Workshop on Cybersecurity in Inland Navigation

River Information Services, e-Navigation ....

An overview of ICT in Inland Waterways vulnerable to Cyber Threats

Bonn – 05/09/2019
Overview

• Focus on RIS for the Inland Waterways
  – River Information Services (Operational Services)
  – RIS Key Technologies (Technical Services)
  – Reference Data

• A short introduction on Cyber

• Cyber Threats in Inland Waterways

• Mitigation measures
Guidelines and Recommendations for River Information Services (WG125) – 2019

PIANC InCom Update on Permanent WG 125 on River Information Services (RIS) (Part I, II, III) has been released!
e-Navigation for Inland Waterways (WG156)

➢ Provide a definition of e-Navigation for Inland Waterways

➢ Whether inland navigation could benefit from the developments in the maritime environment.

➢ In what way the required interaction between maritime transport and inland navigation in this context can be guaranteed to safeguard the required interoperability of future maritime and inland navigation systems.

➢ Identify opportunities for improving the safety, efficiency of transport, logistics and administrative processes.
Goal of the Task Group 204

Raise awareness for cybersecurity in inland navigation among:

• the management of inland waterways,
• ports,
• shipping companies,
• skippers,
• ........

which is due to a dramatically increased complexity of navigational and information systems for IWT based on ICT.
Definition River Information Services (RIS)
(PIANC WG125 Guidelines)

RIS means the **harmonised information services** to support **traffic and transport management** in inland navigation, including **interfaces to other transport modes**. RIS aims at contributing to a **safe and efficient** transport process and utilising the inland waterways to its fullest extent.

**Digitalisation of the Inland Waterway Transport (IWT)**
## Table 3.3
RIVER INFORMATION SERVICES

### Mainly traffic related
1. Fairway information Services (FIS)
2. Traffic information (TI)
   - a) Tactical traffic information (TTI)
   - b) Strategic traffic information (STI)
3. Traffic management (TM)
   - a) Local traffic management (vessel traffic services - VTS)
   - b) Lock and bridge management (LBM)
   - c) Traffic Planning (TP)
4. Calamity abatement support (CAS)

### Mainly transport related
5. Information for transport logistics (ITL)
   - a) Voyage planning (VP)
   - b) Transport management (TPM)
   - c) Inter-modal port and terminal management (PTM)
   - d) Cargo and fleet management (CFM)
6. Information for law enforcement (ILE)
7. Statistics (ST)
8. Waterway charges and harbour dues (CHD)
Structured approach of the implementation of RIS services

Transport Management related

1. FIS – Fairway Information Service
2. TI – Traffic Information
3. TM – Traffic Management
4. CAS – Calamity Abatement Support
5. ITL – Information for Transport Logistics
6. ILE – Information for Law Enforcement
7. ST – Statistics
8. CHD – waterway Charges and Harbour Dues

Traffic Management related
The 4 RIS Key Technologies – Technical Services

• The RIS Directive 2005/44/EC – 7/09/2005 defines 4 Technical regulations:
  ❖ **Notice to Skippers** standard - No 416/2007 of 22 March 2007 concerning the technical specifications for Notices to Skippers.
  ❖ **Electronic Chart Display and Information System for Inland Navigation** – No 990/2013 concerning the technical specifications for Inland ECDIS.
Operational versus Technical Services
Matrix RIS Technical versus Operational Services

<table>
<thead>
<tr>
<th>RIS Key Technologies</th>
<th>Inland ECDIS</th>
<th>Electronic Ship Reporting</th>
<th>Notice to Skippers</th>
<th>Vessel Tracking &amp; Tracing</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIS Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. FIS - Fairway Information Service</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2. TI - Traffic Information</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>3. TM - Traffic Management</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. CAS - Calamity Abatement Support</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>5. ITL - Information for Transport Logistics</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>6. ILE - Information for Law Enforcement</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. ST - Statistics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. CHD - Waterway charges and Harbour Dues</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Reference Data

- **Reference Data**
  - (e.g. ENI, RIS-Index, ADN)

- **Hull-data**
  - static vessel data

- **ERI**
  - Electronic Reporting

- **RIS-Index**
  - unique identifier of waterway objects

- **NtS**
  - Notices to Skippers

- **VTT**
  - Vessel Tracking and Tracing

- **ENC**
  - Inland ECDIS

- **ENC**
  - Inland ECDIS
Comparison with the Maritime World

Automatic Identification System (AIS)  
GPS / Electronic Nautical Charts

Notes to Mariners  
Vessel Traffic Services / Logistics

05/09/2019 - 13
Some Cyber.... keywords

- We are using the term **Cyber** to emphasize that our focus is on electronic systems, computers, computer networks, ...
- We need **Cybersecurity** because there are **Cyber Risks** due to **Cyberattacks**.
- **Cybercrime** is a crime with **ICT as a mean and as a target**.
Cybercrime

• We have moved from the Nerd to the *Cybercriminal*.

• Information is money and power:
  – Stealing Information becomes a business case.
  – Cybercrime is very professionally addressed as a business with a high ROI.
  – Don’t forget espionage.

• *Cybersecurity should be/is THE object/concern for all functionalities produced/provided in IWT which is driven by Digitalisation.*
Some Popular CyberAttacks/Crime Methods

• (D)DoS: (Distributed) Denial of Service (jamming)
• Brute-force attack
• Malware
• Spoofing (e.g. the man in the middle)
• Phishing
• Social engineering
• Hijacking
The man in the middle (spoofing)
Public Key Encryption with PKI Certificates

Source: e-Navigation Underway 2019 - OFFIS

05/09/2019 - 18
Inland Automated Identification System (AIS)
Inland AIS/GPS

• Navigation: position, speed, heading other data about the vessel, ....
• Radio-frequency-enabled technologies are an “easy target” for malicious individuals.
• The signal is unencrypted and access to the service requires no authorisation.
• Old technology based on poor bandwidth
• Possible Attacks:
  – DoS
  – Spoofing
  – Jamming
  – Hijacking
  – ...............
Notice to Skippers (NtS)

- Notices to Skippers (NtS) is a RIS key technology which provides in a standardised manner and language independent:
  - fairway and traffic related information, as well as
  - hydrographical information such as weather information, water level information and ice information.

- Notices to Skippers is supporting Fairway Information Services (FIS) and transport planning as part of the Information for Transport Logistic (ITL).
Electronic Ship Reporting (ERINOT)

• Electronic (Ship) reporting (ERI) is a RIS key technology that facilitates the RIS services; Strategic Traffic Information (STI), Traffic Management (TM), Calamity Abatement Support (CAS), Statistics (ST), Law enforcement (ILE), Waterway charges and harbour dues (CHD) as well as Transport Logistics (TL).

• Electronic Reporting in Inland Navigation facilitates electronic data interchange (EDI) between partners in inland navigation as well as partners in the multi-modal transport chain involving inland navigation, and avoids the reporting of the same information related to a voyage several times to different authorities and/or commercial parties.
Notice to Skipper/Electronic Ship Reporting

• Provides information to users via websites, M2M communications (webservices).

• Possible Attacks
  – Related to Internet Connection and ICT infrastructure (Web/Database servers)
  – (D)DoS: (Distributed) Denial of Service (jamming)
  – Brute-force attack
  – Malware
  – Spoofing (e.g. the man in the middle)
  – Social engineering
  – Hijacking
  – .........................
Inland Electronical Navigation Chart (IENC) and Inland ECDIS
Inland ECDIS/Inland IENC

• Contains:
  – ICT infrastructure / Internet connection
  – Inland IENC’s / NtS Messages
  – Radar overlay / AIS information

• Possible Attacks
  – Related to AIS/GPS
  – Related to NtS Messages
  – Related to Hydro-Meteo Information (water levels, .....)
  – Related to Internet Connection and ICT infrastructure
  – Attacks due to update of the IENC charts, via Internet or USB stick
  – .........................
Cross-border/Corridor Management

• Data exchange/provision from different waterway authorities to fulfil new RIS services like for example corridor management.
• Information is provided to the users via websites, M2M communications, webservies, mail communication, notifications, ......
• Possible Attacks
  – Related to Internet Connection and ICT infrastructure (Web/Database servers)
  – (D)DoS: (Distributed) Denial of Service (jamming)
  – Brute-force attack
  – Malware
  – Spoofing (e.g. the man in the middle)
  – Social engineering
  – Hijacking
  – .....................
• Need to be addressed with cross-border/international cooperation between the involved parties.
New Developments / Smart Shipping

• **Problem**: Today ship control systems; power/valve remote control systems; ballast water systems; wheelhouse systems, remote controls for locks and bridges are driven/monitored by *Supervisory Control And Data Acquisition (SCADA) systems*. Which are often based on very simple (and old) protocols without any encryption. Thus easy to hack.

• Removal of crew removes an element of monitoring which might be needed in the event of a cyberattack.

• The ship becomes an *IoT* (Internet of Things).

• **Assurance will be needed that systems on-board of automated ships would be cyber hardened.**
Important Mitigation Measures

• Each solution as a result of a Digitalisation should be subject to a **Cyber Risk Assessment** to identify the **Cyber Risks** and how to monitor/detect them and define **mitigation measures**.
• Solve all the issues on the physical and logical level of security.
• Monitor your environment continuously and foresee good reporting/alerting tools and define KPI’s.
• Educate and train your users/ make them aware of their actions (it’s so easy/tempting to open a mail).
• **Be aware of social engineering!!!!**
• Take procedures for maintenance personnel and their equipment, certainly for external services (internal and remotely).
• Avoid obvious intruders, may I use your USB stick for a moment ...
• .................
Some important Standards

- In the US, the National Institute of Standards and Technology (NIST) is in the process of issuing a series of profiles intended to help the maritime industry make the most of the wider voluntary Framework for Improving Critical Infrastructure Cybersecurity.

- The NIS Directive (EU 2016/1148) is the first piece of EU-wide cybersecurity legislation. The goal is to enhance cybersecurity across the EU. (ENISA: European Union Agency for Network and Information Security)
  - a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority

- EU General Data Protection Regulation (GDPR REGULATION (EU) 2016/679) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

- ISO/IEC 27032:2012 - Guidelines for cybersecurity, provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:
  - information security,
  - network security,
  - internet security, and
  - critical information infrastructure protection (CIIP).
Thank you for your attention

Ir. Dierik Vermeir
Past Chairman WG156
Vice-Chairman WG125
Vice-Chairman NtS expert group
IALA Industrial Member

CEO ALSIC BVBA
Derbystraat 25
B-9051 Sint Denijs-Westrem

Tel: +32-9-265.91.11
GSM: +32-475-43.66.19

www.alsic.be
dierik.vermeir@alsic.be