User survey on maritime communication security

Background and purpose of survey

Maritime communication is currently undergoing major changes. The development of new e-navigation services requires a transition from traditional analogue voice over VHF-radio to digital messages, either over new VHF data links, SATCOM or other communication systems. Electronic port clearance through the new maritime single window will also require digital submission of FAL forms or other equivalent electronic reports as well as other ship documents to shore.

As technology continues to develop, the importance of cyber security and trusted data transfer to ensure safe and reliable operations increases. To get a better understanding of the actual risk levels associated with data not being trusted, including attacks on ship/shore communication channels, we ask you to provide your best estimate of how critical such problems can be.

This survey is organised by the Research Council of Norway-funded research and development project CySiMS (Cyber Security in Merchant Shipping). The project aims at developing new security solutions for ships that will provide integrated and cost-effective protection against cyber-attacks in relation to information exchange.

The survey is 100% anonymous. The report containing the results of the survey will be made available to those survey participants that ask for it. If you allow us to, we may also contact you at later stages in CySiMS for further collaboration. However, completing the survey does by no means hold any further obligation from your side

We understand that it is very difficult to come up with correct data on all these different combinations, so we are only asking for your best guess!

Link to survey:

https://www.netigate.se/a/s.aspx?s=346035X75141850X34431

Please complete the survey by Sunday 18th of December at the latest.

Structure of survey (useful when completing the survey online)

The next section in the document contains a number of communication scenarios that we believe are typical for future maritime digital services.

Our assumption is that a cyber-security attack or problem will manifest itself as one or more of the following communication faults:

1. ***Data changed***: Data in one or more messages has been changed for hostile purposes.
2. ***Data lost***: One or more messages failed to be received by ship or shore, e.g. because of jamming of the radio channel.
3. ***Data overheard***: Someone picked up one or more messages and use the information for non-authorized commercial- or hostile purposes.
4. ***Data not trusted:*** Sender and receiver disagrees on data actually being sent or on the content of the message.

Our question to you is: *For each scenario, what is the worst-case outcome when a communication faults occurs? Here, worst case is defined as when the sum of severity and frequency is highest (see below).*

For each scenario you will be asked the following questions:

- **How often** does this scenario occur (**per individual ship**)?
    - 4: several times a day
    - 3: several times a week
    - 2: several times a month
    - 1: several times a year or less
- What is the **worst case outcome** (short textual description)?
- What **type of outcome** is this (select from below list)?
- What **communication fault** is most likely to cause this outcome (select one of the four above)?
- What **severity** has this outcome (select from below table)?
- **Given that the communication fault happens, how often** will this worst case outcome occur (select from below table)?

The different ***types of outcomes*** are defined as follows:

1. ***Individual injury*****:** One or more persons are harmed.
2. ***Commercial*****:** The Company, the ship or infrastructure suffers physical damage (grounding, collision, machinery damage etc.) or there are other economic consequences (fines, detention etc.)
3. **Environment:** There is a discharge or other forms of environmental damage.
4. **Reputation:** The Company (or the ship) suffers damage to its reputation. This includes consequences of, e.g. legal punishment, serving jail time etc.

We need you to classify the ***severity*** of the worst-case outcome according to the below table. The consequences can be of different types as listed in the four right-most columns:

Level	Val.	Individual	Commercial	Environment	Reputation
None	0	No damage	No damage	No damage	No damage
Negligible	1	One Minor Injury	500 USD	On site release contained without external assistance	Local complaint/ recognition, impact less than one month
Moderate	2	One Severe Injury or Multiple Minor Injuries	5 000 USD	On site release contained with external assistance.	Local media coverage, impact from 1 to 3 months
High	3	Multiple Severe Injuries	50 000 USD	Uncontained release with potential for moderate environmental impact.	National media coverage, impact lasting more than 3 months
Critical	4	One Death	500 000 USD	Uncontained release with potential for major environmental impact	National and some international coverage, impact lasting more than year
Cata-strophic	5	Multiple Deaths	5 000 000 USD	Uncontained release with potential for very	International coverage, unrecoverable damage

				large environmental impact	

We also need your opinion on ***how often*** the worst-case outcome will happen, given that the communication fault materialised. The following values will be used:

Level	Val.	Description
Always	6	Each time
Likely	5	One in 10 exchanges
Possible	4	One in 100 exchanges
Unlikely	3	One in 1 000 exchanges
Rare	2	One in 10 000 exchanges
Extremely rare	1	One in 100 000 exchanges

The ***worst-case outcome*** for each scenario is when the sum of the "Val." columns are the highest, i.e. Moderate consequence and Always (sum 8) is worse than Catastrophic and Rare (sum 7).

General questions

1. What is your normal role in the shipping business?
   a. Crew
   b. VTS, pilot or other advice giving function
   c. Marine Manager/Safety Manager/SI/CSO
   d. Government administration
   e. Equipment industry, yard or similar
   f. Research, university or similar
   g. Other

The Scenarios

Please read each communication scenario before answering the corresponding questions. The scenarios are described below (and online).

SC1: Navigational real-time information to ship

The ship receives updated navigational information from shore. Examples are weather or ice information and forecast, lists of aids to navigations that are not working, floating containers, whale observations, wrecks etc. Today this is typically maritime safety information (MSI) received by NAVTEX or Safety-Net or wave, tide or virtual aids to navigation received over AIS.

SC2: Nautical document updates to ship

Electronic updates to documents that are required to be carried by the ship for safe navigation (nautical information) such as electronic chart updates, signal lists, notices to mariners, etc.

SC3: Ship reporting to VTS, coastguard or similar

Mandatory reports from ship in specific ship reporting, traffic separation scheme or VTS areas. Typically planned entry and exit times, voyage plan, dangerous goods, etc. Today this is usually voice messages over VHF, but in the future this will probably be automated digital transmissions.

SC4: Mandatory ship documentation and reports to port

This may be transmission, e.g., to port state control, of information that is mandatory to keep on board, e.g., deck or engine logbook, ship certificates, etc. This also includes mandatory reports to coast state authorities before entering port (or national waters). This is typically arrival reports, dangerous cargo manifest, crew list, passenger lists, ISPS reports etc. Failure to provide correct documents can cause detentions, fines or other. Note that crew and passenger lists will normally be considered sensitive and should not be seen by non-authorized parties. Cargo manifest may also be considered sensitive.

SC5: Nautical advice to ship

Advice from shore that can be the basis for new passage or voyage plans generated on the ship. This can be advice to reduce speed due to traffic congestion, ETA to port, etc. This is advice to the master of the ship, has no contractual status and the master can choose to ignore data. This is similar to the function the VTS has today, but may be more extensive and will be transmitted as digital data. This may or may not be data that is broadcast to other ships in the area.

SC6: Nautical commands to ship

In the future, the VTS, port or other entities may send real time directions to ship about speed and course to minimize safety risks and to ensure just in time arrivals. This information will be mandatory instructions to the ships. The master can choose to ignore the directions but this would come with a penalty (commercial disadvantages such as delayed slot time, etc.).

SC7: Remote control of ship, tugs or other port operation

In the future, it may be possible to remote control ship passage through difficult and time-consuming locks, channels or for more efficient berthing. This may also include remote control of tugs from the escorted ship's bridge, e.g. by pilot. This would include functions that could directly control speed and heading of ship or other entities.

SC8: Operational voyage instructions and reports

Information to or from the ship with commercial and operational importance. Some examples are that the ship receives instructions from charterer or manager or from the port or terminal (e.g., adjusted ETA). The ships send acknowledgements and reports such as noon at sea reports, voyage or port reports etc.

SC9: Telemedicine

Critical exchange of information with shore medical experts in the case of a medical emergency on board. This will typically use satellite or mobile data link and may include video or electronic signals from various medical measurement devices kept on the ship. Today this is typically a voice service to a radio-medico centre, but in the future this can be a partly digitalized service.

SC10: Search and Rescue (SAR)

SAR operations are today coordinated via voice over VHF or other channels. It includes an on scene commander which may be a designated ordinary merchant ship or an entity from the coastguard or other public services as well as the ship in distress and other ships assisting. In the future, it is expected that this will be enhanced with digital communication facilities to directly transfer search patterns, other instructions to ships and status updates.

SC11: Configuration

It may be desirable to do configuration of some bridge equipment remotely, e.g. by updating destination and ETA in the AIS from a voyage planning station or even from shore. Another example could be transfers of planned routes to the ECDIS. Attack on the configuration message would cause the equipment to operate with wrong information.

SC12: Network management

Some wireless data exchanges between ship and shore equipment can be used to manage frequencies or slots in a coming VHF Data Exchange network. Attacks on these messages could lead to ship equipment losing connection or misbehaving in other ways.