Cyber-risk analysis of ship systems using STPA

Rishikesh Sahay, PhD
Daniel A. Sepulveda, PhD

25-28 March, 2019
Agenda

- CyberShip problem
- Project Description
- CyberShip Framework
- STPA Process Application
- Next Steps
Project Description
Shipping Operations in the economy
Shipping Operations in the economy
Maersk Line: Surviving from a cyber attack

In June 2017, A.P. Moller - Maersk fell victim to a major cyber-attack caused by the NotPetya malware, which also affected many organisations globally. As a result, Maersk’s operations in transport and logistics businesses were disrupted, leading to unwarranted impact.

The attack was reportedly created huge problems to the company, which transports about 15 per cent of global trade by container ships across the seas and its 76 port terminals around the world grounds. The organisation suffered financial losses up to USD300 million, in addition to the cost of restoration and extraordinary costs related to operations.

All began when an employee in Ukraine responded to a phishing email. The email tricked the system affected and therefore operations practically halted.

The attack successfully occurred regardless the measures that Maersk had implemented. In its 2016 Annual Report, the organization had clearly stated the following: “A.P. Moller - Maersk is involved in complex and wide-ranging global services and engaged in increased digitization of its businesses, making it highly dependent on well-functioning IT systems. The risk is managed through close monitoring and enhancements of cyber resilience.

Shipping company Maersk says June cyberattack could cost it up to $300 million

- Maersk has put in place “different and further protective measures” following the attack.
Cyber Attacks
“Propose a **framework** for improving the **resilience** in the shipping industry to **cyber risks**, with the ship being its main focus”
Basic Definitions

CyberShip Model
Ship Systems
Impact of Attack Traffic

Basic Definitions

Key performance Indicators
Key Performance Indicators


STPA application

Analysis of a Shipping system
Accidents
A1 Shipment late or non arriving
A2 Loss/Harm to life of passengers/crew
A3 Wrong or non delivery to customers
A4 Damage to the Ship
A5 Damage to the cargo
A6 Reputational loss

Hazard
H1 Uncontrolled manoeuvring of the ship
H2 Unidentified cargo items/wrong cargo data
H3 Incorrect functioning of ship components
H4 Uncontrolled transmission of data
H5 Uncontrolled data being transmitted
## Analysis Example

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Control Action</th>
<th>Performed with Hazard</th>
<th>Not Performed with Hazard</th>
<th>Performed too long too short with hazard</th>
<th>Performed too early too late with hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC</td>
<td>Ballast tank Pump</td>
<td>Start Pump</td>
<td>when EC has provided wrong parameter (Velocity, Level) to Pump.</td>
<td>when EC is compromised because of human in the loop</td>
<td>when the requirement was for a shorter period and the pump acted for too long</td>
<td>when there are communication channel congestion</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>when EC receives the wrong parameters (Velocity, Level) from IBC</td>
<td>when EC has been compromised because of component failure</td>
<td>when the requirement was for a longer period and the pump acted for too short</td>
<td>when there is a feedback delay between Actuator to Ballast tank</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>when Ballast tank Pump is not functioning</td>
<td>when EC has been compromised because of external hacker</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>When there is network failure and the control action is not received by Ballast tank</td>
<td>when EC did not receive command from IBC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### UCA

- **Integrated Bridge Controller (IBC)**
- **Engine Controller (EC)**
- **Ballast Tank Pump**
- **Ballast Tank level sensor**
- **Ballast Tank**
Analysis Results

• Scenarios identified in UCA Analysis
  • Component Failure
  • Mis-interaction
    • Network Failure
    • Network Congestion (resulting delay)
  • Controllers Compromised by hackers
  • Human Mistakes (Intentional or unintentional)
  • Incomplete or no feedback provided for decision making
Method Advantages
STPA Method Advantages

- Explicit representation of the shipping IT system
  - Mapping of functions
  - Review of design considerations

- Identification of design requirements
  - Infrastructure requirements
  - Design of communications

- Identification of crucial systems
  - Highest Hazards for UCA detected
  - Highest Accidents for UCAs detected

- Design of a resilience plan
  - Redundancy systems
  - Flexible response design
Research Next Steps

- Comparison of STPA results with
  - Attack fault tree analysis
  - Asset–based risk

- Extending analysis to the whole ship

- Identification of design requirements (CyberShip Project)

- Analysis of an extended shipping system (shore center and several ships)
Thanks for your attention

Rishikesh Sahay, PhD, risa@dtu.dk
Daniel Sepulveda, PhD, dasep@dtu.dk

CyberShip Core team
From Left to right:
- Rishikesh Sahay, PhD
- Prof. Christian D. Jensen
- Prof. Harilaos Psaraftis
- Prof. Michael B. Barfod
- Daniel Sepulveda, PhD.

Research Site