NTNU

Norwegian University of Science and Technology

SUBPRO

SUBSEA PRODUCTION AND PROCESSING

Combining STPA and RAM modelling to identify and evaluate potential losses in controller-based systems with complex interactions

RAMS seminar 04.05.18

Juntao Zhang

HyungJu Kim

Yiliu Liu

Mary Ann Lundteigen

Outline of presentation

❑Background

❑STPA

❑Proposed approach

❑Illustrative case

❑Discussions

- ➢ Background

STPA

Proposed approach

Illustrative case

Discussions

PhD project in SUBPRO

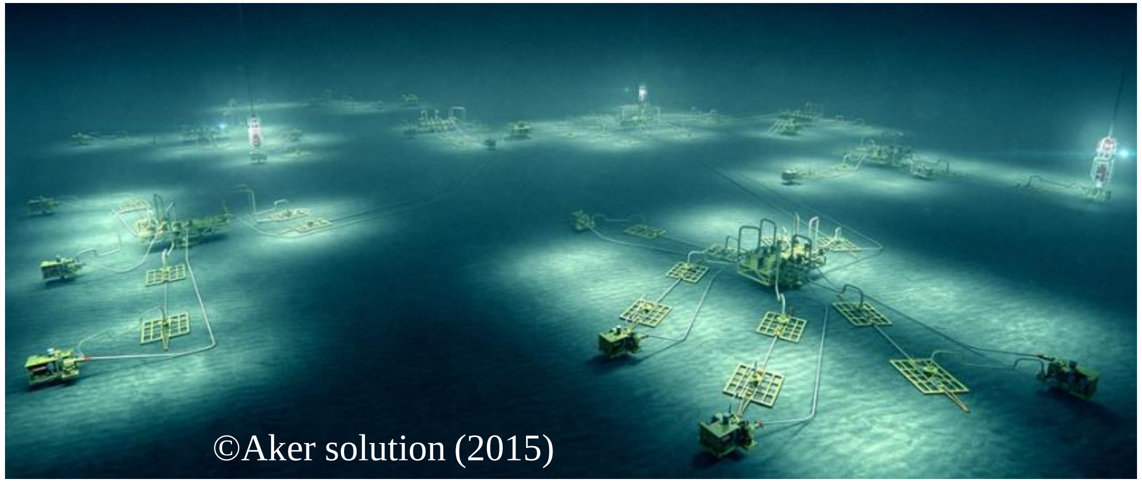
SUBPRO
SUBSEA PRODUCTION AND PROCESSING

Objective: Incorporating RAM analysis for innovative subsea design accounts for:

❑Subsea conditions

❑Early design phase

❑Technology qualification



©Aker solution (2015)

- Background

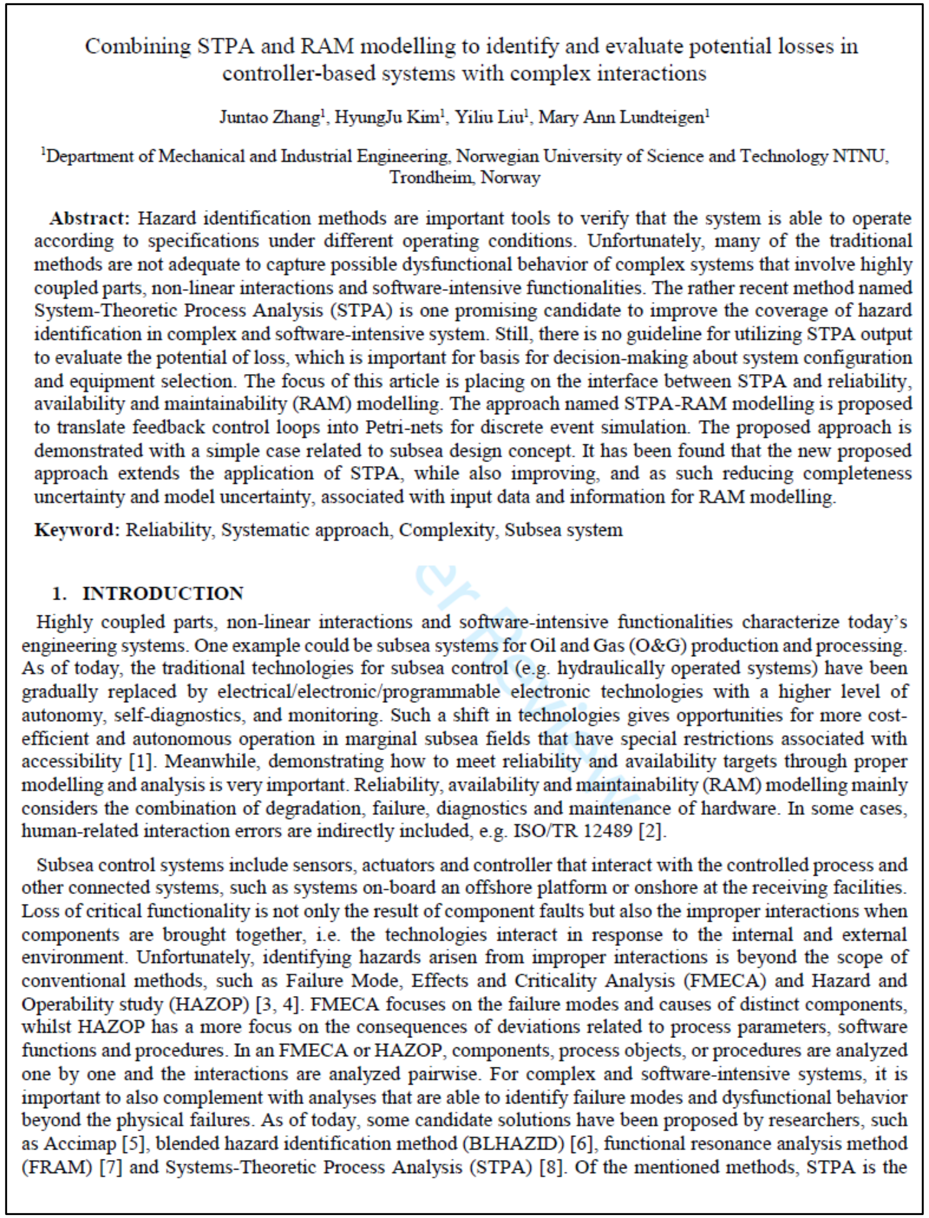
STPA

Proposed approach

Illustrative case

Discussions

Hazard identification: what can go wrong?



Combining STPA and RAM modelling to identify and evaluate potential losses in controller-based systems with complex interactions

Juntao Zhang[1], HyungJu Kim[1], Yiliu Liu[1], Mary Ann Lundteigen[1]

[1]Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology NTNU, Trondheim, Norway

Abstract: Hazard identification methods are important tools to verify that the system is able to operate according to specifications under different operating conditions. Unfortunately, many of the traditional methods are not adequate to capture possible dysfunctional behavior of complex systems that involve highly coupled parts, non-linear interactions and software-intensive functionalities. The rather recent method named System-Theoretic Process Analysis (STPA) is one promising candidate to improve the coverage of hazard identification in complex and software-intensive system. Still, there is no guideline for utilizing STPA output to evaluate the potential of loss, which is important for basis for decision-making about system configuration and equipment selection. The focus of this article is placing on the interface between STPA and reliability, availability and maintainability (RAM) modelling. The approach named STPA-RAM modelling is proposed to translate feedback control loops into Petri-nets for discrete event simulation. The proposed approach is demonstrated with a simple case related to subsea design concept. It has been found that the new proposed approach extends the application of STPA, while also improving, and as such reducing completeness uncertainty and model uncertainty, associated with input data and information for RAM modelling.

Keyword: Reliability, Systematic approach, Complexity, Subsea system

1. INTRODUCTION

Highly coupled parts, non-linear interactions and software-intensive functionalities characterize today's engineering systems. One example could be subsea systems for Oil and Gas (O&G) production and processing. As of today, the traditional technologies for subsea control (e.g. hydraulically operated systems) have been gradually replaced by electrical/electronic/programmable electronic technologies with a higher level of autonomy, self-diagnostics, and monitoring. Such a shift in technologies gives opportunities for more cost-efficient and autonomous operation in marginal subsea fields that have special restrictions associated with accessibility [1]. Meanwhile, demonstrating how to meet reliability and availability targets through proper modelling and analysis is very important. Reliability, availability and maintainability (RAM) modelling mainly considers the combination of degradation, failure, diagnostics and maintenance of hardware. In some cases, human-related interaction errors are indirectly included, e.g. ISO/TR 12489 [2].

Subsea control systems include sensors, actuators and controller that interact with the controlled process and other connected systems, such as systems on-board an offshore platform or onshore at the receiving facilities. Loss of critical functionality is not only the result of component faults but also the improper interactions when components are brought together, i.e. the technologies interact in response to the internal and external environment. Unfortunately, identifying hazards arisen from improper interactions is beyond the scope of conventional methods, such as Failure Mode, Effects and Criticality Analysis (FMECA) and Hazard and Operability study (HAZOP) [3, 4]. FMECA focuses on the failure modes and causes of distinct components, whilst HAZOP has a more focus on the consequences of deviations related to process parameters, software functions and procedures. In an FMECA or HAZOP, components, process objects, or procedures are analyzed one by one and the interactions are analyzed pairwise. For complex and software-intensive systems, it is important to also complement with analyses that are able to identify failure modes and dysfunctional behavior beyond the physical failures. As of today, some candidate solutions have been proposed by researchers, such as Accimap [5], blended hazard identification method (BLHAZID) [6], functional resonance analysis method (FRAM) [7] and Systems-Theoretic Process Analysis (STPA) [8]. Of the mentioned methods, STPA is the

- ➢ Background

STPA

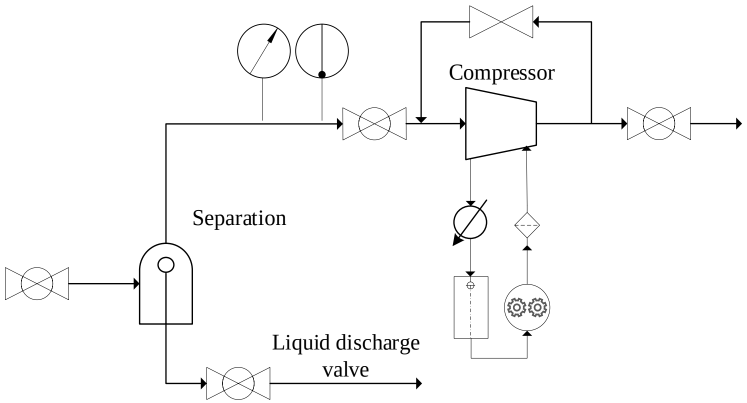
Proposed approach

Illustrative case

Discussions

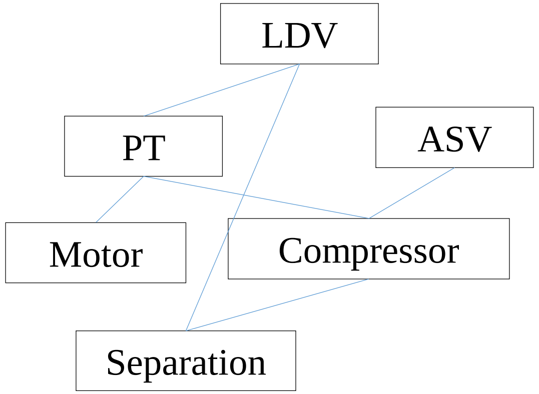
Old approaches for hazard identification

Define

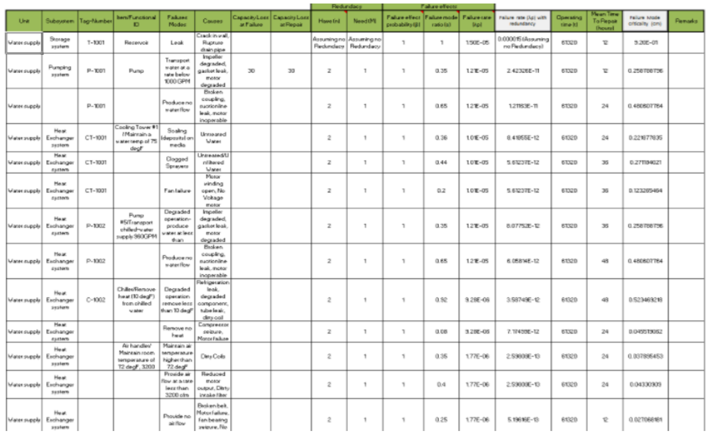


Workflow: analytical reduction

Decompose



Analyse



								Redundancy		Failure effects							
Unit	Subsystem	Tag-Number	Item/Functional ID	Failures Modes	Causes	Capacity Loss at Failure	Capacity Loss at Repair	Have (n)	Need (M)	Failure effect probability (β)	Failure mode ratio (α)	Failure rate (λp)	Failure rate (λp) with redundancy	Operating time (t)	Mean Time To Repair (hours)	Failure Mode criticality (cm)	Remarks
Water supply	Storage system	T-1001	Reservoir	Leak	Crack in wall, Rupture drain pipe			Assuming no Redundancy	Assuming no Redundancy	1	1	1.50E-05	0.000015 (Assuming no Redundancy)	61320	12	9.20E-01	
Water supply	Pumping system	P-1001	Pump	Transport water at a rate below 1000 GPM	Impeller degraded, gasket leak, motor degraded	30	30	2	1	1	0.35	1.21E-05	2.42326E-11	61320	12	0.258788796	
Water supply		P-1001		Produce no water flow	Broken coupling, suctionline leak, motor inoperable			2	1	1	0.65	1.21E-05	1.21163E-11	61320	24	0.480607764	
Water supply	Heat Exchanger system	CT-1001	Cooling Tower #1 / Maintain a water temp of 75 degF	Scaling (deposits) on media	Untreated Water			2	1	1	0.36	1.01E-05	8.41855E-12	61320	24	0.221877835	
Water supply	Heat Exchanger system	CT-1001		Clogged Sprayers	Untreated/Unfiltered Water			2	1	1	0.44	1.01E-05	5.61237E-12	61320	36	0.271184021	
Water supply	Heat Exchanger system	CT-1001		Fan failure	Motor winding open, No Voltage motor			2	1	1	0.2	1.01E-05	5.61237E-12	61320	36	0.123265464	
Water supply	Heat Exchanger system	P-1002	Pump #5/Transport chilled-water supply 960GPM	Degraded operation-produce water at less than	Impeller degraded, gasket leak, motor degraded			2	1	1	0.35	1.21E-05	8.07752E-12	61320	36	0.258788796	
Water supply	Heat Exchanger system	P-1002		Produce no water flow	Broken coupling, suctionline leak, motor inoperable			2	1	1	0.65	1.21E-05	6.05814E-12	61320	48	0.480607764	
Water supply	Heat Exchanger system	C-1002	Chiller/Remove heat (10 degF) from chilled water	Degraded operation remove less than 10 degF	Refrigeration leak, degraded component, tube leak, dirty coil			2	1	1	0.92	9.28E-06	3.58749E-12	61320	48	0.523469218	
Water supply	Heat Exchanger system			Remove no heat	Compressor seizure, Motor failure			2	1	1	0.08	9.28E-06	7.17499E-12	61320	24	0.045519062	
Water supply	Heat Exchanger system		Air handler/ Maintain room temperature of 72 degF, 3200	Maintain air temperature higher than 72 degF	Dirty Coils			2	1	1	0.35	1.77E-06	2.59808E-13	61320	24	0.037895453	
Water supply	Heat Exchanger system			Provide air flow at a rate less than 3200 cfm	Reduced motor output, Dirty intake filter			2	1	1	0.4	1.77E-06	2.59808E-13	61320	24	0.04330909	
Water supply	Heat Exchanger system			Provide no air flow	Broken belt, Motor failure, fan bearing seizure, No			2	1	1	0.25	1.77E-06	5.19616E-13	61320	12	0.027068181	

Bottom up approach

➢ Background

STPA

Proposed approach

Illustrative case

Discussions

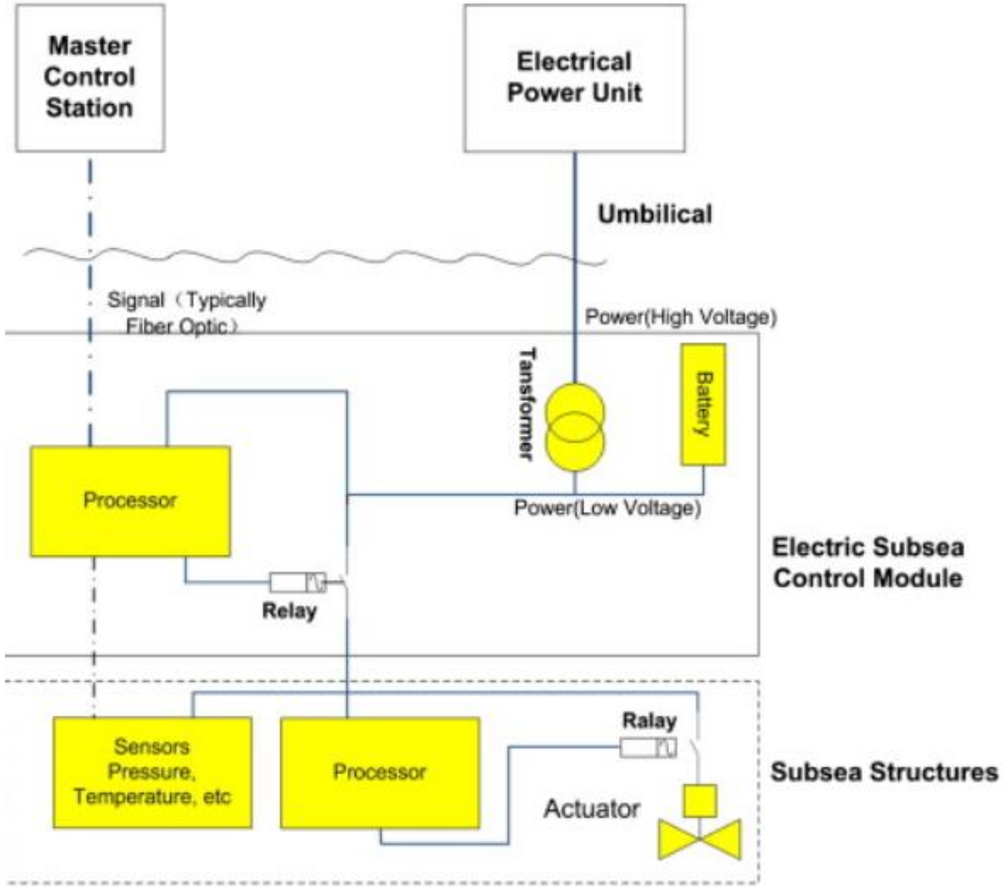
Why new approach is needed?

Old approaches cannot properly handle:

- ❑ Software errors
- ❑ Human-related interactions
- ❑ Design errors
- ❑ ….

Subsea system built today:

- ❑ Highly-coupled
- ❑ Software-intensive
- ❑ Higher level of autonomy



All electric control system. Ref. (Bai & Bai, 2010)

Background

➢ STPA

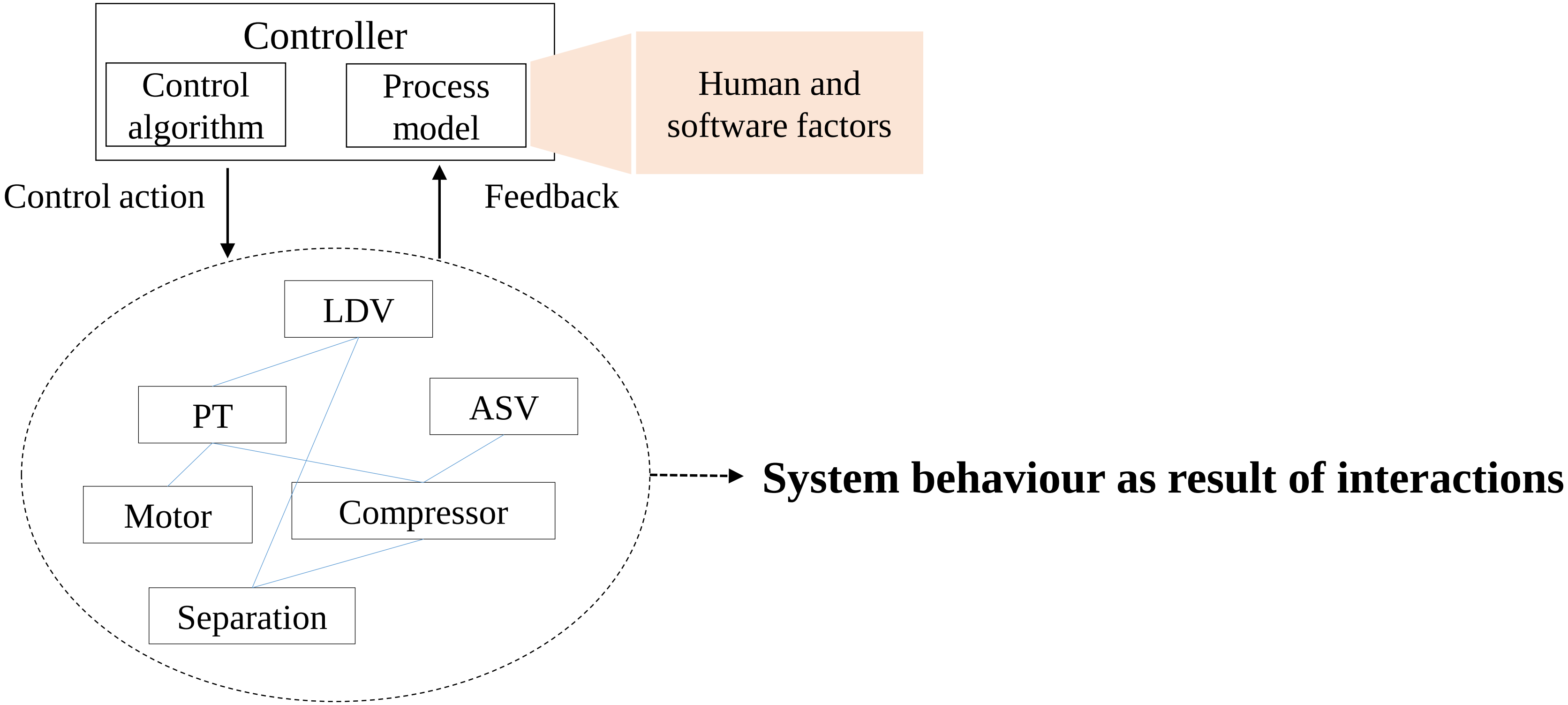
Proposed approach

Illustrative case

Discussions

System-Theoretic Process Analysis (STPA)

System theory and control theory:



System behaviour as result of interactions

STPA features:

- ❑ **Top down** approach
- ❑ Assume that safety is achieved under **adequate control**
- ❑ Interactions of **all actors** for system behaviour are included

Background

➢ STPA

Proposed approach

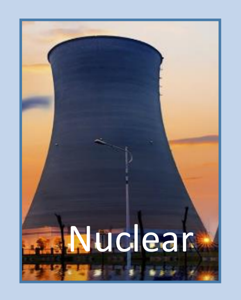
Illustrative case

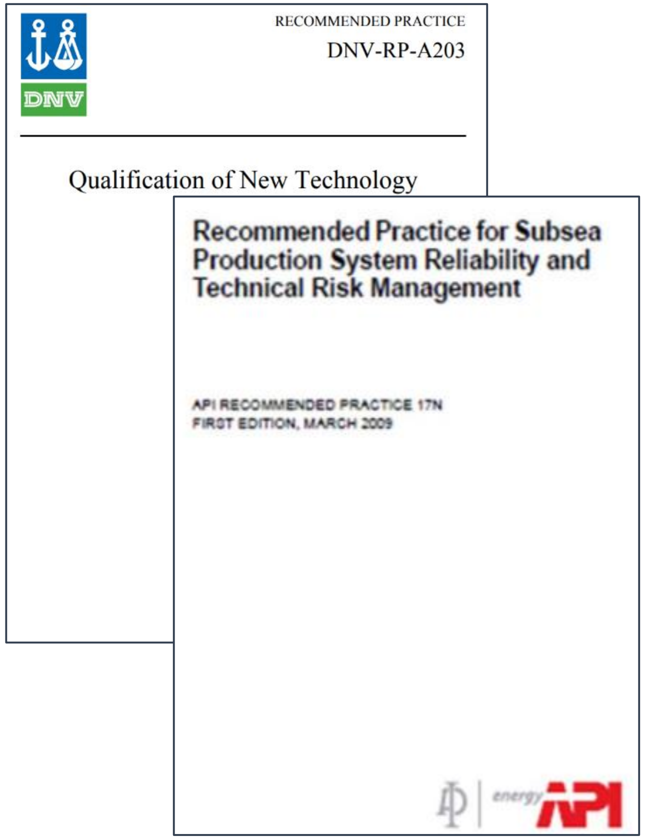
Discussions

Is STPA practicable/useful?

Lessons learnt:

❑ Increase **coverage** of hazards





RECOMMENDED PRACTICE
DNV-RP-A203

DNV

Qualification of New Technology

Recommended Practice for Subsea Production System Reliability and Technical Risk Management

API RECOMMENDED PRACTICE 17N
FIRST EDITION, MARCH 2009

energy API

Not adopted in technology qualification:

❑ How to interpret STPA outputs?

Approach

Background

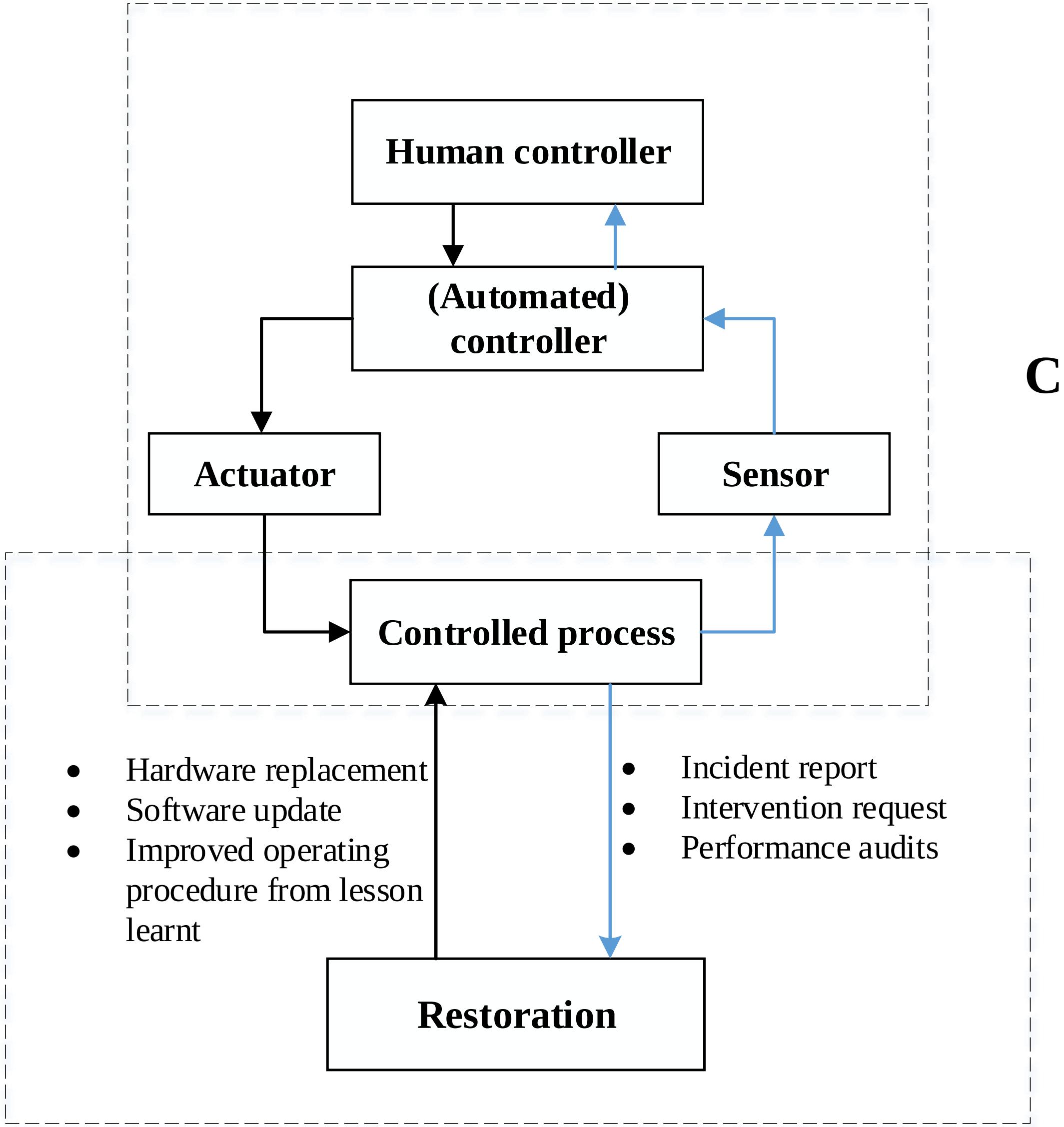
STPA

➢ Proposed approach

Illustrative case

Discussions

Objective: utilize STPA result to improve RAM analysis



- Hardware replacement
- Software update
- Improved operating procedure from lesson learnt

- Incident report
- Intervention request
- Performance audits

Step I: Carry out STPA

Covert into state-space modelling

Step II: Develop RAM model

Background

STPA

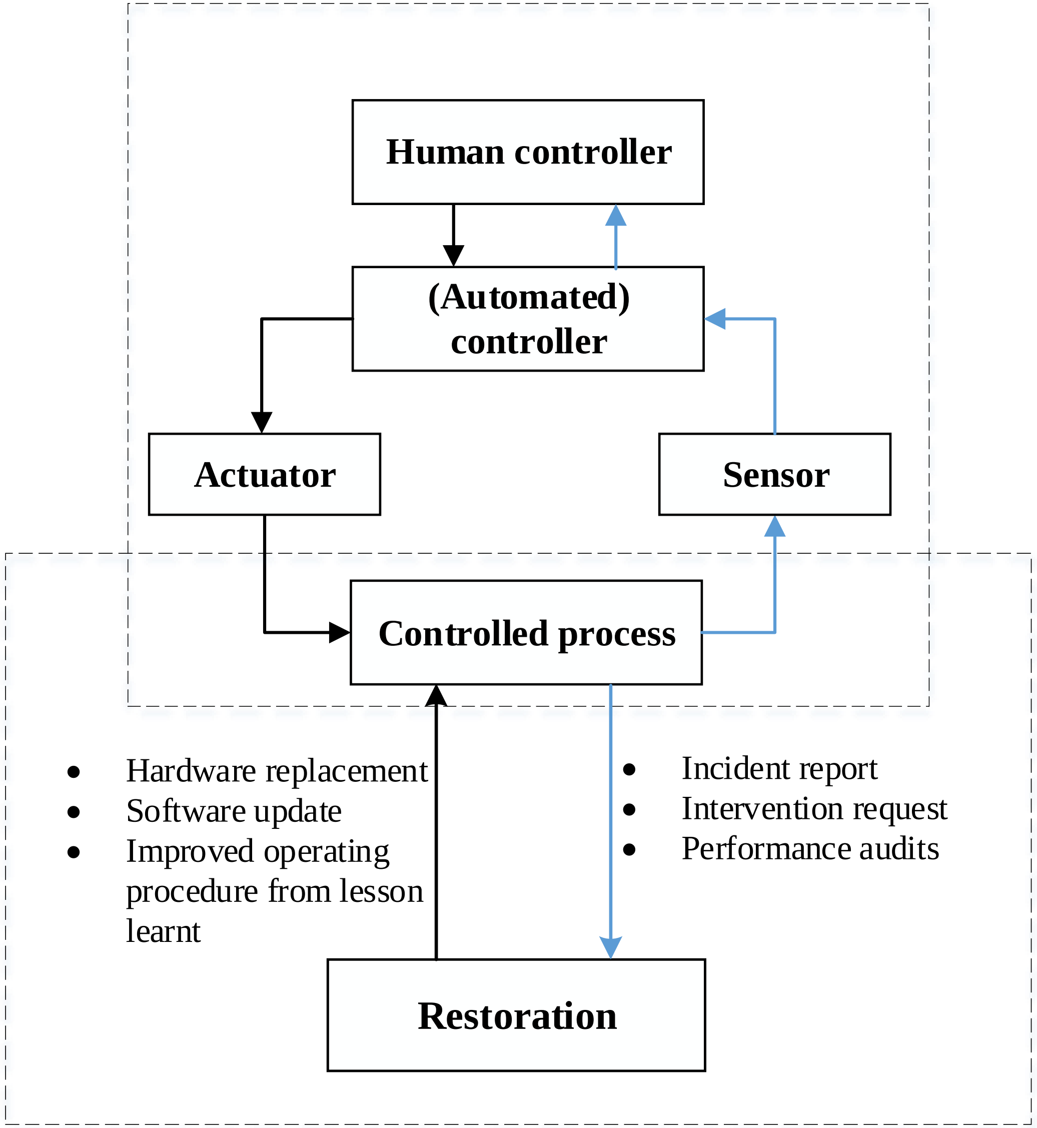
➢ Proposed approach

Illustrative case

Discussions

Approach

Objective: utilize STPA result to improve RAM analysis



Human controller

(Automated) controller

Actuator

Sensor

Controlled process

- Hardware replacement
- Software update
- Improved operating procedure from lesson learnt

- Incident report
- Intervention request
- Performance audits

Restoration

Step I: Carry out STPA

Selection of experiments

Step II: Develop RAM model

Background

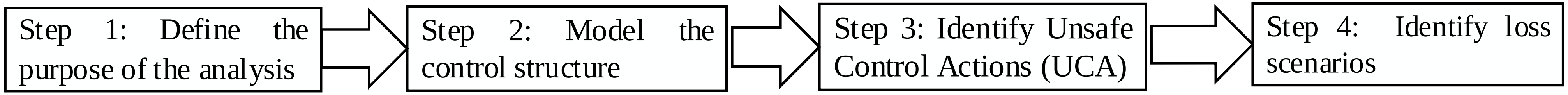
STPA

➢ Proposed approach

Illustrative case

Discussions

Step I: carry out STPA

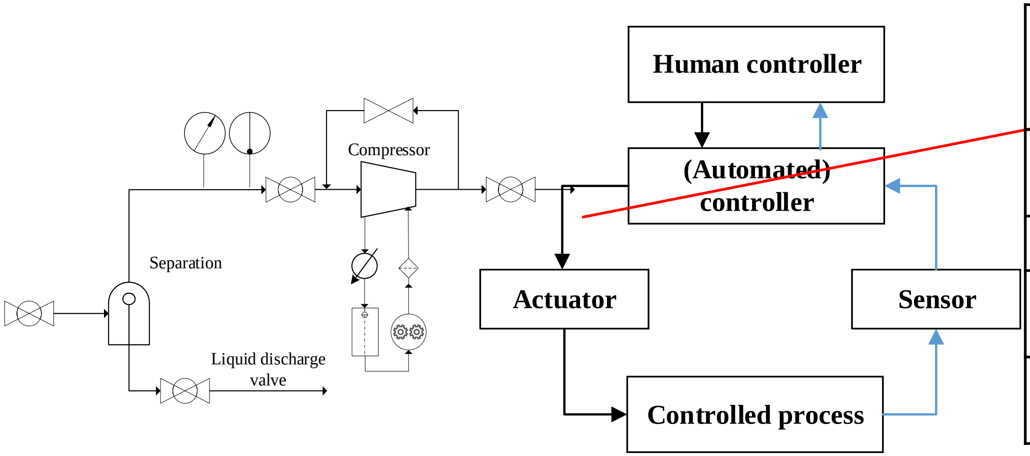


Step 1: Define the purpose of the analysis

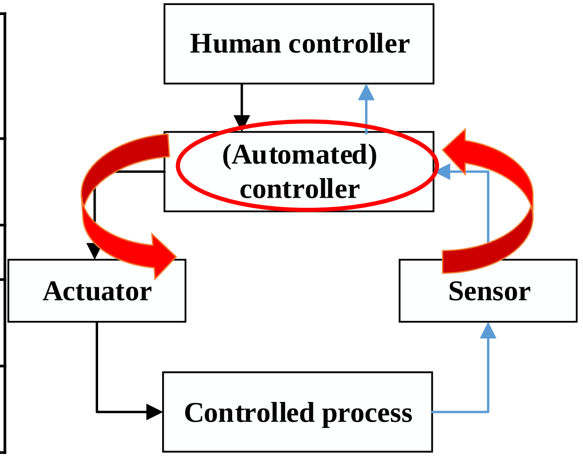
Step 2: Model the control structure

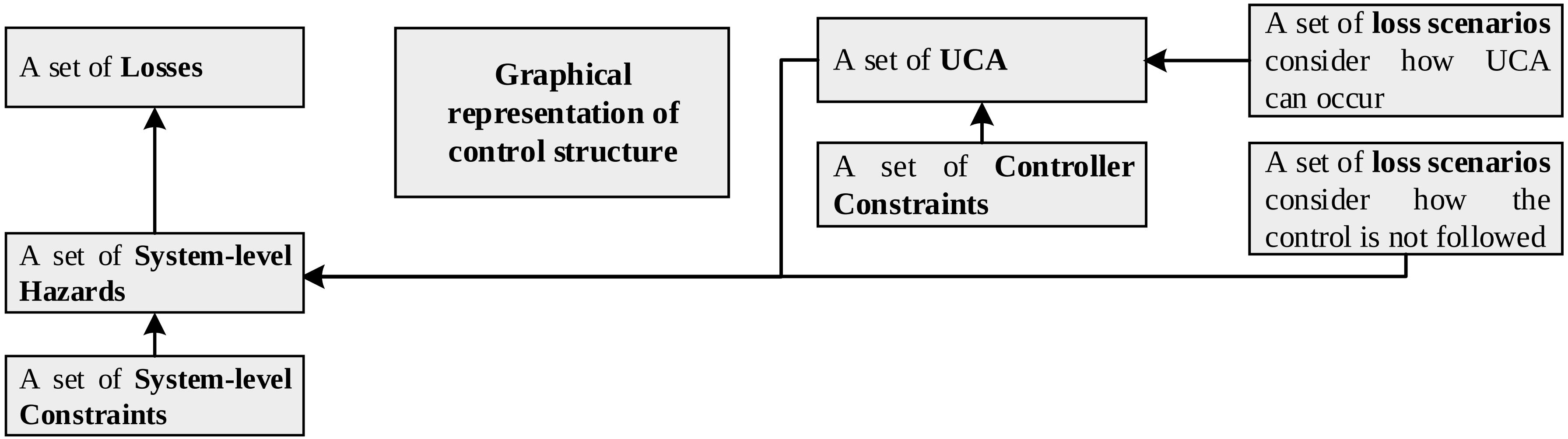
Step 3: Identify Unsafe Control Actions (UCA)

Step 4: Identify loss scenarios



	Context	Close valve
Not provided		
Provided		
Wrong timing		
Too soon or too long		





A set of **Losses**

A set of **System-level Hazards**

A set of **System-level Constraints**

Graphical representation of control structure

A set of **UCA**

A set of **Controller Constraints**

A set of **loss scenarios** consider how UCA can occur

A set of **loss scenarios** consider how the control is not followed

Background

STPA

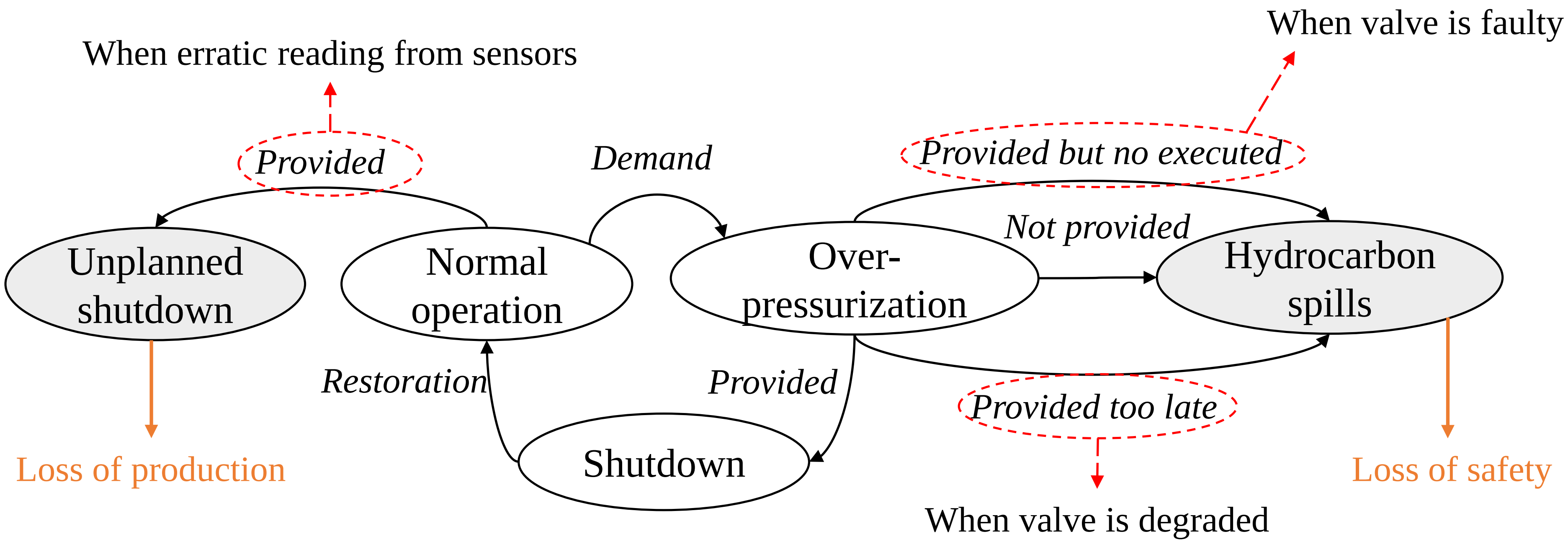
➢ Proposed approach

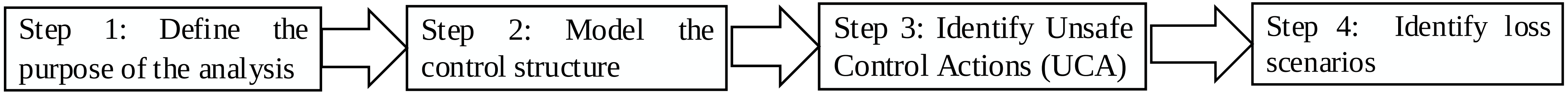
Illustrative case

Discussions

State-space modelling of STPA output

Example control action: close shutdown valve




Step 1: Define the purpose of the analysis

Step 2: Model the control structure

Step 3: Identify Unsafe Control Actions (UCA)

Step 4: Identify loss scenarios

Background

STPA

➢ Proposed approach

Illustrative case

Discussions

Step II: Develop RAM model

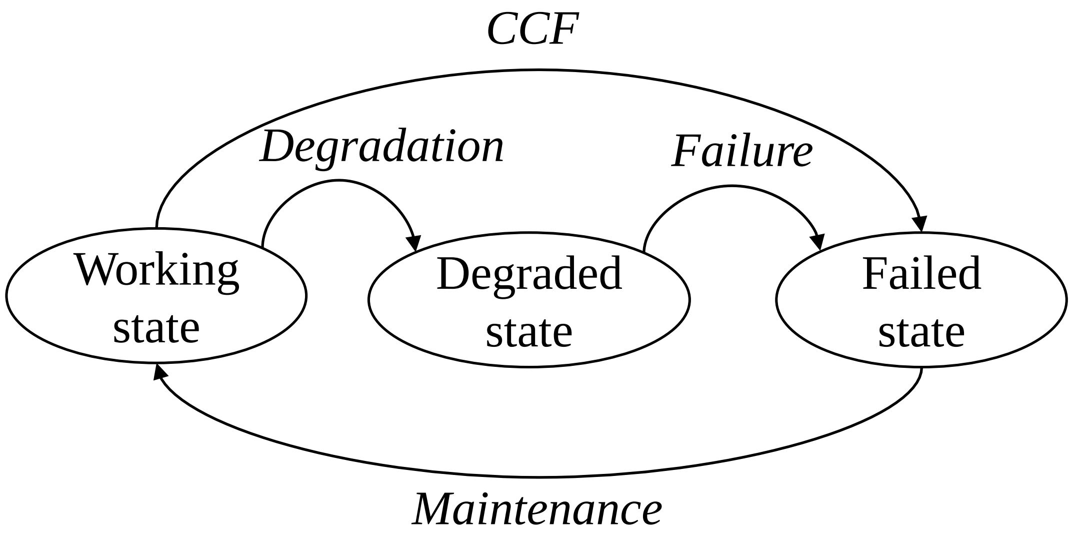
How can system fails:

❑ Failure modes
❑ Common cause failure
❑ Degradation
❑ …

How can system recover:

❑ Inspection
❑ Maintenance
❑ …

State transitions for valve:



Background

STPA

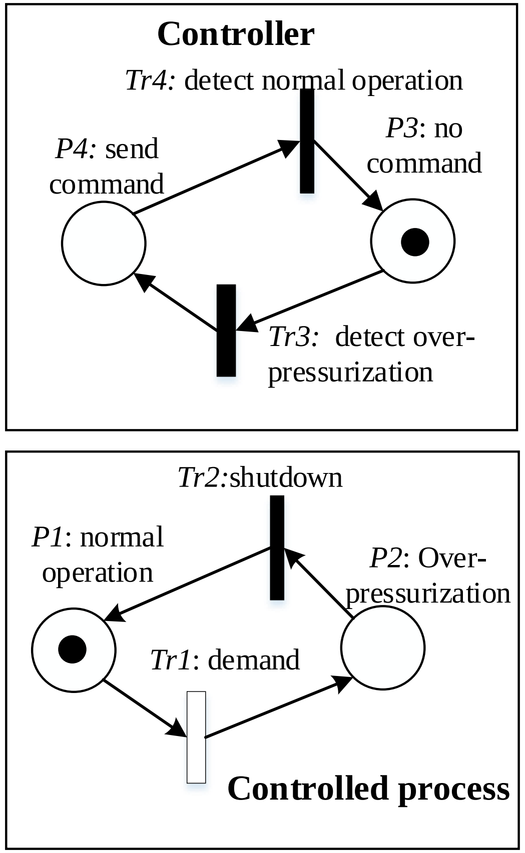
➢ Proposed approach

Illustrative case

Discussions

Petri-nets with Predicates

Safe control scenario:

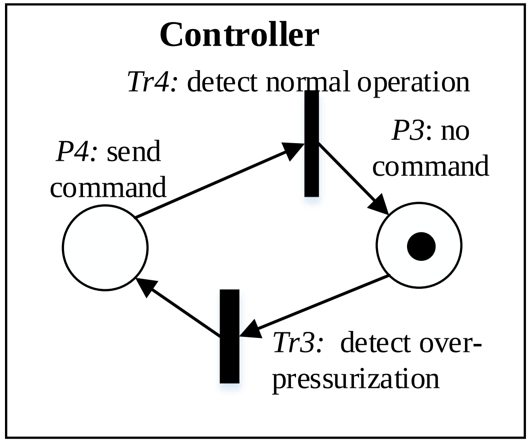


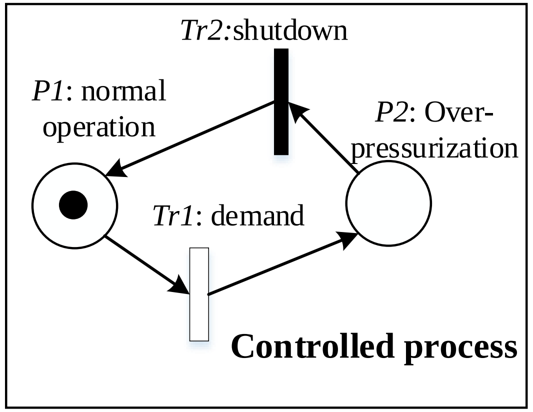
Transition	Predicate	Assertion
Tr1		normal_state=false
Tr2	reset ==true	normal_state=true
Tr3	normal_state== false	reset =true
Tr4	normal_state ==true	reset =false

Petri-nets with Predicates

- Background
- STPA
- ➢ Proposed approach
- Illustrative case
- Discussions

Safe control scenario:

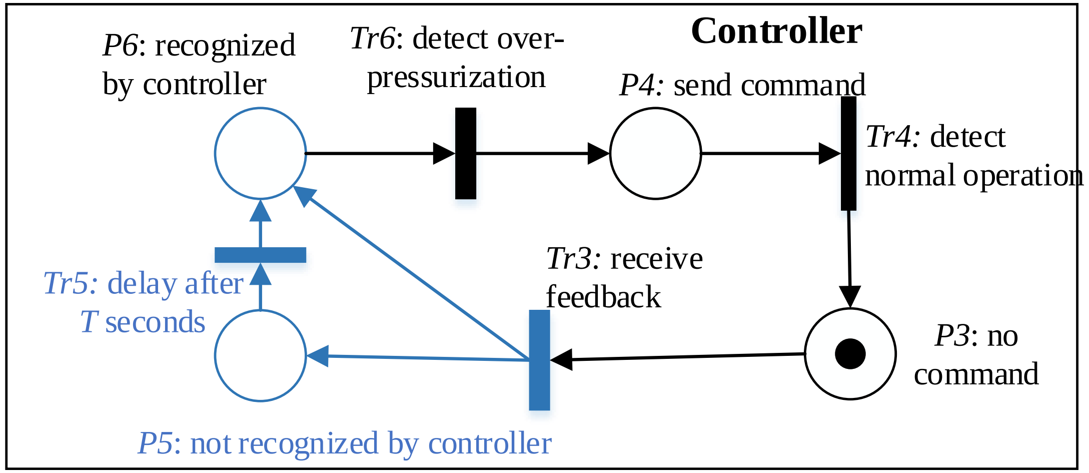


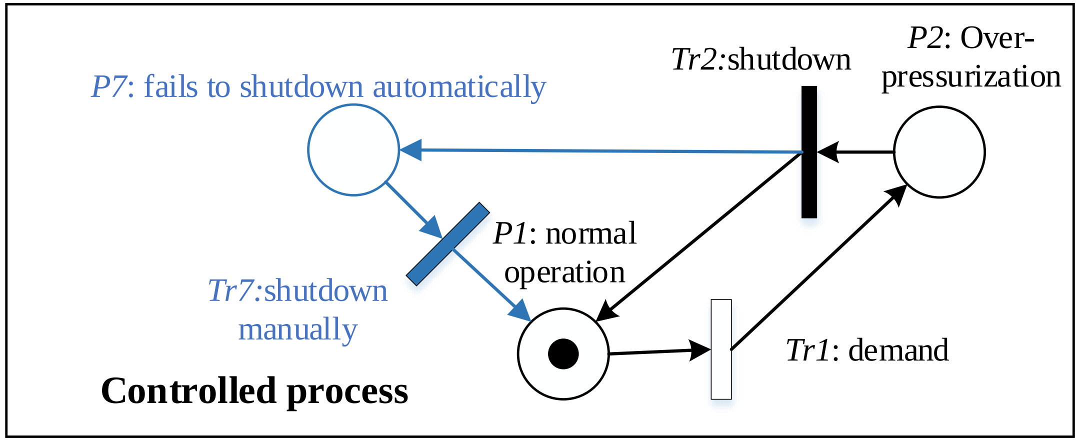


Controller sends the command **too late** (after *T* seconds)

Controlled process is **not successful activated**

Safe control scenario+ two loss scenarios:


P6: recognized by controller
Tr6: detect over-pressurization
Controller
P4: send command
Tr4: detect normal operation
Tr5: delay after T seconds
Tr3: receive feedback
P3: no command
P5: not recognized by controller



Background

STPA

➢ Proposed approach

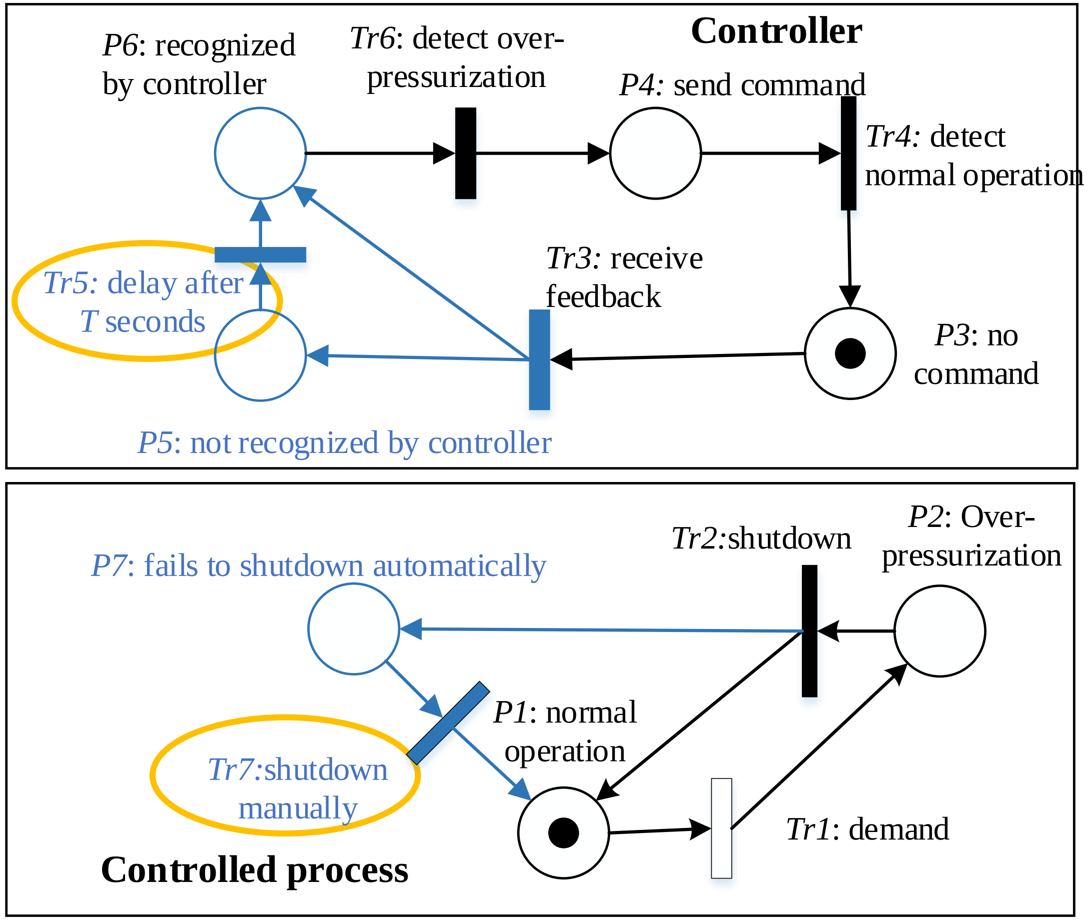
Illustrative case

Discussions

Petri-nets with Predicates

Transition	Predicate	Assertion	Delay of transition
Tr1		normal_state= false	stochastic delay, λ
Tr2	reset =true	normal_state =true	X seconds
Tr3	normal_state =false		0
Tr4	normal_state =true	reset =false	0
Tr5			*T* seconds
Tr6		reset =true	0
Tr7		$\lambda = \lambda \times (1 + \alpha)$	0

Safe control scenario+ two loss scenarios:


Controller
P6: recognized by controller
Tr6: detect over-pressurization
P4: send command
Tr4: detect normal operation
Tr5: delay after *T* seconds
Tr3: receive feedback
P3: no command
P5: not recognized by controller
Tr2:shutdown
P2: Over-pressurization
P7: fails to shutdown automatically
P1: normal operation
Tr7:shutdown manually
Tr1: demand
Controlled process

Background

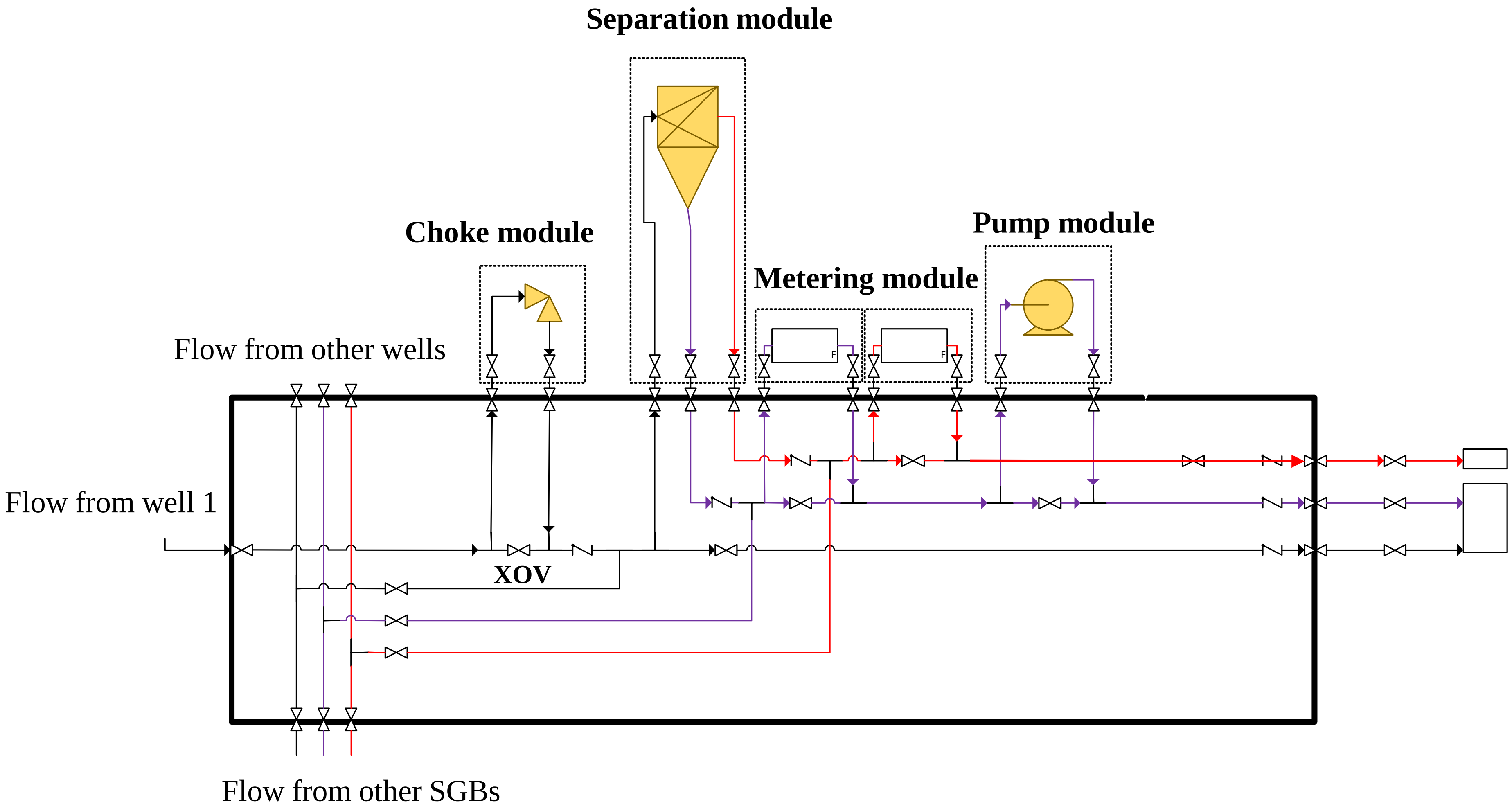
STPA

Proposed approach

➢ Illustrative case

Discussions

Subsea Gate box (SGB)



Ref. (Mariana, 2017)

Background

STPA

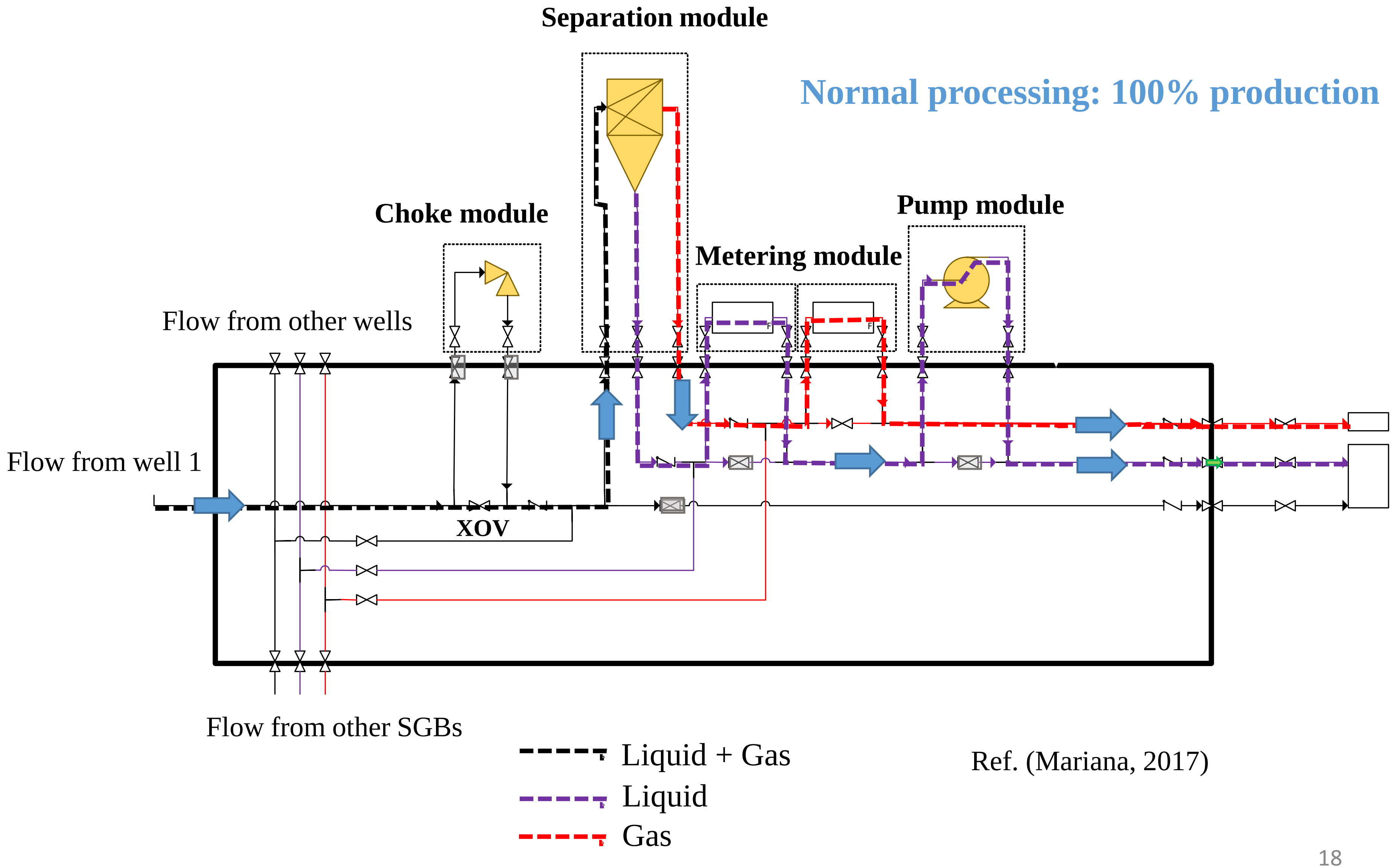
Proposed approach

➢ Illustrative case

Discussions

Normal processing (SGB-NP)

Normal processing: 100% production



Ref. (Mariana, 2017)

Background

STPA

Proposed approach

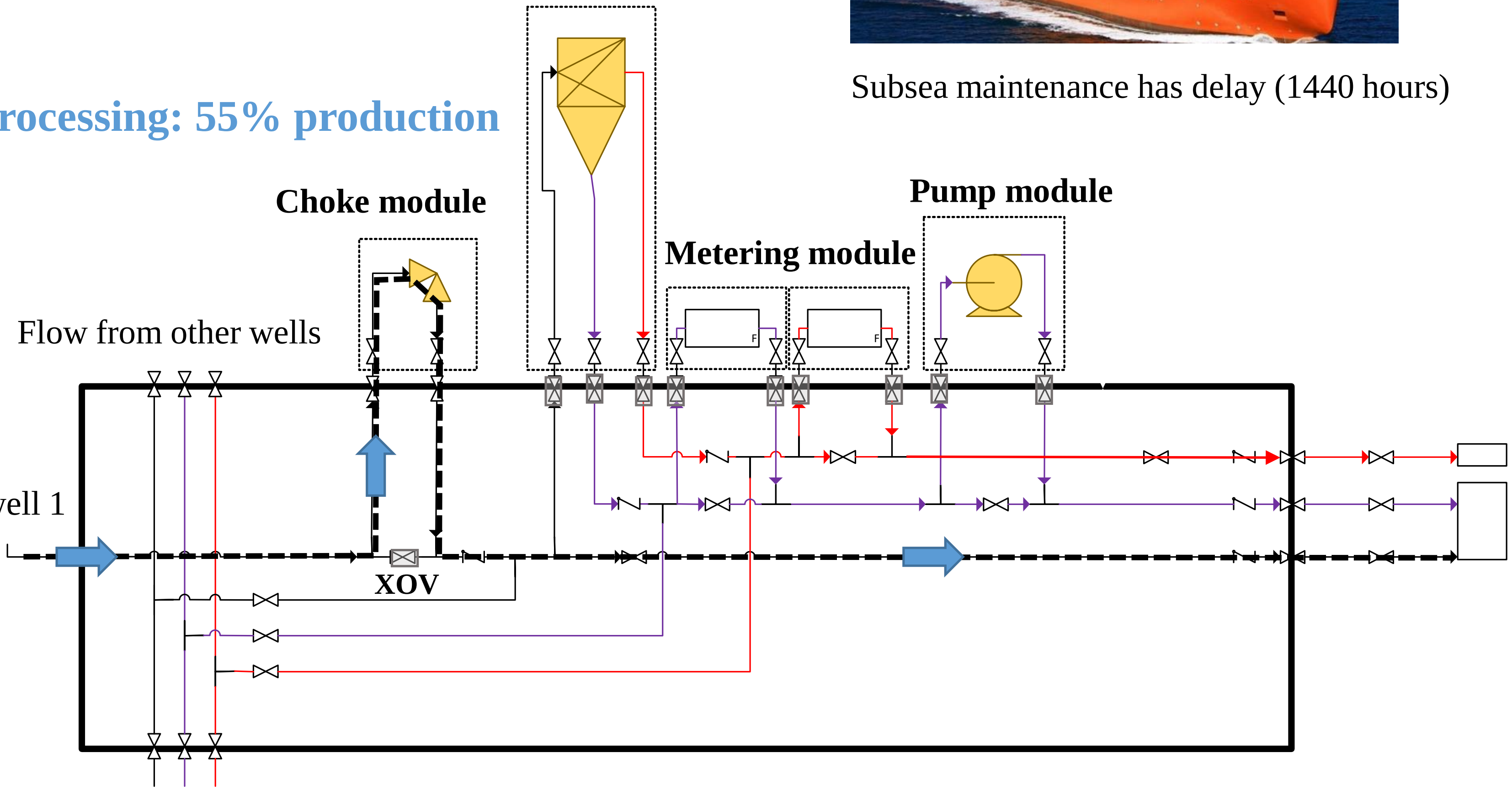
➢ Illustrative case

Discussions

Bypass processing (SGB-BP)

Subsea maintenance has delay (1440 hours)

Bypass processing: 55% production



- - - - Liquid + Gas
- - - - Liquid
- - - - Gas

Ref. (Mariana, 2017)

Background

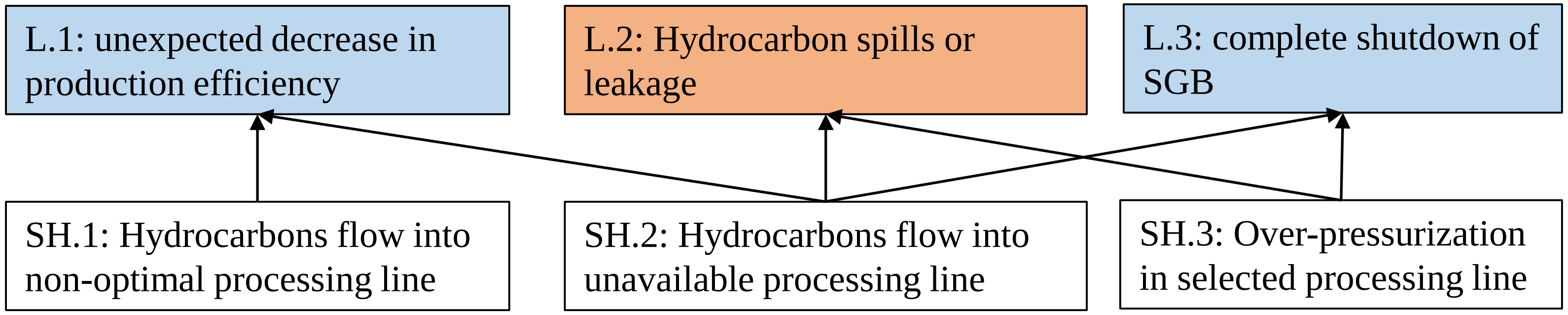
STPA

Proposed approach

➢ Illustrative case

Discussions

Step I: Carry out STPA


L.1: unexpected decrease in production efficiency

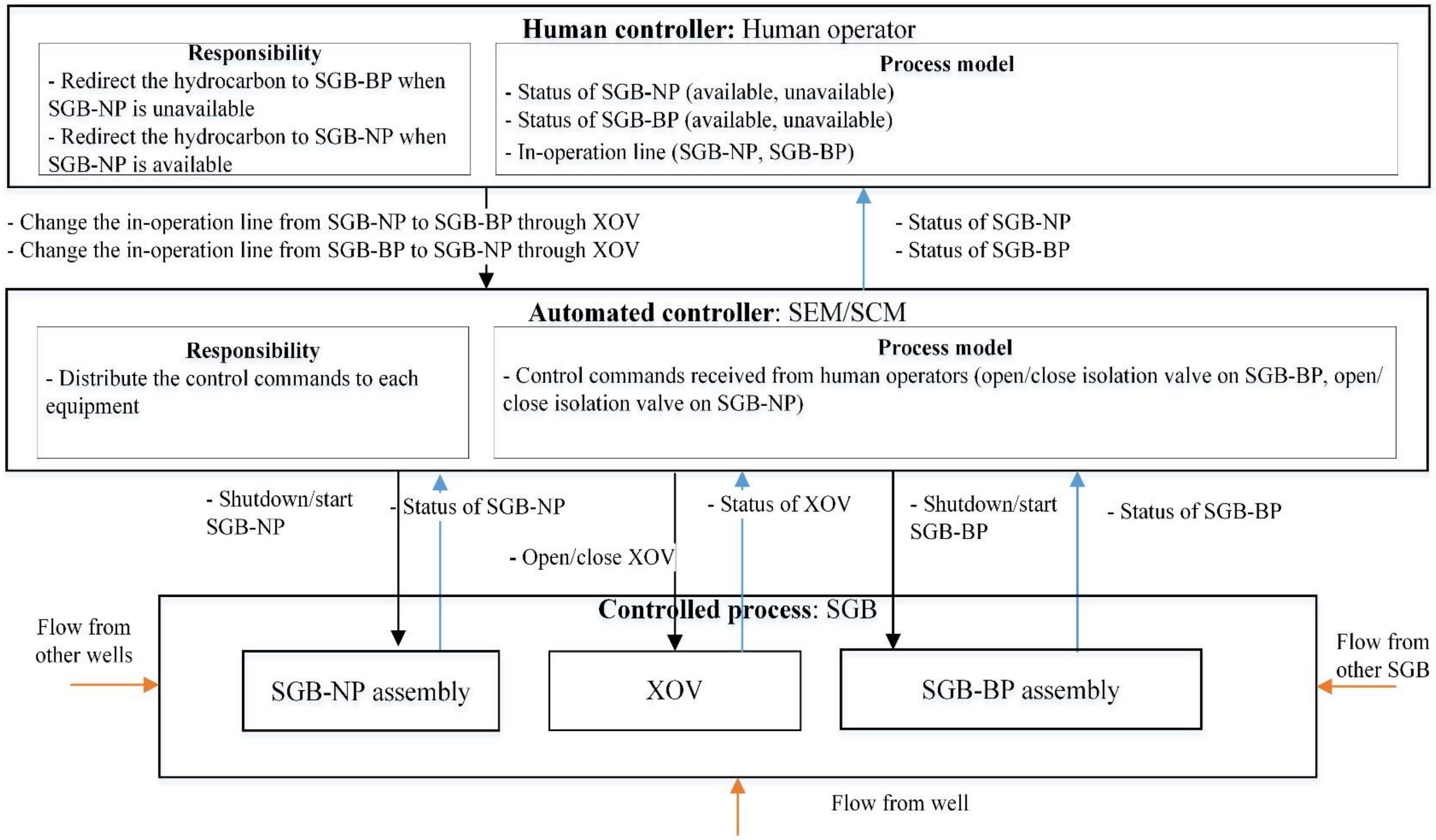
L.2: Hydrocarbon spills or leakage

L.3: complete shutdown of SGB

SH.1: Hydrocarbons flow into non-optimal processing line

SH.2: Hydrocarbons flow into unavailable processing line

SH.3: Over-pressurization in selected processing line


Human controller: Human operator

Responsibility

- Redirect the hydrocarbon to SGB-BP when SGB-NP is unavailable
- Redirect the hydrocarbon to SGB-NP when SGB-NP is available

Process model

- Status of SGB-NP (available, unavailable)
- Status of SGB-BP (available, unavailable)
- In-operation line (SGB-NP, SGB-BP)

- Change the in-operation line from SGB-NP to SGB-BP through XOV
- Change the in-operation line from SGB-BP to SGB-NP through XOV

- Status of SGB-NP
- Status of SGB-BP

Automated controller: SEM/SCM

Responsibility

- Distribute the control commands to each equipment

Process model

- Control commands received from human operators (open/close isolation valve on SGB-BP, open/close isolation valve on SGB-NP)

- Shutdown/start SGB-NP

- Status of SGB-NP

- Open/close XOV

- Status of XOV

- Shutdown/start SGB-BP

- Status of SGB-BP

Controlled process: SGB

SGB-NP assembly

XOV

SGB-BP assembly

Flow from other wells

Flow from other SGB

Flow from well

Background

STPA

Proposed approach

➢ Illustrative case

Discussions

Step I: Carry out STPA

Control action from SEM/SCM	Identification of UCAs			
Change the in-operation line from SGB-NP to SGB-BP through XOV	Not provided	Provided	Wrong timing or order	Too soon or too long
	UCA.1: Control command is not provided when SGB-NP is faulty and XOV is available [SH.1, SH.2,]	UCA.2: Control command is provided when both SGB-NP and XOV are available [SH.1]	UCA.4: Control command is provided too late when SGB-NP is faulty and XOV is available [SH.2, SH.3]	UCA.5: Control command is stopped too soon before XOV is fully closed when SGB-NP is faulty [SH.2, SH.3]
		UCA.3: Control command is provided when both SGB-NP and SGB-BP are faulty [SH.1, SH.2]		

UCA.1: Change the in-operation line from SGB-NP to SGB-BP through XOV is not provided by SCM/SEM on command from human operator when SGB-NP is faulty and XOV is available [SH.1, SH.2]	
Loss scenarios	Suggested countermeasures
SO.1 for UCA.1: Human operator receives correct feedback but interprets it incorrectly so SEM/SCM does not receive control command from human operator. The causal factor is that human operator lacks sufficient understanding for abnormal situation.	Must provide the sufficient training for operators to deal with specified hazardous situations.
SO.2 for UCA.1: Human operator receives correct feedback but makes mistakes so SEM/SCM does not receive control command from human operator. The causal factor is that human operator is overstressed when there are too many process to be considered.	The reference document must be presented to provide guidance for operation.
SO.3 for UCA.1: Human operator receives incorrect feedback about conditions of SGB-NP so wrongly believes that the SGB-NP is working but it is not. The casual factor is that the sensor on SGB-NP provides erratic readings.	Sensors must be monitored continuously and be calibrated when erratic reading was detected

Loss scenarios	Suggested countermeasures
SO.4: The control command is initiated by human operator but not received by SCM/SEM. The casual factor is that there is a critical failure on SEM/SCM [SH.1, SH.2].	The status of SCM/SEM must be checked before operation and after each updates.
SO.5: The control command is provided by SCM/SEM on command from human operator, but actuator does not responds to this control command. The casual factor is critical failures on XOV (actuator) [SH.1, SH.2].	XOV must be checked regularly and be repaired when critical failure is revealed.

Background

STPA

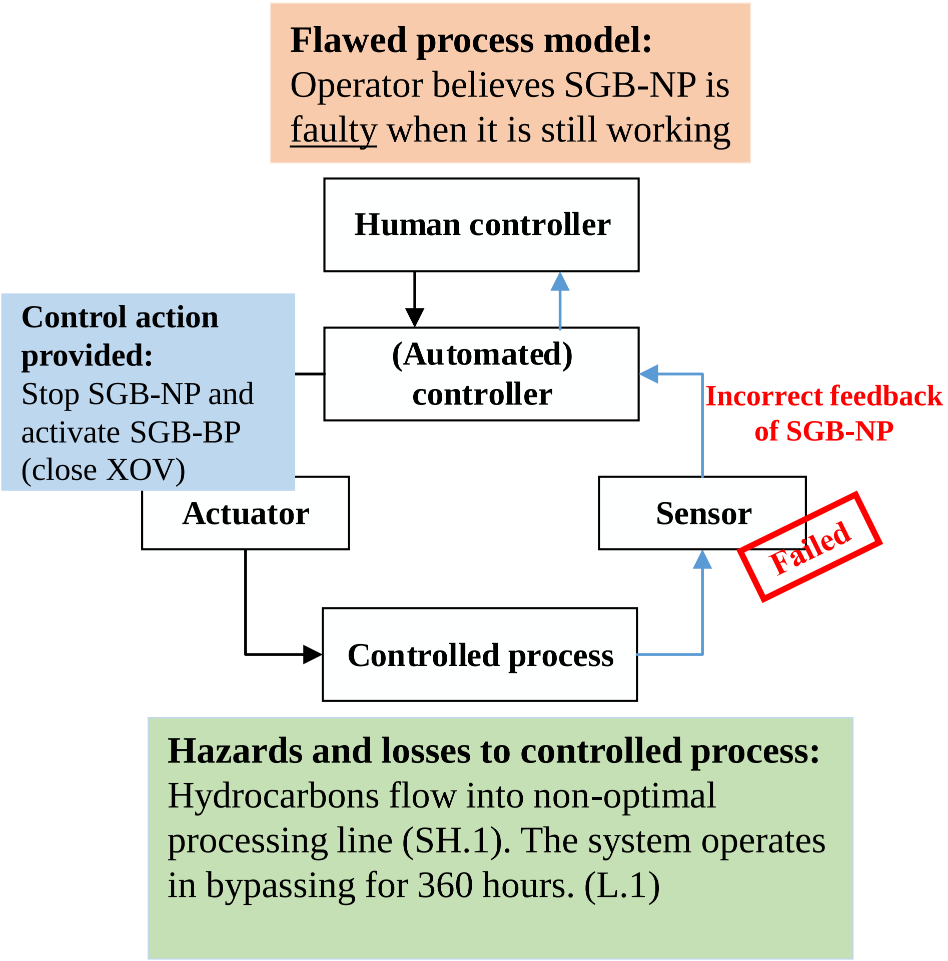
Proposed approach

- Illustrative case

Discussions

Step I: Carry out STPA

Loss scenario 1

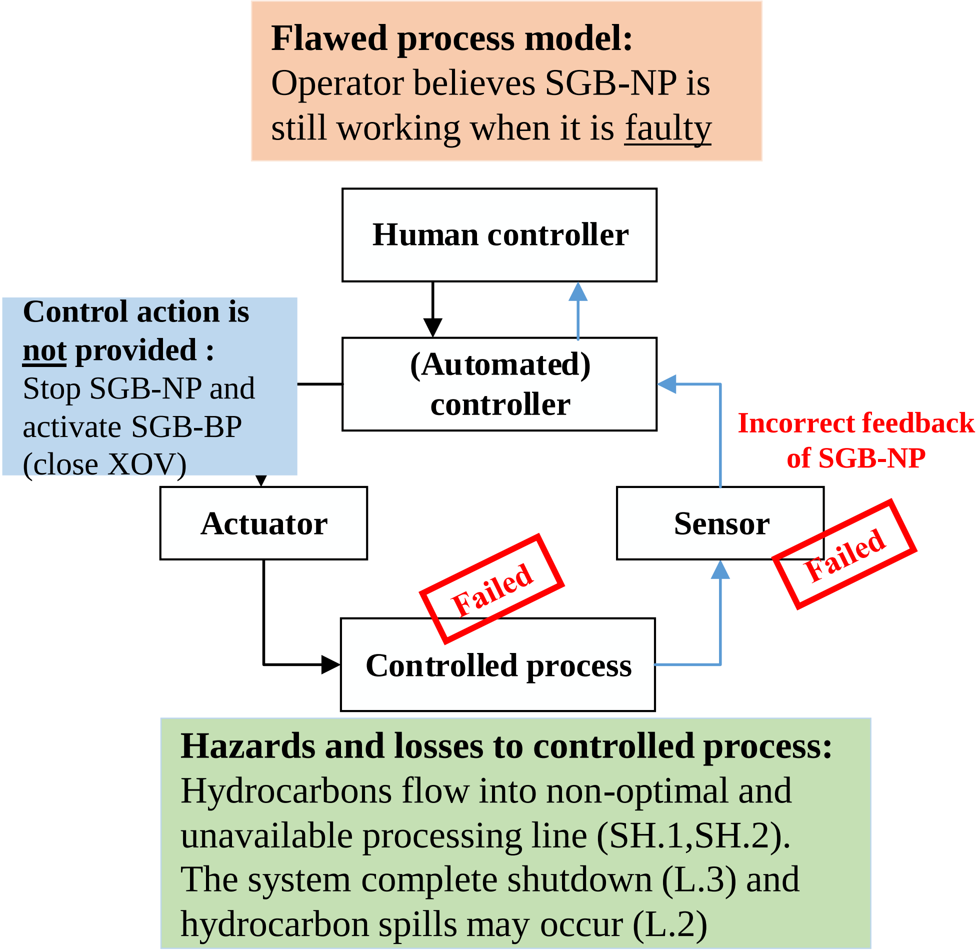


Flawed process model: Operator believes SGB-NP is faulty when it is still working

Control action provided: Stop SGB-NP and activate SGB-BP (close XOV)

Hazards and losses to controlled process: Hydrocarbons flow into non-optimal processing line (SH.1). The system operates in bypassing for 360 hours. (L.1)

Loss scenario 2



Flawed process model: Operator believes SGB-NP is still working when it is faulty

Control action is not provided : Stop SGB-NP and activate SGB-BP (close XOV)

Hazards and losses to controlled process: Hydrocarbons flow into non-optimal and unavailable processing line (SH.1,SH.2). The system complete shutdown (L.3) and hydrocarbon spills may occur (L.2)

Background

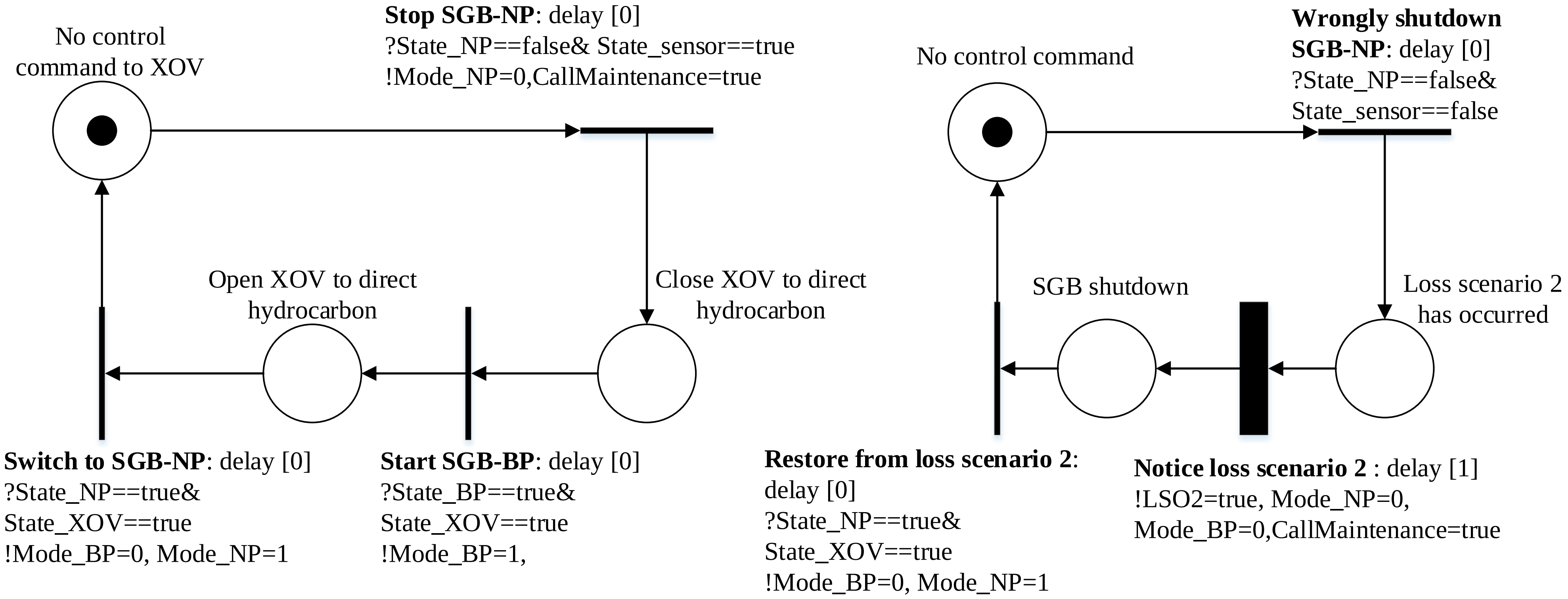
STPA

Proposed approach

➢ Illustrative case

Discussions

Petri-nets for loss scenario 2 and safe scenario


No control command to XOV
Stop SGB-NP: delay [0]
?State_NP==false& State_sensor==true
!Mode_NP=0,CallMaintenance=true
Open XOV to direct hydrocarbon
Close XOV to direct hydrocarbon
Switch to SGB-NP: delay [0]
?State_NP==true&
State_XOV==true
!Mode_BP=0, Mode_NP=1
Start SGB-BP: delay [0]
?State_BP==true&
State_XOV==true
!Mode_BP=1,
No control command
Wrongly shutdown SGB-NP: delay [0]
?State_NP==false&
State_sensor==false
SGB shutdown
Loss scenario 2 has occurred
Restore from loss scenario 2:
delay [0]
?State_NP==true&
State_XOV==true
!Mode_BP=0, Mode_NP=1
Notice loss scenario 2 : delay [1]
!LSO2=true, Mode_NP=0,
Mode_BP=0,CallMaintenance=true

Background

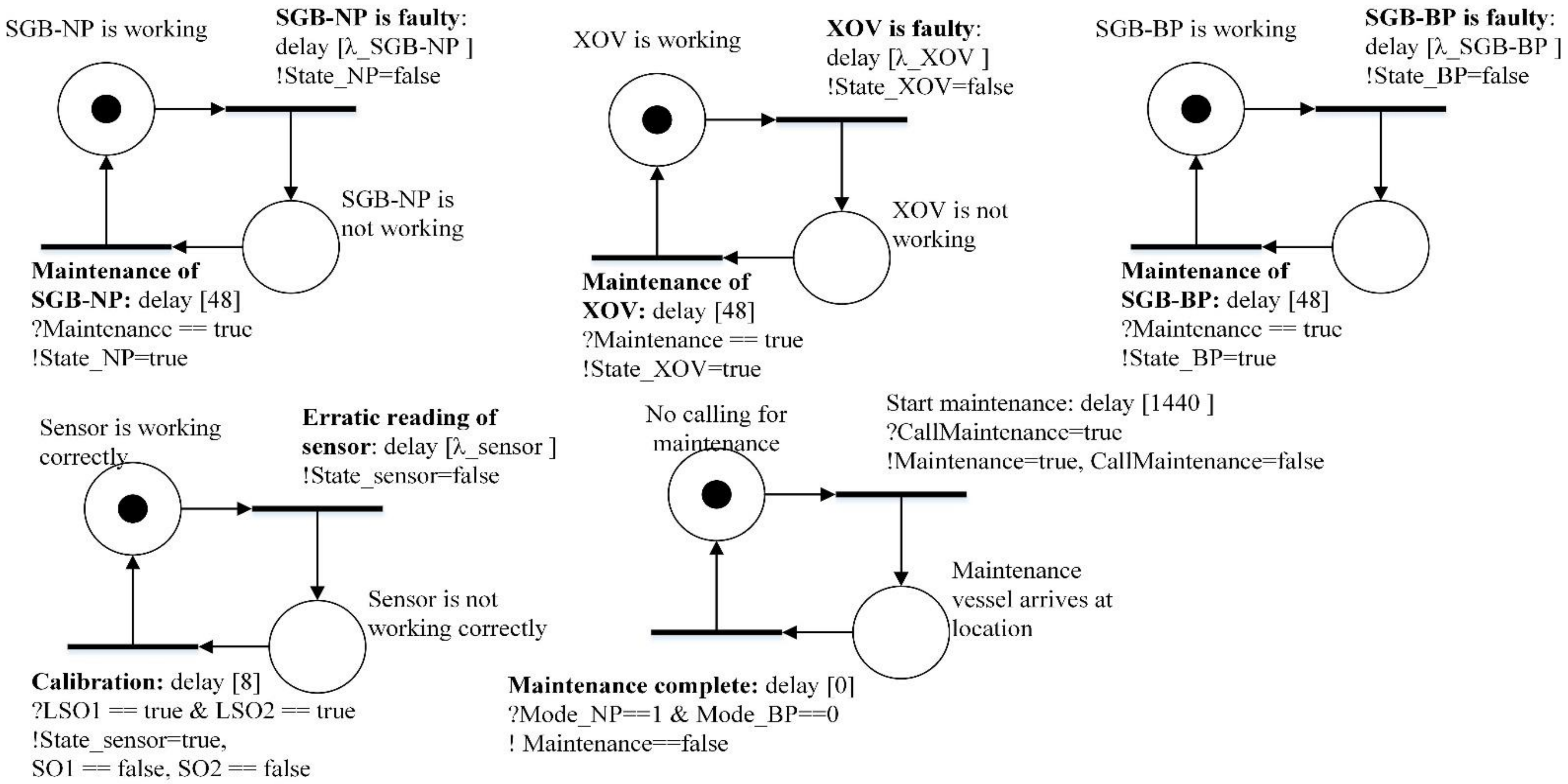
STPA

Proposed approach

➢ Illustrative case

Discussions

Step II: Develop RAM model



SGB-NP is working

SGB-NP is faulty: delay [λ_SGB-NP] !State_NP=false

SGB-NP is not working

Maintenance of SGB-NP: delay [48] ?Maintenance == true !State_NP=true

XOV is working

XOV is faulty: delay [λ_XOV] !State_XOV=false

XOV is not working

Maintenance of XOV: delay [48] ?Maintenance == true !State_XOV=true

SGB-BP is working

SGB-BP is faulty: delay [λ_SGB-BP] !State_BP=false

Maintenance of SGB-BP: delay [48] ?Maintenance == true !State_BP=true

Sensor is working correctly

Erratic reading of sensor: delay [λ_sensor] !State_sensor=false

Sensor is not working correctly

Calibration: delay [8] ?LSO1 == true & LSO2 == true !State_sensor=true, SO1 == false, SO2 == false

No calling for maintenance

Start maintenance: delay [1440] ?CallMaintenance=true !Maintenance=true, CallMaintenance=false

Maintenance vessel arrives at location

Maintenance complete: delay [0] ?Mode_NP==1 & Mode_BP==0 ! Maintenance==false

Case 0: λ_sensor= 0×10^{-5} hour^{-1} → Only safe scenario

Case 1: λ_sensor= 0.5×10^{-5} hour^{-1}

Case 2: λ_sensor= 1×10^{-5} hour^{-1}

Case 3: λ_sensor= 1.5×10^{-5} hour^{-1}

Loss scenario 1 & 2

Background

STPA

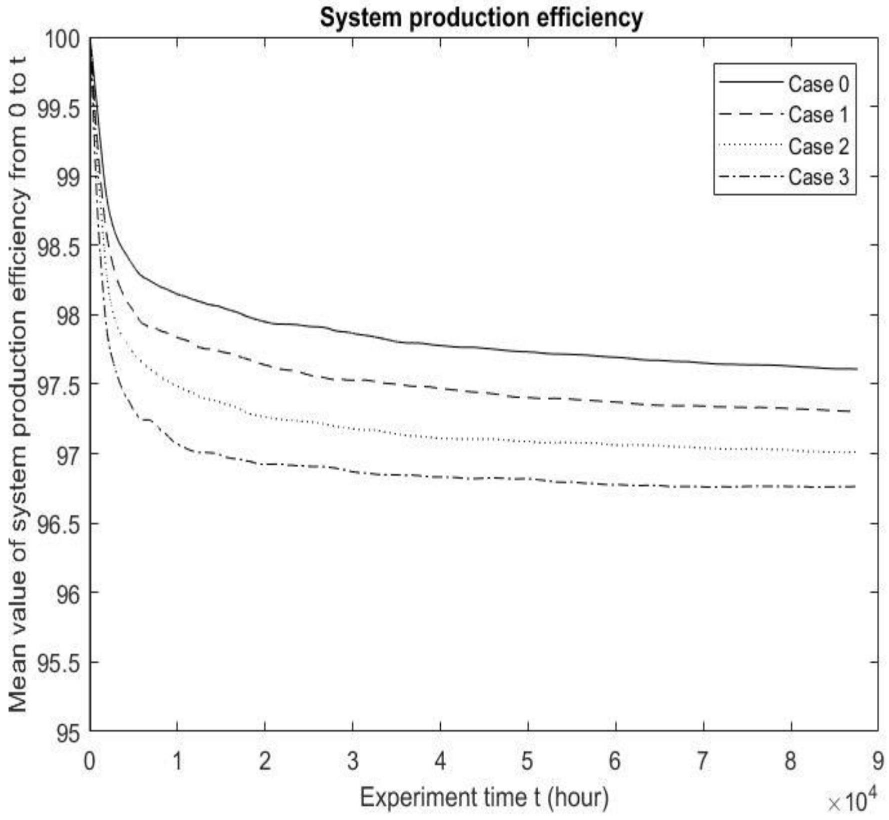
Proposed approach

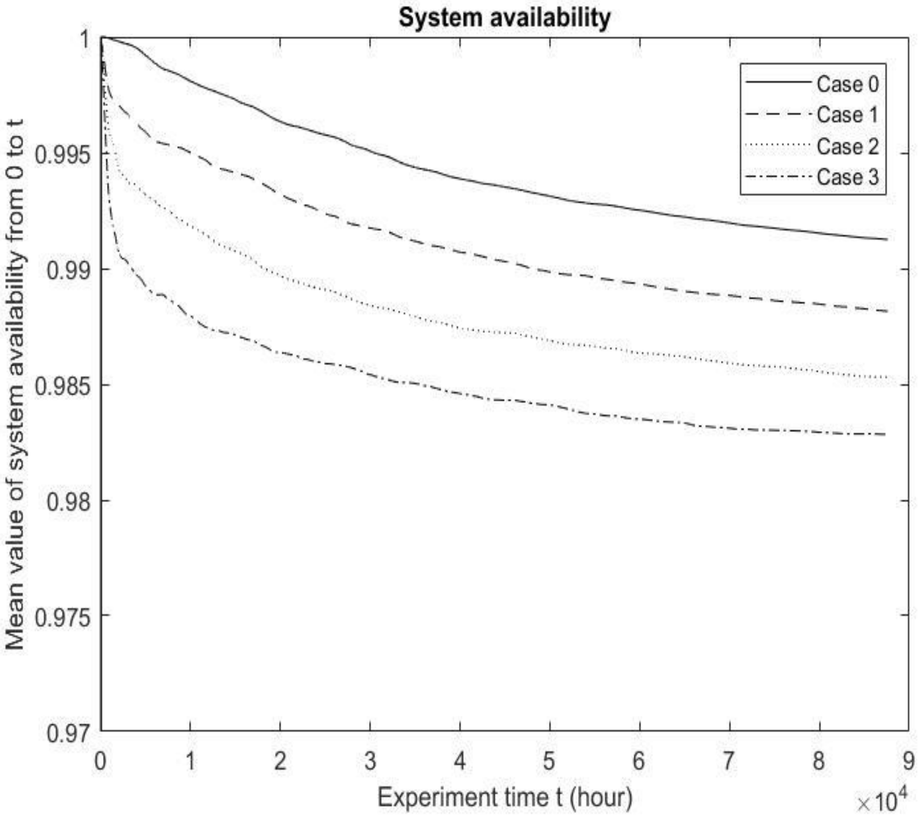
➢ Illustrative case

Discussions

Numerical results

	Loss scenario 1 (L.1)	Loss scenario 2 (L.1, L.2, L.3)
Case 1	7.028×10^{-2} year^{-1}	3.3×10^{-4} year^{-1}
Case 2	1.427×10^{-1} year^{-1}	5.7×10^{-4} year^{-1}
Case 3	2.033×10^{-1} year^{-1}	7.9×10^{-4} year^{-1}





Uncertainty level

Background

STPA

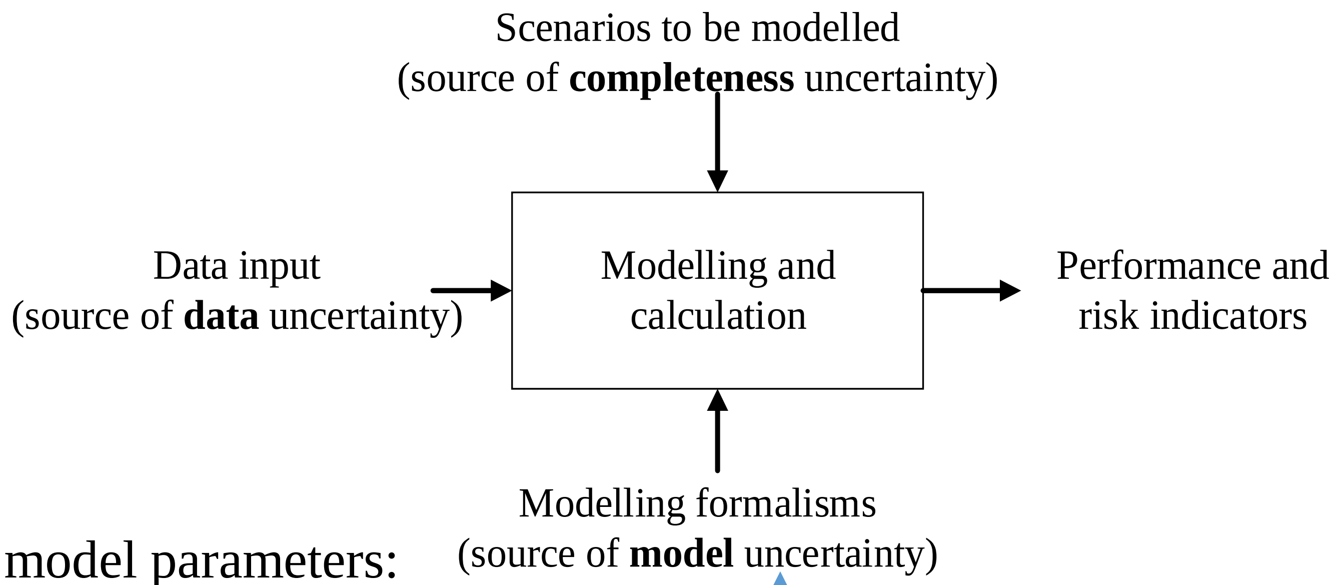
Proposed approach

Illustrative case

➢ Discussions

incomplete scope of analysis

❑ STPA increase coverage of hazard


Scenarios to be modelled
(source of **completeness** uncertainty)
Data input
(source of **data** uncertainty)
Modelling and calculation
Performance and risk indicators
Modelling formalisms
(source of **model** uncertainty)

Unreliable model parameters:

❑ Evaluate the level of background knowledge and assess the sensitivity of assumptions (Aven, 2013)

low **suitability** of model:

❑ Petri-nets do not distort the phenomenon

Background

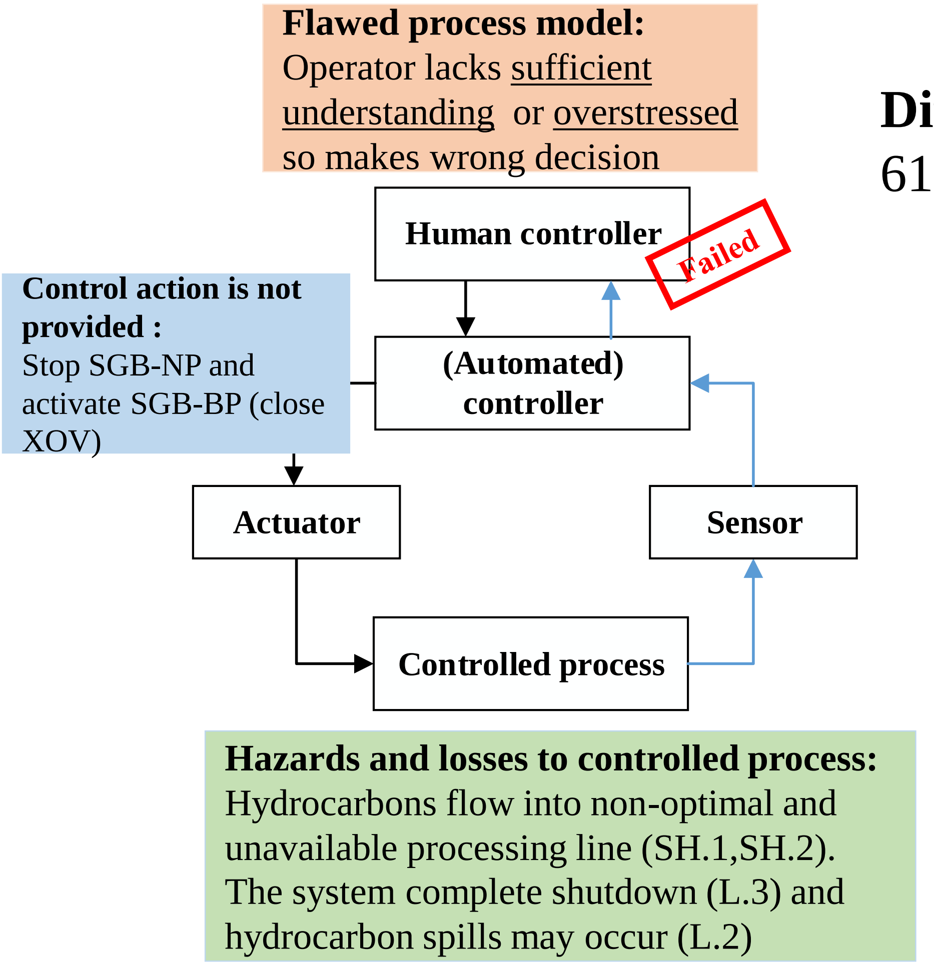
STPA

Proposed approach

Illustrative case

➢ Discussions

Potential for modelling human and software



Flawed process model: Operator lacks sufficient understanding or overstressed so makes wrong decision

Control action is not provided : Stop SGB-NP and activate SGB-BP (close XOV)

Hazards and losses to controlled process: Hydrocarbons flow into non-optimal and unavailable processing line (SH.1,SH.2). The system complete shutdown (L.3) and hydrocarbon spills may occur (L.2)

Different strategies for human factors in IEC 61508 (2010) and ISO TR 12489 (2013)

Background

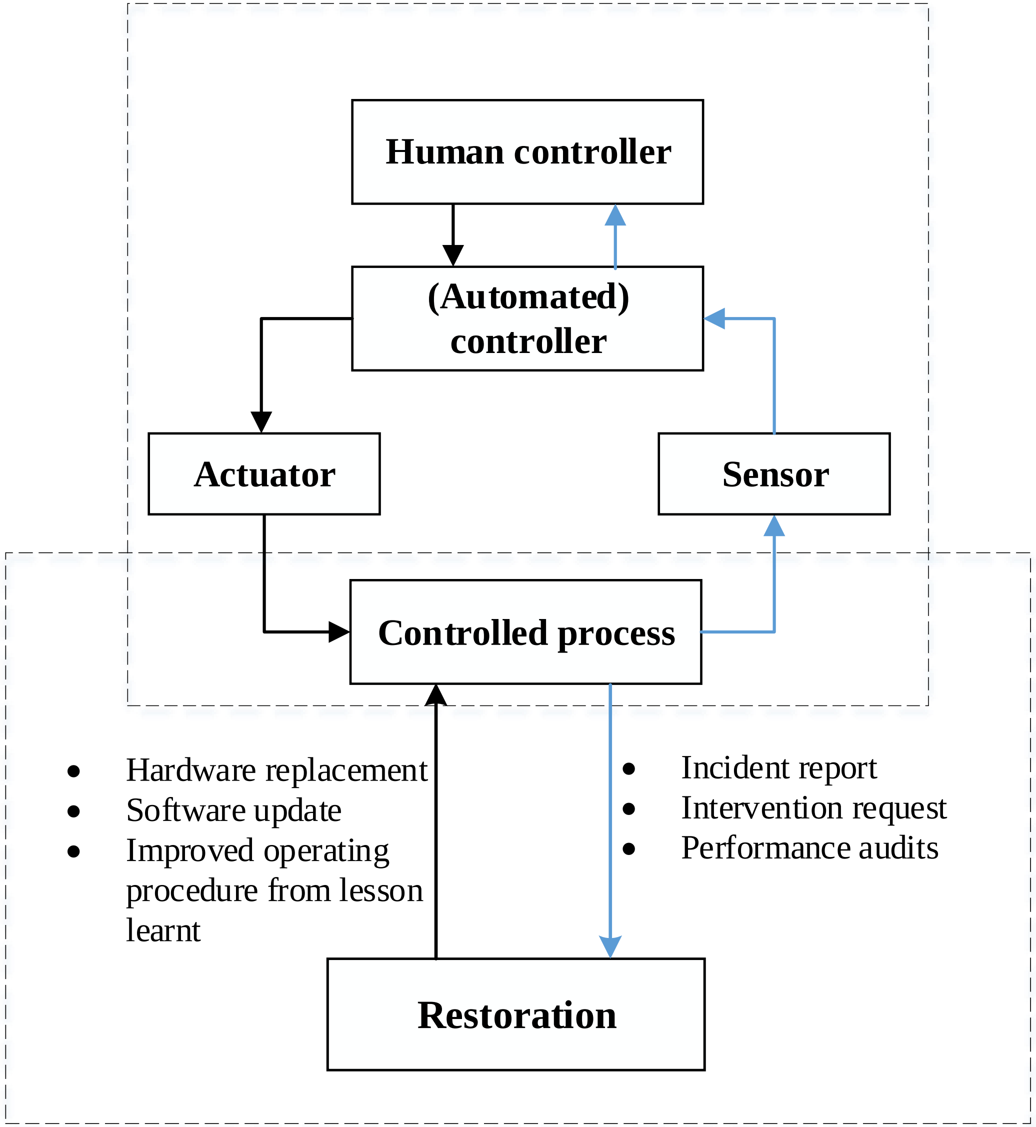
STPA

Proposed approach

Illustrative case

➢ Discussions

Prioritization and screening



Human controller

(Automated) controller

Actuator

Sensor

Controlled process

- Hardware replacement
- Software update
- Improved operating procedure from lesson learnt

- Incident report
- Intervention request
- Performance audits

Restoration

Additional step: Screen out critical scenarios

Step I: Carry out STPA

Selection of experiments

Step II: Develop RAM model

Background

STPA

Proposed approach

Illustrative case

➢ Discussions

Concluding remarks

Conclusion:

- The proposed approach clarifies (1) how to devise better simulation on basis of STPA output (2) to what extent STPA can contribute to decision-making (e.g. system production, maintenance and emergency management)

Future work:

- There is a need to screen out the most critical scenario to **decrease computational burden** in simulation.

- **Managing data uncertainty** is the potential improvement to the proposed approach .

Thanks for listening!

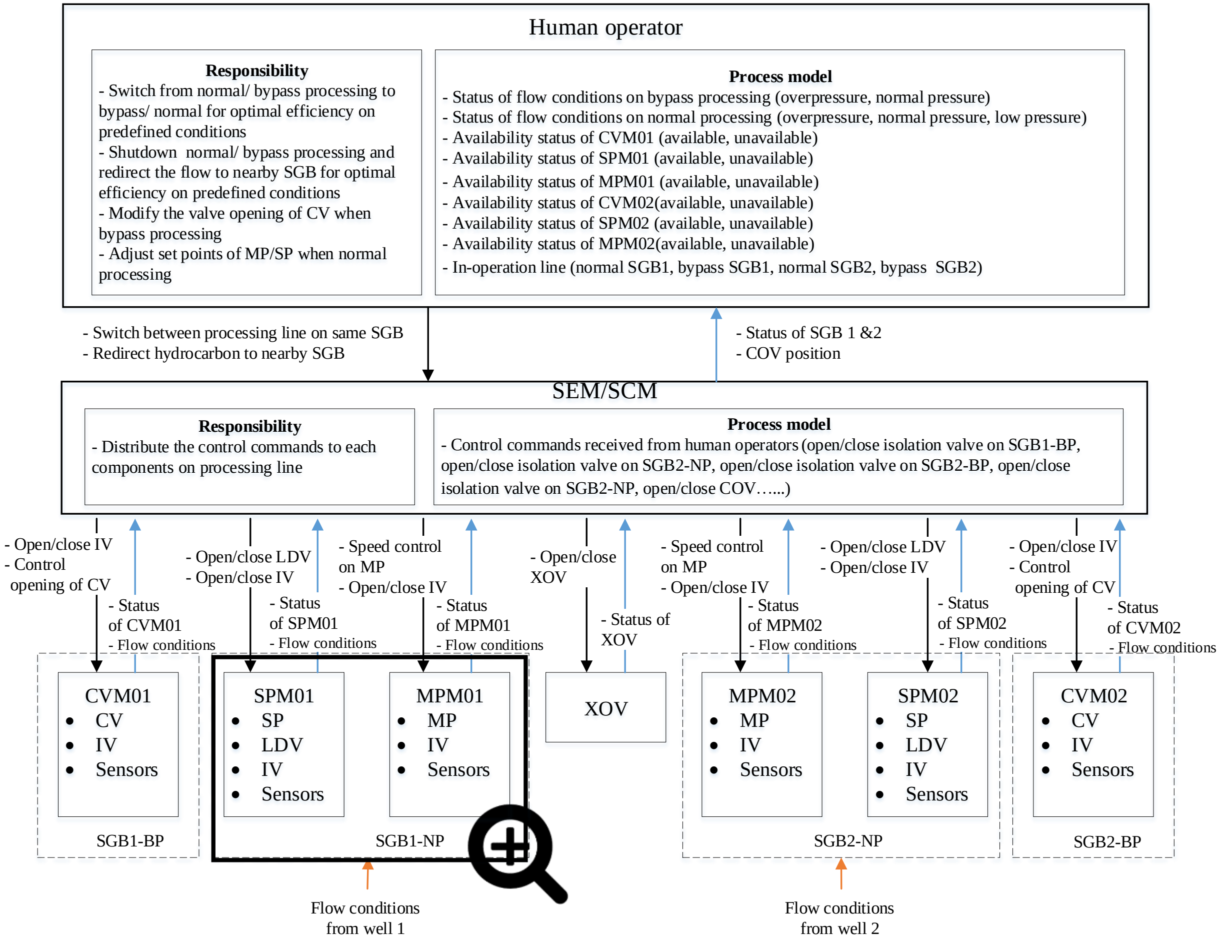
Any questions?

```
domain  Submodulestate = {Working, Degraded, Failed,
In_Repair}
domain  Mode = {Operation, Maintenance}
class Compressor
                Modulestate state (init= Working);
        Mode phase (init= Operation);
        Mode command (init= Operation) ;
                event degradation (delay=0),
                event failure (delay=exponential(lambda)),
                event repair (delay=mu),
                event startRepair (delay=0),
                event endRepair (delay=0);
                parameter Real lambda =1.0e-6,
                parameter Real mu =1440;
                transition
                degradation : state==Working and
phase==Operation and loss==true  -> state:= Degraded;
                failure : state==Degraded and
phase==Operation -> state:= Failed;
                repair: state==In_Repair -> state:= Working;
                startRepair: phase ==Operation and command
== Maintenance -> phase := Maintenance;
                endRepair: phase == Maintenance and
command==Operation -> {phase := Operation;
if state==Failed then state:= In_Repair;
if state==Degraded then state:= In_Repair};
end
```

```
class Separation
                Mode command (init=Operation);
                Mode state(init= Operation);
                event startRepair (delay=gamma),
                event failure (delay=exponential(lambda))
                event endRepair (delay=0);
                parameter Real gamma =720;
                transition
                                startRepair: state==
Maintenance -> command := Maintenance;
                                endRepair : state==
Operation -> command := Operation;
end
```

```
block Controller
Submodule Compressor, Separation;
Operator O;
assertion
O.state:= if Compressor.state== Failed or
Separation.state==Failed then Maintenance  else
Operation;
end
```

Detailed STPA:



Human operator

Responsibility
- Switch from normal/ bypass processing to bypass/ normal for optimal efficiency on predefined conditions
- Shutdown normal/ bypass processing and redirect the flow to nearby SGB for optimal efficiency on predefined conditions
- Modify the valve opening of CV when bypass processing
- Adjust set points of MP/SP when normal processing

Process model
- Status of flow conditions on bypass processing (overpressure, normal pressure)
- Status of flow conditions on normal processing (overpressure, normal pressure, low pressure)
- Availability status of CVM01 (available, unavailable)
- Availability status of SPM01 (available, unavailable)
- Availability status of MPM01 (available, unavailable)
- Availability status of CVM02(available, unavailable)
- Availability status of SPM02 (available, unavailable)
- Availability status of MPM02(available, unavailable)
- In-operation line (normal SGB1, bypass SGB1, normal SGB2, bypass SGB2)

- Switch between processing line on same SGB
- Redirect hydrocarbon to nearby SGB

- Status of SGB 1 &2
- COV position

SEM/SCM

Responsibility
- Distribute the control commands to each components on processing line

Process model
- Control commands received from human operators (open/close isolation valve on SGB1-BP, open/close isolation valve on SGB2-NP, open/close isolation valve on SGB2-BP, open/close isolation valve on SGB2-NP, open/close COV…...)

- Open/close IV
- Control opening of CV

- Status of CVM01
- Flow conditions

- Open/close LDV
- Open/close IV

- Status of SPM01
- Flow conditions

- Speed control on MP
- Open/close IV

- Status of MPM01
- Flow conditions

- Open/close XOV

- Status of XOV

- Speed control on MP
- Open/close IV

- Status of MPM02
- Flow conditions

- Open/close LDV
- Open/close IV

- Status of SPM02
- Flow conditions

- Open/close IV
- Control opening of CV

- Status of CVM02
- Flow conditions

CVM01
- CV
- IV
- Sensors

SGB1-BP

SPM01
- SP
- LDV
- IV
- Sensors

MPM01
- MP
- IV
- Sensors

SGB1-NP

XOV

MPM02
- MP
- IV
- Sensors

SPM02
- SP
- LDV
- IV
- Sensors

SGB2-NP

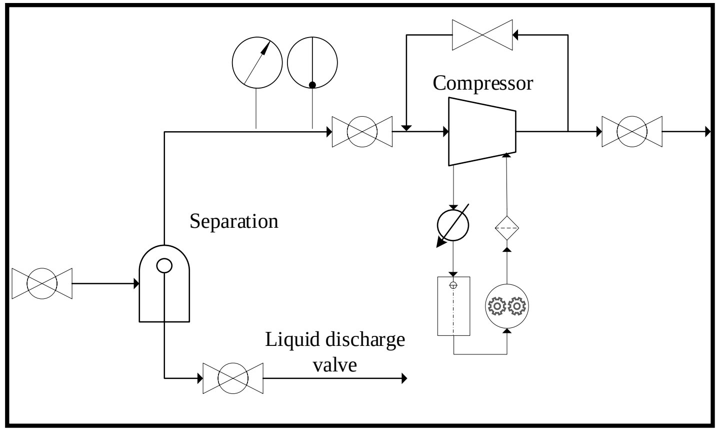
CVM02
- CV
- IV
- Sensors

SGB2-BP

Flow conditions from well 1

Flow conditions from well 2

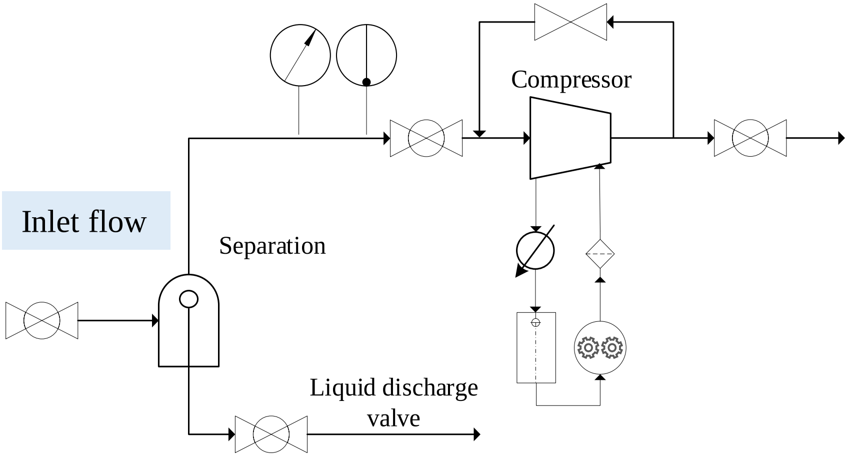
SGB-NP



Example: SO.xx-UCA.xx: The liquid level in separator is above defined value, but the operator does not provide the valve open command. The causal factor is that the **<u>signal cable from the transmitter is disconnected</u>**. As a result, liquid may flow into the gas compressor [SH.xx].

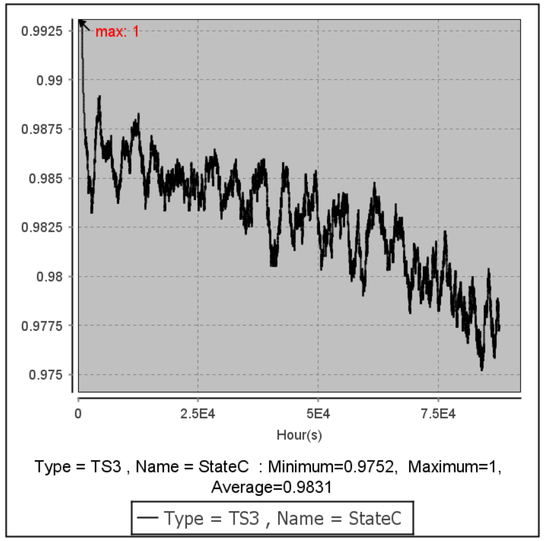
Detailed modelling:

Loss scenario: The **<u>liquid level</u>** in separator is above defined value, but the operator does not provide the valve open command. The causal factor is that the signal cable from the transmitter is disconnected. As a result, liquid may flow into the gas compressor [SH.xx].



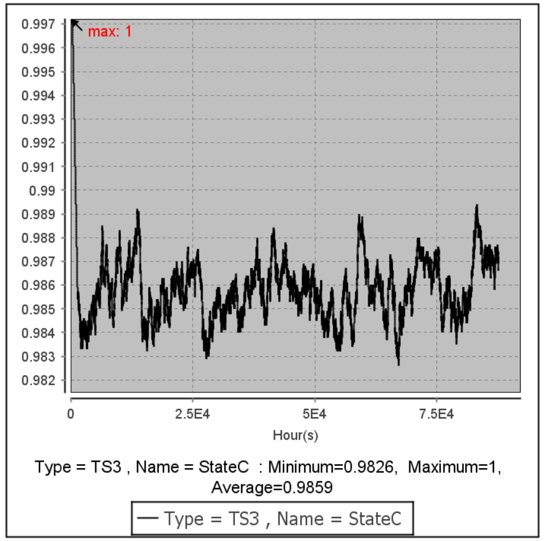
Open/close of Liquid Discharge Valve

Consider loss scenario



Type = TS3 , Name = StateC : Minimum=0.9752, Maximum=1, Average=0.9831

Without considering loss scenario



Type = TS3 , Name = StateC : Minimum=0.9826, Maximum=1, Average=0.9859

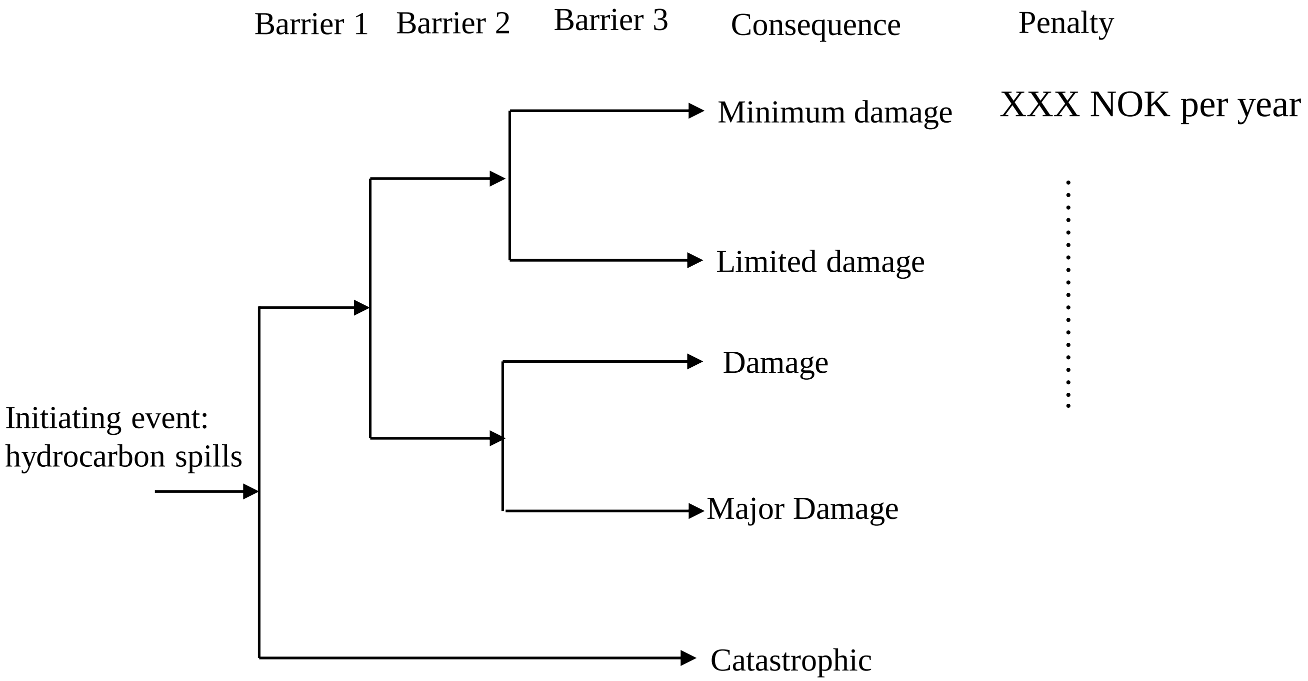
Risk-based decision context

How worse are L.1 and L.3?

If assume that SGB can produce 2 million Norwegian kroner (NOK) worth oil and gas per day, then the expected difference between case 0 and case 3 is 6.862 million NOK per year in stakeholder’s favor.

How worse are L.2?

Need further information about emergency barrier, e.g. Event tree analysis


Barrier 1
Barrier 2
Barrier 3
Consequence
Penalty
Minimum damage
XXX NOK per year
Limited damage
Damage
Initiating event:
hydrocarbon spills
Major Damage
Catastrophic