Advantages of IT connectivity versus the Cyber Security Challenge

Maritime Zukunftskonferenz am 8. und 9. September 2021

Svante Einarsson, Team Leader Cyber Security, DNV Maritime Advisory

9 September 2021
Advantages of IT/OT connectivity

Notice what has come true...

Hugo Gernsback (1884-1967) inventor, writer, editor, publisher, best known for publications including the first science fiction magazine.
The future holds more…

Monitoring of CO2 emissions

Condition Based Maintenance

Digital wearables for crew & passengers

Autonomous vessels
Growing complexity creates new challenges
The maritime industry have also experienced large attacks on their IT infrastructure and Control systems.
Downtime & incidents due to more complex systems are increasing - Software complexity is one of the main drivers!

Sources: www.autocar.co.uk, www.popularmechanics.com, www.theregister.co.uk
Warning to offshore industry on blocking of data communications in dynamic positioning systems

Introduction:

A serious incident occurred where a diving support vessel’s dynamic positioning (DP) system, designated as ACO, caused a loss of control in the reverse direction of its position while working in the field. Investigations have shown that a probable cause of the DP failure was a single fault that caused blocking of the DP system’s internal data communications.

Dynamically positioned (DP) vessels undertake a range of safety-critical activities such as diving support, oil and gas platform support, and support for scientific exploration. They are critical to the offshore industry and are heavily regulated to ensure safety and efficiency.
# Events from the past

<table>
<thead>
<tr>
<th>Unintentional</th>
<th>Intentional</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal</strong></td>
<td><strong>Intentional</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Crew member posts login credentials on navigation</td>
<td>Someone installs a GPS signal disturbance device on the bridge</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Software update causes loss of fuel control and ballast water valves</td>
<td>Ransomware spreads from IT computer to main switchboard</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Safety</td>
<td>Cyber Security</td>
</tr>
</tbody>
</table>
Key reasons why incidents happen

Cyber Security

1. The increasing connectivity and interdependency of systems making them a high value target

2. Crew awareness of cyber security is in its infancy

3. Slow growing interest in putting cyber security requirements into NB specifications

4. Lack of practical cyber security management systems tailored for onboard conditions

5. Organised crime are many times better informed of their victims than the victims themself
Key reasons why incidents happen

**Cyber Safety**

1. No use of effective, well-known system and software methods to ensure quality
2. Owner & operator does not put requirements to SW
3. Software and system configurations are not being systematically and consistently managed throughout the lifecycle
4. Obsolescence and upgrades are not being planned for and thus become surprises
5. Lack of transparency in development and delivery projects
DNV has followed up with support to the industry.
All stakeholders can benefit from more focus on software and hardware integration, quality and security

- **Owner & operator**
  Reduced risk of operational downtime and improved support during operation

- **Yard**
  Reduced risk of costly delays and unexpected warranty issues during initial operation

- **Supplier**
  Better products and enhanced service and support using digital technologies

- **Ship classification**
  Improved assurance and better management of risks in times of digital transformation
Thank you for your attention!

Svante Einarsson
Team Leader Cyber Security
DNV Maritime Advisory

Svante.Einarsson@dnv.com
+49 175 49 100 74

www.dnv.com