**Project acronym:** NOVIMAR
**Project full title:** Novel Iwt and Maritime Transport Concepts
**Grant agreement No.** 723009
**Coordinator:** Netherlands Maritime Technology Foundation

# Deliverable 5.3 - Safety and Cybersecurity Assessment

Duration: 48 months
Project Start: 01/06/2017
Project End: 31/05/2021

**Deliverable data**

| | | | |
|---|---|---|---|
| **Deliverable No** | 5.3 | | |
| **Deliverable Title** | Safety and cybersecurity assessment | | |
| **Work Package no: title** | WP5: Safety issues and human skills | | |
| **Task(s)** | T5.3 – Safety assessment and cybersecurity issues | | |
| **Dissemination level** | Confidential | Deliverable type | Report. |
| **Lead beneficiary** | BV M&O | | |
| **Responsible author** | Wa Nzengu Nzengu | | |
| **Co-author** | | | |
| **Date of delivery** | 8/06/2021 | | |
| **Approved** | **Name (partner)** | | Date |
| **Peer reviewer 1** | Igor Bačkalov (BU) | | 8-06-2021 |
| **Peer reviewer 2** | Robert Hekkenberg (TU) | | 8-06-2021 |
| **Peer reviewer 3** | Edwin Van Hassel (UANTW) | | 8-06-2021 |
| **QA manager** | Michael Goldan (NMTF) | | 20-06-2021 |

**Document history**

| **Version** | **Date** | **Description** |
|---|---|---|
| 0 | 11/05/2020 | First draft |
| 1 | 25/05/2020 | Second draft |
| 2 | 7/05/2021 | Third draft |
| 3 | 8/06/2021 | Fourth draft |
| 4 | 5/07/2021 | Fifth draft, taking into account QA manager comments/remarks |

*The research leading to these results has received funding from the European Union Horizon 2020 Program under grant agreement n° 723009.*

# 1 EXECUTIVE SUMMARY

## 1.1 Problem definition

The operation of vessel trains at sea and in particular on inland waterways poses considerable challenges from the point of view of navigational safety and cyber safety & security. Interaction with other waterborne traffic of individual vessels and / or other vessel trains, the presence of lowly crewed vessels in busy waterways, unexpected situations onboard and outside vessels and severe weather conditions are some examples of such challenges.

The main problem to be addressed by work package 5 – Safety issues and human skills is the way to account for the VT related navigational and functional safety and security issues and the VT impact on human working conditions and skills. The overall objectives are to develop methods to assess the safety level of a VT operation and to derive recommendations for the VT designers, operators and regulatory bodies.

In this context, the main objectives of Task 5.3 are to:

- evaluate the VT developments and implementation made in the project against the safety functions and relevant requirements and scenarios as defined in task T5.1
- make a preliminary assessment of the cyber security issues relevant to the VT concept and operations.

## 1.2 Technical approach and work plan

The activities in Task 5.3 are organised around three main sub-tasks:

- Review of implemented solutions addressing navigation rules, safety functions and critical component failures as identified in task T5.1. For navigation it will be verified that all VT operations are covered by existing rules, the need for new rules will be investigated
- Assess the scenarios as developed in task T5.1 by means of numerical and full mission bridge simulations to check the effectiveness of the implemented safety measures. When needed, modifications of implemented safety measures, or additional ones, will be proposed
- Carry out a preliminary cyber-security assessment following Bureau Veritas Rule Note NR659 - Rules on Cyber Security for the Classification of Marine Units [8]. It will consist in understanding the cyber threats relevant to the vessel train concept and developed solutions, by identifying the threats and vulnerabilities of the whole system.

## 1.3 Results

### 1.3.1 General

The outcomes of the safety and cybersecurity assessment should be interpreted with caution for a few reasons, namely:

- The control system needs further development or changes to allow a safe use on high traffic waterways, in particular on inland waterways. The current system cannot solve the same dynamic traffic situations, e.g avoiding moving objects, as a conventional vessel could [2].
- Within the scope of the full-mission bridge simulations that were carried out within the tasks T3.5 – Demonstrator results and T5.2 – Human elements, it was not possible to assess specific assumptions and outcomes of the VT operation safety assessment for various

reasons. However, the outcomes of these simulations could be exploited, namely, for the definition of VT operational scenarios and needed inputs for safety assessment.

### 1.3.2 Safety assessment

The VT operation safety assessment has been carried out according to the scope and methodology described in section 8.1, using the principle of equivalent safety with conventional vessels.

The VT operation safety assessment shows that a vessel train may be operated safely within the operational limitations defined by the VT control system capabilities, crewing of the follower vessels while operating in the VT, operational conditions on the fairway and individual technical features of the vessels in the VT.

At least one crew member managing unexpected events such as flooding, fire or black-out, is to be provided on the follower vessels.

Considering the global impact on the VT safety of all recommendations assigned to one hazardous scenario, analysis of the assessment results shows that:

For IWT:

- With an active monitoring on the FV bridge, the VT operation would be as safe as a conventional vessel for about 60% of hazardous situations, and would be safer than a conventional vessel for 40% of hazardous situations.
- Without active monitoring on the FV bridge the VT operation would be less safe than a conventional vessel for about 30% of hazardous situations. The VT operation would be as safe as a conventional vessel for about 43% of hazardous situations, and would be safer than a conventional vessel for 27% of hazardous situations.

For SSS:

- With an active monitoring on the FV bridge, the VT operation would be as safe as a conventional vessel for about 77% of hazardous situations, and would be safer than a conventional vessel for 23% of hazardous situations.
- Without active monitoring on the FV bridge the VT operation would be less safe than a conventional vessel for about 27% of hazardous situations. The VT operation would be as safe as a conventional vessel for about 64% of hazardous situations and would be safer than a conventional vessel for 9% of hazardous situations.

Considering the effectiveness of each individual recommendation, analysis of the assessment results shows that:

For IWT:

- with active monitoring on the FV bridge, the implementation of 29% of recommendations would make the VT operation safer than a conventional vessel, while 71% of recommendations would result in a VT operation as safe as a conventional vessel
- without active monitoring on the FV bridge, the implementation of 26% of recommendations would make the VT safer than a conventional vessel, 49% of recommendations would result in a VT operation as safe as a conventional vessel, while 25% of recommendations would fail to lead to a VT operation at least as safe as a conventional vessel.

For SSS:

- with active monitoring on the FV bridge, the implementation of 14% of recommendations would make the VT operation safer than a conventional vessel, while 86% of recommendations would result in a VT operation as safe as a conventional vessel

- without active monitoring on the FV bridge, the implementation of 12% of recommendations would make the VT operation safer than a conventional vessel, 64% of recommendations would result in a VT operation as safe as a conventional vessel, while 24% of recommendations would fail to lead to a VT operation at least as safe as a conventional vessel.

The outcomes of safety assessment indicate the need for human active monitoring on the FV bridge to ensure safe operation of the FV, based on the assumption that human reaction on deviations is the most effective solution. The VT concept however is researched to find solutions to safely operate a train of vessels under operational control and responsibility of a LV, whilst the FV's follow with unmanned wheelhouse. Based on this principle, the need for the presence of any crew member on the FV is primary dictated by the need for performing tasks, for which at present time no automated solutions are available. In order to get a better understanding of this specific outcome of the safety assessment, a thorough safety assessment focused on the situation where a FV operates in a VT without continuous active human monitoring in the wheelhouse carried out according to chapter 9 shows that, provided that all requirements and procedures for VT safe operation are implemented, there is no need for continuous human attendance in the FV's wheelhouse for monitoring functions during normal operations. In urgent conditions human attendance is needed in the FV's wheelhouse for monitoring functions to reduce the probability of certain hazards to occur. Most of these situations can be predicted and should be part of the voyage plan, identifying beforehand the need for human attendance. Under critical conditions, the VT cannot operate. VT operations need to be postponed to reduce the probability of certain hazards to occur.

### **1.3.3** Cybersecurity assessment

In order to provide an understanding of cyber threats relevant to the vessel train control system as developed by NOVIMAR, two scenarios were investigated supplemented with the results of the FMEA. The research shows that the VT control system can be exposed to external and internal attacks.
The source of external attacks could be a spoofing system, with the purpose to disrupt functionalities of those technical systems that in turn affect the correct operation of the VT control system. Systems vulnerable for a spoofing signal are the GNSS, AIS, Radar and the direct wireless communication system. From these four systems, the most critical situation would be the intrusion of the direct wireless system as this intrusion will most likely spread between the other vessels in the VT and/or within the affected vessel. The source of an internal attack would be a human having physical access to the systems. Such attack can be on purpose or unintended.

When the VT control system is embedded in an existing or new ships infrastructure, caution is needed. The question is whether the existing ships infrastructure is already cybersecure or not. Interfaces with existing equipment need to be investigated on cyberthreats. When connection is needed with the internet e.g for maintenance or services (like water depth information, etc.), the components of the VT control system must be protected. Crews need to be alert on communication spoofing whilst using the VHF system. The likelihood of identified sources of attack has not been explored.
For the further development of the VT control system into a market ready system, it is recommended to address cyber security in the developments.
For the implementation of the VT control system onboard of a retrofit ship or new ship, it is recommended to incorporate cyber security specialism in the technical team.

The outcomes of NR 659 – Cyber Risk Analysis Flow Methodology steps 1 and 2, can be used as starting point to perform a full cyber security assessment leading to a cyber security class notation.
When preparing the installation of a VT control system, the architecture shall include the following:

- Tailored network segregation limiting the network usage to the strict minimum
- Hardened critical equipment limiting escalade of privileges
- Layer 3 encryption and authentication restricting the remote access to the VT Control
- Authentication-based GNSS receivers countering spoofing
- Human monitoring and logging of systems activity, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
- Dedicated software countermeasures against corrupted WiFi packets
- Regulated systems lifecycle and patch management plan.

### 1.3.4 Safety and security conditions

The vessel train may be operated safely if appropriate safety and security conditions are met. The safety and security conditions are defined through the recommendations resulting from the safety and cybersecurity assessment workshop, in addition to those developed during the preliminary HAZID study [1]. Developed recommendations cover different aspects of the VT operation as well as the VT vessels and systems design and arrangements, including the identification of the need for new or adapted Rules and Regulations provisions development.

a) VT vessels and systems capabilities are addressed by the recommendations through suitability of the level of functionality and reliability to be ensured for systems associated with essential services involved in the operation of vessel trains.
b) VT operational aspect is covered by specific recommendations including, e.g:
    - The VT operating limits, i.e., parameters resulting from risk analysis to which the operators should refer for the VT operation, e.g traffic conditions, VT length
    - The need for VT identification
    - The hazards arising from the reduction of crew on board and from the use of remote control
    - The availability of direct control of the follower vessels by the FV operators in case of emergency or system failure
    - The need for the development of appropriate procedures related to VT operation in normal conditions or in case of emergency.
c) VT related human factors are also addressed, namely in terms of operators skills and training need, working environment, HMI design, fatigue and minimum manning.
d) The recommendations related to cybercecurity issues include technical and organizational aspects related e.g. to equipment protection, cyber Security Policy, etc, in accordance with the Bureau Veritas Rule Note NR 659 [8].

## 1.4 Conclusions and recommendation

The VT operation safety assessment shows that a vessel train may be operated safely within the operational limitations defined by the VT control system capabilities, crewing of the follower vessels while operating in the VT, operational conditions on the fairway and individual technical features of the vessels in the VT.

At least one crew member managing unexpected events such as flooding, fire or black-out, is to be provided on the follower vessels.
A thorough risk analysis focused on the situation where a FV operates in a VT without continuous active human monitoring in the wheelhouse carried out according to chapter 9 shows that, provided that all requirements and procedures for VT safe operation are implemented, there is no need for continuous human attendance in the FV's wheelhouse for monitoring functions during normal operations. In urgent conditions human attendance is needed in the FV's wheelhouse for monitoring functions to reduce the probability of certain hazards to occur. Most of these situations can be predicted and should be part of the voyage plan, identifying beforehand the need for human attendance. Under critical conditions VT operations need to be postponed to reduce the probability of certain hazards to occur.

To meet the cybersecurity assessment recommendations according to section 1.3.3, the vessel train should comply with the requirements for the assignment of the additional class notation "Cyber secure", according to Bureau Veritas Rule Note NR 659 [8]. The scope of the additional class notation "Cyber secure" includes a cyber management as well as equipment and vessels securing by design.

Based on the outcomes of the VT operation safety and cybersecurity assessment, we make the following recommendations:

1) Assumption 1 (IWT / LV+2FVs) and Assumption 2 (IWT / LV+4FVs) present the same level of safety.The influence of the VT length on the operation safety when the number of follower vessels exceeds four, needs to be investigated.
2) Analysis of the recommendations with regard to vessel design and equipment shows that some of them (15%) are more severe than the provisions of the current Rules and Regulations, but have a high positive impact on the VT operation safety. It may be more complex to implement such recommendations on existing vessels by means of retrofit. A cost-benefit analysis would be of importance in order to conclude on the profitability of such an option.
3) Deployment of required technical and organizational cyber measures would be achieved through compliance of the VT with the requirements for the assignment of the additional class notation "Cyber secure", according to Bureau Veritas Rule Note NR 659. The scope of the additional class notation "Cyber secure" includes a cyber management as well as equipment and vessels securing by design.
4) Procedures for VT operation approval need to be defined and implemented at two levels:
   - Approval of the VT operation to be implemented by the competent Authority/Administration. Where the VT operational parameters are out of the range of those considered for safety and cybersecurity assessment, the approval process should be supplemented by a risk assessment in order to establish the suitability of the safety level of the VT operation.
   - Check and verification to be performed by the shipping company whenever a VT is formed.
5) In addition to the areas of the existing regulatory framework requirements challenging the VT concept as identified in the deliverable D5.1 [1], the need for new or adapted Rules and Regulations provisions is addressed through defined safety functions. Recommendations to regulatory bodies and waterborne transportation operators, defining needed modifications to current Rules and Regulations and operational principles should be developed.
6) Preparing Regulations adapted to the vessel train concept could be a complex and long process. An alternative way to authorize VT operation could be to prepare a request for a derogation with a pilot project. This is possible, e.g., in the scope of article 25 of European Directive 2016/1629

in order to encourage innovation and the use of new technologies in inland navigation. An appropriate approval procedure should be developed.