STPA Dynamic Positioning
Simulator-based testing of DP control system software
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
Introduction - maritime and offshore industry

Vessel new building project

- Equipment supplier 1
- Equipment supplier n
- Control system 1
- Control system n
- System of systems integration
- Class rules /Certification
- Ship yard (system integrator)
- Class Society
- Asset owner
Class rule update

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

<table>
<thead>
<tr>
<th>Applicable system</th>
<th>Description of documentation</th>
</tr>
</thead>
</table>
| Control system    | Upon request, a failure mode description describing relevant failures in sub-systems and their 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 failures  
  - 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. |

---end---of---guide---ance---not---end---
Dynamic Positioning
Simulator-based testing

Normal operation; DP controlling the vessel movement
Simulator-based testing, cont.

Test setup; DP controlling the vessel model
Project objective

My job was to link our master test cases to the output of the STPA
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.
### DP unsafe control actions

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

**Controller operation**
- Unsafe inputs
- Unsafe control algorithm
- Wrong (inconsistent, incomplete, incorrect) process model
- Actuators and controlled process

**Coordination and communication among controllers**

**System-Theoretic Process Analysis (STPA) DP control structure**

**Operator input**
- Waypoint computer
- Electronic chart system

**Ship Sensors**
- Waypoint table (Auto track)
- Follow target
- Pipe lay

**Reference setpoint generation**
- Waypoint table (Auto track)
- Follow target
- Pipe lay

**Reference point**
- Speed setpoint, manual current input etc.

**Controller operation**
- Inputs
- Control algorithm

**Process model**
- Actuator model
- Vessel model

**Actuator and controlled process**
- Actuators
- Power system
- Auxiliaries
- Environmental & other external forces

**Controlled process**
- Vessel Position

**External control systems**
- TCS
- PMS
- IAS

**Controller operation**
- DP Sensors

Sometimes the actual feedback is fed to the process model, other times the controller output is fed to the process model.
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)
Further work

- 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
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
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
Testing Position setpoint generation – “Follow target”
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
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
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?)
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
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**.
Thank you!

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

www.dnvgl.com

SAFER, SMARTER, GREENER

Ungraded