Cyber Enabled Systems

Introduction and Type Approval of Components within Cyber Enabled Systems

Lloyd's Register

Working together
for a safer world

What do we mean by Cyber Enabled Systems?

Ship-based cyber systems can include:

- Navigation systems, including electronic charts, global positioning systems (GPS), and dynamic positioning systems (DP)
- Radar and automatic identification systems (AIS)
- Communications systems
- Integrated bridge systems
- Control systems for the wide range of electro-mechanical systems on board ships, such as main engine, generators, converter drives, etc.

Reasons for Increased Interest in Cyber

- The ability to capture and analyse a wide range of data, including operational, service and monitoring.
- The provision of operational support and guidance
- A shortfall in crew competence
- The ability to easily update products based on software
- The ability to future proof ships

New Cyber-related Notations and certifications from LR

Four new Class descriptive Notations and certifications are being introduced to recognise the Autonomy Level achieved in the following areas of Cyber enablement.

- **Cyber-SAFE**
  Ship can be operated safely at defined Autonomy Level
- **Cyber-MAINTAIN Conditioned Based Maintenance**
  Cyber enabled CBM. Supported by an update to MCM/MCBM ShipRight
- **Cyber-SECURE**
  Cyber-security assured at a level beyond that required for safe operation at a defined Autonomy Level
- **Cyber-PERFORMANCE**
  Ship can safely achieve performance targets through cyber-enablement to a defined Autonomy Level.

Cyber Enabled Ships Documents

We are delivering consultancy and assurance services for the assignment of Autonomous Level (AL) Descriptive notes supported by the Lloyd’s Register Cyber Enabled Ships Autonomous Ships ShipRight procedure and Guidelines.

Supported by the new Type Approval of Cyber Enabled Systems Components procedure.

These documents have been written to the needs of industry by Lloyd’s Register subject matter experts, addressing the key elements of emerging cyber enabled systems.

Cyber-enabled ships

Deploying information and communications technology in shipping – Lloyd’s Register’s approach to assurance

First edition, February 2016

A Lloyd’s Register Guidance Note

Cyber-enabled ships

ShipRight procedure – autonomous ships

First edition, July 2016

A Lloyd’s Register guidance document

Cyber-enabled Ships

Type Approval of Cyber Enabled Systems Components

First Edition

A Lloyd’s Register Guidance Note

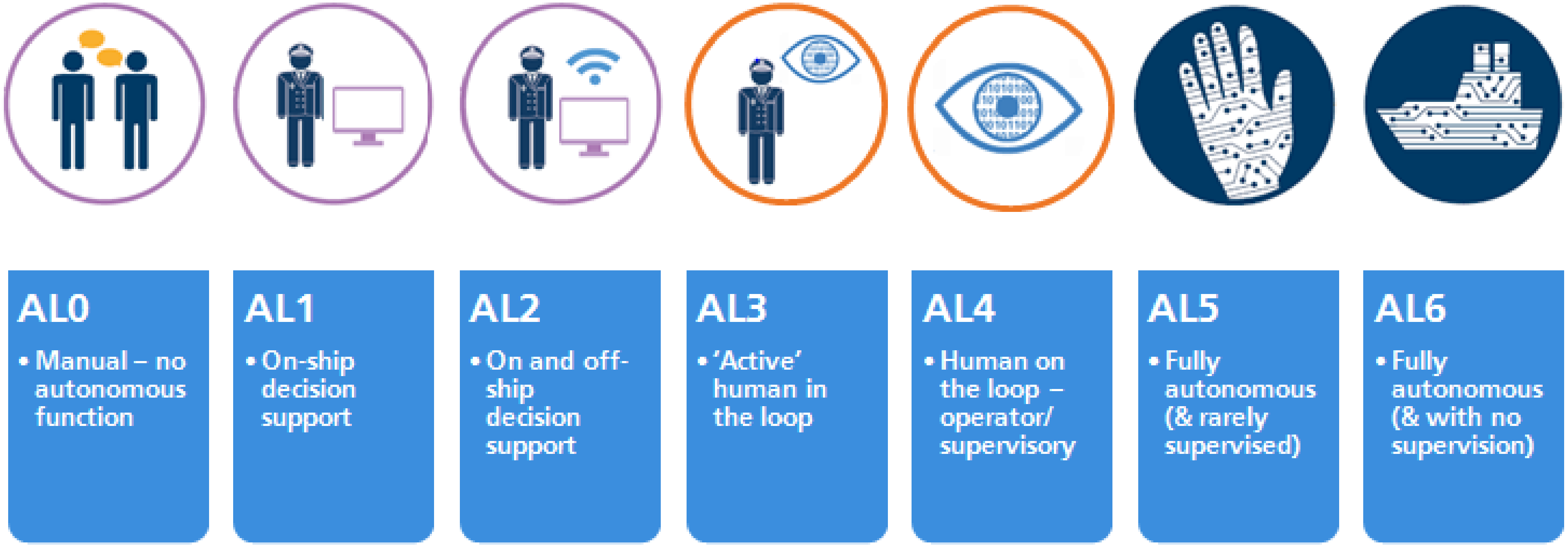
Type Approval of Components within Cyber Enabled Systems
The LR Approach

Lloyd’s Register has finalised the Type Approval of Cyber Enabled Components using the following high level approach:

System level	LR Assurance	Activities	LR Document
Ship	Cyber ship certification	Risk Assessment(HAZID) Design Appraisal Survey (On board test)	Cyber-enabled ships ShipRight Procedure
Ship systems	Cyber Systems Approval	Risk Assessment(HAZID) – Design Appraisal Survey	Cyber-enabled ships ShipRight Procedure
Components	Cyber System Component Type Approval	Design Appraisal Type Testing Production Assessment	LR Type Approval Procedure for components within cyber enabled ship’s systems + TA Test Spec 1

Cyber Enabled Ships: Autonomous Levels

Autonomous levels have been assigned, based on the degree of autonomy or remote access granted at the systems level:



AL0
- Manual – no autonomous function

AL1
- On-ship decision support

AL2
- On and off-ship decision support

AL3
- 'Active' human in the loop

AL4
- Human on the loop – operator/ supervisory

AL5
- Fully autonomous (& rarely supervised)

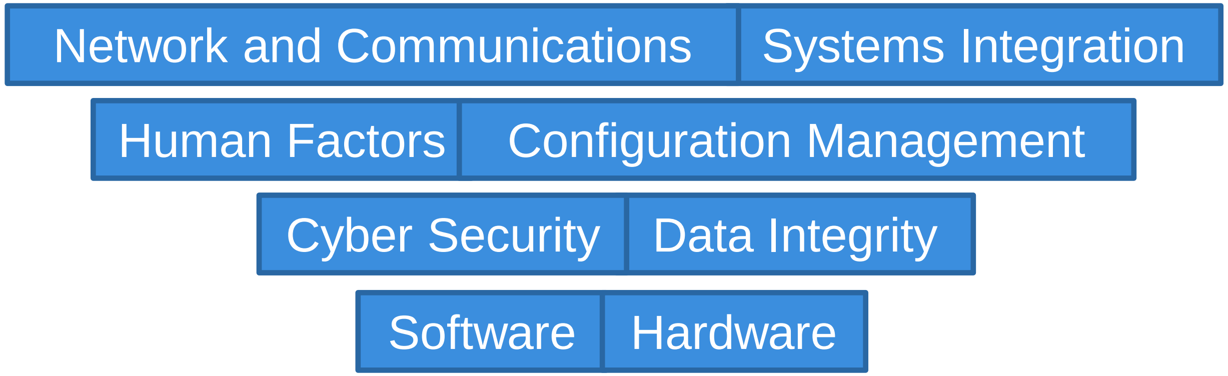
AL6
- Fully autonomous (& with no supervision)

Cyber Enabled Ships: Assurance

The boundaries of the ship change when considering the ‘off-ship’ support provided to an **autonomous** or **remotely operated** (drone) ship.

The main goal of marine classification societies in providing assurance of cyber enabled systems should be to ensure that new technologies or processes do not introduce key hazards during their implementation. Cyber technologies can be complex, multi-faceted systems and must be assessed in a robust, pragmatic and safety conscious way.

There are many factors to be included in this assessment, including:



Network and Communications

Systems Integration

Human Factors

Configuration Management

Cyber Security

Data Integrity

Software

Hardware

Example Case: Cyber Security Assurance

Lloyd’s Register uses the NIST framework core functions in the assessment of the cybersecurity resilience of systems and assets to potential cyber security events.

Identify	Protect	Detect	Respond	Recover
This is the foundation to demonstrating your organisations understanding of cyber security risks to your systems, assets, data and capabilities. --- You should understand the business context, resources critical to functions and the related cyber security risks.	This function supports the ability to limit or contain the impact of a potential cyber security event to ensure continued delivery of critical services. --- Examples of protect actions can be Access Control, Data Security, Protective Technology, Awareness and Training.	The purpose of the ‘Detect’ element is to ensure that your systems can discover/identify cyber security events in a timely manner. --- Examples of Detect actions can be Anomalies and Events, Security Continuous Monitoring and Detection Processes.	The ‘Respond’ function secures that your system has developed and deployed solutions to take action regarding a detected cyber security incident. --- Examples of this in action can be Response Planning, Communications, Analysis, Mitigation and Improvements.	Systems through the ‘Recover’ function to ensure resilience and an ability to restore any capabilities or services affected by a cyber security event. --- Examples of this can be Recovery Planning, Improvements and Communications

Example Case: Data Assurance

As part of the Cyber Enabled Ships ShipRight procedure in assigning Cyber-SAFE, to assure data, the following criteria must be addressed:

- Integrity; the trustworthiness of data
- availability
- authentication
- confidentiality
- authorisation
- non-repudiation
- data properties that preserve safety

Project: MAXCMAS

MAXCMAS: MAchine eXecutable Collision regulations for Marine Autonomous Systems

Aim: develop a Collision Avoidance System (CAM) for marine surface vessels capable of executing standard COLREGS avoidance manoeuvres.

CAM is meant for safe operation of autonomous vessels at sea.

LR's input is the safety assurance activity incl. software assurance.

(is about: Technical-, Confidence-, Compliance argument)

It resulted to LR's cyber levels definitions for autonomous ships and unmanned surface vessels.

Project with Multiple partners: **Rolls Royce, Atlas Electronic UK, Southampton Solent University's Warsash Maritime Academy, Queen's university Belfast**.

Cyber Security on Ships

What can go wrong? A small example we tested in reality

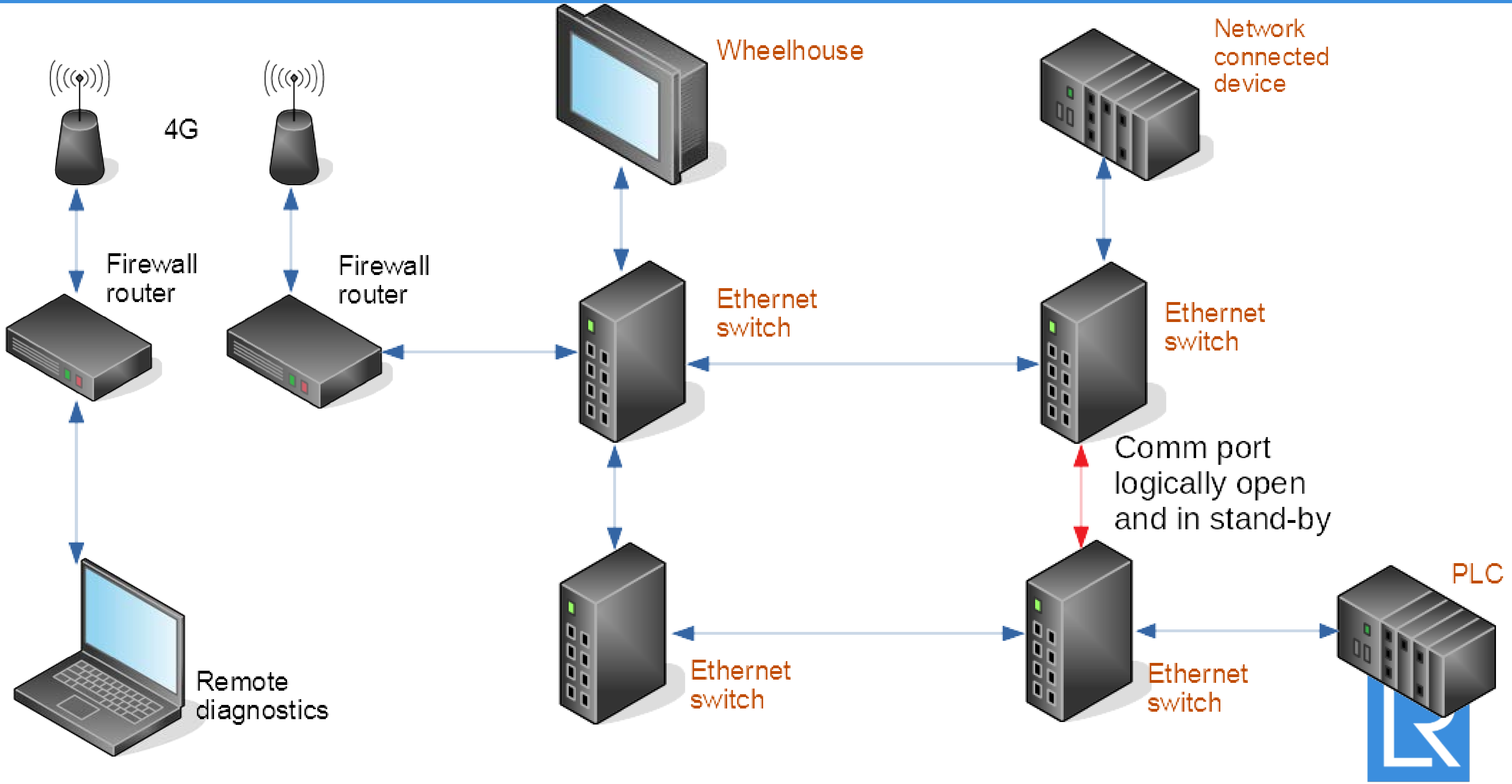
Lloyd's Register

Working together
for a safer world

Introduction

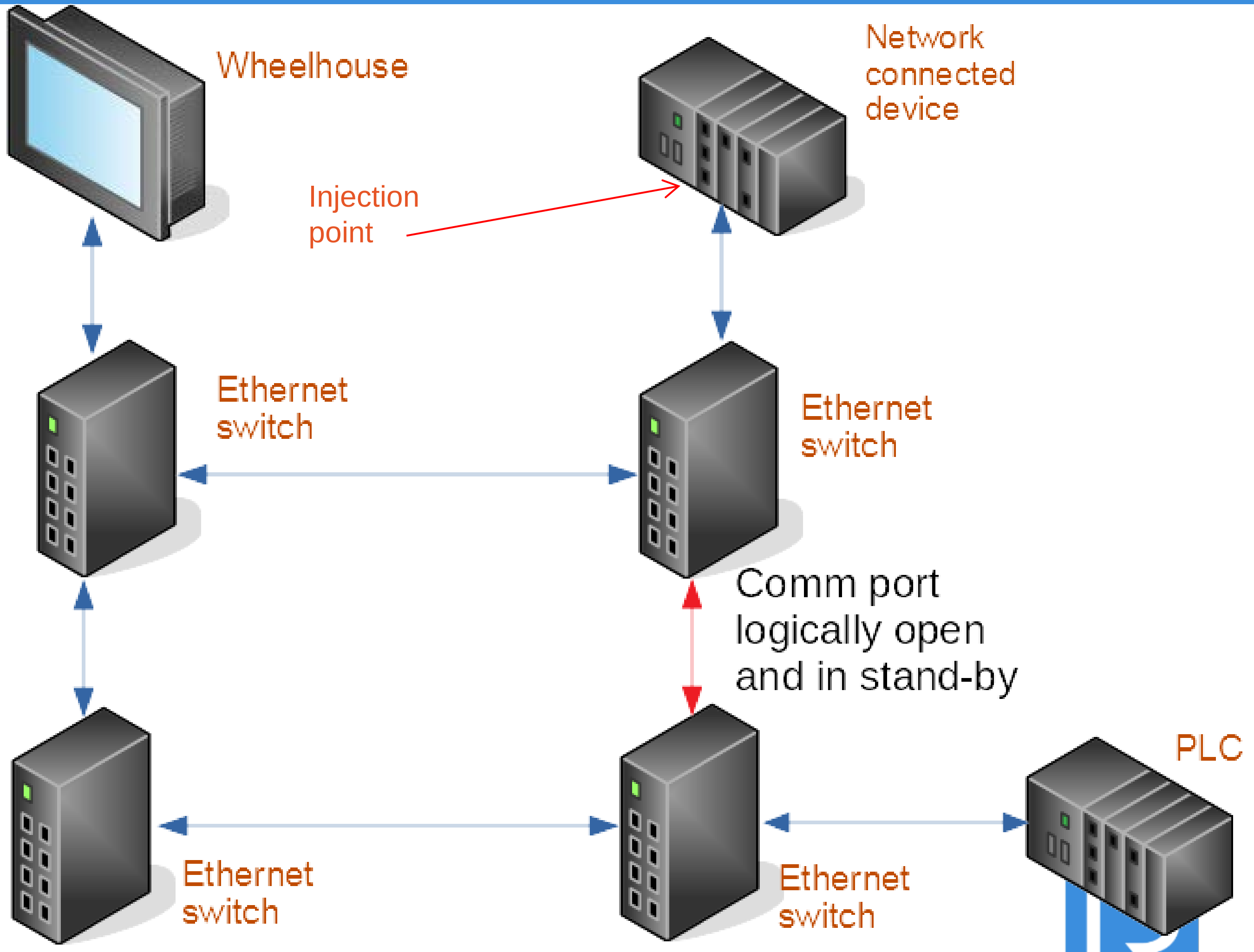
- As technology progresses fast, so do ships.
- More and more ships are getting “connected”, for various reasons, like remote monitoring of machinery systems, fault finding and shore based assistance. Some companies go even further, with ship’s routing calculated on shore and transferred on board for crew to use.
- Getting ships connected is and will represent a problem for cyber security.
- On board systems are more and more integrated and “connected”, and that presents an interest to cyber attackers.
- What we try to show you next, a very small scale of an successful attack consequences.

Setup, items marked red on the ship



Consequences – how bad can it go?

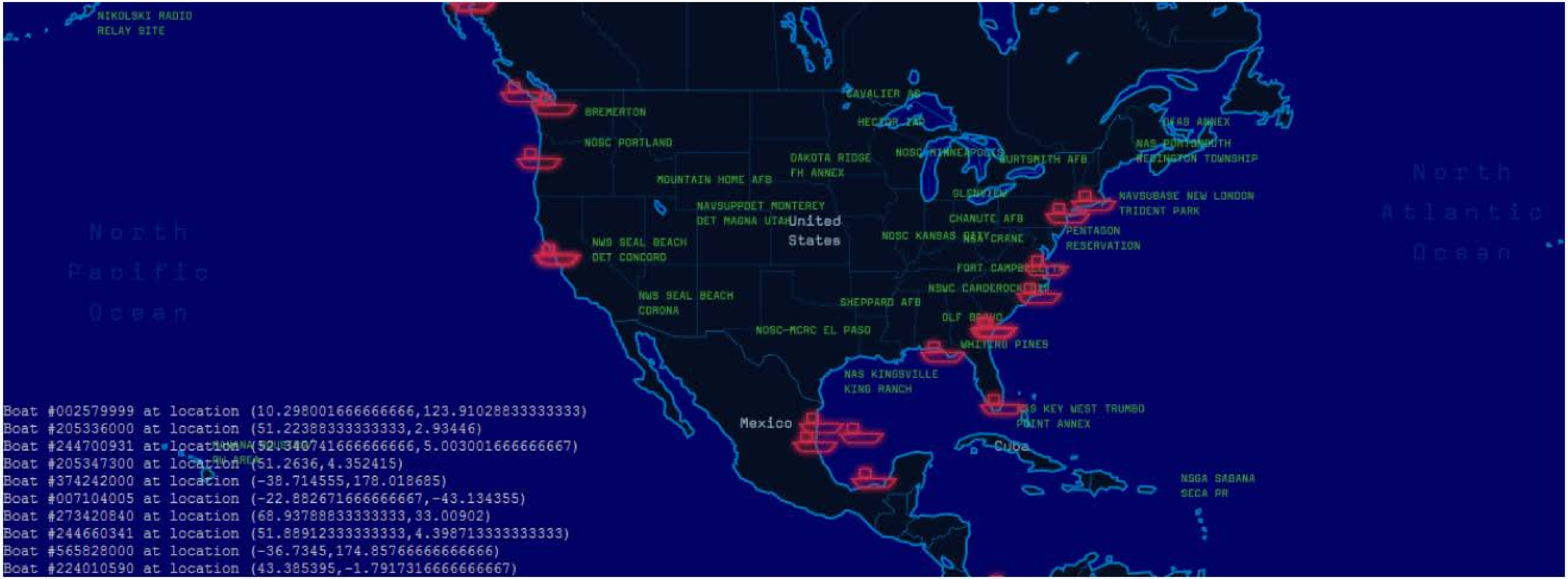
- A network storm is just one of the possible consequences, as there are multiple options for attackers to achieve their goals.
- Can attackers obtain control over propulsion and steering systems?
- Can attackers use this method to create a Denial of Service to ship's systems?
- We need to remember, it is not necessarily that such a problem is caused by external factors.



Are there any solutions?

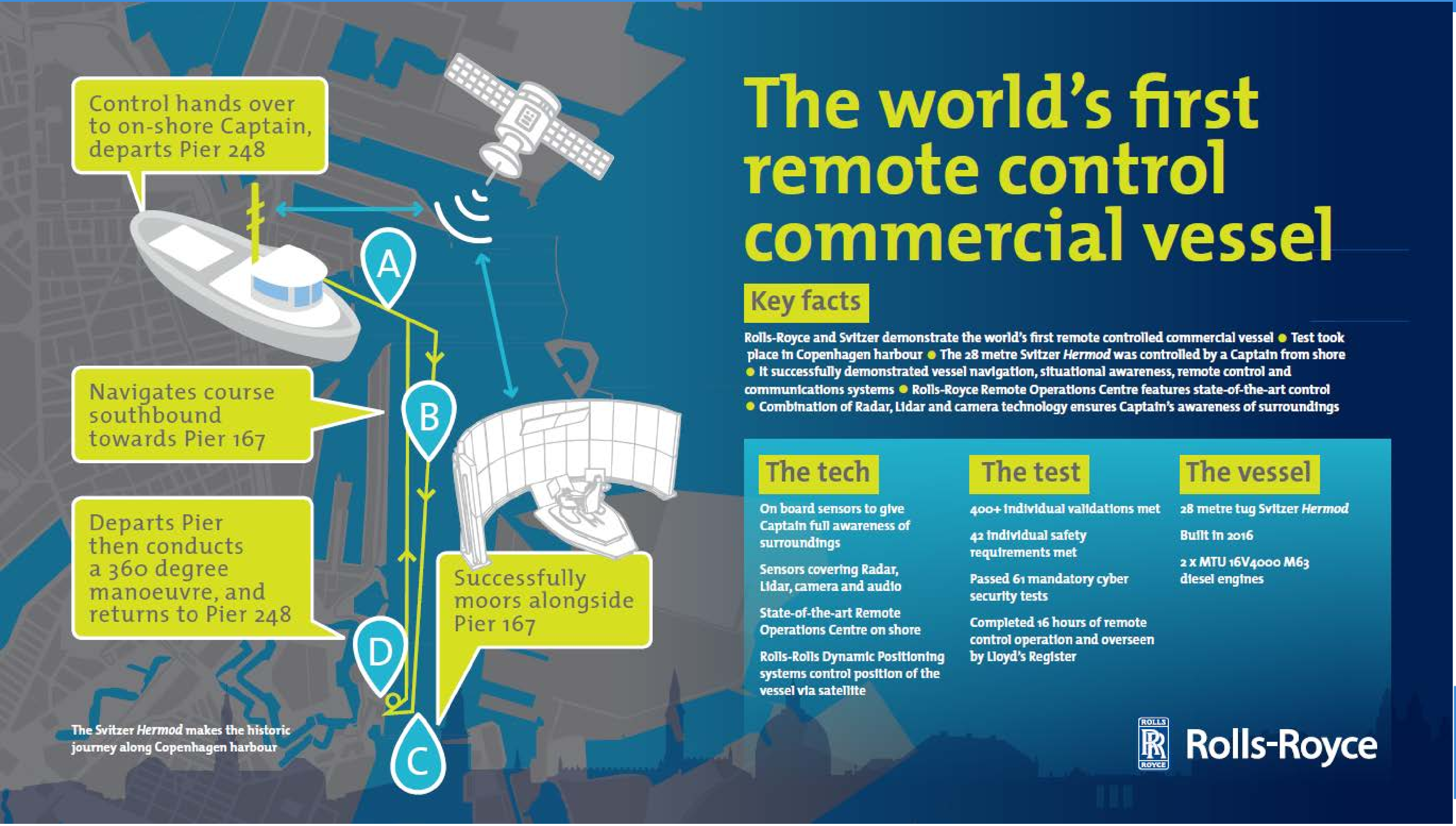
- For sure yes.
- It requires common effort and the focus not only being on the ship side of equipment but also on the office / remote site.
- We have to think of what can go wrong.
- How far do we allow integration and connectivity?
- How far we allow open usb and ethernet ports exposed to “innocent portable devices”?
- Are there options for the crew to take back control (e.g. kill switch and software restore)?
- Are remote offices well protected for “man-in-the-middle” attack?
- Are equipment settings (firewalls, network switches) properly configured and up to date anti-virus software used?
- *Learn from hackers as they learn too from you.*

Problem: due to big data AIS and VSAT data can be correlated



```
Boat #002579999 at location (10.298001666666666,123.91028833333333)
Boat #205336000 at location (51.223883333333333,2.93446)
Boat #244700931 at location (52.340741666666666,5.003001666666667)
Boat #205347300 at location (51.2636,4.352415)
Boat #374242000 at location (-38.714555,178.018685)
Boat #007104005 at location (-22.882671666666667,-43.134355)
Boat #273420840 at location (68.937888333333333,33.00902)
Boat #244660341 at location (51.889123333333333,4.398713333333333)
Boat #565828000 at location (-36.7345,174.85766666666666)
Boat #224010590 at location (43.385395,-1.791731666666667)
```

Project SISU: Rolls Royce/ Svitzer/Maersk/LR partnership and demonstration on SVITZER HERMOD



Control hands over to on-shore Captain, departs Pier 248

Navigates course southbound towards Pier 167

Departs Pier then conducts a 360 degree manoeuvre, and returns to Pier 248

Successfully moors alongside Pier 167

The Svitzer *Hermod* makes the historic journey along Copenhagen harbour

The world's first remote control commercial vessel

Key facts

Rolls-Royce and Svitzer demonstrate the world's first remote controlled commercial vessel ● Test took place in Copenhagen harbour ● The 28 metre Svitzer *Hermod* was controlled by a Captain from shore ● It successfully demonstrated vessel navigation, situational awareness, remote control and communications systems ● Rolls-Royce Remote Operations Centre features state-of-the-art control ● Combination of Radar, Lidar and camera technology ensures Captain's awareness of surroundings

The tech

On board sensors to give Captain full awareness of surroundings

Sensors covering Radar, Lidar, camera and audio

State-of-the-art Remote Operations Centre on shore

Rolls-Rolls Dynamic Positioning systems control position of the vessel via satellite

The test

400+ individual validations met

42 individual safety requirements met

Passed 61 mandatory cyber security tests

Completed 16 hours of remote control operation and overseen by Lloyd's Register

The vessel

28 metre tug Svitzer *Hermod*

Built in 2016

2 x MTU 16V4000 M63 diesel engines

Rolls-Royce

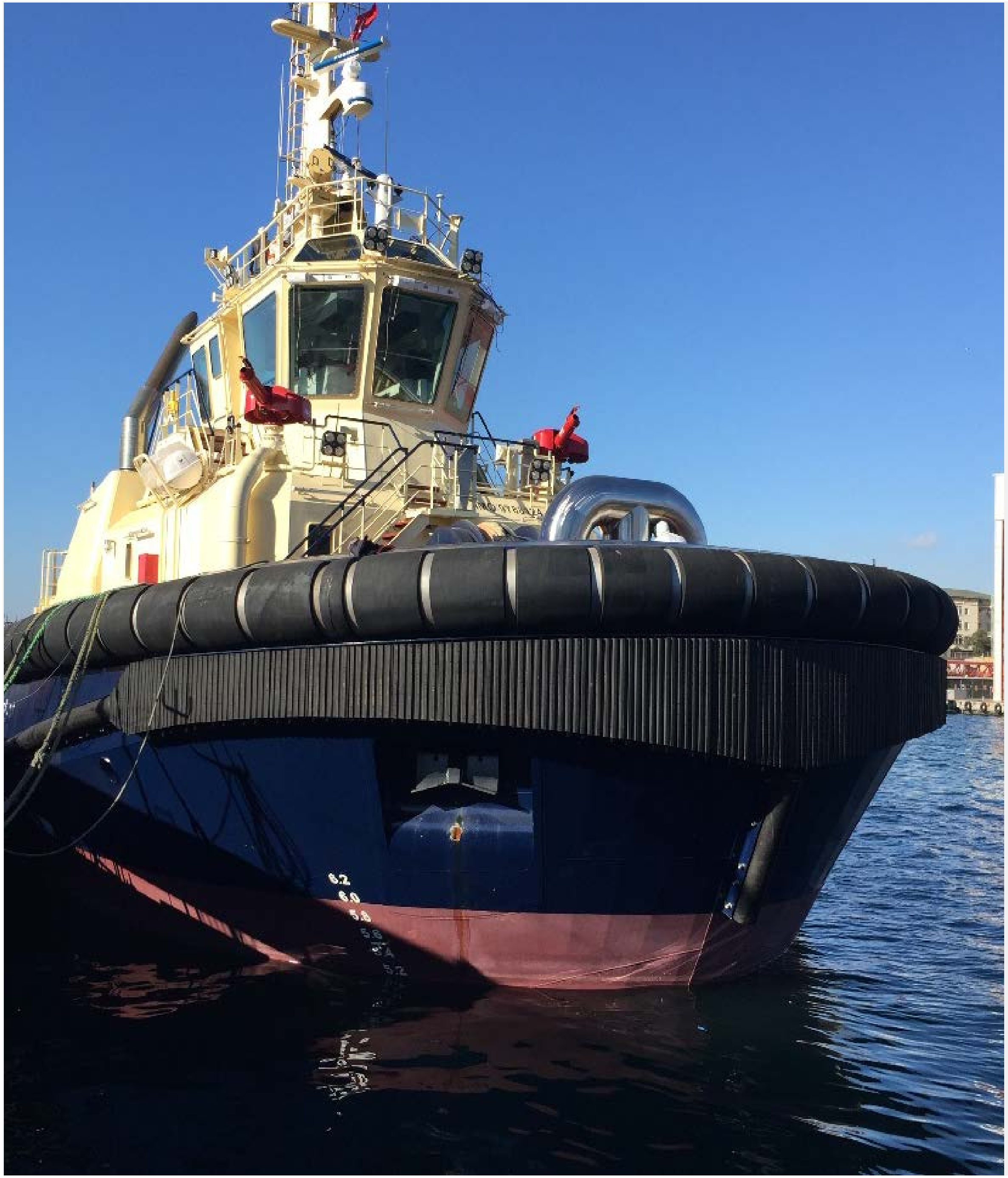
SISU / OPTIMUS

06 February 2017 and update

Lloyd's Register

Rolls-Royce

MAERSK



Lloyd’s Register perspective

- Classification
- Lloyd’s Register Procedures
- Lloyd’s Register Integrated Project Team
- Project SISU / OPTIMUS – Phase 2
- Conclusions

Classification

- There are currently no prescriptive Classification Society Rules or International Standards dealing with this innovative technology.

- Lloyd's Register Regulations - GOALS:-
  1. the structural strength of (and where necessary the watertight integrity of) all essential parts of the hull and its appendages;
  2. **<u>the safety and reliability of the propulsion and steering systems</u>**; and
  3. the effectiveness of those other features and auxiliary systems which have been built into the ship in order to establish and maintain basic conditions on board whereby appropriate cargoes and personnel can be safely carried whilst the ship is at sea, at anchor, or moored in harbour.

- Safety and security had to be assured by alternative means to demonstrate due diligence.

Lloyd’s Register Procedures

- Use of Lloyd’s Register’s ShipRight procedure for the 'Cyber Enabled Ship' ensured that LR’s Regulations and Statutory requirements were not compromised, as the boundaries of the system extend beyond the vessel.

- Risk based approach using, HAZID, FMECA were undertaken for:
  - Vessel Propulsion and Dynamic Positioning System
  - Connectivity & Cyber Security
  - Situation Awareness
  - ROC (Remote Operating Centre)

- Human Element and shipboard operational requirements were considered in the context of the operator’s safety management system and shipboard procedures.

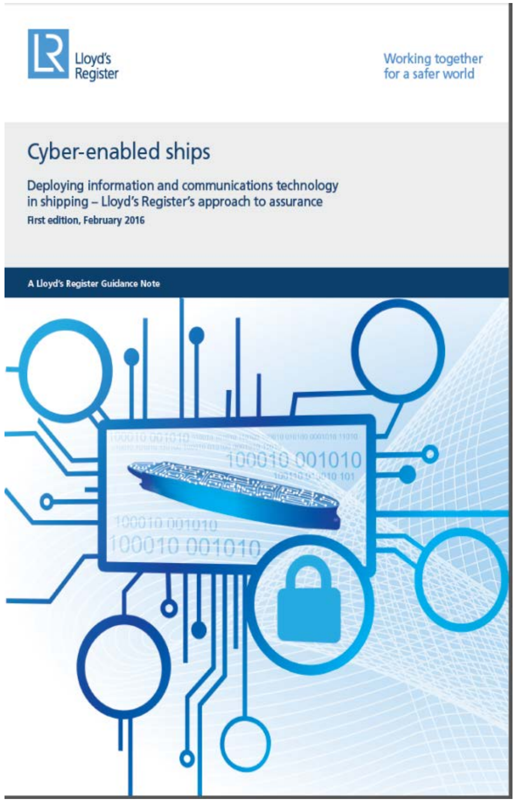
- Validation and Verification trials were undertaken during extensive harbour and sea trials.

Lloyd’s Register Integrated Project Team

- Lloyd’s Register established a project team fully integrated with the designer and operator, consisting of experts in the fields of:-
    - Project management
    - Systems engineering
    - Software Assurance
    - Human element
    - Electrotechnical and Mechanical Engineers with previous sea going operational experience including ISM and ISPS Codes

Project SISU / OPTIMUS – Phase 2

- LR has confidence that Phase 2 of the project will be successful, whilst commitment of stakeholders to the following approach is ensured:
    - All stakeholders agree on vessel capabilities to match business needs
    - Risks are rigorously identified by all relevant stakeholders
    - Risks are mitigated by:
        - Design considering systems engineering (holistic approach)
        - Human element considerations being addressed
        - Completion of Software Verification & Validation
        - Security and Data Assurance being considered as paramount
        - Collaborative working arrangement



Lloyd's Register

Working together for a safer world

Cyber-enabled ships

Deploying information and communications technology in shipping – Lloyd's Register's approach to assurance

First edition, February 2016

A Lloyd's Register Guidance Note

Conclusions

- Lack of prescriptive Rules was no barrier for “de-risking” the project.

- Partnership & collaboration with Maersk/Svitzer/Rolls Royce & Lloyd’s Register project teams was paramount to the success of the project.

- Successfully demonstrated that the remote operation of the vessel did not introduce any key hazards and it was proven to be safe and secure within the project boundaries.

- Procedure followed will result in Lloyd’s Register Rule amendments and support to Flag States and subsequently IMO as required

Thank You

You can find more information on our Cyber products and services here, at:

www.lr.org/cyber

Cyber-enabled Ships

Type Approval of Cyber Enabled Systems Components

First Edition

A Lloyd's Register Guidance Note

Luis Benito
Innovation and Strategic Marketing
Marine & Offshore

Lloyd's Register Group Limited
Global Technology Centre, Southampton Boldrewood Innovation Campus, Burgess Road,
Southampton SO16 7QF, UK

Lloyd's Register
Marine

Working together
for a safer world