

The Fairway of the Future: Important Technical Learnings

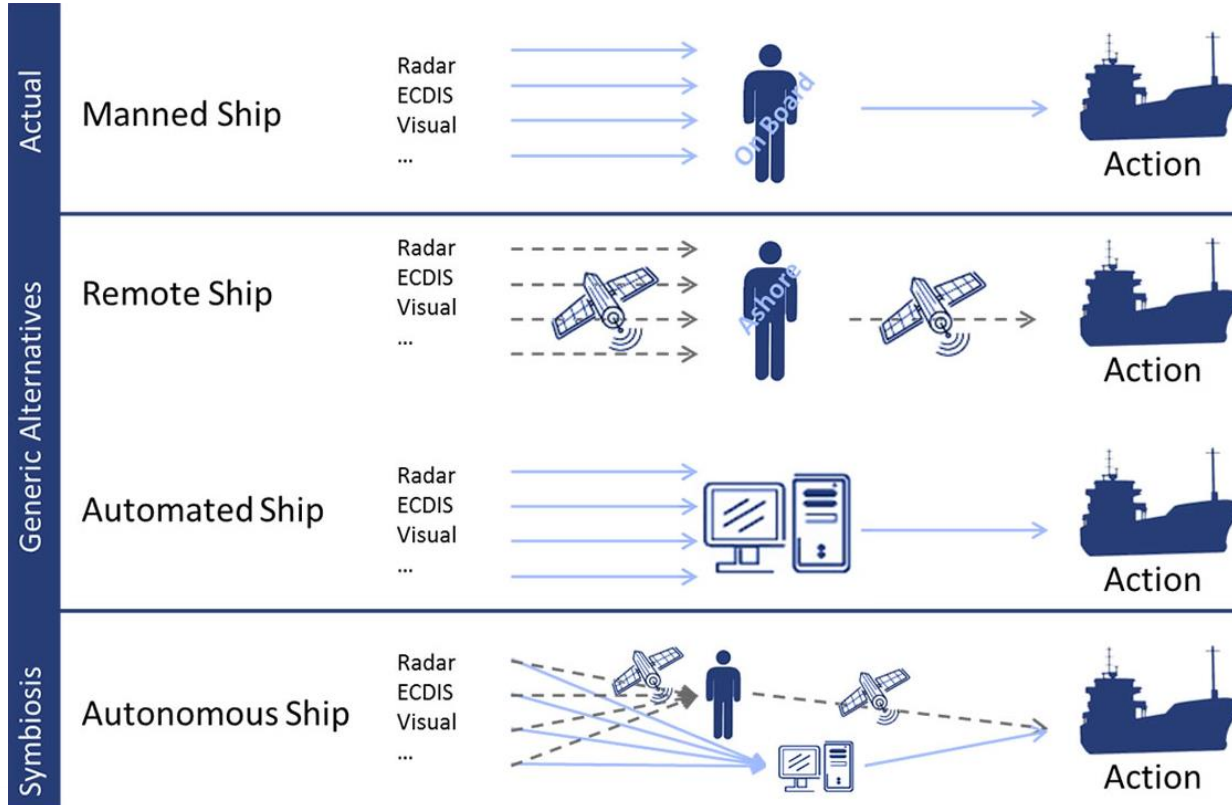
Bill Silverajan

Unit of Computing Sciences
Tampere University, Finland

Background: Maritime Industry

- One of the oldest industries known to mankind, and is heavily regulated by maritime rules
- Remains a vital part of the global economy, responsible for over 90% of trade around the world trade
- There are heavy investments in digital transformation, for the introduction of smart ships and smart ports, which will impact the technology in fairways and waterways
- Digital transformation significantly based on advanced terrestrial connectivity, Industrial IoT developments, Data Management, Image Processing, Mapping, Artificial Intelligence and Machine Learning

Preparing For Increasingly Smart Ships



Smart Port Developments Around The World



DIGITISATION PRESS RELEASE 31 January 2018

Port of Rotterdam teams with IBM Internet of Things to digitize operations

Full steam ahead for new Tuas mega port

FUTURE PORT

The Tuas mega port, slated to open in phases from 2021 will incorporate smart and green technologies into its operations. Some of these will be tested at the MPA Living Lab. The Straits Times looks at the journey of a container through the port of the future.

Drones

- Drones can be used to fulfill the shore-ship deliveries.
- They can also be sent in to inspect vessels for damage, among other checks.

Automated technology

- Quay cranes, yard cranes and guided vehicles will be automated.
- Automated loading/unloading operations.
- Computers, sensors and cameras ensure the safe and precise handling of containers.
- 50% of wharf operation supervisors and up to 80% of yard crane operators and prime mover drivers will be retrained for higher-skilled roles.

Green technology

- The cranes and automated guided vehicles will be fully electric.
- Solar energy will be harvested and waste heat recovered from building cooling systems.

Floating platforms

- Currently, if a berth is not available, the vessel waits at anchorage in the sea.
- The Maritime and Port Authority of Singapore (MPA) is now exploring the use of multi-purpose floating platforms so that while waiting, immigration checks, re-fuelling and top-up of supplies can be done. More ships moored to the platforms will free up space at sea.

Teaching arriving vessels

- Today, a captain of a vessel entering the Singapore port has to alert MPA of its arrival at least 24 hours ahead by e-mail, fax or faxes (not standardised and optional).
- In future, the information will be conveyed digitally.
- A new Vessel Traffic Management System will use cloud computing, data analytics, smart algorithms, sensors and advanced communication systems to manage and track the vessels, whose communication will be minimal.

Single sharing portal

- Currently, the captain has to submit documents to MPA, Immigration and Checkpoints Authority and National Environment Agency separately to seek for vessel clearance, CA for crew/passenger clearance and MSA for health clearance.
- In future, this will be done through a single government portal.

Just-in-Time Arrival System

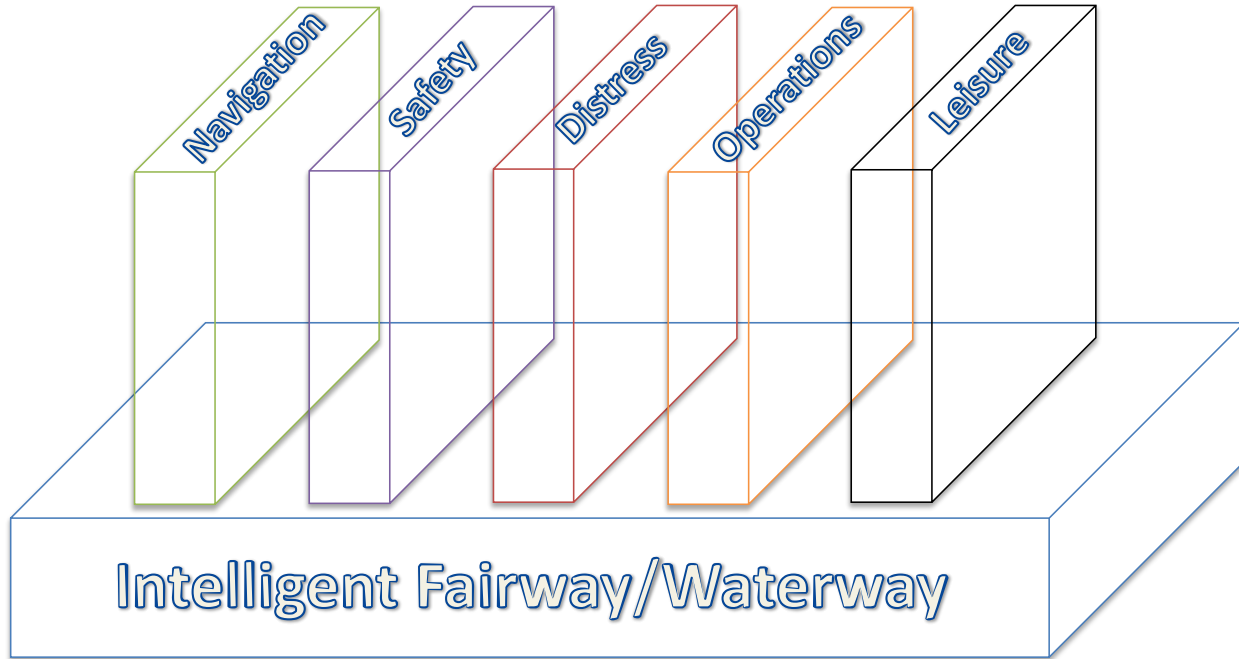
- When the vessel enters the Singapore Strait, the captain now reports vessels by HF radio to MPA and radicon PSA Marine to arrange for a marine pilot who will guide the vessel through Singapore waters.
- In future, the Just-in-Time Arrival system will take over the coordination. This will cut delays and waiting times of calling vessels and optimise port resources and resource deployment.

Intelligent Fairway Infrastructure (or Platform)

- Sensors
 - Bathymetric, acoustic, positioning, movement, environmental
- Processing
 - Visual Analytics, Sensor Fusion, Trajectory Detection and Forecasting
- Communication and Cloud
 - Base stations, Transponders, Gateways, Access Points, VHF
- Auxilliary Systems
 - Vessel Tracking Services, AIS



Intelligent Fairway Infrastructure and Services



Testbed Requirements for Intelligent Fairways

- Testbeds serve as a fundamental technical block to understand what the infrastructure and service needs can be
- Form a stepping stone to providing a digital twin
- Emulate, develop and deploy shore-based maritime services, such as clouds and data servers
- Technically delineate how and where the “edge” lies. Is it the fairway, is it the vessel
- Provide edge infrastructure for testing digital communication, traffic shaping and integrating various network topologies
- Deliver connectivity for sensors and equipment
- Understand, model and visualize security risks and threats

Testbeds As A Stepping Stone Towards Digital Twins

- Many ports, ships and fleet-based operations system depend heavily on legacy systems
- Compared with other industrial sectors, cybersecurity awareness is low in the maritime industry
- 87% of survey respondents from the shipping industry believed cyber attacks would increase over the next five years - a level that was higher than counterparts in the aviation, rail and logistics industries.

Connectivity Considerations

- When fairways are close to the shore, current cellular coverage with LTE, in Finland is excellent
- Nevertheless, different radio technologies are still needed in order to meet connectivity needs
- Fairway sensors and equipment further away from the coast or in blindspots need connectivity as well and not all sensors support cellular connectivity
- Incoming vessels may be equipped with other technologies such as VHF and Satellite for ship to shore communication

Communication Considerations

- The first attempt towards the digitalization of maritime transportation was Automatic Identification System (AIS)
- Main driver for AIS was safety, and the main goal was broadcast communication
 - But new services have arisen, with support for Application Specific Messages
- To prevent overloading AIS, ITU is standardizing a new radio interface of VHF Data Exchange System which can be a hybrid of terrestrial and satellite communication
- This is in addition to using only terrestrial and satellite communication

Communication Considerations

- There exists a general consensus that IP-based communication would emerge as the dominant technology
- However what communication protocols are used on top of IP can become very confusing, especially for sensor traffic
 - The solutions are use-case and business specific currently
- Communication paradigms also differ based on needs
 - Publish/Subscribe, REST and RPC are the available options
- Commonly used protocols are based on TLS, DTLS, MQTT, HTTP and CoAP

Exchange And Transfer Of Sensor Data

- Sensor data can be transmitted over a variety of wired and wireless networks conforming to device and technology specific requirements (NMEA, CAN bus, etc) but over IP networks, sensor payloads using JSON is increasingly dominant
- JSON is well supported using HTTP APIs from 3rd party providers as well as over REST protocols
- JSON-based data representations can be converted into other formats such as XML for compatibility, or compacted into CBOR to achieve better compression
- However, there seems to be lack of standard data models

Security Considerations

- Many ports, ships and fleet-based operations system depend heavily on legacy systems
- Compared with other industrial sectors, cybersecurity awareness is low in the maritime industry
- 87% of survey respondents from the shipping industry believed cyber attacks would increase over the next five years
 - This is higher than counterparts in the aviation, rail and logistics industries.

Security Considerations

- Many ports, ships and fleet-based operations system depend heavily on legacy systems
- Compared with other industrial sectors, cybersecurity awareness is low in the maritime industry
- 87% of survey respondents from the shipping industry believed cyber attacks would increase over the next five years
 - This is higher than counterparts in the aviation, rail and logistics industries.

Security Considerations



NEWS

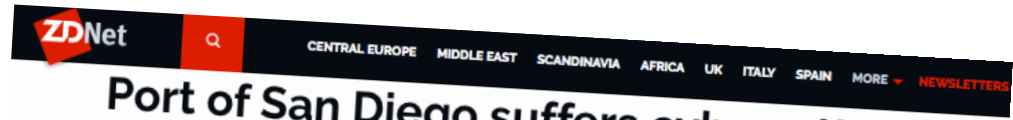
Technology

Ship hack 'risks chaos in English Channel'

WEDNESDAY, DECEMBER 9, 2015

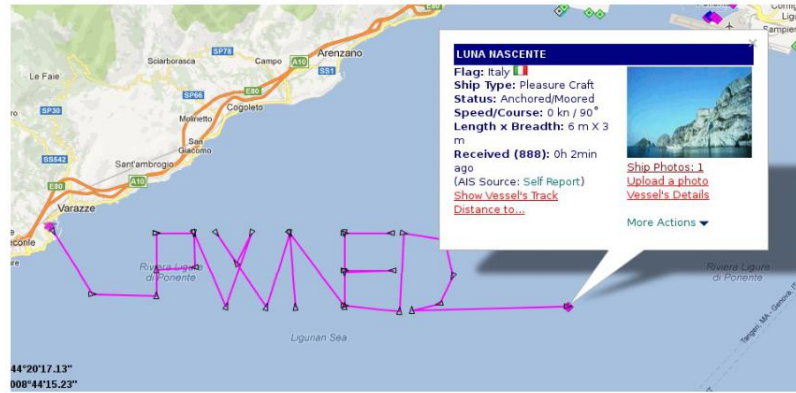
Maritime Security: Hacking into a Voyage Data Recorder (VDR)

by Ruben Santamarta @reversemode



Port of San Diego suffers cyber-attack, second port in a week after Barcelona

Cyber-attacks have now been reported at three ports in the last two months



GPS spoofing makes ships in Russian waters think they're on land

Findings: Communication and Data Transfer

- When high-speed broadband communication channels exist and bandwidth is abundant, the choice of security mechanisms, communication protocol and data payload formats are not significantly different
- When radio signalling costs are high compared to amount of data transferred, again application layer performance does not matter
- However, when the radio channel is congested, lossy or experiences severe latency, then using protocols such as TLS and DTLS will become impossible
 - In such cases, consider signing and encryption of data at the application protocol layer instead of transport layer
 - Consider also smaller payload formats and sizes

Findings: Cybersecurity Strategies

- Employ preventative defensive methods (Hardening VDR, endpoint protection, user and device authentication) and securing communication
- Develop new defensive strategies which depend on information sharing, data correlation and increasing cybersecurity awareness

Findings: Data Sharing and Data models

- Scalable, able to allow multiple stakeholders to participate
 - This means it should have a standard vocabulary and data model to express data
 - Based on open standards to avoid vendor lock-in
 - Ability to integrate easily into existing workflow, particularly integration to Web and REST-communication
- Extensible and flexible data models
 - Data model should allow future extensions, such as new sensor and incident data for smart ships and smart ports
 - Format should allow expressing multiple measurements occurring within a specific time period, or associating related data happening in different locations and times
 - Format should be simple enough for machine-based interaction, so that report generation and processing can be automated
- Resilient, secure and can tolerate connectivity disruption or intermittence
 - This allows the cybersecurity incidents to be securely exchanged between ship and shore

Looking Forward

- Sea4Value FFN as a technical blueprint for a future fairway infrastructure has been extremely informative
- Sea4Value FFN as a technical blueprint for minimum requirements for enabling remote piloting revealed it is already technically possible today with minimal disruptions to ship systems, while increasing safety and security of piloting services

The Fairway of the Future: Important Technical Learnings

Thank you for your time!