MARINE CYBERNETICS SERVICES

STPA Dynamic Positioning

Simulator-based testing of DP control system software

22 March 2016

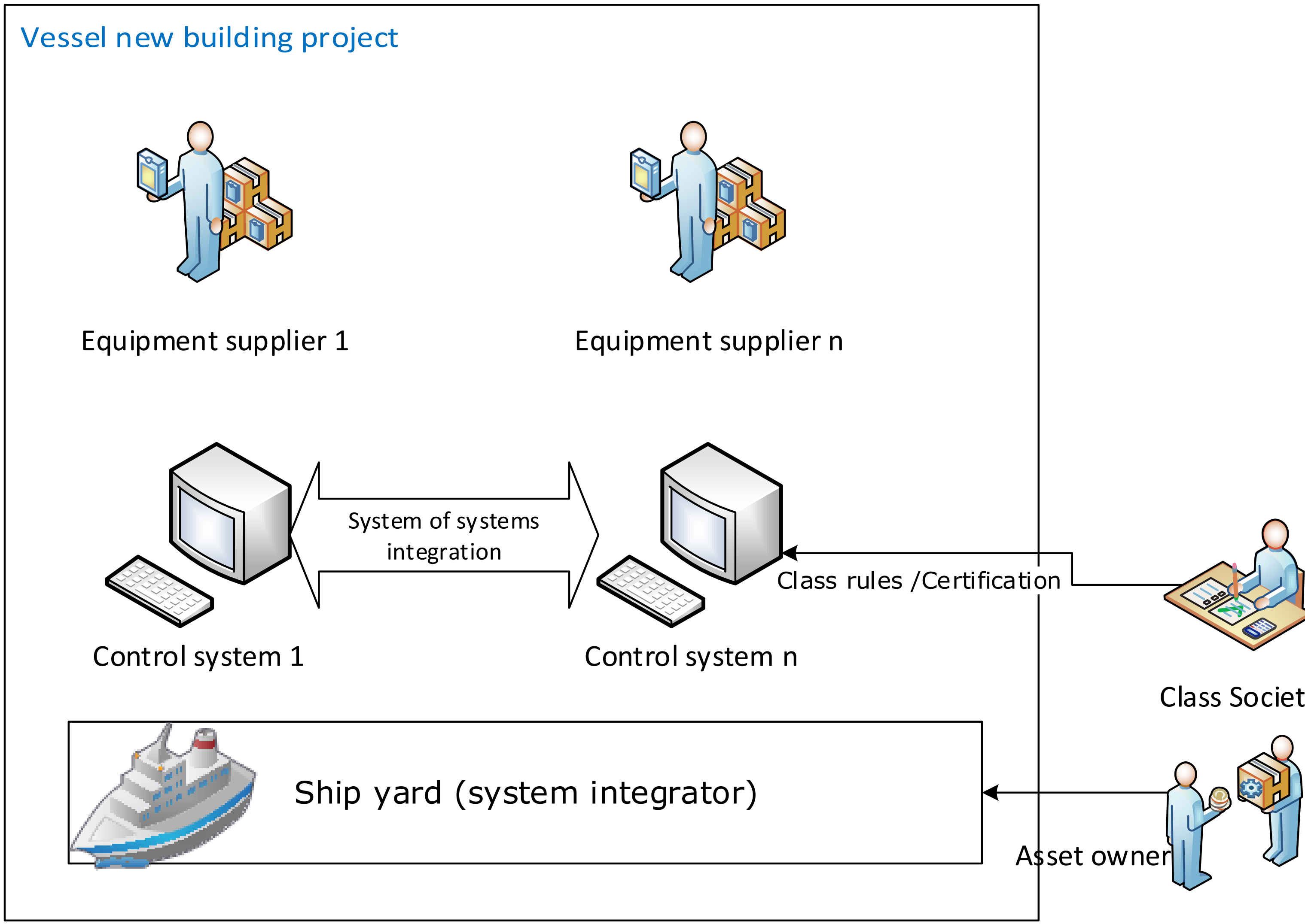
Ungraded

Content

- Introduction
  - Introduction to the maritime and offshore industry
  - Marine Cybernetics Services
  - Dynamic Positioning (DP)
  - Simulator-based testing
  - Project goal
- STPA DP
  - DP Control actions
  - UCAs, Scenarios, Causal factors
- DP control diagram
- Linking test cases to causal factors
- Further work
- Example

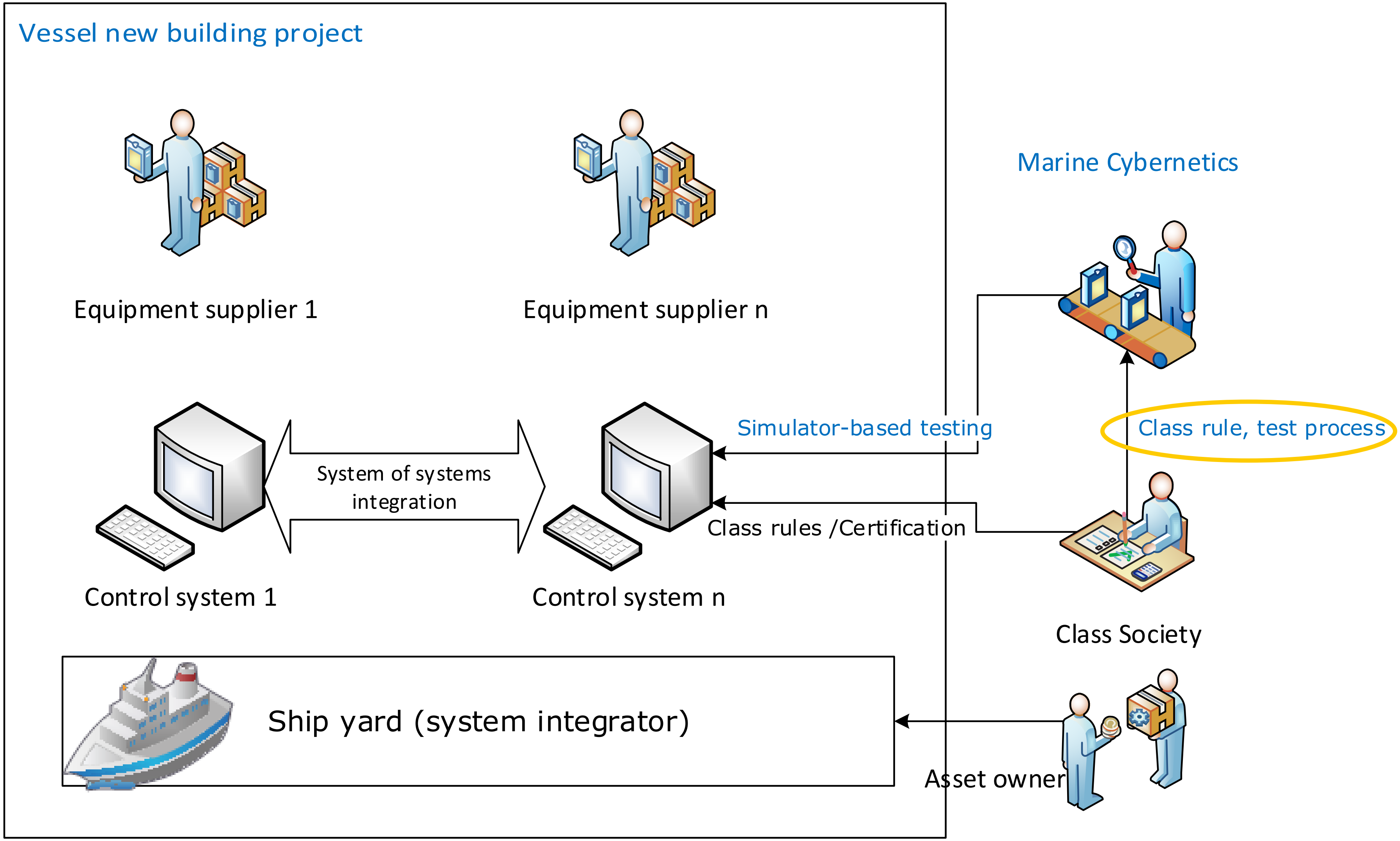
Ungraded

Introduction - maritime and offshore industry



Ungraded

Marine Cybernetics Services



Ungraded

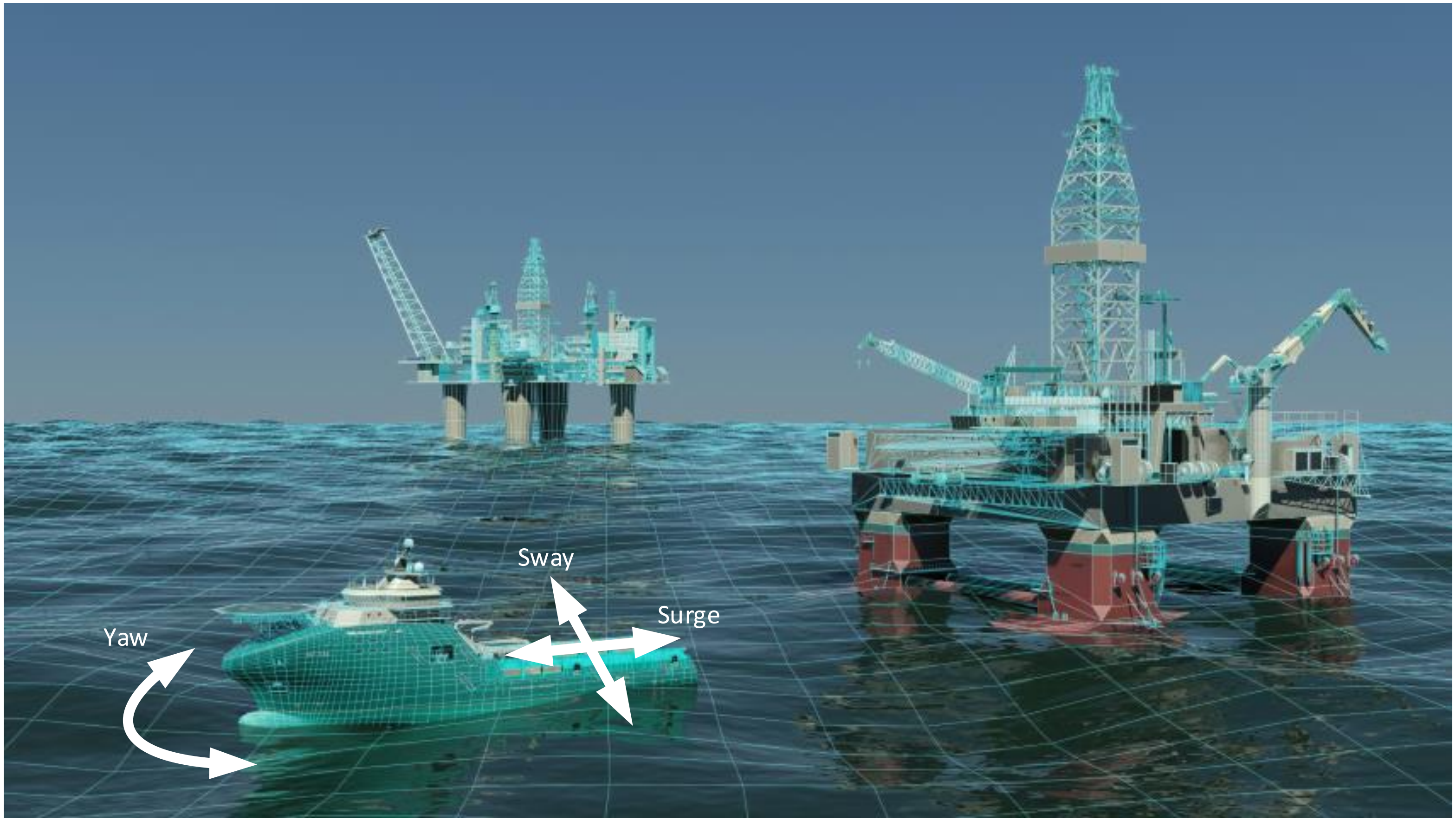
Class rule update

- ESV update, January 2016
  - Part 6 Chapter 5 Section 13, sub chapter 3.1.3, Table 5 HIL test program package:

Applicable system	*Description of documentation*
Control system	Upon request, a failure mode description describing relevant failures in sub-systems and theirs interfaces and how it will affect the target system(s). The following aspects shall as a minimum be covered: — identification of relevant failures and their potential cause(s) — description of the system expected response to each of the above failures — comments to the consequence of each of these failure — reference to the relevant HIL test case **Guidance note:** In addition to the target system it selves, this description should also identify and describe relevant failures in sub-systems and other relevant systems. As an example, reference system and sensors of the DP Control System, power systems and thruster systems will typical be part of the failure mode description for DP-HIL. ---e-n-d---of---g-u-i-d-a-n-c-e---n-o-t-e---

Ungraded

Dynamic Positioning



Ungraded

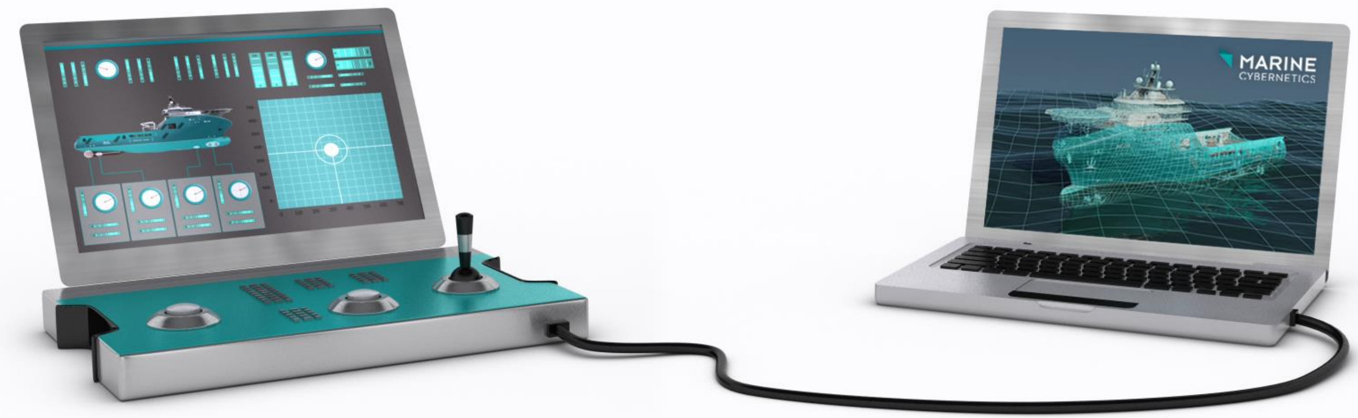
Simulator-based testing

Normal operation; DP controlling the vessel movement

Ungraded

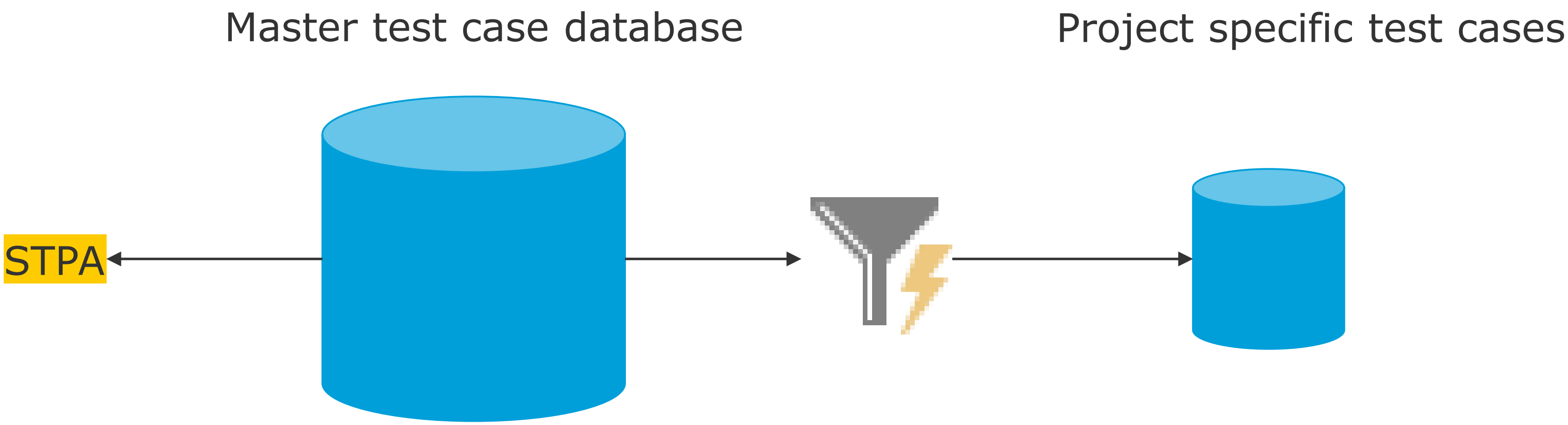
Simulator-based testing, cont.

Test setup; DP controlling the vessel model



Ungraded

Project objective



My job was to link our master test cases to the output of the STPA

Ungraded

DNV·GL

STPA DP

- Hazards
  - Loss of position or heading
  - A priori loss of position alarm not provided

- Control actions
  - Command thrusters
  - Provide alarm if loss of components causes loss of position or heading

- A few examples of system constraints (from DNVGL DP class rules):
  - 6.3.4: *Loss of one or multiple position reference system input and/or one or multiple sensor inputs shall not lead to significant change in thrust output*
  - 6.7.6 When several systems are combined to provide a mean reference, the mean value used shall not change abruptly by one system being selected or deselected.

Ungraded

DP unsafe control actions

Control action	Not providing causes hazard	Providing causes hazard	Wrong timing or order	Stopped too soon/Applied too long
Command thrusters	UCA1: DPC does not command thrusters	UCA2: DPC provides too much thrust command	UCA5: DPC commands thrusters too late	UCA6: DPC applies thruster command too long
		UCA3: DPC provides too little thrust command		UCA7: DPC stops thruster command too soon
		UCA4: DPC provides thruster command in wrong direction		
Provide alarm if loss of components causes loss of position	UCA8: DPC/OS does not provide the alarms	Not hazardous	UCA9: DPC/OS delays the alarm too long	UCA10: DPC/OS automatically de-activates the alarm

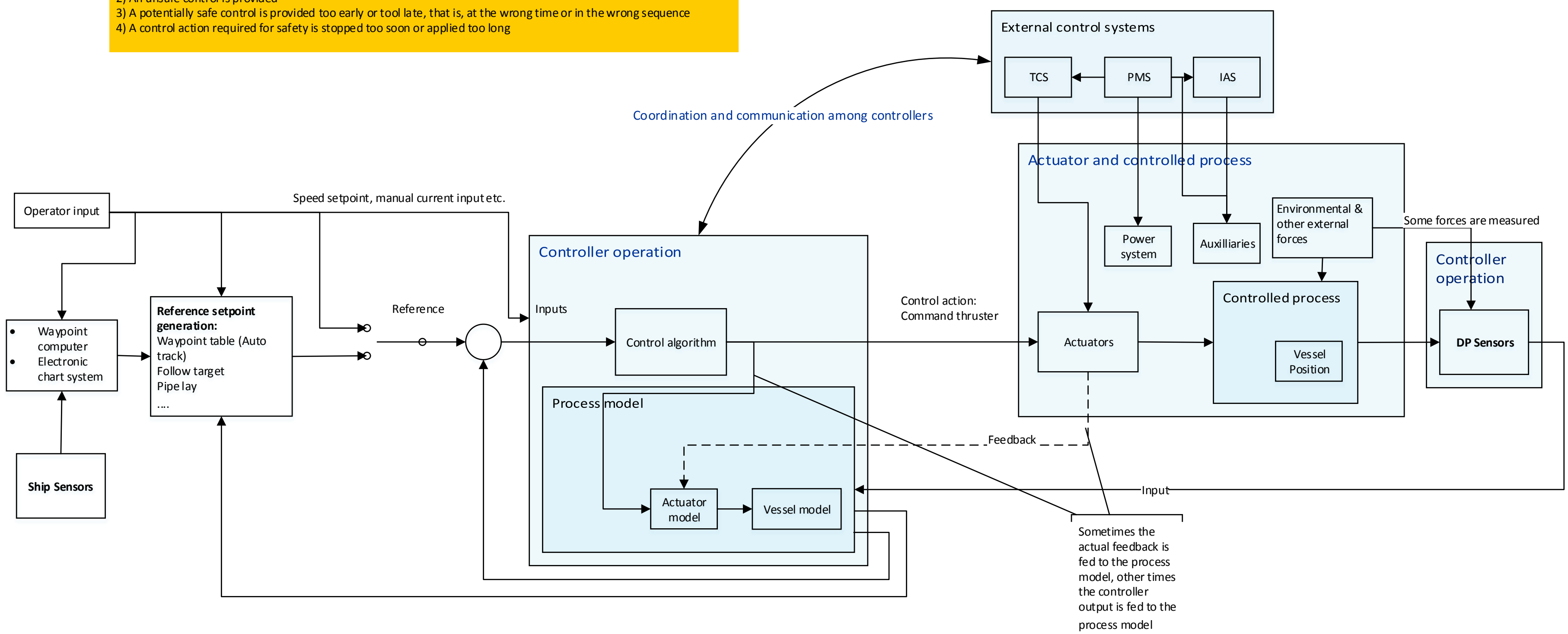
Ungraded

DP control diagram

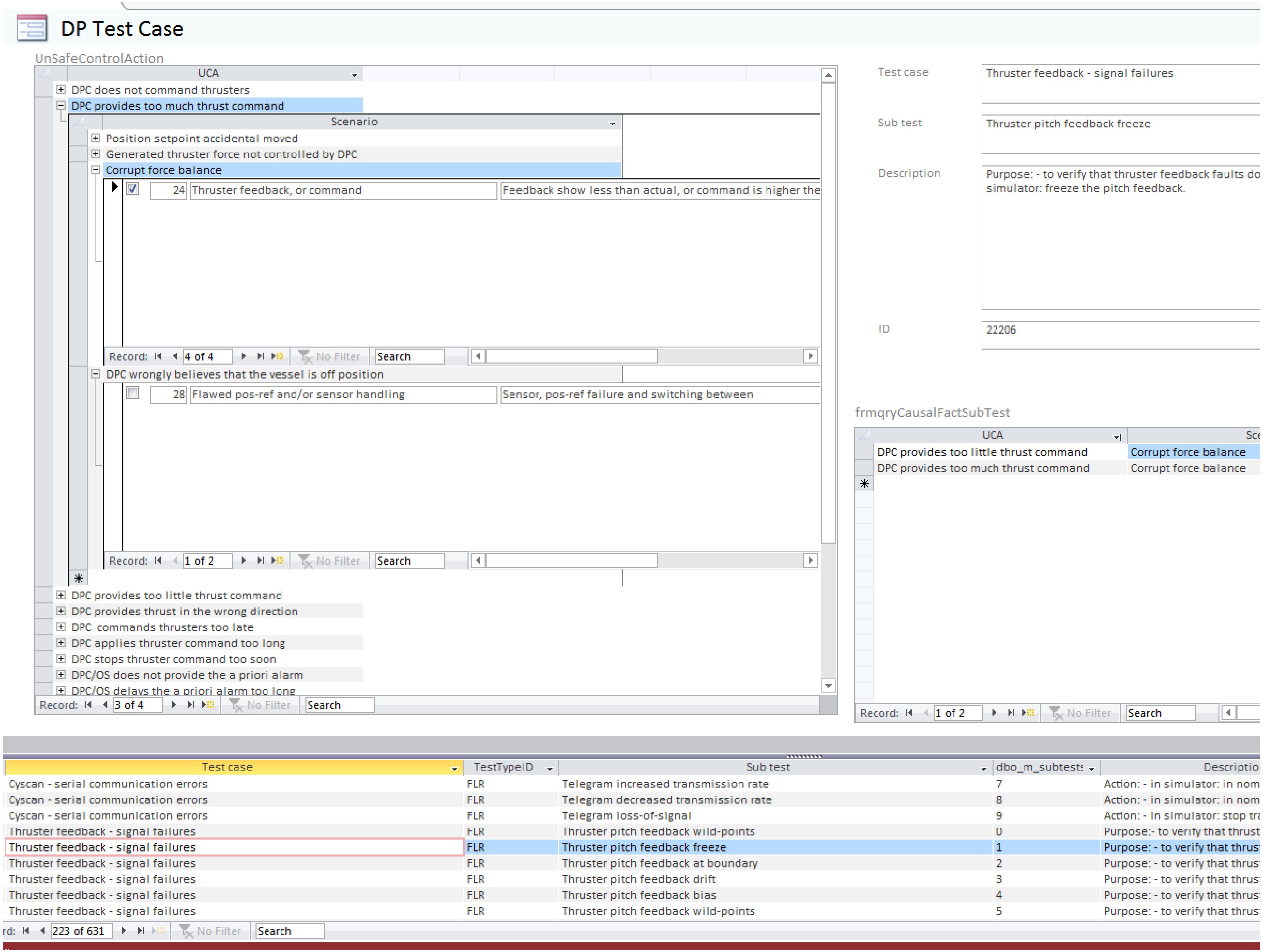
- Controller operation
  - Unsafe inputs
  - Unsafe control algorithm
  - Wrong (inconsistent, incomplete, incorrect) process model
  - Actuators and controlled process
- Coordination and communication among controllers

From the book:
1) A control action required for safety is not provided or is not followed
2) An unsafe control is provided
3) A potentially safe control is provided too early or tool late, that is, at the wrong time or in the wrong sequence
4) A control action required for safety is stopped too soon or applied too long

System-Theoretic Process Analysis (STPA) DP control structure



Ungraded


DP Test Case
UnSafeControlAction
UCA
DPC does not command thrusters
DPC provides too much thrust command
Scenario
Position setpoint accidental moved
Generated thruster force not controlled by DPC
Corrupt force balance
24 Thruster feedback, or command
Feedback show less than actual, or command is higher the
Record: 4 of 4
No Filter
Search
DPC wrongly believes that the vessel is off position
28 Flawed pos-ref and/or sensor handling
Sensor, pos-ref failure and switching between
Record: 1 of 2
No Filter
Search
DPC provides too little thrust command
DPC provides thrust in the wrong direction
DPC commands thrusters too late
DPC applies thruster command too long
DPC stops thruster command too soon
DPC/OS does not provide the a priori alarm
DPC/OS delays the a priori alarm too long
Record: 3 of 4
No Filter
Search
Test case
Thruster feedback - signal failures
Sub test
Thruster pitch feedback freeze
Description
Purpose: - to verify that thruster feedback faults do
simulator: freeze the pitch feedback.
ID
22206
frmqryCausalFactSubTest
UCA
DPC provides too little thrust command
Corrupt force balance
DPC provides too much thrust command
Corrupt force balance
Record: 1 of 2
No Filter
Search
Test case
TestTypeID
Sub test
dbo_m_subtest
Descriptio
Cyscan - serial communication errors
FLR
Telegram increased transmission rate
7
Action: - in simulator: in nom
Cyscan - serial communication errors
FLR
Telegram decreased transmission rate
8
Action: - in simulator: in nom
Cyscan - serial communication errors
FLR
Telegram loss-of-signal
9
Action: - in simulator: stop tra
Thruster feedback - signal failures
FLR
Thruster pitch feedback wild-points
0
Purpose:- to verify that thrust
Thruster feedback - signal failures
FLR
Thruster pitch feedback freeze
1
Purpose: - to verify that thrus
Thruster feedback - signal failures
FLR
Thruster pitch feedback at boundary
2
Purpose: - to verify that thrus
Thruster feedback - signal failures
FLR
Thruster pitch feedback drift
3
Purpose: - to verify that thrus
Thruster feedback - signal failures
FLR
Thruster pitch feedback bias
4
Purpose: - to verify that thrus
Thruster feedback - signal failures
FLR
Thruster pitch feedback wild-points
5
Purpose: - to verify that thrus
rd: 223 of 631
No Filter
Search

Identify scenarios and causal factors

- From previous table: “UCA2: DPC provides too much thrust command“
  - Scenarios:
    - Position setpoint accidental moved
    - Generated thruster force not controlled by DP Controller
    - Wrong force balance
    - DPC wrongly believes that the vessel is off position

- How, then, can the “Position setpoint be accidental moved”?
  - Synchronizing between DPC's or Operator Stations
  - Position setpoint generation (Follow target, Autotrack etc.)
  - Setpoint handling when changing between DP modes (and center of rotation)

Ungraded

Further work

Identify context for each
causal factor (Test Conditions)

- STPA
  - UCA
  - Scenarios
  - Causal factors

- Test case design
  - Test coverage (UCA?)

ISO/IEC/IEEE 29119-4

Software and system engineering

Software testing

Part 4: Test techniques

Ungraded

ISO/IEC/IEEE 29119-4 Software and system engineering Software testing, Part 4: Test techniques

- Black-box testing:
  - Equivalence Partitioning
  - Classification Tree
  - Boundary Value Analysis
  - Syntax Testing
  - Combinatorial Testing (e.g. pairwise testing)
  - Decision Table Testing
  - Cause-Effect Graphing
  - State Transition Testing
  - Scenario Testing
  - Random Testing

Ungraded

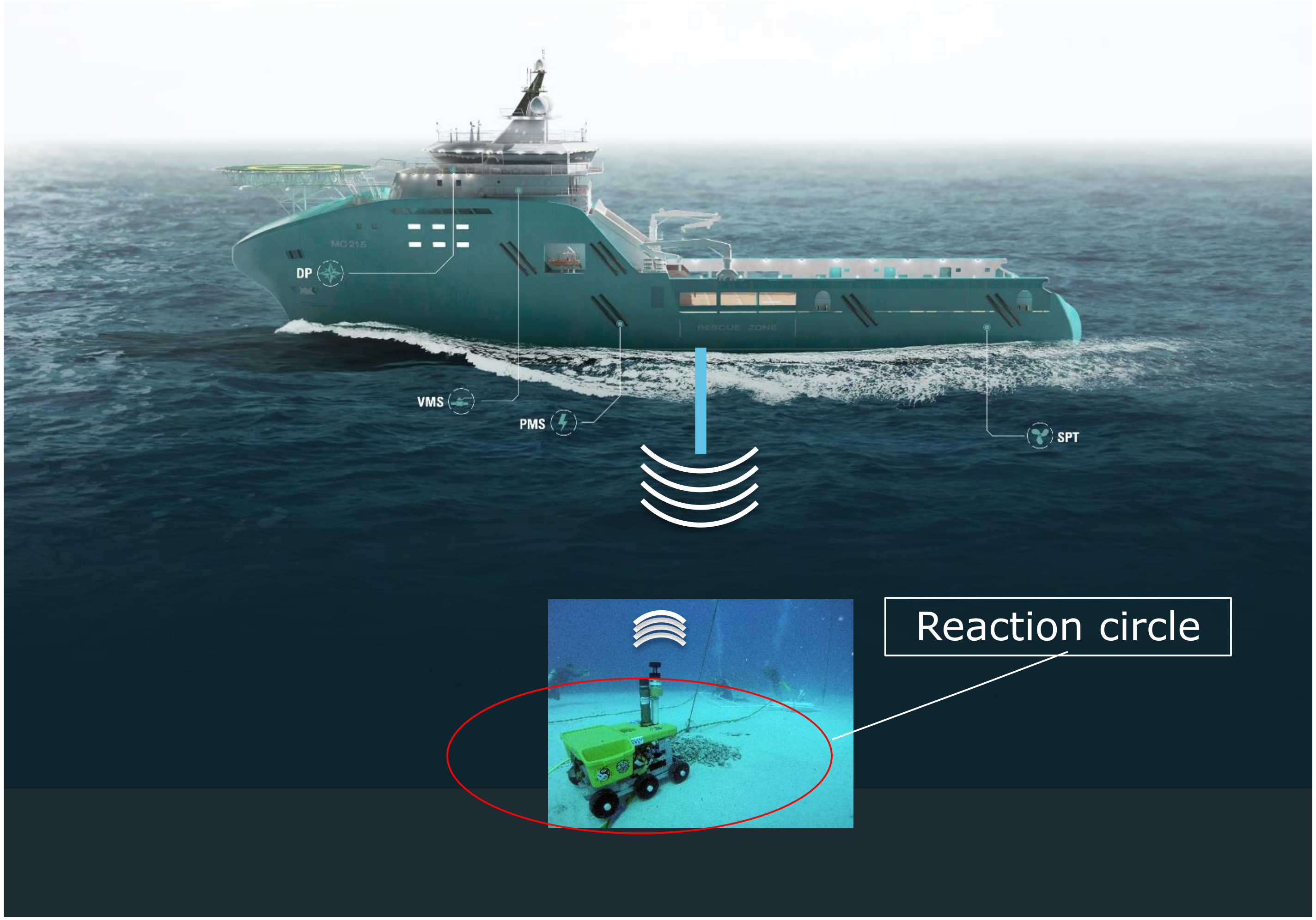
Identify scenarios and causal factors

- From previous table: “UCA2: DPC provides too much thrust command“
  - Scenarios:
    - **Position setpoint accidental moved**
    - Generated thruster force not controlled by DP Controller
    - Wrong force balance
    - DPC wrongly believes that the vessel is off position

- How, then, can the “Position setpoint be accidental moved”?
  - Synchronizing between DPC's or Operator Stations
  - **Position setpoint generation - Follow target**
  - Setpoint handling when changing between DP modes

Ungraded

Testing Position setpoint generation – "Follow target "



Ungraded

How to test?

- UCA: Position setpoint accidental moved
  - Position setpoint generation- Follow target

- What might influence, or challenge the algorithm with respect to functional correctness and (component) fault tolerance?

- Black box testing - Combinatorial Testing (According to ISO29119)
  - Three aspects are chosen as example:

1. Operational scenarios (functional correctness)
2. Change reaction circle radius (functional correctness)
3. Transponder fault mode tolerance

Ungraded

1. Operational scenarios – test conditions (context)

- Mobile transponder movement characteristics
  - Transponder stationary – suddenly moves outside reaction circle
  - Transponder stationary – suddenly moves outside reaction circle and returns to original position
  - Transponder constant speed
- Size of reaction circle
  - Small (must define what is "small")
  - Large
  - Zero
- Follow target speed setpoint
  - Slow
  - Fast
- Follow target heading setpoint change
  - Yes
  - No

Ungraded

2. Change reaction radius – test conditions (context)

- Starting size of reaction circle
  - Small (must be defined, possibly through operations characteristics)
  - Large (must be defined, ...)
  - Zero
- Change to reaction circle (size)
  - From Small to Large
  - From Large to Small
  - From any to Zero
  - From Zero to any

- Target ends up (after radius change)
  - From outside to inside (only for "From Zero to any)
  - Remains outside (only for "From Zero to any)
  - Remains inside circle
  - From inside to outside
- Rotation point
  - Centre of Gravity (CG)
  - Other (must be defined – e.g. moonpool?)

Ungraded

3. Transponder fault mode tolerance – test conditions (context)

- Mobile transponder fault mode (Position measurement)
  - Slow drift
  - Bias
  - Noise
- Reaction circle size
  - Normal (must be defined)
  - Zero
- Transponder position in reaction circle
  - Close to circle centre
  - Close to boundary

Ungraded

Conclusion

- It seems like a certain type of test cases that is more readily linked to the output from STPA identifies more defects
- Have not checked the distribution of the severity of the defects
- More investigation is needed to conclude, but **STPA as a hazard analysis method for test case design looks promising**

Ungraded

Thank you!

Odd Ivar Haugen
odd.ivar.haugen@dnvgl.com
+47 91715040

www.dnvgl.com

SAFER, SMARTER, GREENER

Ungraded

DNV·GL