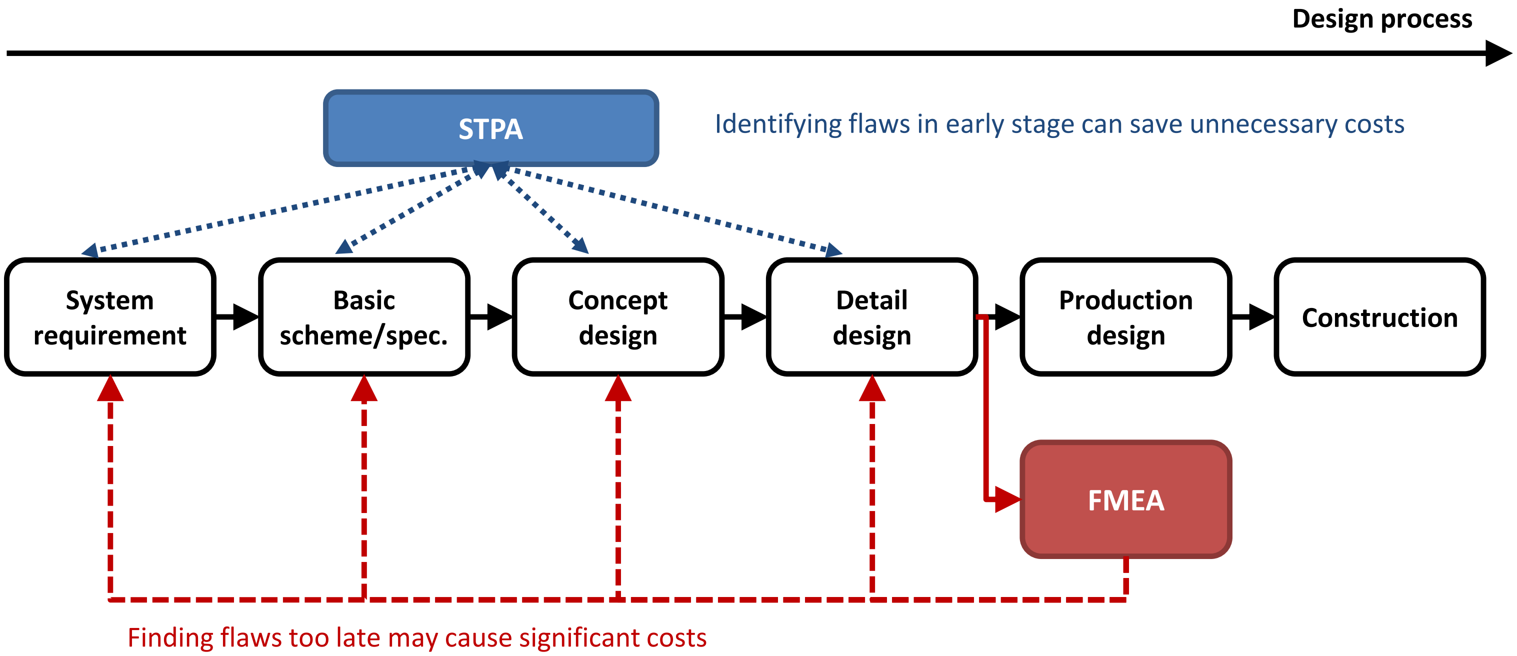
Why STPA?

1) STPA was recently developed for modern complex systems



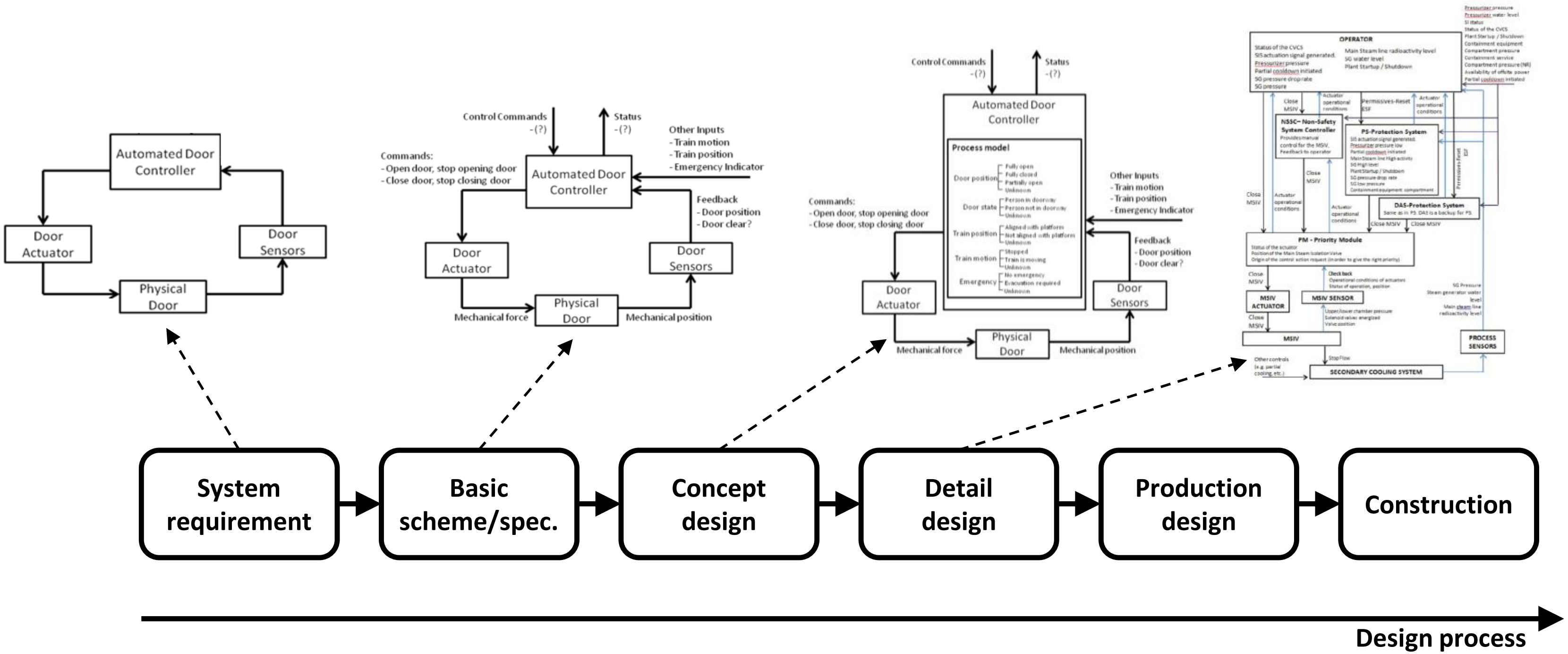
Why STPA?

2) STPA is a top-down approach: analysis can be conducted from the beginning of a project



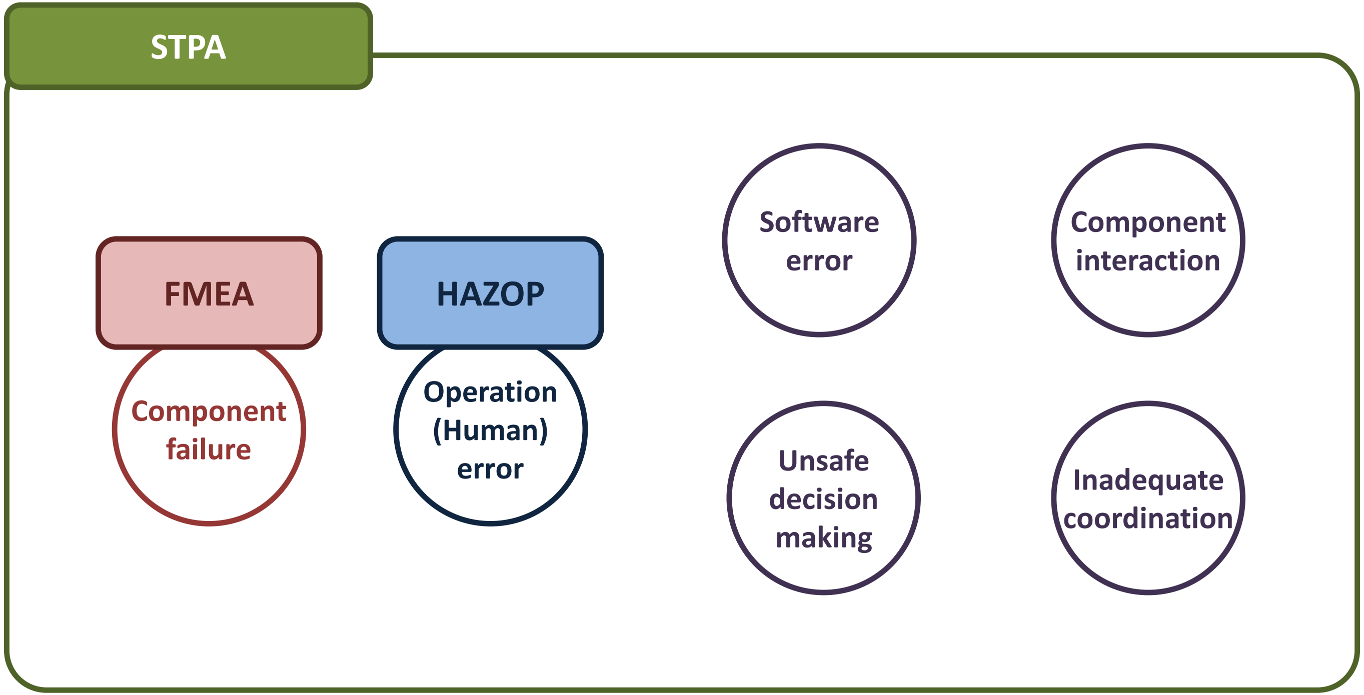
Why STPA?

2) STPA is a top-down approach: analysis can be conducted from the beginning of a project



Why STPA?

3) STPA can (theoretically) provide wider scope compared to other methods



Why STPA?

3) STPA can (theoretically) provide wider scope compared to other methods

U.S. Missile Defence System (Pereira et al. 2006)

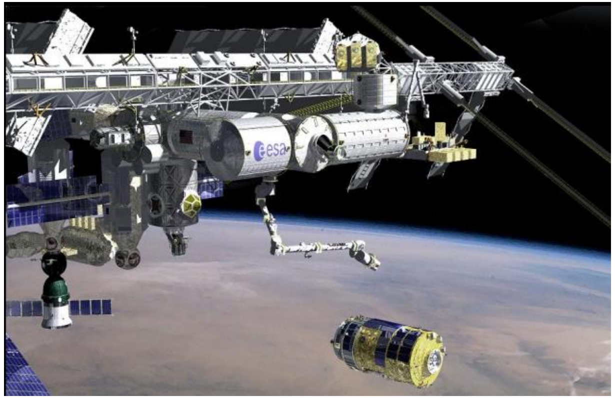
- The system had been subjected to standard hazard analysis methods, but one more additional analysis was required
- STPA found so many flaws (by two persons for only three month analysis), so that the deployment was delayed for six months to fix them

Why STPA?

3) STPA can (theoretically) provide wider scope compared to other methods

Japanese Aerospace Exploration Agency (JAXA) (Ishimatsu et al. 2014)

- JAXA used STPA experimentally on their unmanned spacecraft
- STPA found everything identified in fault tree analysis
- STPA found additional hazardous scenarios related to system design flaws, software errors, hazardous interactions, etc.



How to STPA?

STPA Step 0
Establish System Engineering Foundation

Sub-steps of STPA Step 0
1) Identify system level accidents/hazards
2) Identify system safety constraints
3) Identify functional control structure

Output of STPA Step 0
- List of system level accident, hazards, safety constraints
- Control loop diagram

STPA Step 1
Identify Unsafe Control Actions (UCAs)

Sub-steps of STPA Step 1
1) Identify control actions and conditions
2) Examine each combination
3) Identify and summarise UCAs

Output of STPA Step 1
- List of UCAs

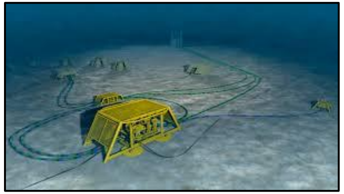
STPA Step 2
Identify Causes of the UCAs

Sub-steps of STPA Step 2
1) Identify scenarios and causal factors for each UCA
2) Develop detailed requirement to avoid the hazards

Output of STPA Step 2
- List of scenarios and causal factors of each UCA
- List of safety requirements of each scenario and causal factor

STPA Studies in RAMS Group

STPA Studies in RAMS Group



- Subsea Gatebox (prioritization) – Master thesis (Nanda)
- Subsea Gatebox (post process) – Journal paper (Juntao)
- Isolation of subsea wells – OTC 2018
- Subsea gas compression – ESREL 2018
- To be continued…

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

- Securing maintenance are – Master thesis (Sunniva)

Description of the Papers

ESREL 2018	OTC 2018
Title: Application of Systems-Theoretic Process Analysis to a Subsea Gas Compression System	**Title**: Application of Systems-Theoretic Process Analysis to the isolation of subsea wells

Main Objective

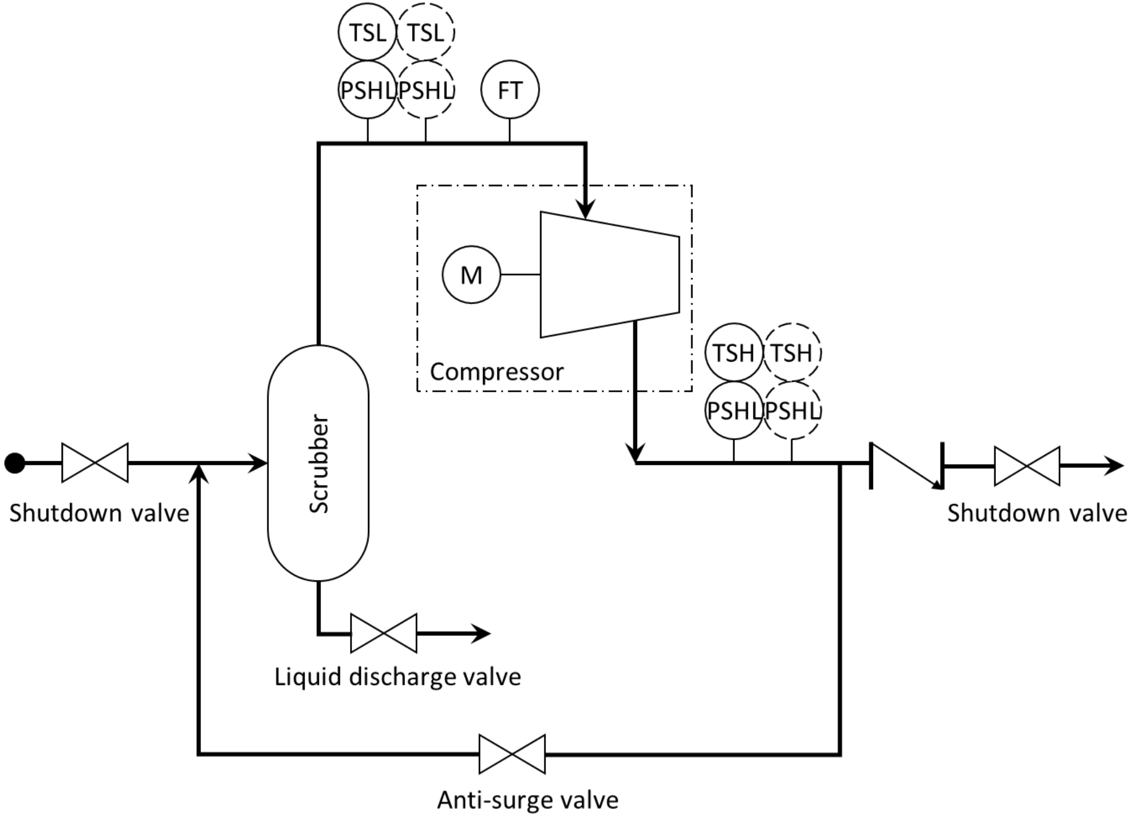
Discuss opportunities and challenges of the application of STPA to subsea systems

ESREL 2018	OTC 2018
Focus: Subsea processing system (Extend the discussion to the general use of STPA)	**Focus**: Subsea safety system (More focus on specific features of subsea systems)

STPA to Subsea Gas Compression

ESREL 2018

System Description

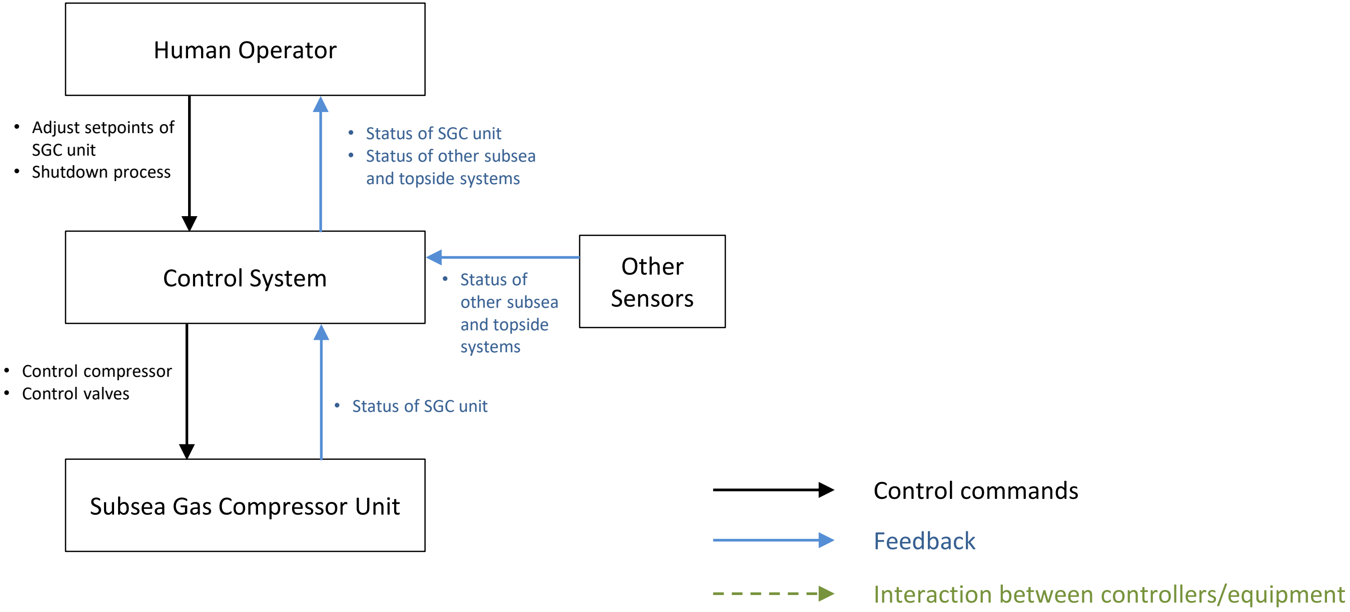


STPA Step 0 – System level accidents/hazards/safety constraints

System	System-Level Accident	System-Level Hazard	System-Level Safety Constraints
Subsea Gas Compression System*	SLA1: People die or are injured due to large amount of gas release (e.g., loss of buoyancy of nearby vessels, fire/explosion on topside) SLA2: The sea is polluted due to large amount of gas release	SLH1: SGC unit continues to supply gas when gas leaks to the environment	SLSC1: SGC unit must stop compressing gas when gas leaks to the environment
	SLA3: Valuable subsea components are damaged	SLH2: Compressor operates outside normal operation conditions	SLSC2: Compressor must be protected from extreme operating conditions that can damage the compressor
	SLA4: Production is reduced or interrupted when compression is needed	SLH3: SGC unit stops compressing gas when compression is needed	SLSC3: SGC unit must never stop compressing gas when gas compression is needed
		SLH4: Compressor operates outside optimal conditions	SLSC4: SGC must be operated within optimal conditions

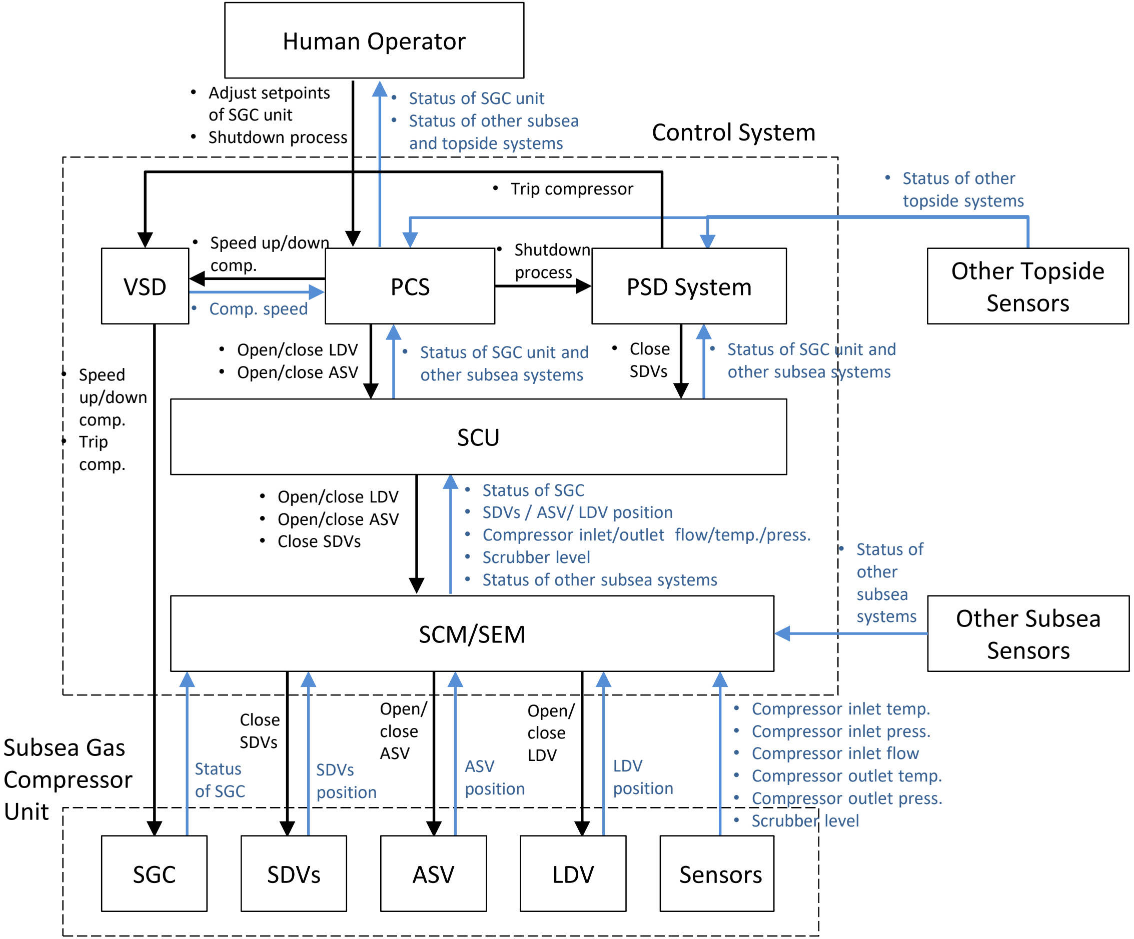
*It is assumed that the system is designed inherently safe

STPA Step 0 – Functional control structure



Scope: Processing after starting up (turning on compressor, opening shutdown valves are not included)

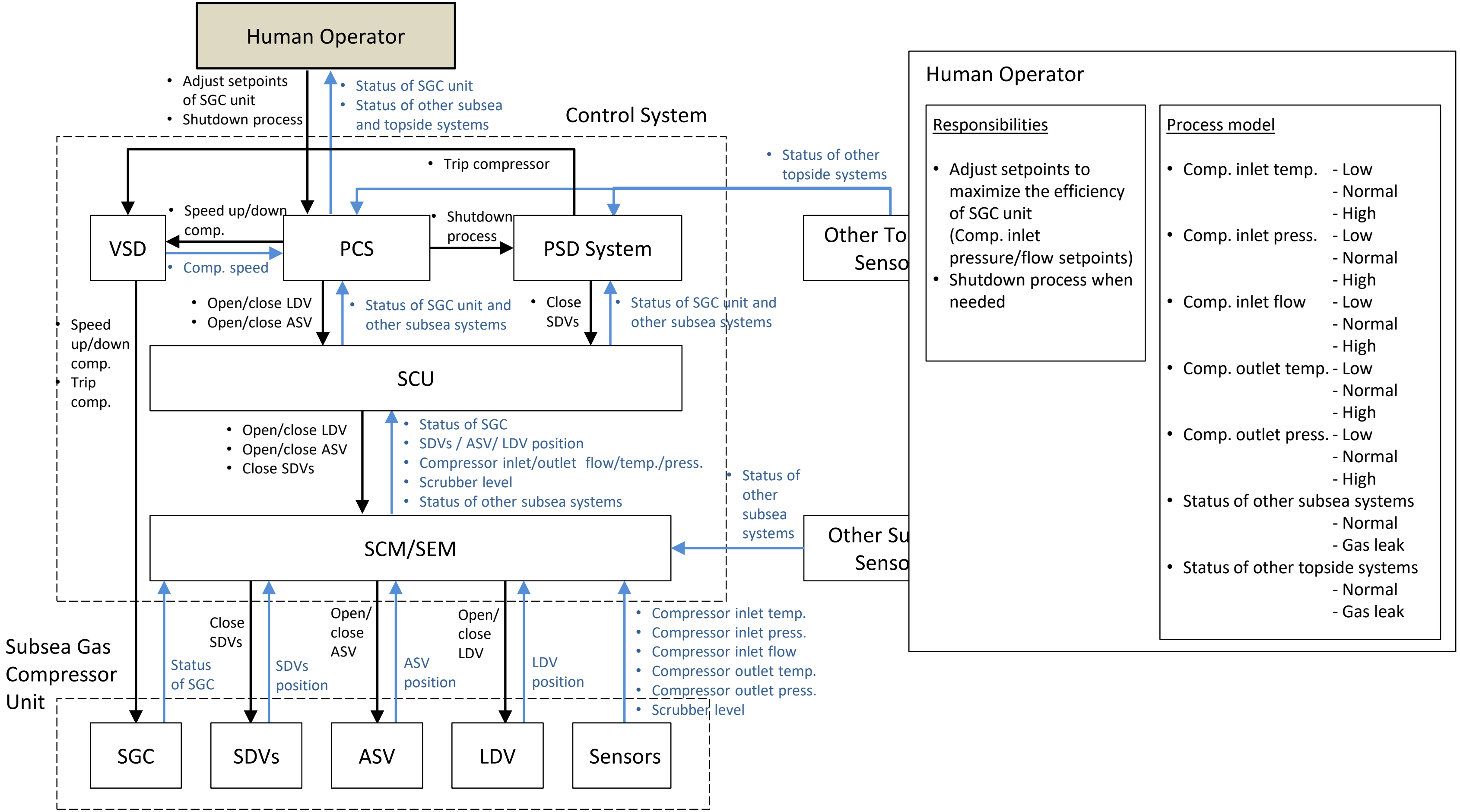
STPA Step 0 – Functional control structure



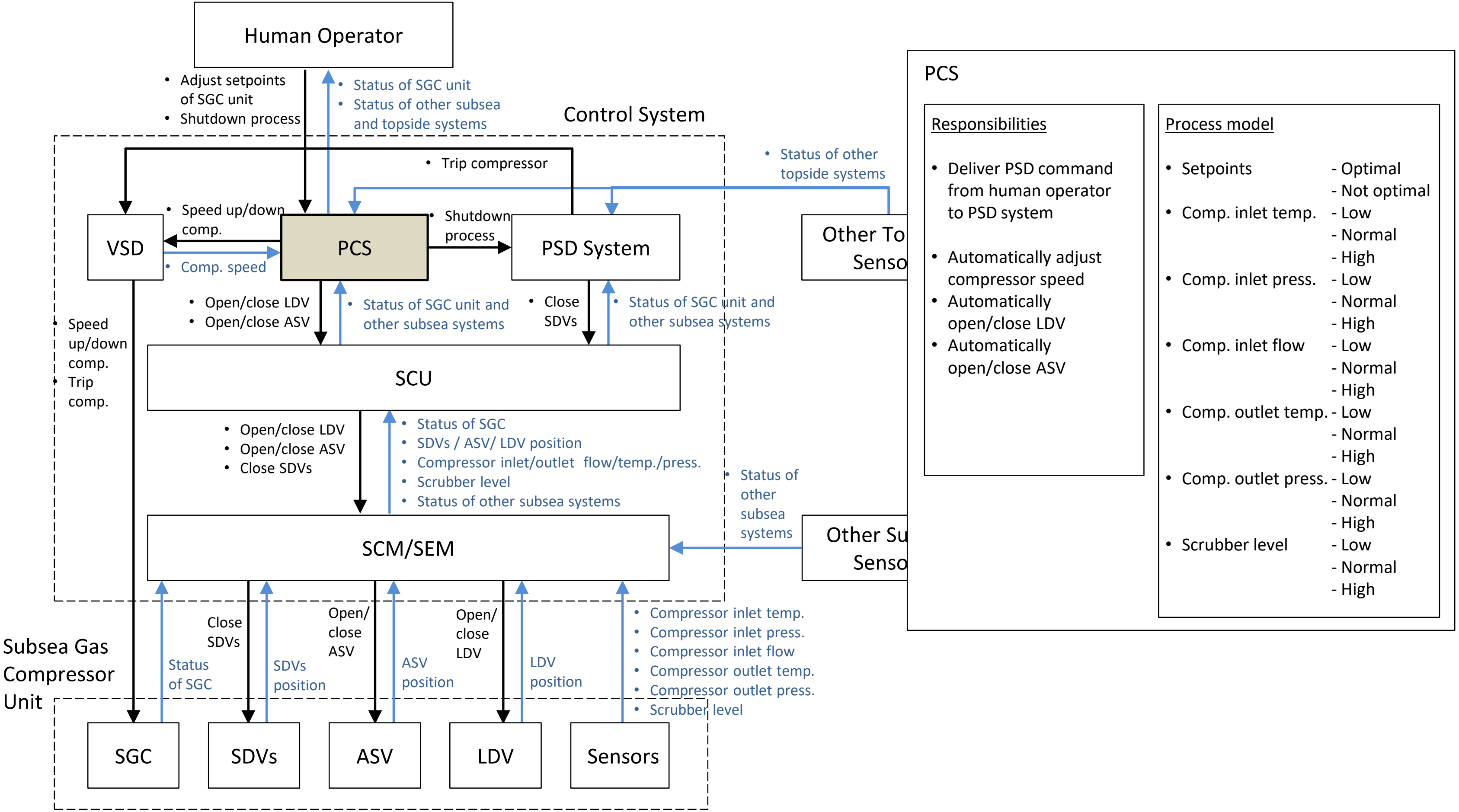
Abbreviation

- 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

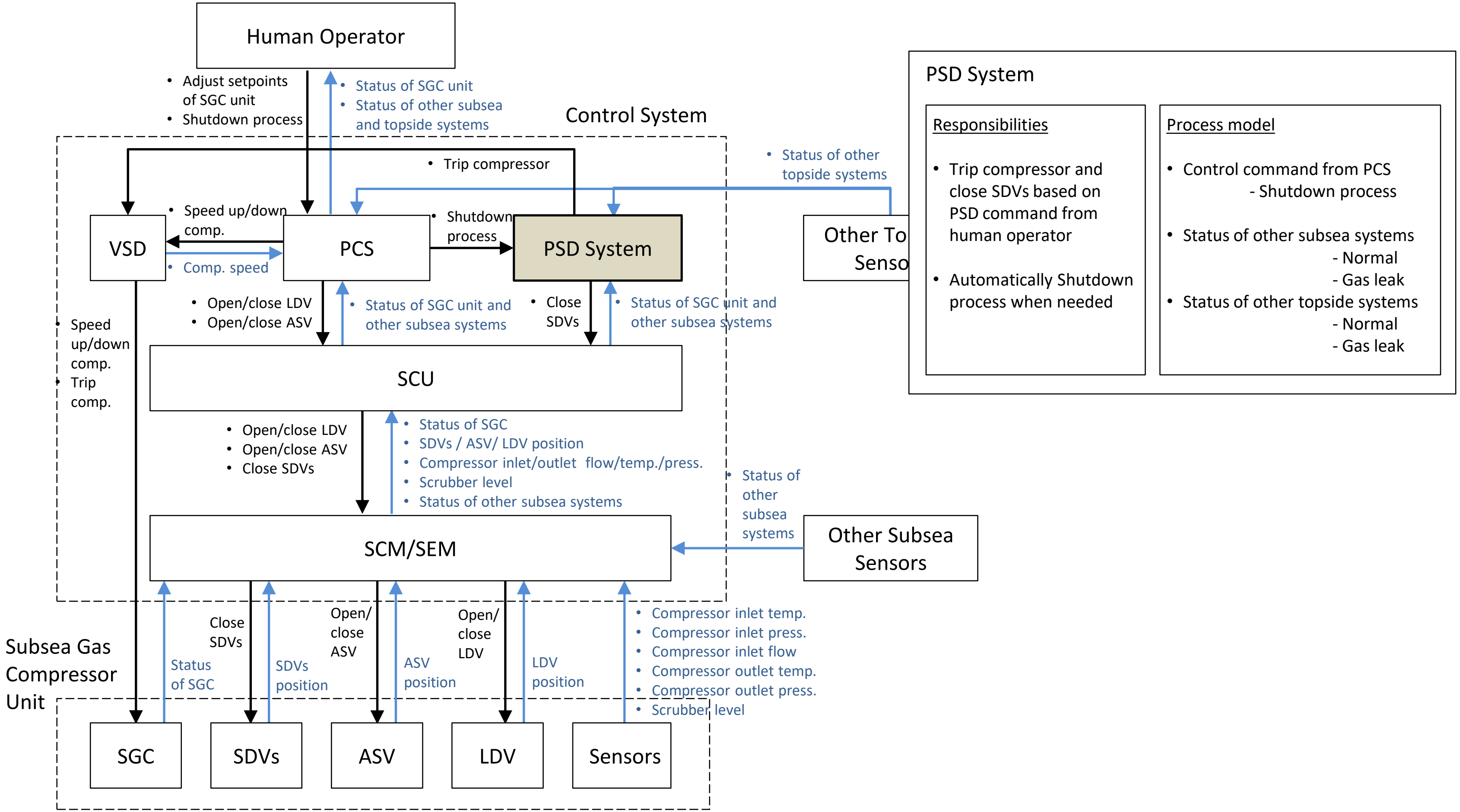
STPA Step 0 – Functional control structure



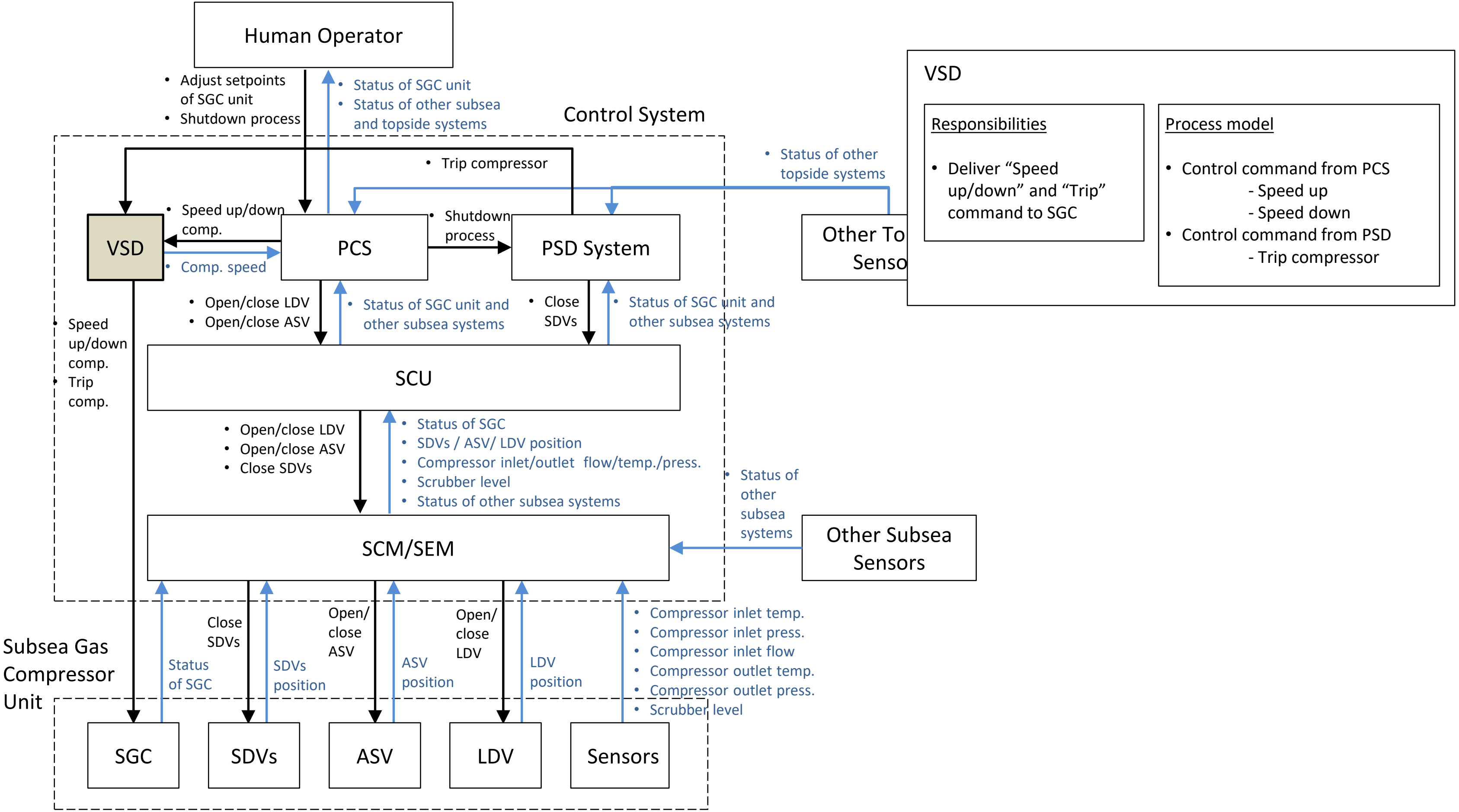
STPA Step 0 – Functional control structure



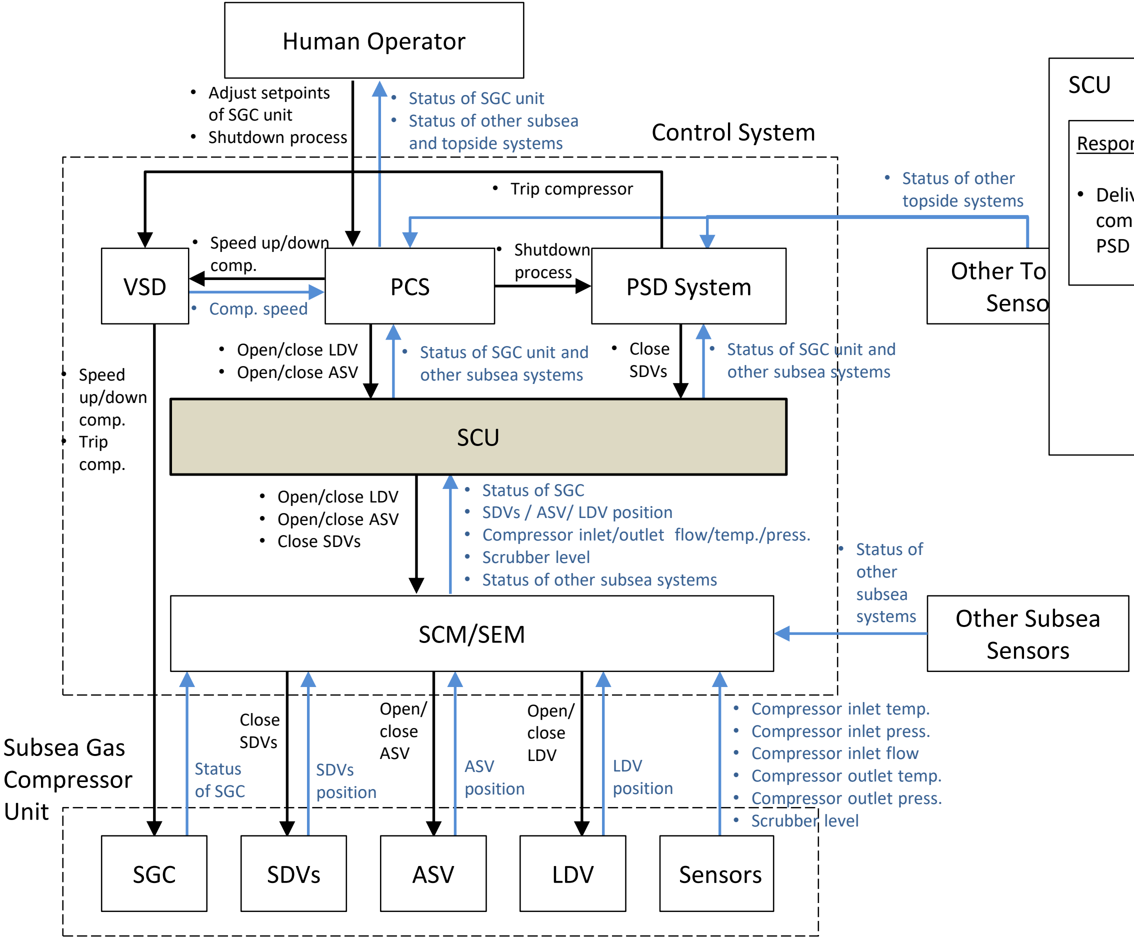
STPA Step 0 – Functional control structure



STPA Step 0 – Functional control structure



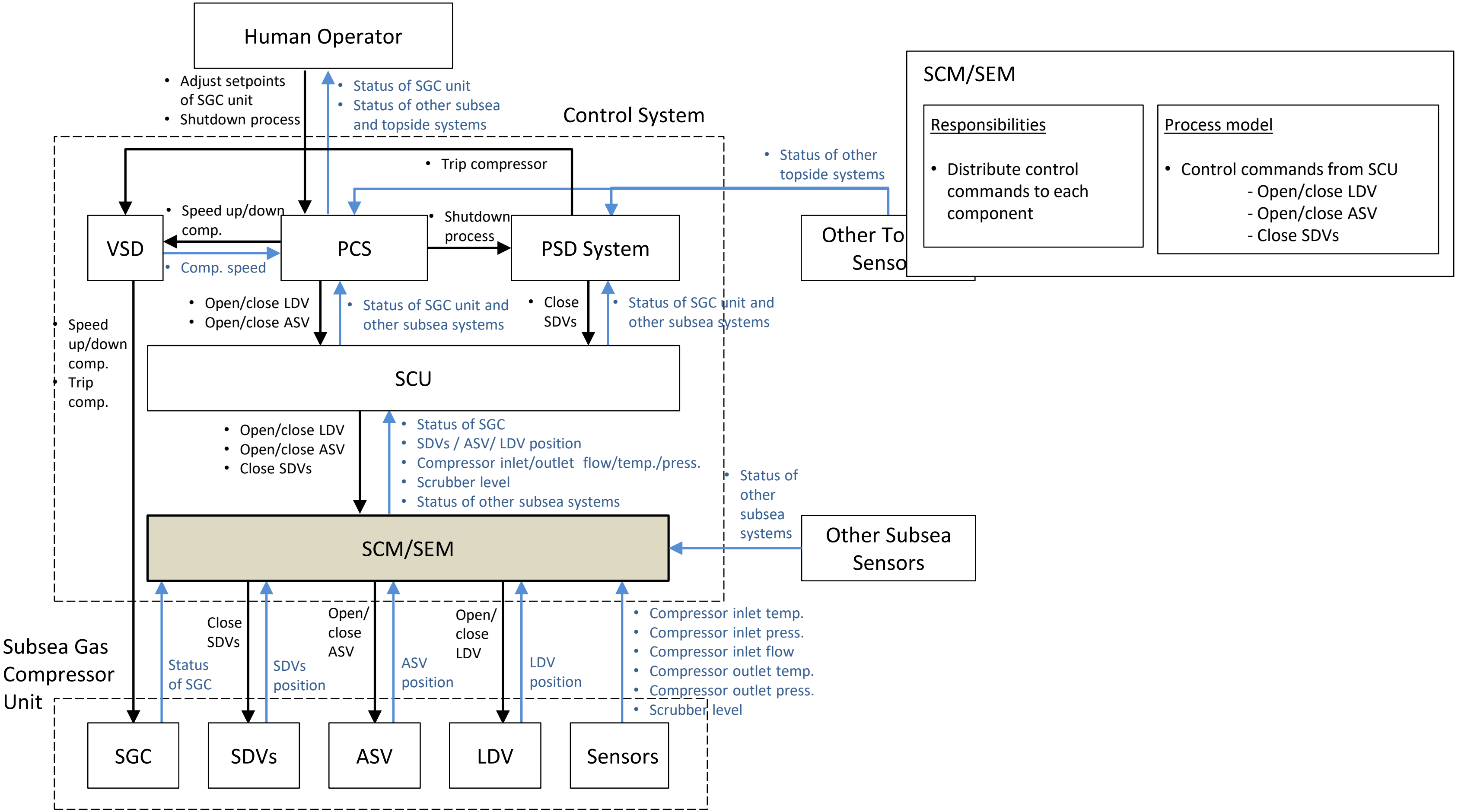
STPA Step 0 – Functional control structure



SCU

Responsibilities	Process model
• Deliver control commands from PCS and PSD system to SCM/SEM	• Control commands from PCS - Open/close LDV - Open/close ASV • Control commands from PSD sys. - Close SDVs

STPA Step 0 – Functional control structure



STPA Step 1 – Identifying UCAs

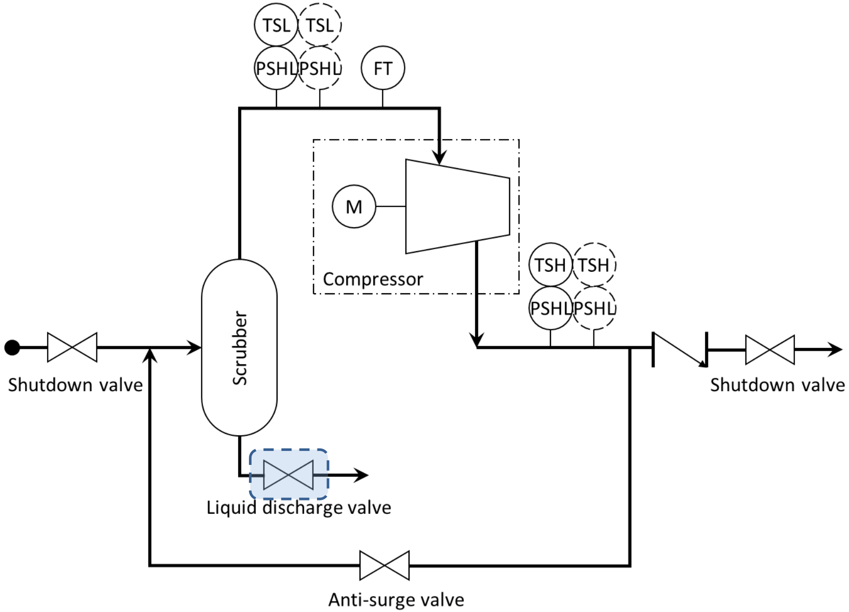
PCS

Responsibilities

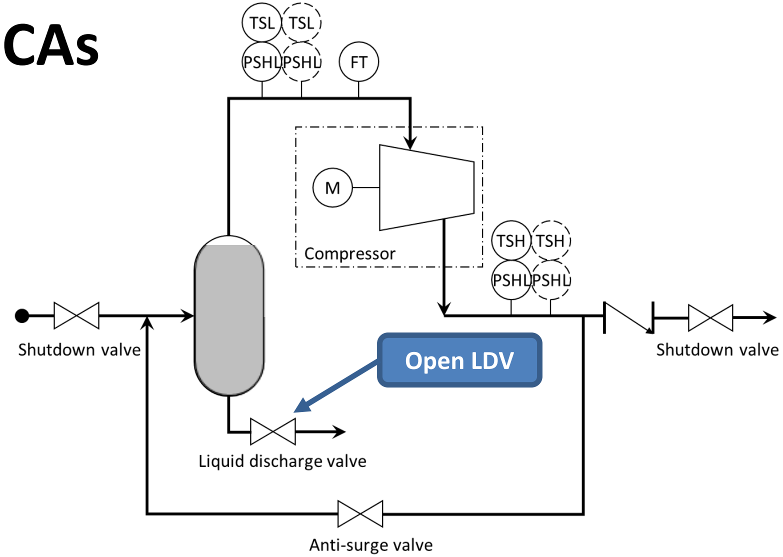
- Deliver PSD command from human operator to PSD system
- Automatically adjust compressor speed
- Automatically open/close LDV
- Automatically open/close ASV

Process model

- Set points - Optimal
  - Not optimal
- Comp. inlet temp. - Low
  - Normal
  - High
- Comp. inlet press. - Low
  - Normal
  - High
- Comp. inlet flow - Low
  - Normal
  - High
- Comp. outlet temp. - Low
  - Normal
  - High
- Comp. outlet press. - Low
  - Normal
  - High
- Scrubber level - Low
  - Normal
  - High



STPA Step 1 – Identifying UCAs



Controller : PCS								
No	Control Action	Condition	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						

STPA Step 1 – Identifying UCAs

Controller : PCS								
No	Control Action	Condition	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: *Open LDV* command is not provided when scrubber level is high

UCA.PCS.LDV.002: *Open LDV* command is provided too late when scrubber level is high

UCA.PCS.LDV.003: *Open LDV* command is provided too short when scrubber level is high

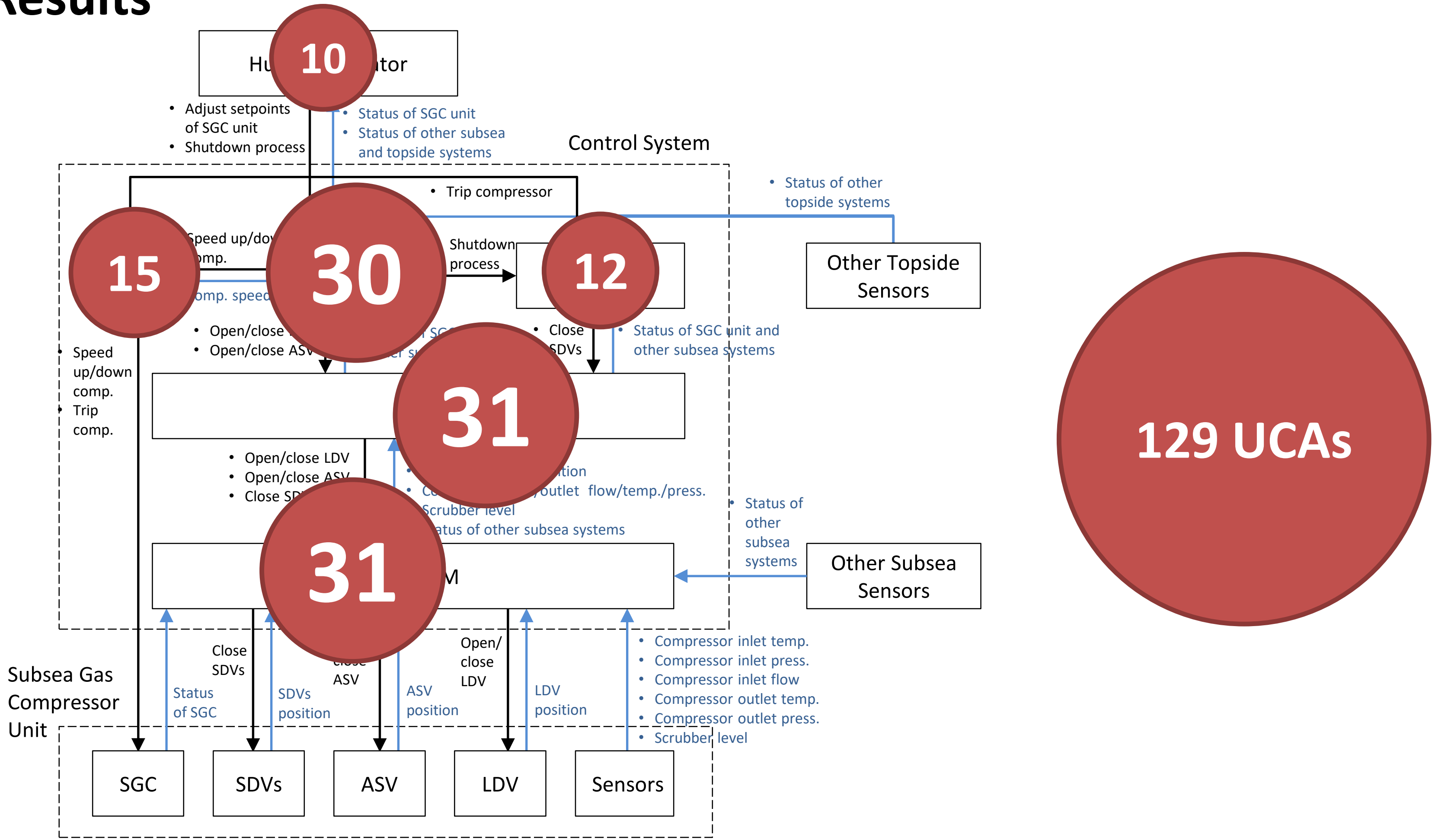
UCA.PCS.LDV.004: *Open LDV* command is provided when scrubber level is low

UCA.PCS.LDV.005: *Close LDV* command is provided when scrubber level is high

STPA Step 2: Identifying Causes of UCAs and Safety Constrains

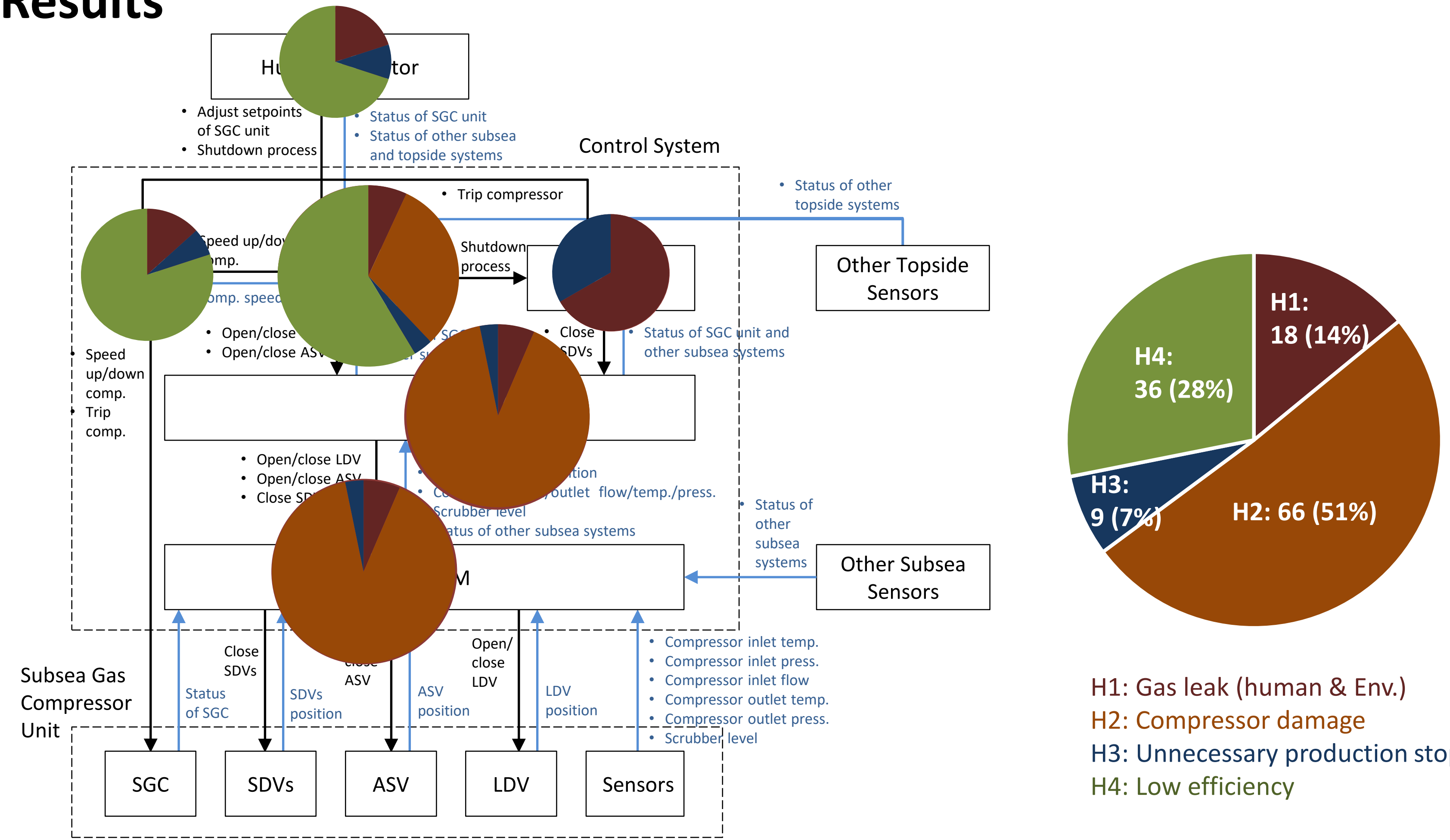
UCA-PCS001: Open LDV command is not provided when scrubber level is high		
Scenario	**Associated Causal Factors**	**Safety Constraints**
PCS receives wrong measurement of scrubber level	Drift of scrubber LT	SC-PCS001-01: Scrubber LT must be calibrated periodically SC-PCS001-02: Scrubber LT must have 2oo3 configuration
PCS receives no measurement of scrubber level	No power supply to scrubber LT	SC-PCS001-03: PCS must generate an alarm when no signal is received from scrubber LT SC-PCS001-04: Scrubber LT must be connected to UPS
	Broken signal wires from scrubber LT to PCS	SC-PCS001-03: PCS must generate an alarm when no signal is received from scrubber LT SC-PCS001-05: Signal wires must be inspected periodically
PCS receives correct measurement, but PCS does not provide open LDV command	Wrong logic inside PCS	SC-PCS001-06: PCS logic to generate “open LDV” command must be fully tested during commissioning period

Results



10
Adjust setpoints of SGC unit
Shutdown process
Status of SGC unit
Status of other subsea and topside systems
Control System
Trip compressor
Status of other topside systems
15
30
12
Shutdown process
Other Topside Sensors
Open/close
Open/close ASV
Close SDVs
Status of SGC unit and other subsea systems
Speed up/down comp.
Trip comp.
31
129 UCAs
Open/close LDV
Open/close ASV
outlet flow/temp./press.
Scrubber level
Status of other subsea systems
Status of other subsea systems
Other Subsea Sensors
31
Close SDVs
ASV
Open/ close LDV
Compressor inlet temp.
Compressor inlet press.
Compressor inlet flow
Compressor outlet temp.
Compressor outlet press.
Scrubber level
Subsea Gas Compressor Unit
Status of SGC
SDVs position
ASV position
LDV position
SGC
SDVs
ASV
LDV
Sensors

Results



H1: Gas leak (human & Env.)

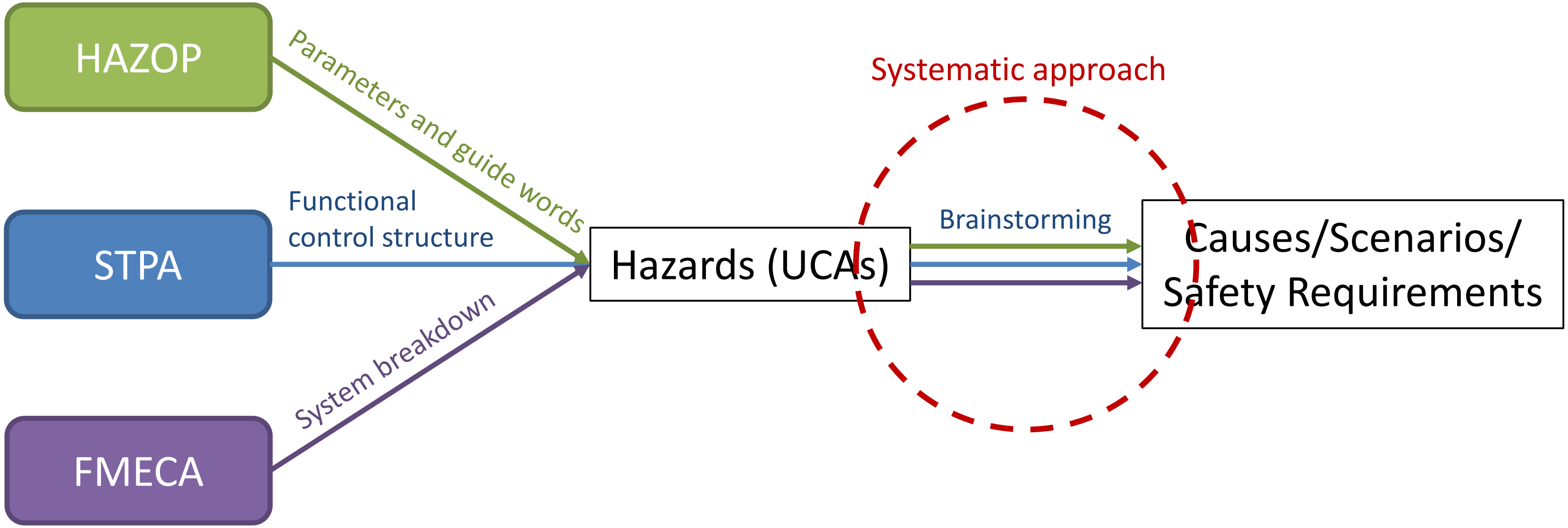
H2: Compressor damage

H3: Unnecessary production stop

H4: Low efficiency

Discussion

1) Identifying Causes, Scenarios, and Safety Requirements



Discussion

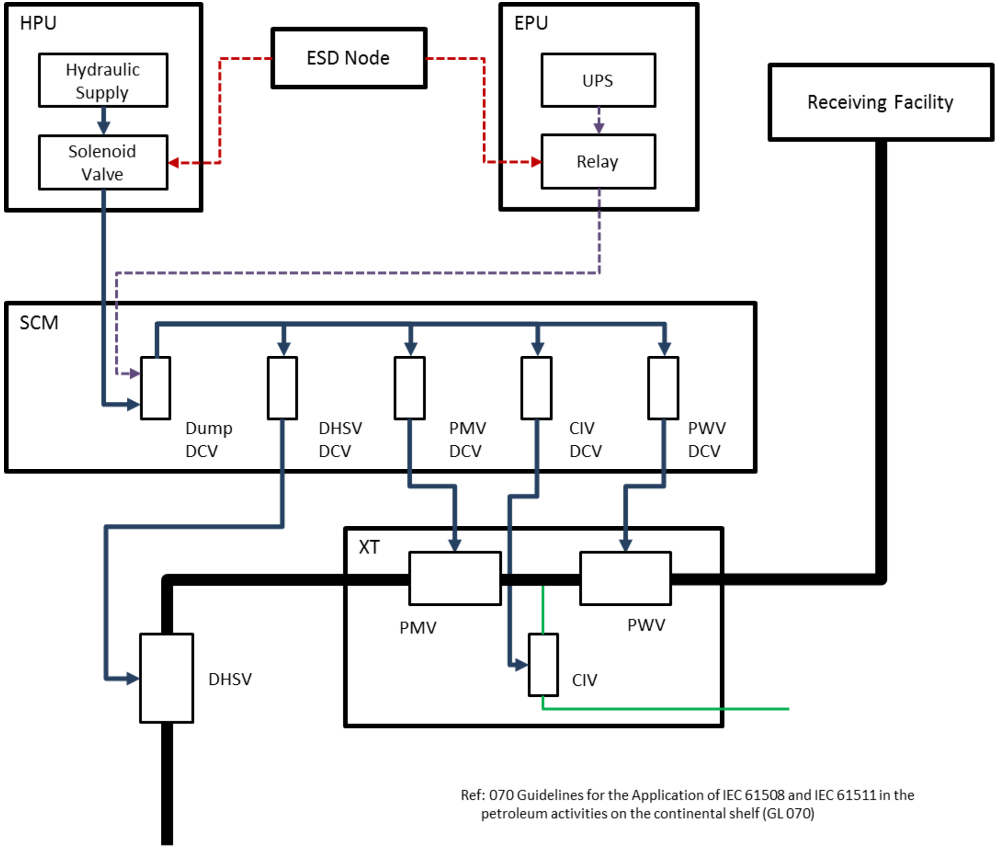
2) Quantification (evaluation, prioritization)

UCA-PCS001: Open LDV command is not provided when scrubber level is high		
Scenario	**Associated Causal Factors**	**Safety Constraints**
PCS receives wrong measurement of scrubber level	Drift of scrubber LT	SC-PCS001-01: Scrubber LT must be calibrated periodically SC-PCS001-02: Scrubber LT must have 2oo3 configuration
PCS receives no measurement of scrubber level	No power supply to scrubber LT	SC-PCS001-03: PCS must generate an alarm when no signal is received from scrubber LT SC-PCS001-04: Scrubber LT must be connected to UPS
	Broken signal wires from scrubber LT to PCS	SC-PCS001-03: PCS must generate an alarm when no signal is received from scrubber LT SC-PCS001-05: Signal wires must be inspected periodically
PCS receives correct measurement, but PCS does not provide open LDV command	Wrong logic inside PCS	SC-PCS001-06: PCS logic to generate “open LDV” command must be fully tested during commissioning period

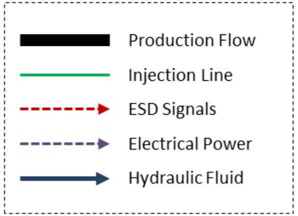
STPA to Isolation of Subsea Wells

OTC 2018

System Description



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

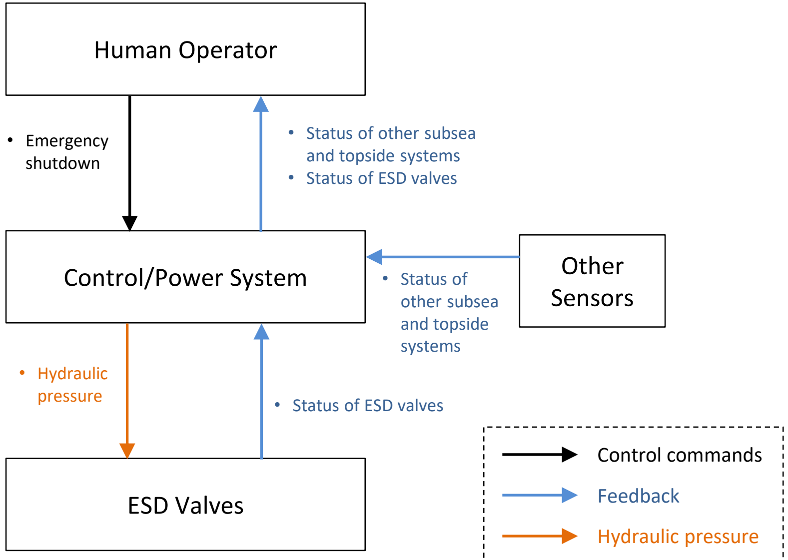


Ref: 070 Guidelines for the Application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf (GL 070)

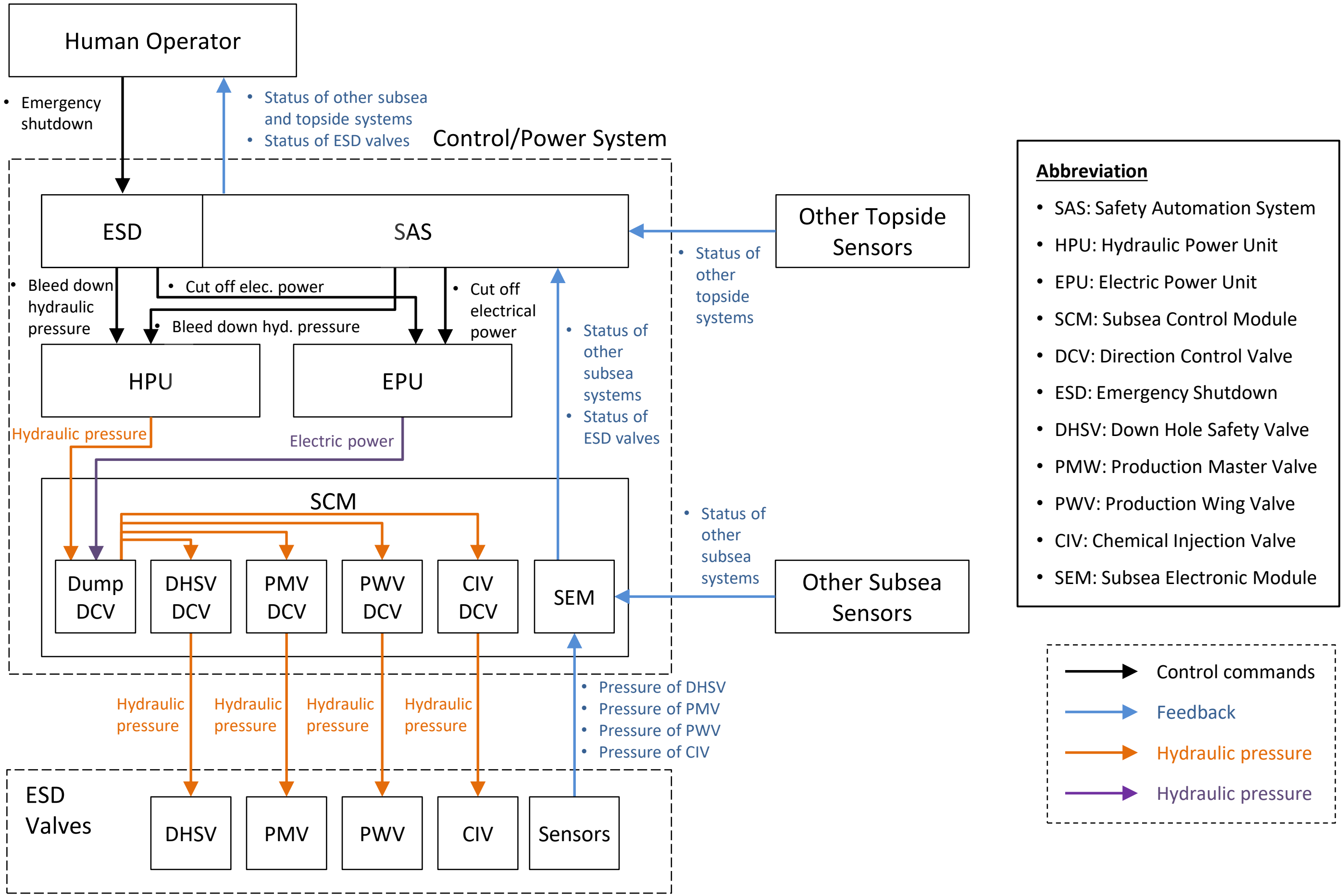
STPA Step 0 – System level accidents/hazards/safety constraints

System	Accident	Hazard	Safety Constraints
Emergency Shut Down (ESD) System – Isolation of Subsea Well	SLA1: People die or are injured due to fire and/or explosion	SLH1: Hydrocarbons are released at manned platform or inside safety zone, and ignite	SLSC1: Hydrocarbons must never be released at manned platform or inside safety zone SLSC2: Released hydrocarbons must never be ignited
	SLA2: The sea is polluted due to hydrocarbon release	SLH2: ESD system is not able to shut down subsea wells when hydrocarbons are released to the environment	SLSC3: ESD system must always shut down subsea wells when hydrocarbons are released to the environment
	SLA3: Production is interrupted unnecessarily	SLH3: ESD system shuts down subsea wells when hydrocarbons are not released to the environment	SLSC4: ESD system must never shut down subsea wells when there is no hydrocarbon release

STPA Step 0 – Functional control structure



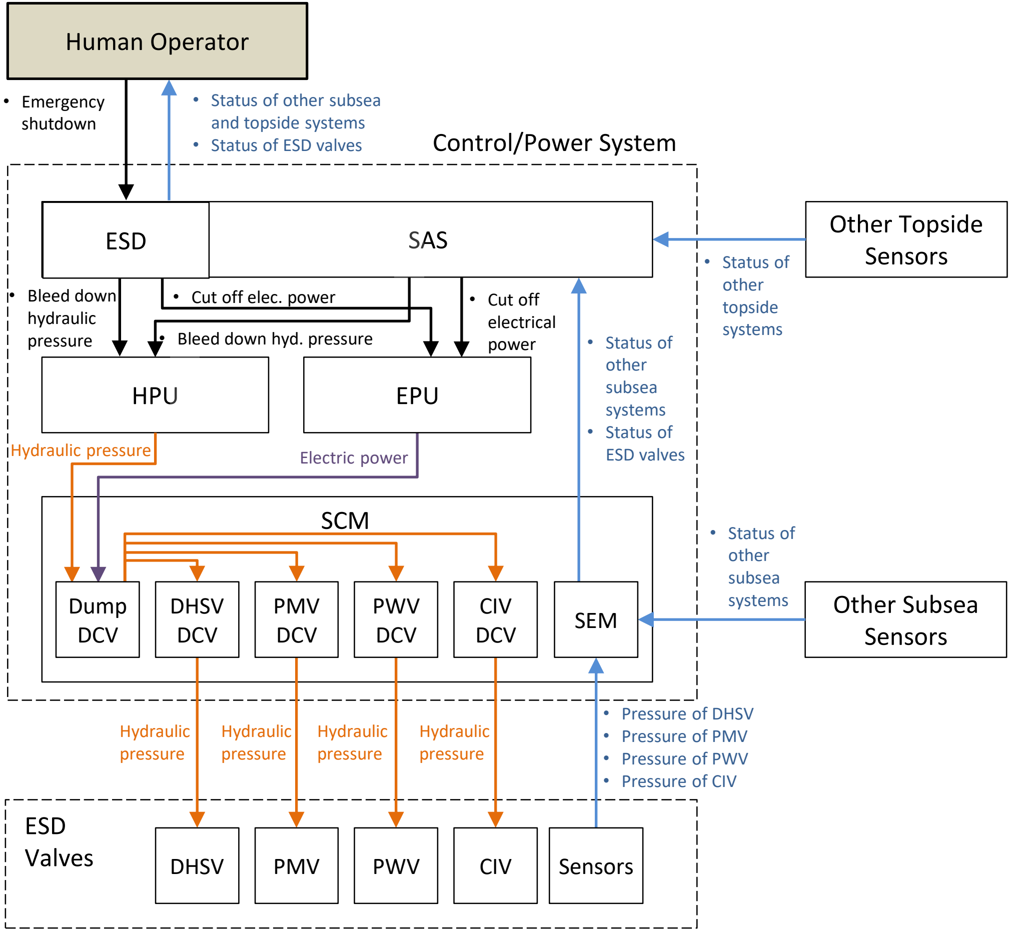
STPA Step 0 – Functional control structure



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

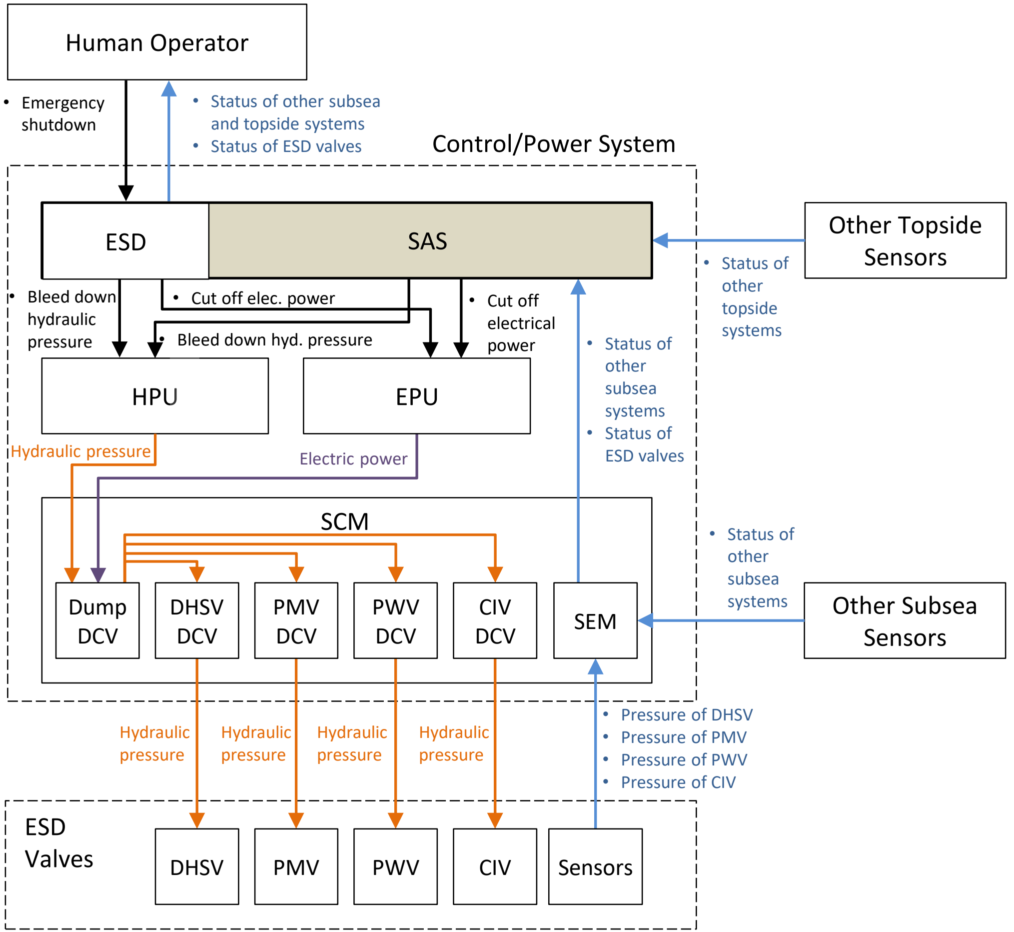
STPA Step 0 – Functional control structure



Human Operator

Responsibilities	Process model
• Manually shutdown ESD valves in an emergency	• Occurrence of an emergency – Yes - No

STPA Step 0 – Functional control structure



SAS

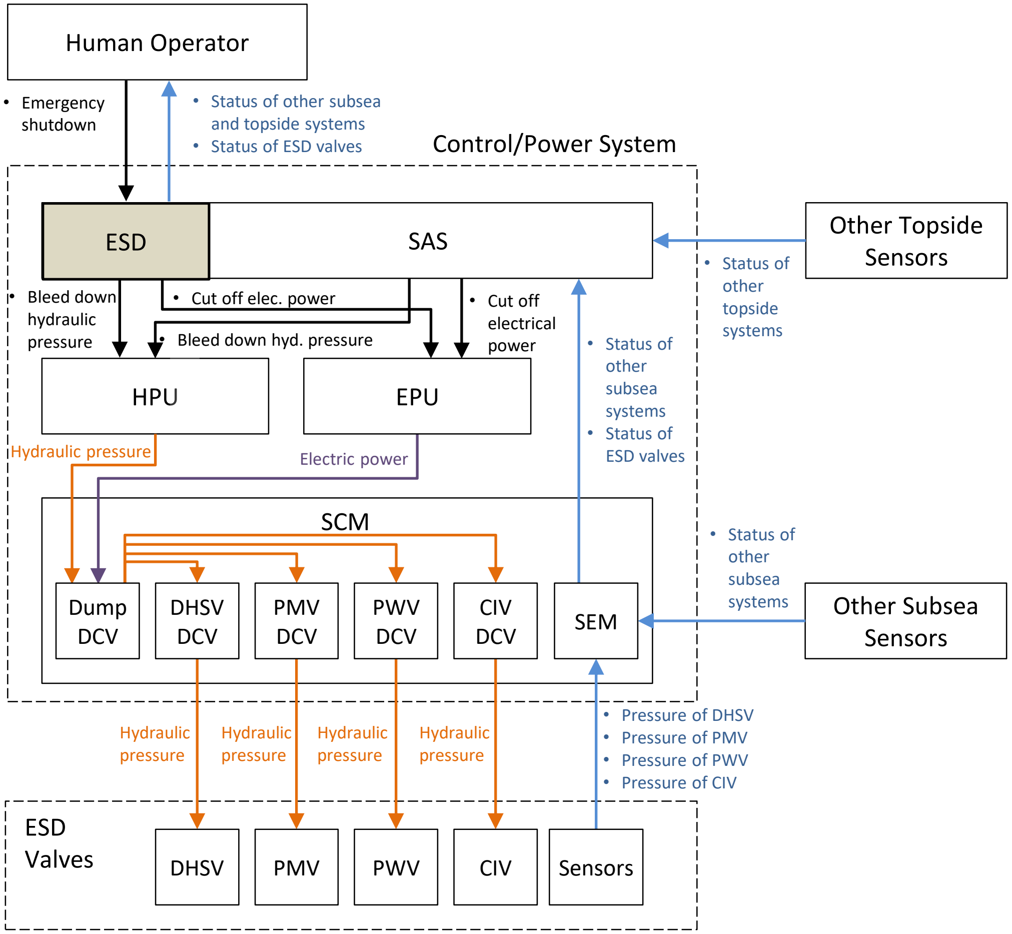
Responsibilities

- Automatically shutdown ESD valves when pre-defined abnormal conditions are detected

Process model

- Gas at HVAC inlet - Detected - Not detected
- Gas in non-hazardous area - Detected - Not detected
- Gas in hazardous area - Detected - Not detected
- Fire in hazardous area - Detected - Not detected
- Gas/water heat exchanger tube - Ruptured - Normal

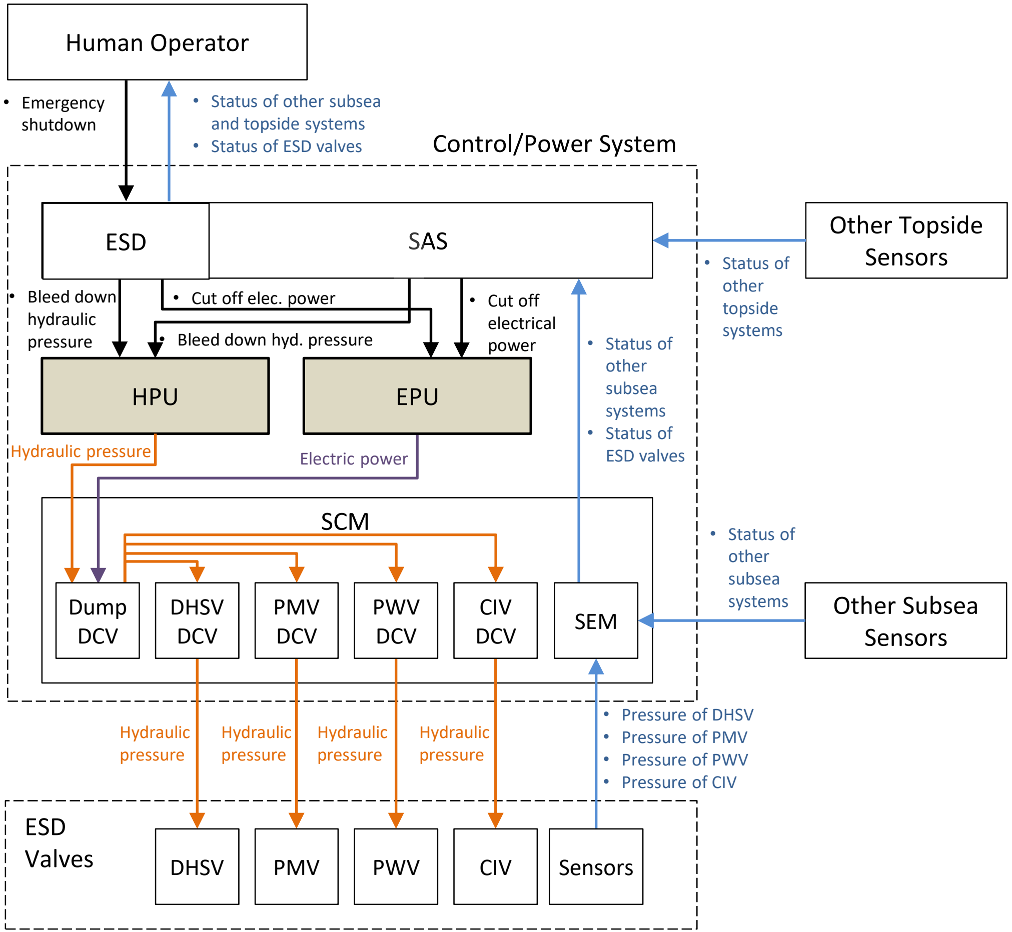
STPA Step 0 – Functional control structure



ESD

Responsibilities	Process model
• Shutdown ESD valves when human operator provides emergency shutdown command	• Control command from human - Emergency shutdown - None

STPA Step 0 – Functional control structure



HPU

Responsibilities

- Bleed down hydraulic pressure when ESD or SAS provides bleed down hydraulic pressure command

Process model

- Control command from ESD or SAS
  - Bleed down hydraulic pressure
  - None

EPU

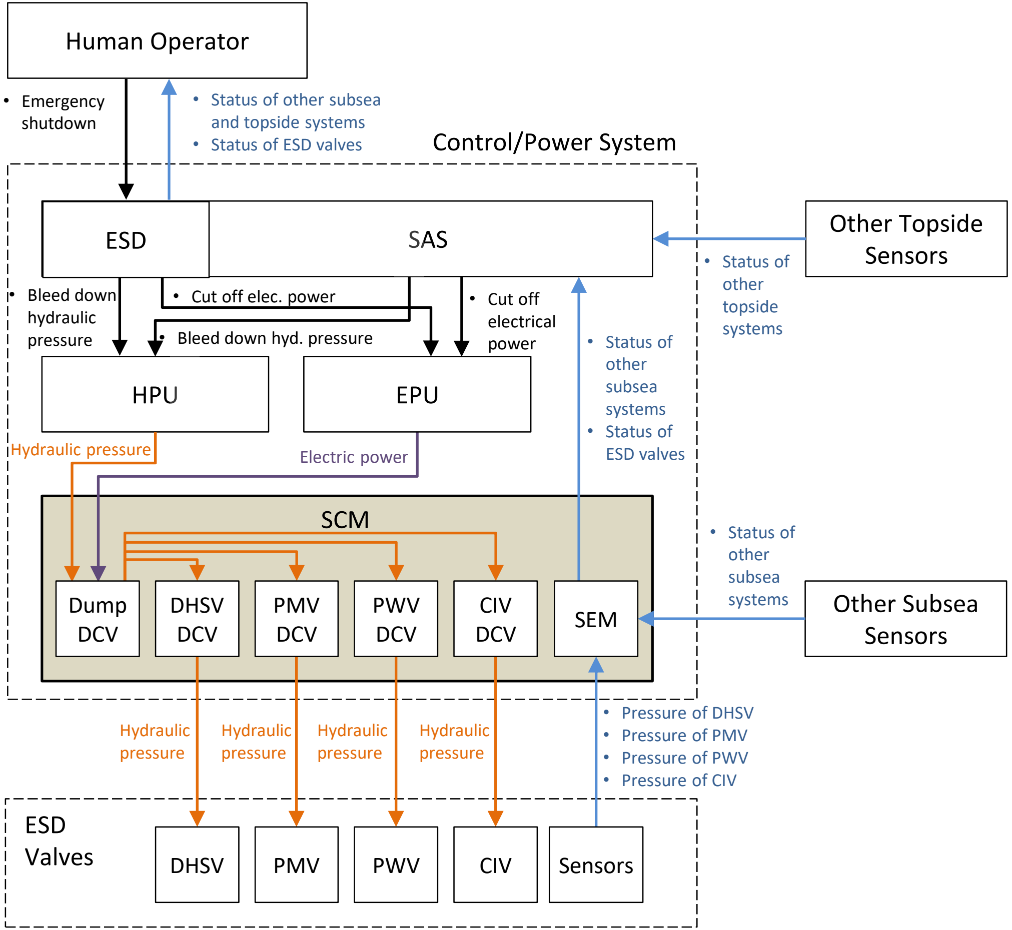
Responsibilities

- Cut off electrical power when Human Operator or SAS provides cut off electrical power command

Process model

- Control command from ESD or SAS
  - Cut off electric power
  - None

STPA Step 0 – Functional control structure



SCM

Responsibilities	Process model
• Distribute or disconnect hydraulic pressure to each ESD valves	• Hydraulic pressure from HPU - Provided - Not provided • Electric power from HPU - Provided - Not provided

STPA Step 1 – Identifying UCAs

SAS

Responsibilities

- Automatically shutdown ESD valves when pre-defined abnormal conditions are detected

Process model

- Gas at HVAC inlet
  - Detected
  - Not detected
- Gas in non-hazardous area
  - Detected
  - Not detected
- Gas in hazardous area
  - Detected
  - Not detected
- Fire in hazardous area
  - Detected
  - Not detected
- Gas/water heat exchanger tube
  - Ruptured
  - Normal

Controller : SAS

No	Control Action	Condition: Pre-defined abnormal 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

STPA Step 1 – Identifying UCAs

No	UCAs
UCA.HOP.001	Human Operator does not provide emergency shutdown command when an emergency occurs [H1,H2]
UCA.HOP.002	Human Operator provides emergency shutdown command too late when an emergency occurs [H1,H2]
UCA.HOP.003	Human Operator provides emergency shutdown command when an emergency does not occur [H3]
UCA.ESD.001	ESD does not provide bleed down hydraulic pressure command when Human Operator provides emergency shutdown command [H1,H2]
UCA.ESD.002	ESD provides bleed down hydraulic pressure command too late when Human Operator provides emergency shutdown command [H1,H2]
UCA.ESD.003	ESD provides bleed down hydraulic pressure command too short when Human Operator provides emergency shutdown command [H1,H2]
UCA.ESD.004	ESD provides bleed down hydraulic pressure command when Human Operator does not provide emergency shutdown command [H3]
UCA.ESD.005	ESD does not provide cut off electrical power command when Human Operator provides emergency shutdown command [H1,H2]
UCA.ESD.006	ESD provides cut off electrical power command too late when Human Operator provides emergency shutdown command [H1,H2]
UCA.ESD.007	ESD provides cut off electrical power command too short when Human Operator provides emergency shutdown command [H1,H2]
UCA.ESD.008	ESD provides cut off electrical power command when Human Operator does not provide emergency shutdown command [H3]
UCA.SAS.001	SAS does not provide bleed down hydraulic pressure command when pre-defined abnormal conditions are detected [H1,H2]
UCA.SAS.002	SAS provides bleed down hydraulic pressure command too late when pre-defined abnormal conditions are detected [H1,H2]
UCA.SAS.003	SAS provides bleed down hydraulic pressure command too short when pre-defined abnormal conditions are detected [H1,H2]
UCA.SAS.004	SAS provides bleed down hydraulic pressure command when pre-defined abnormal conditions are not detected [H3]
UCA.SAS.005	SAS does not provide cut off electrical power command when pre-defined abnormal conditions are detected [H1,H2]
UCA.SAS.006	SAS provides cut off electrical power command too late when pre-defined abnormal conditions are detected [H1,H2]
UCA.SAS.007	SAS provides cut off electrical power command too short when pre-defined abnormal conditions are detected [H1,H2]
UCA.SAS.008	SAS provides cut off electrical power command when pre-defined abnormal conditions are not detected [H3]
UCA.HPU.001	HPU provides hydraulic pressure when ESD or SAS provides bleed down hydraulic pressure command [H1,H2]
UCA.HPU.002	HPU does not provide hydraulic pressure too late when ESD or SAS provides bleed down hydraulic pressure command [H1,H2]
UCA.HPU.003	HPU does not provide hydraulic pressure too short when ESD or SAS provides bleed down hydraulic pressure command [H1,H2]
UCA.HPU.004	HPU does not provide hydraulic pressure when ESD or SAS does not provide bleed down hydraulic pressure command [H3]
UCA.EPU.001	EPU provides electric power when ESD or SAS provides cut off electrical power command [H1,H2]
UCA.EPU.002	EPU does not provide electric power too late when ESD or SAS provides cut off electrical power command [H1,H2]
UCA.EPU.003	EPU does not provide electric power too short when ESD or SAS provides cut off electrical power command [H1,H2]
UCA.EPU.004	EPU does not provide electric power when ESD or SAS does not provide cut off electrical power command [H3]
UCA.SCM.001	SCM does not distribute hydraulic pressure when hydraulic pressure or electric power is supplied [H3]
UCA.SCM.002	SCM distributes hydraulic pressure when hydraulic pressure or electric power is not supplied [H1,H2]
UCA.SCM.003	SCM does not distribute hydraulic pressure too late when hydraulic pressure or electric power is not supplied [H1,H2]

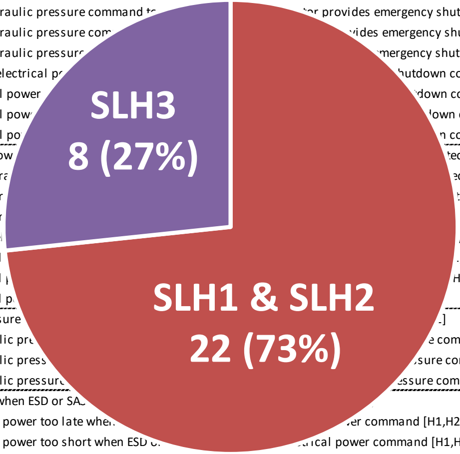
STPA Step 2: Identifying Causes of UCAs and Safety Constrains

UCA.SAS.001: SAS does not provide bleed down hydraulic pressure command when pre-defined abnormal conditions have occurred		
Scenario	**Associated Causal Factors**	**Safety Constraints**
SNR.SAS.001.02 SAS receives no information about pre-defined conditions	Failure of sensors	SC.SAS.001.02.01 All sensors for pre-defined conditions must be tested periodically SC.SAS.001.02.02 All sensors for pre-defined conditions must have redundancy (e.g., 2oo3 configuration)
	Broken signal wires between sensors and SAS	SC.SAS.001.02.03 All signal wires for pre-defined conditions must be inspected periodically SC.SAS.001.02.04 SAS must generate an alarm when no signal is received from any sensors for pre-defined conditions
	No power supply to sensors	SC.SAS.001.02.05 All sensors for pre-defined conditions must be connected to redundant power supply or UPS SC.SAS.001.02.04 SAS must generate an alarm when no signal is received from any sensors for pre-defined conditions

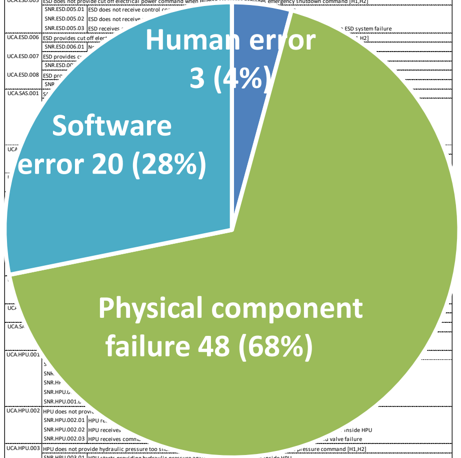
Results

- 30 UCAs
- 71 Scenarios

No	UCAs
UCA.HOP.001	Human Operator does not provide emergency shutdown command when an emergency occurs [H1,H2]
UCA.HOP.002	Human Operator provides emergency shutdown command too late when an emergency occurs [H1,H2]
UCA.HOP.003	Human Operator provides emergency shutdown command when an emergency does not occur [H3]
UCA.ESD.001	ESD does not provide bleed down hydraulic pressure command when Human Operator provides emergency shutdown command [H1,H2]
UCA.ESD.002	ESD provides bleed down hydraulic pressure command t ...or provides emergency shutdown command [H1,H2]
UCA.ESD.003	ESD provides bleed down hydraulic pressure com ...vides emergency shutdown command [H1,H2]
UCA.ESD.004	ESD provides bleed down hydraulic pressur ...mergency shutdown command [H3]
UCA.ESD.005	ESD does not provide cut off electrical p ...utdown command [H1,H2]
UCA.ESD.006	ESD provides cut off electrical power ...down command [H1,H2]
UCA.ESD.007	ESD provides cut off electrical pow ...own command [H1,H2]
UCA.ESD.008	ESD provides cut off electrical po ...n command [H3]
UCA.SAS.001	SAS does not provide bleed dow ...tected [H1,H2]
UCA.SAS.002	SAS provides bleed down hydra ...ected [H1,H2]
UCA.SAS.003	SAS provides bleed down hydr ...tected [H1,H2]
UCA.SAS.004	SAS provides bleed down hydr ... [H3]
UCA.SAS.005	SAS does not provide cut off e ...,H2]
UCA.SAS.006	SAS provides cut off electrical ...,H2]
UCA.SAS.007	SAS provides cut off electrical ...H1,H2]
UCA.SAS.008	SAS provides cut off electrical p
UCA.HPU.001	HPU provides hydraulic pressure ...]
UCA.HPU.002	HPU does not provide hydraulic pr ...e command [H1,H2]
UCA.HPU.003	HPU does not provide hydraulic press ...sure command [H1,H2]
UCA.HPU.004	HPU does not provide hydraulic pressur ...essure command [H3]
UCA.EPU.001	EPU provides electric power when ESD or SA
UCA.EPU.002	EPU does not provide electric power too late whe ...er command [H1,H2]
UCA.EPU.003	EPU does not provide electric power too short when ESD ...ctrical power command [H1,H2]
UCA.EPU.004	EPU does not provide electric power when ESD or SAS does not provide cut off electrical power command [H3]
UCA.SCM.001	SCM does not distribute hydraulic pressure when hydraulic pressure or electric power is supplied [H3]
UCA.SCM.002	SCM distributes hydraulic pressure when hydraulic pressure or electric power is not supplied [H1,H2]
UCA.SCM.003	SCM does not distribute hydraulic pressure too late when hydraulic pressure or electric power is not supplied [H1,H2]



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
UCA.ESD.002	ESD provides bleed down hydraulic pressure command too late when Human Operator provides emergency shutdown command [H1,H2]	
	SNR.ESD.002.01	No possible scenario
UCA.ESD.003	ESD provides bleed down hydraulic pressure command too short when Human Operator provides emergency shutdown command [H1,H2]	
	SNR.ESD.003.01	No possible scenario
UCA.ESD.004	ESD provides bleed down hydraulic pressure command when Human Operator does not provide emergency shutdown command [H3]	
	SNR.ESD.004.01	ESD provides control command due to short circuit
UCA.ESD.005	ESD does not provide cut off electrical power command when Hum ...vides emergency shutdown command [H1,H2]	
	SNR.ESD.005.01	ESD does not receive control c
	SNR.ESD.005.02	ESD does not receive
	SNR.ESD.005.03	ESD receives ... ESD system failure
UCA.ESD.006	ESD provides cut off elec ...H2]	
	SNR.ESD.006.01	N
UCA.ESD.007	ESD provides c	
	SNR.ESD.00	
UCA.ESD.008	ESD pro	
	SNR	
UCA.SAS.001	S	
UCA.HPU.001		
	S	
	SNR.	
	SNR.H	
	SNR.HPU.0	
	SNR.HPU.001.0	
UCA.HPU.002	HPU does not provi	
	SNR.HPU.002.01	HPU re
	SNR.HPU.002.02	HPU receives ... inside HPU
	SNR.HPU.002.03	HPU receives comm ...d valve failure
UCA.HPU.003	HPU does not provide hydraulic pressure too sh ...pressure command [H1,H2]	
	SNR.HPU.003.01	HPU starts providing hydraulic pressure again ...r 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 failre
	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 faliure
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 failre
	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 faliure
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 failre
	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 faliure
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	Dut to long distance between HPU and SCM



Discussion

1) Advantages of STPA – Wider scope

- STPA can cover human errors, software flaws, and physical component failures

SNR.HOP.001.02
The Human Operator is unaware of the emergency because sensors fail to detect the emergency, and therefore, the Human Operator does not provide the emergency shutdown command when an emergency occurs.

SNR.HOP.001.06
The Human Operator is unaware of the emergency because the SAS provides no alarm to the Human Operator due to a software flaw, and therefore, the Human Operator does not provide the emergency shutdown command when an emergency occurs.

Discussion

1) 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	Condition	Unsafe Control Actions?					
		Pre-defined abnormal conditions	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

Discussion

Controller : SAS													
No	Control Action	Condition					Unsafe Control Actions?					
		Gas at HVAC inlet	GAS in non-hazardous area	Gas in hazardous area	Fire in hazardous area	Gas/water heat exchanger	Not provided	Provided	Too early	Too late	Too short	Too long
1	Bleed down hydraulic pressure	Not detected	Not detected	Not detected	Not detected	Normal						
2		Detected	Not detected	Not detected	Not detected	Normal						
3		Not detected	Detected	Not detected	Not detected	Normal						
4		Not detected	Not detected	Detected	Not detected	Normal						
5		Not detected	Not detected	Not detected	Detected	Normal						
6		Not detected	Not detected	Not detected	Not detected	Ruptured						
7		Detected	Detected	Not detected	Not detected	Normal						
8		Detected	Not detected	Detected	Not detected	Normal						
9		Detected	Not detected	Not detected	Detected	Normal						
10		Detected	Not detected	Not detected	Not detected	Ruptured						
11		Not detected	Detected	Detected	Not detected	Normal						
12		Not detected	Detected	Not detected	Detected	Normal						
13		Not detected	Detected	Not detected	Not detected	Ruptured						
14		Not detected	Not detected	Detected	Detected	Normal						
15		Not detected	Not detected	Detected	Not detected	Ruptured						
16		Not detected	Not detected	Not detected	Detected	Ruptured						
17		Detected	Detected	Detected	Not detected	Normal						
18		Detected	Detected	Not detected	Detected	Normal						
19		Detected	Detected	Not detected	Not detected	Ruptured						
20		Detected	Not detected	Detected	Detected	Normal						
21		Detected	Not detected	Detected	Not detected	Ruptured						
22		Detected	Not detected	Not detected	Detected	Ruptured						
23		Not detected	Detected	Detected	Detected	Normal						
24		Not detected	Detected	Detected	Not detected	Ruptured						
25		Not detected	Detected	Not detected	Detected	Ruptured						
26		Not detected	Not detected	Detected	Detected	Ruptured						
27		Detected	Detected	Detected	Detected	Normal						
28		Detected	Detected	Detected	Not detected	Ruptured						
29		Detected	Detected	Not detected	Detected	Ruptured						
30		Detected	Not detected	Detected	Detected	Ruptured						
31		Not detected	Detected	Detected	Detected	Ruptured						
32		Detected	Detected	Detected	Detected	Ruptured						

Discussion

1) Advantages of STPA – Top-down approach

- Analysis can be refined with more details

SNR.HOP.001.02
The Human Operator is unaware of the emergency because ***sensors*** fail to detect the emergency, and therefore, the Human Operator does not provide the emergency shutdown command when an emergency occurs.

SNR.HOP.001.02-1
The Human Operator is unaware of the emergency because ***gas detectors at the HVAC inlet*** fail to detect the emergency, and therefore, the Human Operator does not provide the emergency shutdown command when an emergency occurs.

SNR.HOP.001.02-2
The Human Operator is unaware of the emergency because ***gas detectors in a hazardous area*** fail to detect the emergency, and therefore, the Human Operator does not provide the emergency shutdown command when an emergency occurs.

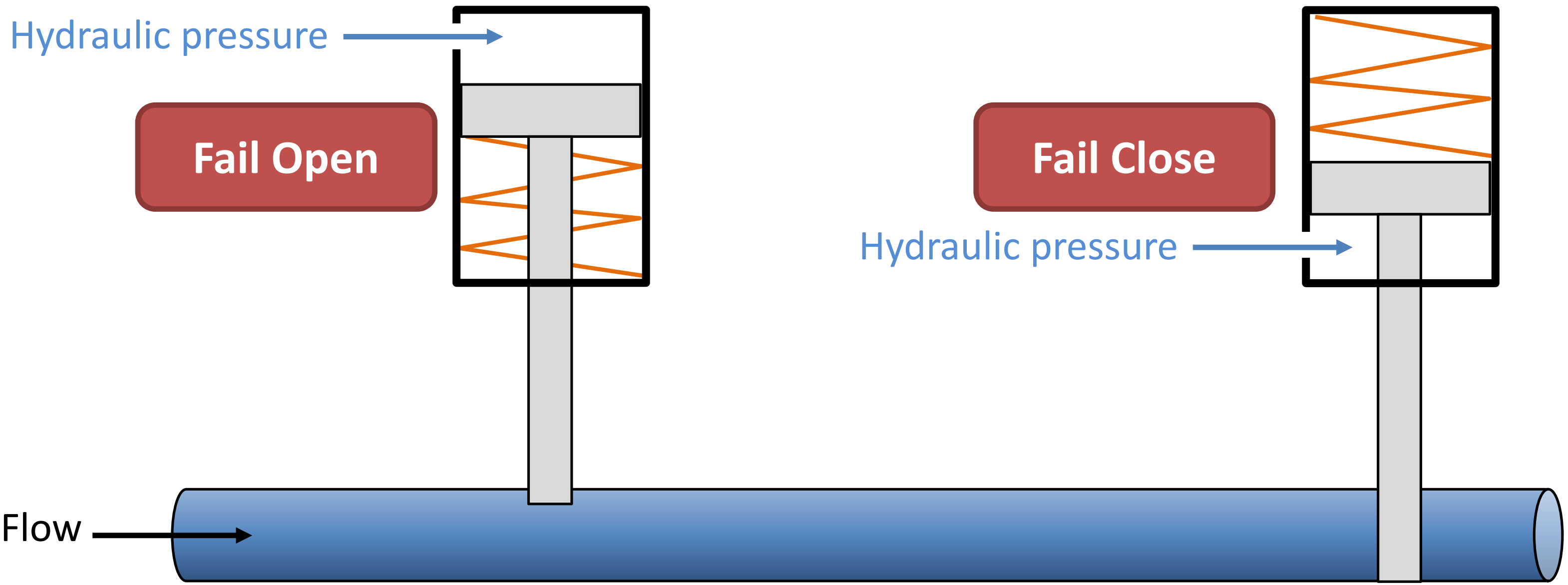
SNR.HOP.001.02-3
The Human Operator is unaware of the emergency because ***fire detectors in a hazardous area*** fail to detect the emergency, and therefore, the Human Operator does not provide the emergency shutdown command when an emergency occurs.

Discussion

2) Suggestions – Modelling of fail-safe functions

Fail Safe Valve

- Returns to a safe condition in a fault condition
- Can be fail open or fail close
- Usually equipped with a mechanical spring



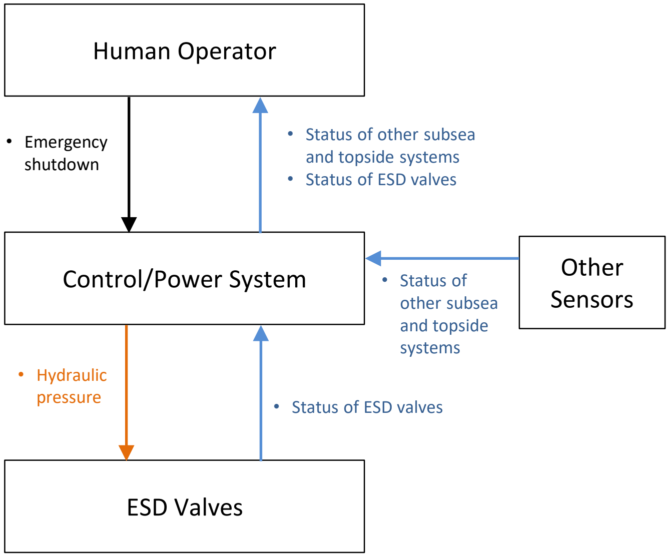
Discussion

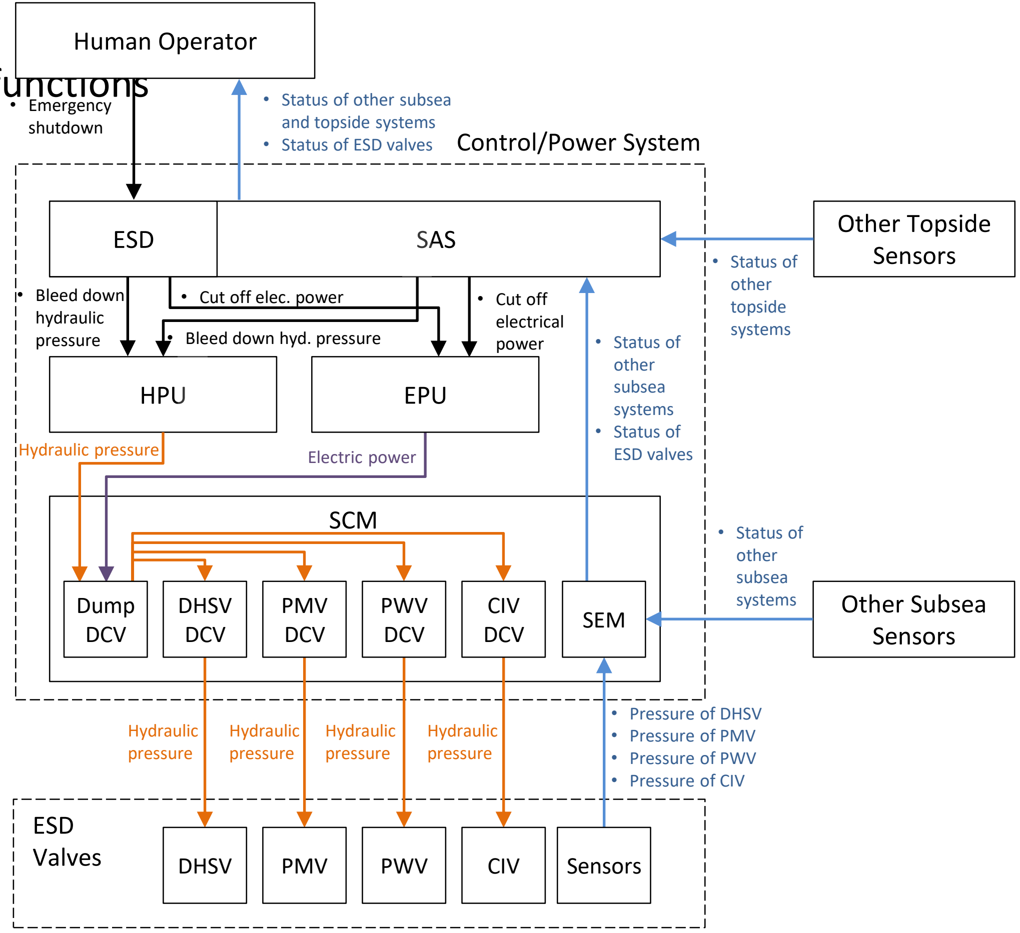
2) Suggestions – Modelling of fail-safe functions

- Fails-safe valves are closed by bleeding down hydraulic pressure (or cutting off electric power supply)
- Is bleeding down hydraulic pressure a control command?
- Yes, because the SDVs are closed by these actions
- No, because (1) HPU is not a controller and (2) these actions can occur accidently by hydraulic oil leak
- Regardless of this discussion, we need to consider these actions as control commands for the anlaysis

Discussion

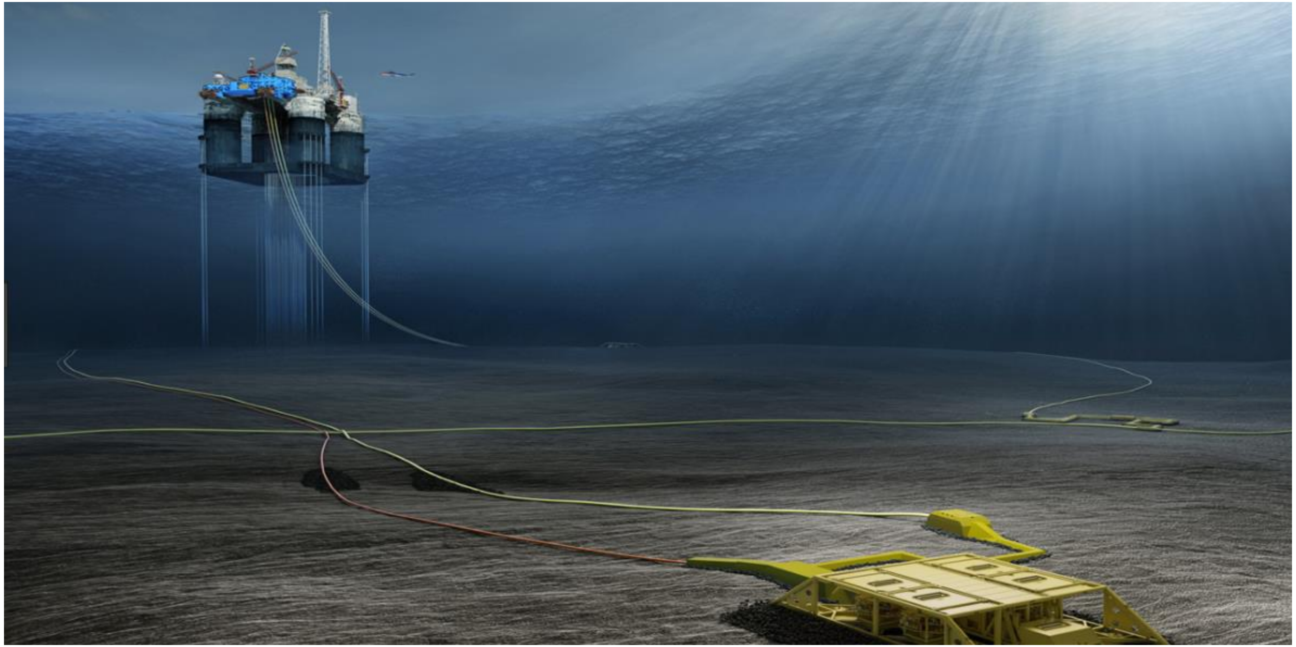
2) Suggestions – Modelling of fail-safe functions





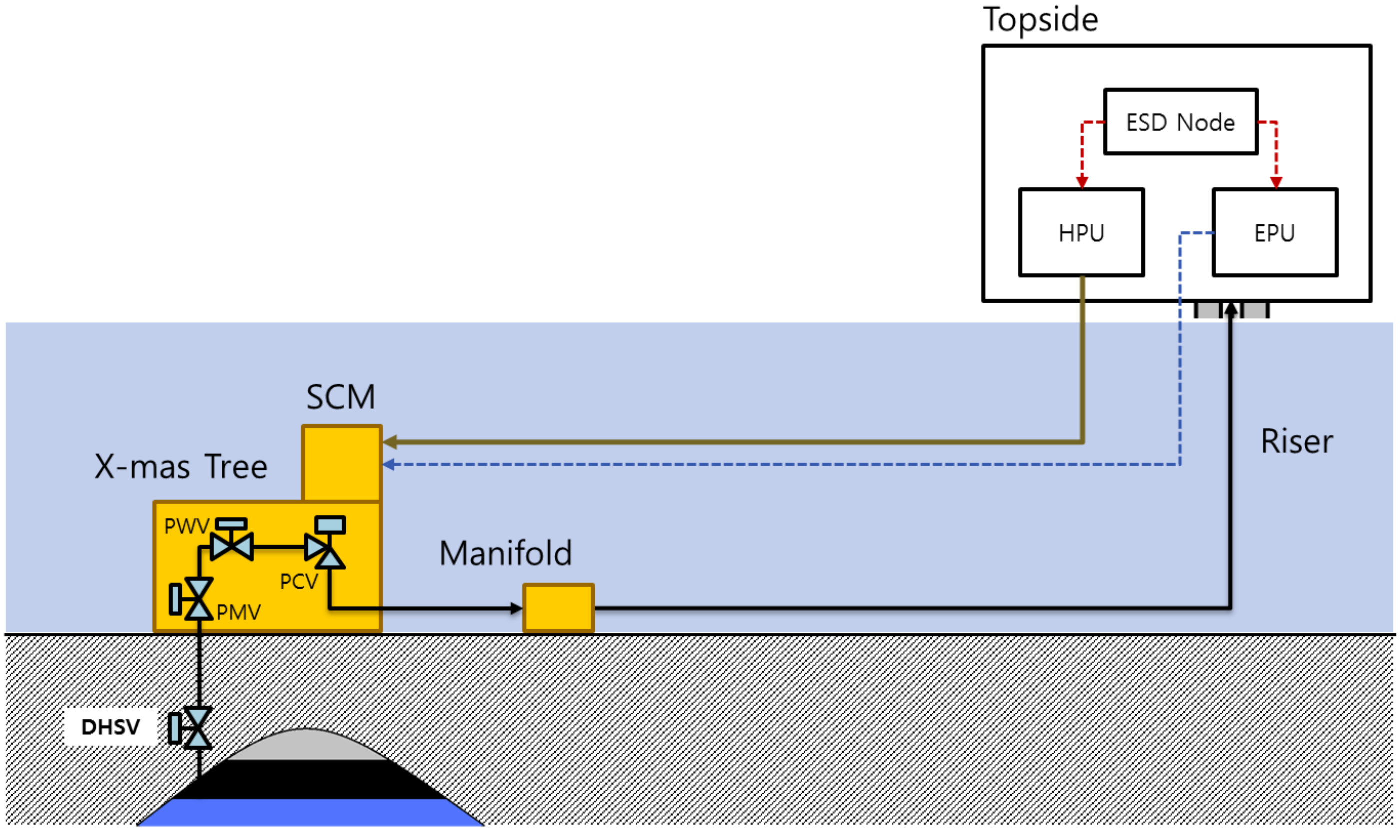
Discussion

2) Suggestions – Long distance between controller and actuator



Discussion

2) Suggestions – Long distance between controller and actuator



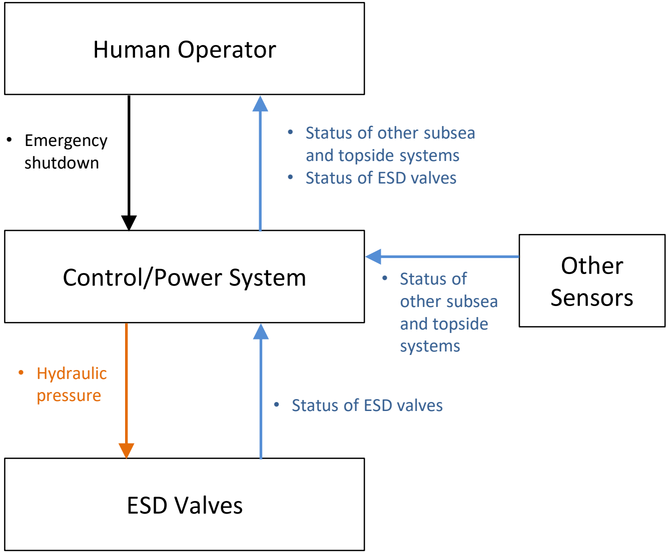
Discussion

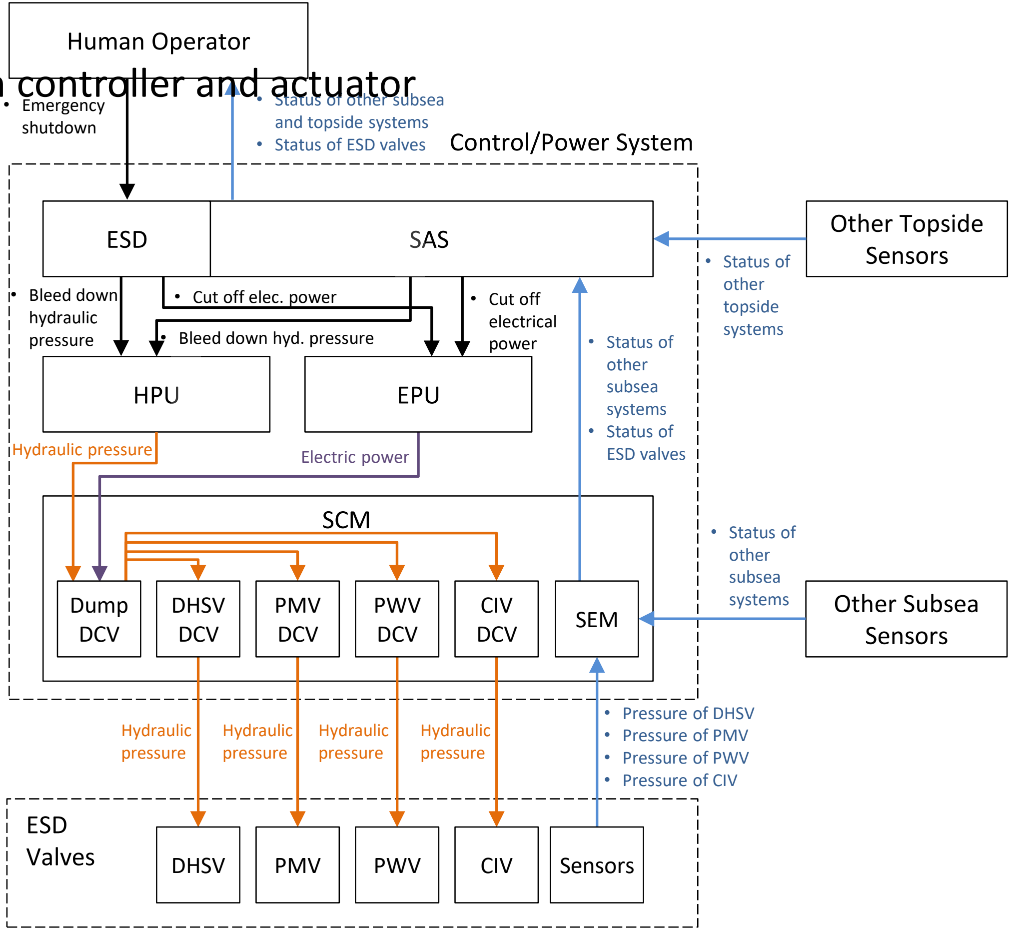
2) Suggestions – Long distance between controller and actuator

- SCM delivers and distributes control commands to SDVs
- Is SCM a controller?
- Yes, because the SDVs are controlled by SCM
- No, because SCM makes no decision
- Regardless of this discussion, we need to consider SCM as a controller for the analysis

Discussion

2) Suggestions – Long distance between controller and actuator

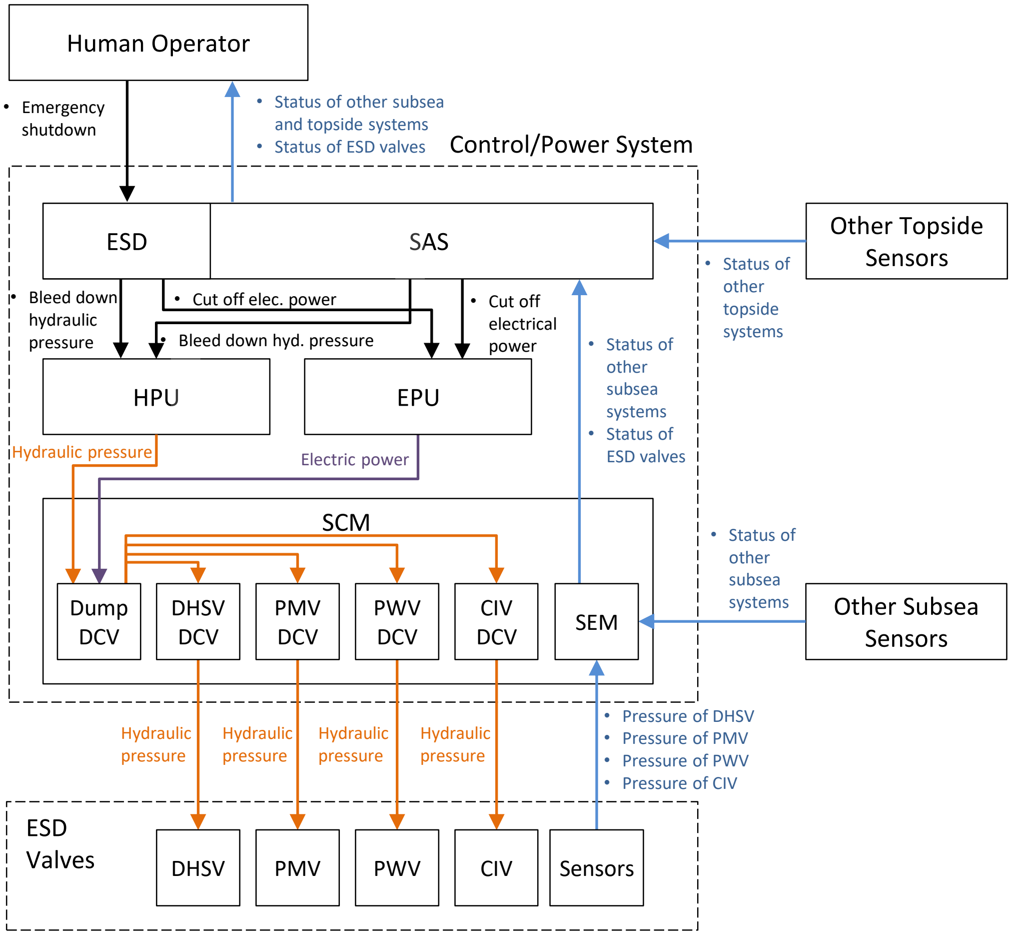




Discussion

3) Remaining Challenges

- Dynamic control structure



Discussion

3) Remaining Challenges

- When to stop the analysis?

UCA.SAS.001: SAS does not provide bleed down hydraulic pressure command when pre-defined abnormal conditions have occurred		
Scenario	**Associated Causal Factors**	**Safety Constraints**
SNR.SAS.001.02 SAS receives no information about pre-defined conditions	Failure of sensors	SC.SAS.001.02.01 All sensors for pre-defined conditions must be tested periodically SC.SAS.001.02.02 All sensors for pre-defined conditions must have redundancy (e.g., 2oo3 configuration)
	No power supply to sensors	SC.SAS.001.02.05 All sensors for pre-defined conditions must be connected to redundant power supply or UPS SC.SAS.001.02.04 SAS must generate an alarm when no signal is received from any sensors for pre-defined conditions

Conclusion and Future Work

Conclusion

- Advantages of STPA - systematic approach to identify hazards
  - wide scope
  - top-down approach

- Challenges of STPA - Quantification of the results
  - STPA Step 2 relies on brainstorming
  - Dynamic control structure

Future Work

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

→

- Summarize overall challenges and provide solutions

NTNU


thank you
© 1996, 2002 SANRIO CO., LTD.