Vessel Cybersecurity Risk Analysis

Alejandro Gómez Bermejo
Cybersecurity Manager and Consultant
BEng, PMP, CISA, CRISC, ITIL, AMNI, Yachtmaster
www.erawat.es

Introduction

In this article, I introduce vessel cybersecurity risk analysis and show an example of its application to the Information and Communications Technology ICT assets in the Integrated Bridge System of a vessel.

First, I present some information security concepts and a methodology to develop vessel cybersecurity risk analysis.

Then, I show the application of the risk methodology to the systems in a vessel bridge where the information assets are considered the potential target of attackers.

Information security is usually characterized by three dimensions as defined in the information security standard ISO27000:

- Confidentiality: Information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity: Information and assets are accurate and complete.
- Availability: Information and assets are accessible and usable upon demand by an authorized entity.

According to NIST SP800-30, risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, typically a function of:

- Adverse impacts that would arise if the circumstance or event occurs
- Likelihood of occurrence.

When an attacker compromises an ICT asset, any of its information security dimensions can be affected.

Information security risks in the maritime context can be defined as those risks that arise from the loss of confidentiality, integrity or availability of information or ICT systems with the potential to cause adverse impacts in ship or port operations.

The impact from the loss of confidentiality, integrity or availability will be different depending on the mission of the organization. For a business firm confidentiality is usually important. However, in navigating a vessel the important dimensions will usually be integrity and availability.

We evaluate risk as the probability of a threat exploiting a vulnerability that results in an undesirable consequence. The evaluation of risk can be calculated as:

Risk=Threat x Vulnerability x Impact

The threat level will be evaluated taking into account the cyber threats that may be present in the context of the vessel bridge.

Vulnerability level will be evaluated as a function of the vulnerabilities in the ICT assets that enable the materialization of threats.

We calculate impact as the asset aggregated loss value of its three security dimensions Confidentiality, Integrity or Availability in case any of these are compromised.

For this example, we use a semi-quantitative approach for the values of threats and vulnerabilities with possible values low, medium and high. Impact and risk will be calculated using ad-hoc numbered scales as follows:

- Asset impact level will range from 0 (no impact) to 10 (maximum impact)
- Likelihood of threats will be assigned low probability (1), medium probability (2) or high probability (3).
- Vulnerabilities will be assigned values as low (1), medium (2) or high (3).
- Aggregate likelihood of the incident will be calculated as the product of the likelihood of the threat and the level of vulnerability of the asset from 1(lowest) to 9 (maximum).
- Risk is assigned a number between 1 (lowest) to 100 (highest).

As we can see, when calculating risks in this example we give equal importance to threat and vulnerability levels and significantly more relevance to asset impact and risk values.

The proposed risk analysis methodology is comprised of these steps:

- Define scope of the analysis and assets to evaluate
- Identify threat sources and events
- Identify vulnerabilities
- Determine likelihood of occurrence
- Determine magnitude of impact
- Determine Risk
- Communicate risk
- Manage risk levels
- Revise the analysis periodically

In the following paragraphs I apply the above methodology to develop a cybersecurity risk analysis in the context of an Integrated Bridge System.

Define scope of the analysis and assets to evaluate

The first step is defining the context and scope of the system to be analyzed.

In this case, the context of the analysis is the bridge of a vessel subject to SOLAS regulations and the risks derived from possible cyber attacks.

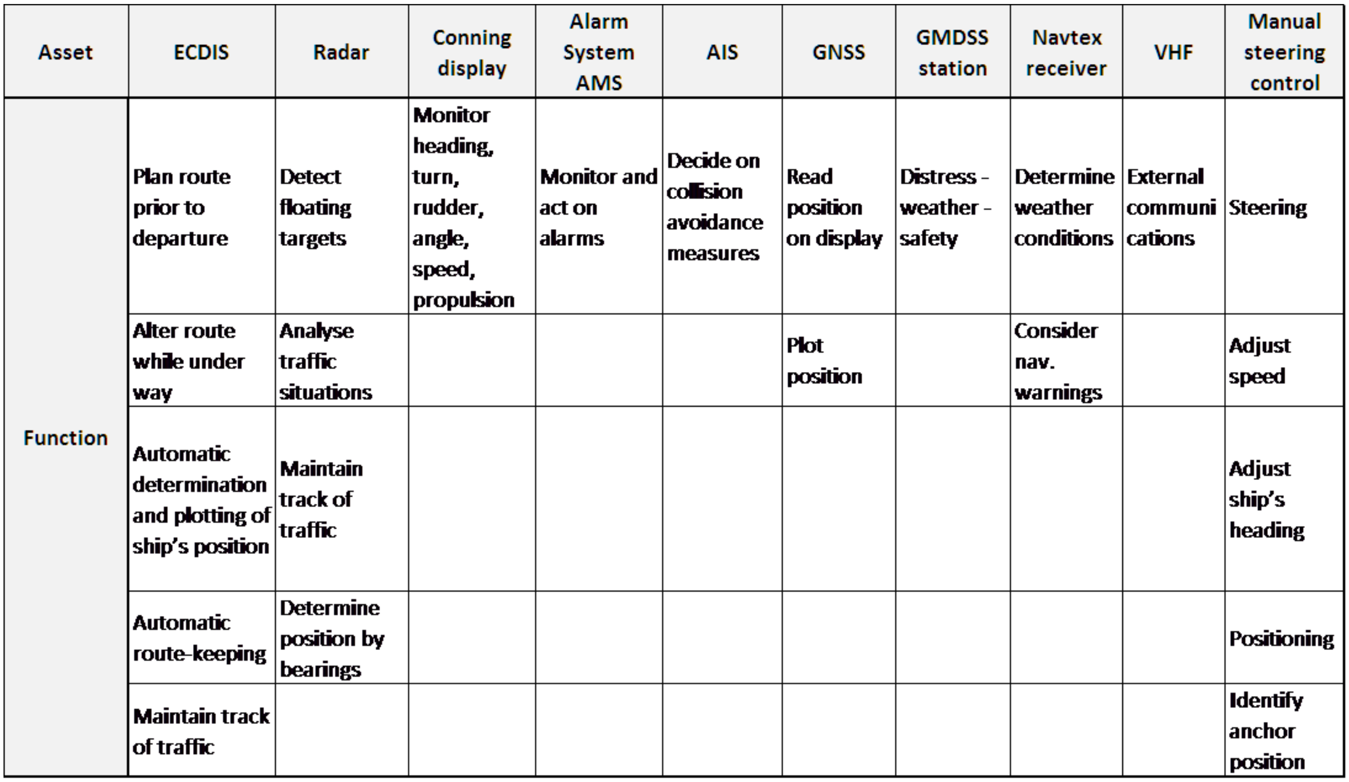
The scope will include the bridge ICT assets that support the operations of the vessel as well as potential impacts in case confidentiality, integrity or availability are compromised.

The threats considered will be of adversarial type originating in individuals, groups or organizations seeking to exploit the vessel dependence on cyber resources.

Other threats like accidental, human, environmental, structural or economic will not be considered. These threats will normally be covered in the Ship Safety Management System or the Company Corporate Risk Management.

For the identification of assets and functions I have made a selection of the assets mentioned in the IACS recommendation for the application of SOLAS regulation V/15 Bridge Design, Equipment Arrangement and Procedures (BDEAP), in particular annex A, with some modifications for this example.

The following table reflects the selected assets and its functions as performed in the bridge.



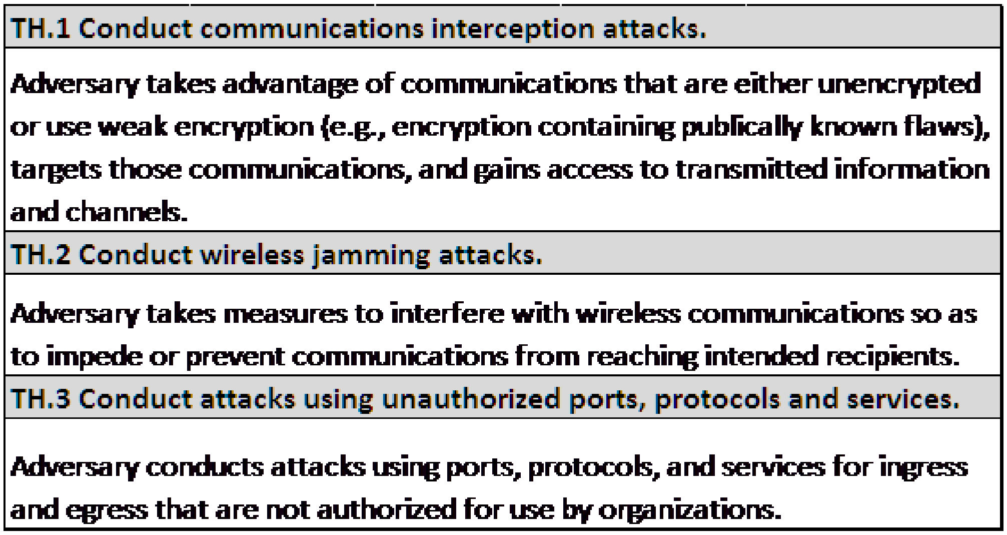
Asset	ECDIS	Radar	Conning display	Alarm System AMS	AIS	GNSS	GMDSS station	Navtex receiver	VHF	Manual steering control
Function	Plan route prior to departure	Detect floating targets	Monitor heading, turn, rudder, angle, speed, propulsion	Monitor and act on alarms	Decide on collision avoidance measures	Read position on display	Distress - weather - safety	Determine weather conditions	External communications	Steering
	Alter route while under way	Analyse traffic situations				Plot position		Consider nav. warnings		Adjust speed
	Automatic determination and plotting of ship's position	Maintain track of traffic								Adjust ship's heading
	Automatic route-keeping	Determine position by bearings								Positioning
	Maintain track of traffic									Identify anchor position

Identify threat sources and events

Threats applicable to the vessel and bridge should be identified.

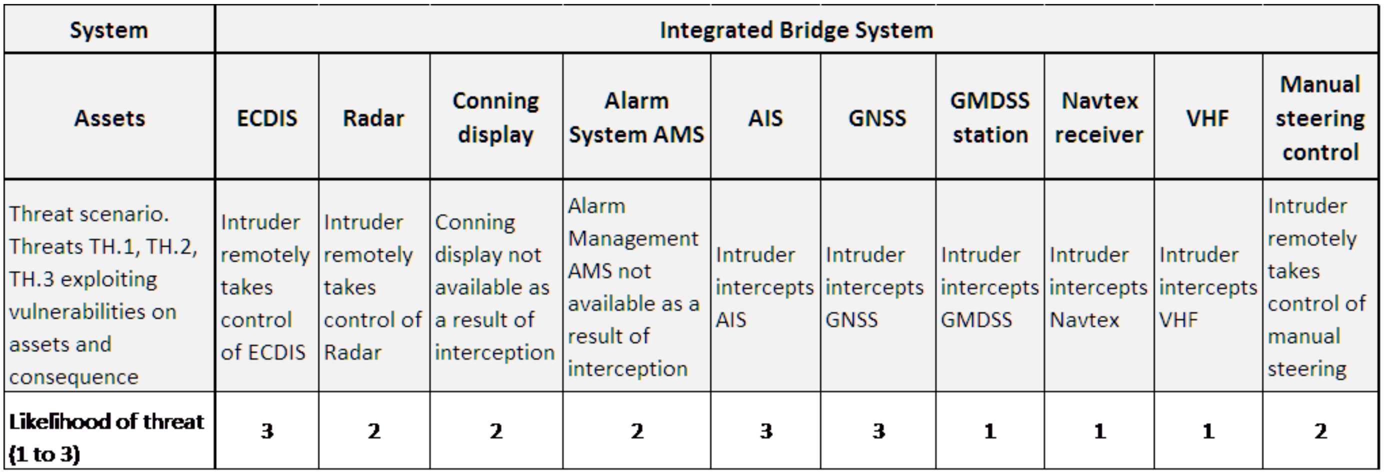
For this step, several Information Security Risk Assessment guides like NIST SP800-30 and ISO27005 are available.

I have selected some sample threats from the threat catalog in NIST SP800-30, appendix E, table E-2 “Representative examples – Adversarial Threat events”.



TH.1 Conduct communications interception attacks.
Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publically known flaws), targets those communications, and gains access to transmitted information and channels.
TH.2 Conduct wireless jamming attacks.
Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
TH.3 Conduct attacks using unauthorized ports, protocols and services.
Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.

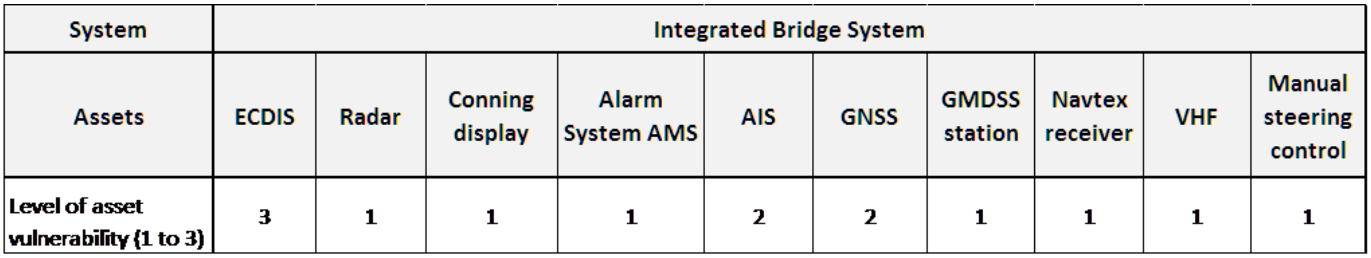
We need to calculate the likelihood that these threat events are present in the context of the vessel bridge and its values as low probability (1), medium probability (2) and high probability (3).



System	Integrated Bridge System									
Assets	ECDIS	Radar	Conning display	Alarm System AMS	AIS	GNSS	GMDSS station	Navtex receiver	VHF	Manual steering control
Threat scenario. Threats TH.1, TH.2, TH.3 exploiting vulnerabilities on assets and consequence	Intruder remotely takes control of ECDIS	Intruder remotely takes control of Radar	Conning display not available as a result of interception	Alarm Management AMS not available as a result of interception	Intruder intercepts AIS	Intruder intercepts GNSS	Intruder intercepts GMDSS	Intruder intercepts Navtex	Intruder intercepts VHF	Intruder remotely takes control of manual steering
Likelihood of threat (1 to 3)	3	2	2	2	3	3	1	1	1	2

Identify vulnerabilities

In this step we need to identify the level of vulnerability of each asset. For this example, we define three levels of vulnerability: low (1), medium (2) or high (3).



System	Integrated Bridge System									
Assets	ECDIS	Radar	Conning display	Alarm System AMS	AIS	GNSS	GMDSS station	Navtex receiver	VHF	Manual steering control
Level of asset vulnerability (1 to 3)	3	1	1	1	2	2	1	1	1	1

I have assumed medium levels of vulnerability in GNSS and AIS because these systems are susceptible to jamming and interception.

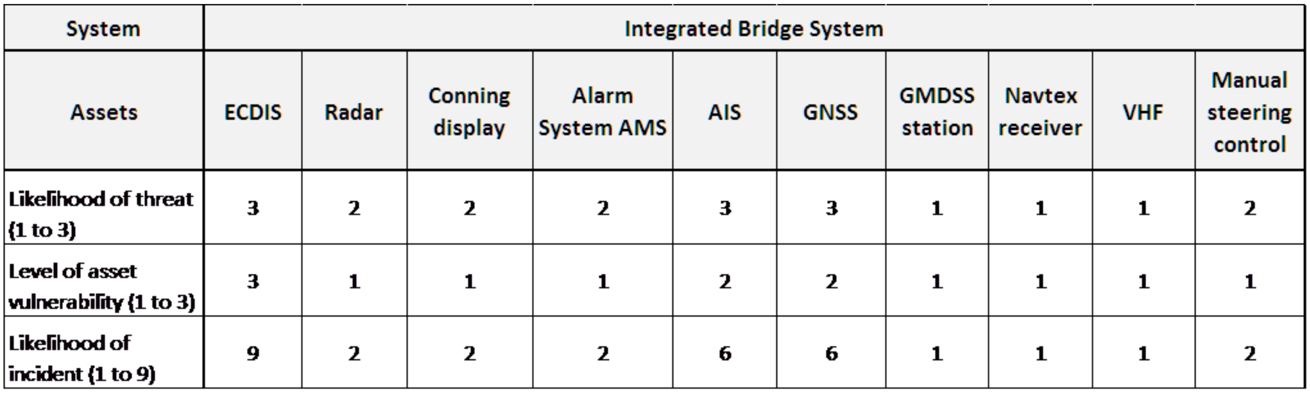
In this example, the ECDIS is assigned the highest level of vulnerability because the particular ECDIS is running on an old (more than three years) Windows machine, security patches have not been applied in the last three years and no anti-virus or anti-malware software is running in the system.

For the rest of the systems, I have assumed they have a low level of vulnerability.

Determine likelihood of occurrence

Now we need to determine the aggregate likelihood of occurrence of the risk. This is determined as the probability that the threats will exploit vulnerabilities in the system under analysis.

The aggregate likelihood of the incident is calculated as the product of the likelihood of the threat and the level of vulnerability of the asset.

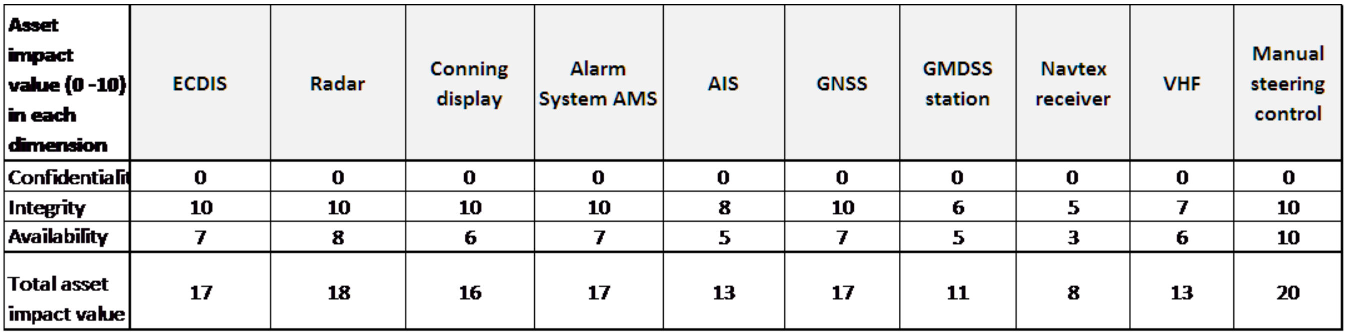


System	Integrated Bridge System									
Assets	ECDIS	Radar	Conning display	Alarm System AMS	AIS	GNSS	GMDSS station	Navtex receiver	VHF	Manual steering control
Likelihood of threat (1 to 3)	3	2	2	2	3	3	1	1	1	2
Level of asset vulnerability (1 to 3)	3	1	1	1	2	2	1	1	1	1
Likelihood of incident (1 to 9)	9	2	2	2	6	6	1	1	1	2

Determine magnitude of impact

The impact value is calculated as the loss value in case confidentiality, integrity or availability of the information that the asset relies on or the assets are compromised.

In this example, the impact on the assets due to the loss of the confidentiality, integrity or availability is assigned a value between 0 (no loss) to 10 (maximum loss). The aggregated impact value is the sum of the individual impacts on each asset.



Asset impact value (0 -10) in each dimension	ECDIS	Radar	Conning display	Alarm System AMS	AIS	GNSS	GMDSS station	Navtex receiver	VHF	Manual steering control
Confidentialit	0	0	0	0	0	0	0	0	0	0
Integrity	10	10	10	10	8	10	6	5	7	10
Availability	7	8	6	7	5	7	5	3	6	10
Total asset impact value	17	18	16	17	13	17	11	8	13	20

I have assumed null impact values in confidentiality loss. Integrity and availability loss are assigned non zero values.

Individual impact values on the assets take into account possible asset dependencies. For example, the loss of GNSS would significantly degrade the ECDIS functionality although not totally since electronic charts, route planning and Estimated Positions would still be available.

In a real case scenario, the impact evaluation should be specific to the vessel and bridge analyzed and determined with the participation of the master and officers. And the final impact values must be approved by the master of the vessel.

Determine Risk

Now we calculate the risk level for each asset and the total risk for the bridge system.

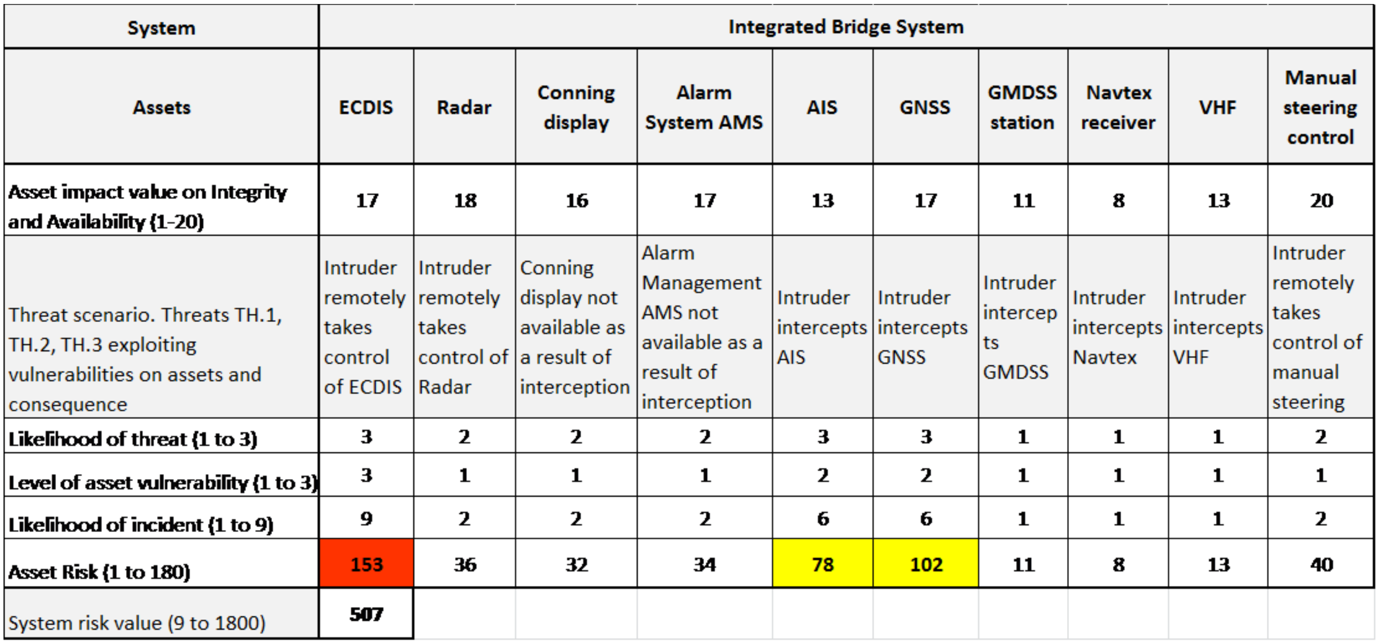
The risk level of each asset is calculated as the product of:

- Asset impact value on Integrity and Availability (2-20)
- Likelihood of incident (1 to 9)

This gives an asset risk level between 2 (lowest) and 180 (highest).

The risk level for the bridge system is calculated as the sum of the asset risk levels.

This gives a system risk level that depends on the number of assets ranging in this case from 20 (2 x 10 lowest) to 1800 (180 x 10 highest).

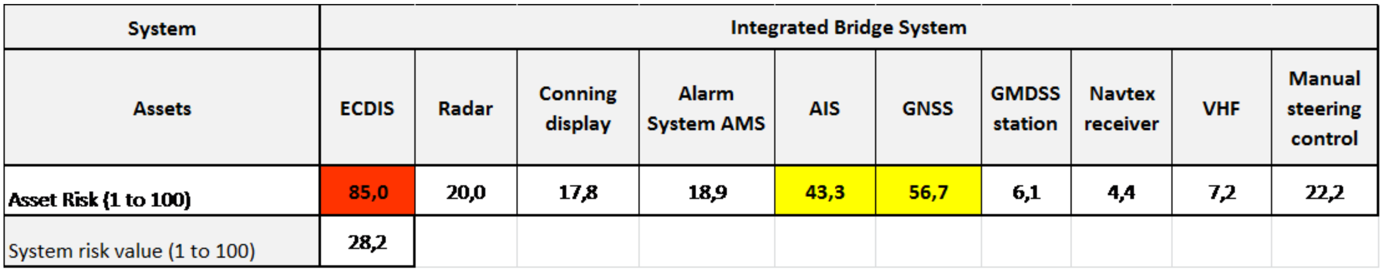


System	Integrated Bridge System									
Assets	ECDIS	Radar	Conning display	Alarm System AMS	AIS	GNSS	GMDSS station	Navtex receiver	VHF	Manual steering control
Asset impact value on Integrity and Availability (1-20)	17	18	16	17	13	17	11	8	13	20
Threat scenario. Threats TH.1, TH.2, TH.3 exploiting vulnerabilities on assets and consequence	Intruder remotely takes control of ECDIS	Intruder remotely takes control of Radar	Conning display not available as a result of interception	Alarm Management AMS not available as a result of interception	Intruder intercepts AIS	Intruder intercepts GNSS	Intruder intercepts GMDSS	Intruder intercepts Navtex	Intruder intercepts VHF	Intruder remotely takes control of manual steering
Likelihood of threat (1 to 3)	3	2	2	2	3	3	1	1	1	2
Level of asset vulnerability (1 to 3)	3	1	1	1	2	2	1	1	1	1
Likelihood of incident (1 to 9)	9	2	2	2	6	6	1	1	1	2
Asset Risk (1 to 180)	153	36	32	34	78	102	11	8	13	40
System risk value (9 to 1800)	507									

We now need to set the risk level according to the scale selected (1-100). For this we apply the following formula:

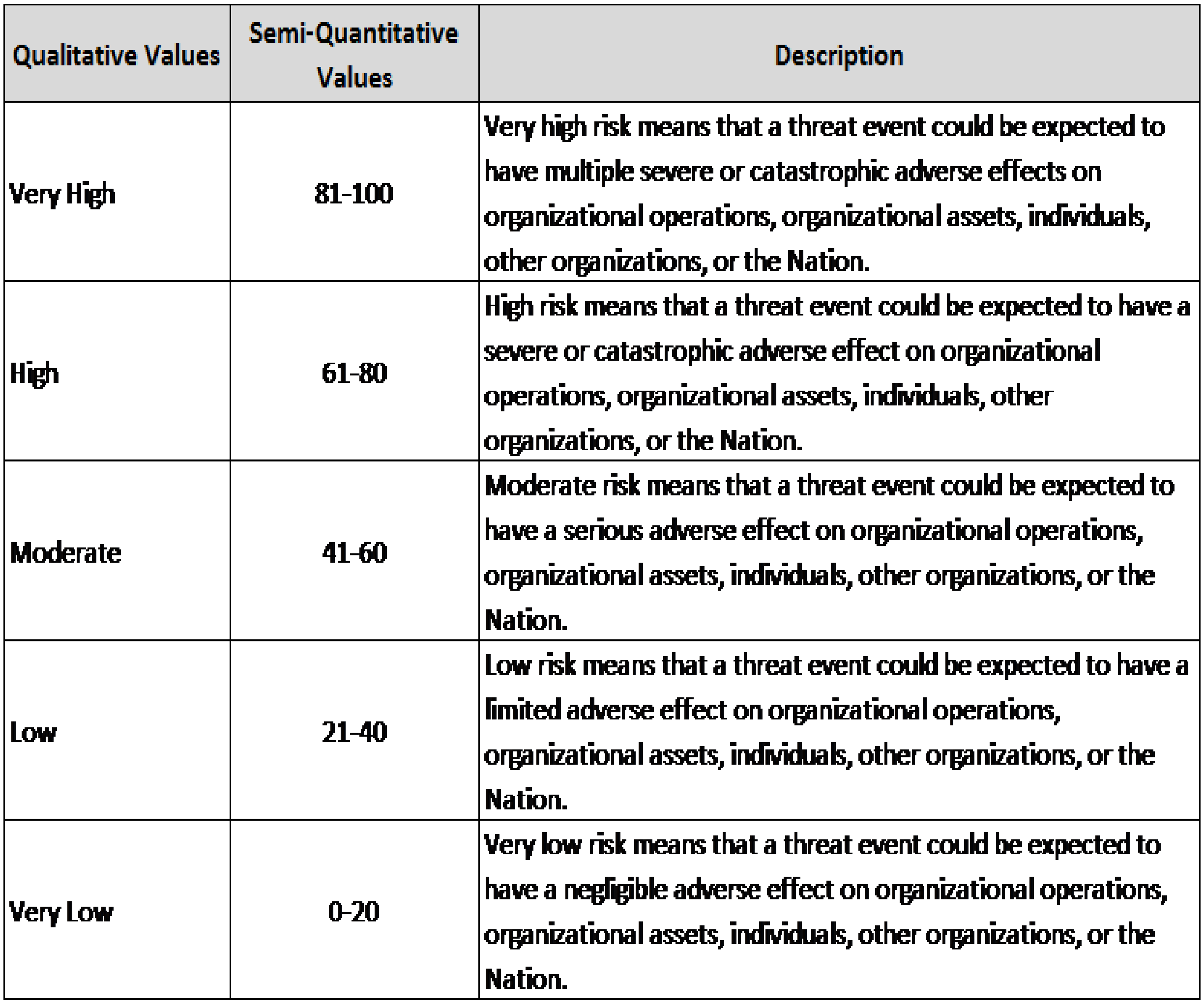
- Asset risk (1-100) = [Asset risk (2-180) /180]*100 ; with 180 being the maximum risk value of individual assets.
- System risk (1-100) = [Σ Asset risk (2-180) / 1800]*100 ; with 1800 being the maximum system risk value.

And the results of the risk analysis:



System	Integrated Bridge System									
Assets	ECDIS	Radar	Conning display	Alarm System AMS	AIS	GNSS	GMDSS station	Navtex receiver	VHF	Manual steering control
Asset Risk (1 to 100)	85,0	20,0	17,8	18,9	43,3	56,7	6,1	4,4	7,2	22,2
System risk value (1 to 100)	28,2									

For assessing risk levels we use the following table adapted with modifications from NIST SP800-30 r1. Table I-3 Assessment scale level of risk:



Qualitative Values	Semi-Quantitative Values	Description
Very High	81-100	Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	61-80	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	41-60	Moderate risk means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	21-40	Low risk means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-20	Very low risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

The organization should determine the level of acceptable risk. For this example, we have assumed that risks are unacceptable if any of these conditions apply:

- Asset risk level is greater than 40.
- System risk level is greater than 50.

In this example we see that although system risk level is acceptable, we need to manage unacceptable risk for the assets ECDIS, AIS and GNSS.

The risk calculated so far we name inherent risks. In the next step, once we managed unacceptable risks we will have new risk levels that we will name residual risks.

Communicate risk

The results are communicated to the relevant persons in the vessel and the company.

At least the Master of the vessel and the ISM designated person in the company should be informed and given recommendations on next steps to follow.

This is specially important in case a high risk situation is deemed to exist by the risk analyst.

Manage risk and implement controls

Risk management deals with the reduction of the levels of risks to acceptable levels.

Three factors determine if an attack will be successful:

- Capability of the attacker to exploit a vulnerability
- Opportunity of the attacker to take advantage of the vulnerability
- Intention and benefit of the attacker if attack is successful

We normally cannot act on the capability and intention of the attacker so we should act to reduce the probability of threats exploiting vulnerabilities and its impact.

In this example we have GNSS and AIS with moderate risk levels and ECDIS with very high risk level.

We assume that we reduce risk by defining and implementing the following controls.

To reduce the level of vulnerabilities:

- ECDIS is patched and anti-virus installed.
- Manufactures of AIS and GNSS are consulted to check any information security advisory warnings related to interception and manufacturer recommendations are applied.
- A company policy is approved to periodically check possible vulnerabilities with the manufactures of ECDIS, GNSS and AIS and apply remediation patches at the earliest possible.

With this controls applied, the new vulnerability levels are:

- ECDIS: low (1)
- AIS: low (1)
- GNSS: low (1)

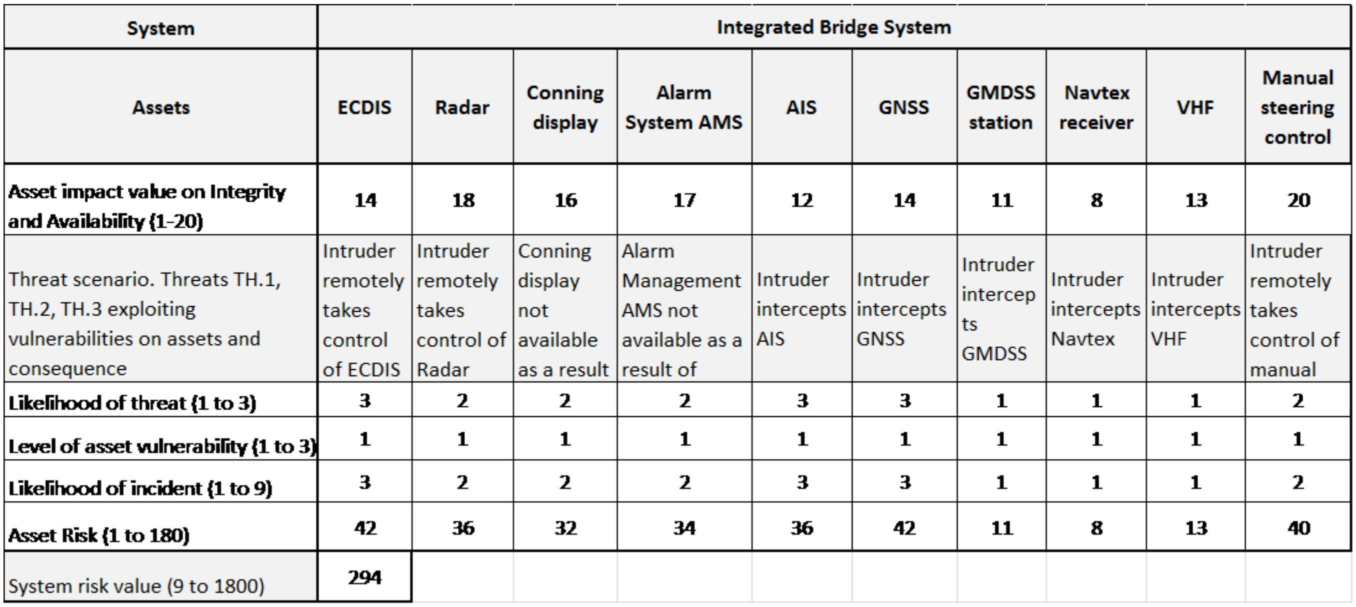
To reduce impact levels we do the following:

- The Safety Management System SMS will be updated to include detailed operational safety procedures in case ECDIS, AIS or GNSS are unavailable.
- Officers will attend a simulation course to practice operational procedures if ECDIS, AIS and GNSS become unavailable in the bridge.

With this controls applied, we reduce the impact of availability to value 4. The new asset impact levels are:

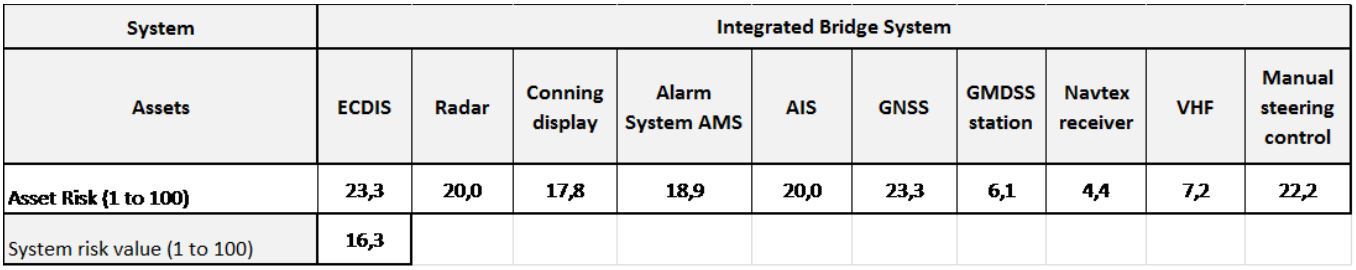
- ECDIS: 14
- AIS: 12
- GNSS: 14

And the residual risk matrix is:



System	Integrated Bridge System									
Assets	ECDIS	Radar	Conning display	Alarm System AMS	AIS	GNSS	GMDSS station	Navtex receiver	VHF	Manual steering control
Asset impact value on Integrity and Availability (1-20)	14	18	16	17	12	14	11	8	13	20
Threat scenario. Threats TH.1, TH.2, TH.3 exploiting vulnerabilities on assets and consequence	Intruder remotely takes control of ECDIS	Intruder remotely takes control of Radar	Conning display not available as a result	Alarm Management AMS not available as a result of	Intruder intercepts AIS	Intruder intercepts GNSS	Intruder intercepts GMDSS	Intruder intercepts Navtex	Intruder intercepts VHF	Intruder remotely takes control of manual
Likelihood of threat (1 to 3)	3	2	2	2	3	3	1	1	1	2
Level of asset vulnerability (1 to 3)	1	1	1	1	1	1	1	1	1	1
Likelihood of incident (1 to 9)	3	2	2	2	3	3	1	1	1	2
Asset Risk (1 to 180)	42	36	32	34	36	42	11	8	13	40
System risk value (9 to 1800)	294									

Setting the risk level according to the scale selected (1-100):



System	Integrated Bridge System									
Assets	ECDIS	Radar	Conning display	Alarm System AMS	AIS	GNSS	GMDSS station	Navtex receiver	VHF	Manual steering control
Asset Risk (1 to 100)	23,3	20,0	17,8	18,9	20,0	23,3	6,1	4,4	7,2	22,2
System risk value (1 to 100)	16,3									

The new matrix shows that asset risk levels and system risk level are now within acceptable criteria.

The results are communicated to the relevant persons in the vessel and the company. The Master of the vessel and designated person in the company should be informed and the residual risk levels or risk appetite must be approved.

Revise the analysis periodically

The vessel cybersecurity risk analysis should be performed periodically and the results communicated to the all interested parties in the vessel and the company so appropriate measures for reducing risk to acceptable levels can be applied.

Conclusion

The vessel cybersecurity risk analysis should be calculated not only for the bridge but for other relevant vessel systems like engine room, cargo control and ballast, business and auxiliary systems, social and entertainment systems.

For this example, I have used a IT risk methodology, selected a few threats and vulnerabilities and calculated results with an Excel spreadsheet.

When complex systems are analyzed or if the system under analysis is composed of many interdependent assets, it is recommended the use of an automated tool that implements a mathematical model as well as threat, vulnerability and controls catalogs. For a list of possible risk tools you can check “ENISA Risk management tools” in the references section below.

The risk analysis should be performed periodically and the results communicated adequately. The designated person and especially the Master of the vessel will normally define and approve the risk appetite. That is, the maximum level of risk that can be tolerated.

Also, the Master and company designated person should play an important role in making sure that cybersecurity risks are reduced to acceptable levels by defining and implementing cybersecurity controls.

References:

- IACS recommendation for the application of SOLAS regulation V/15 Bridge Design, Equipment Arrangement and Procedures (BDEAP) http://www.iacs.org.uk/vdguidelinesandrecommendations/rec_95_pdf688.pdf
- NIST SP800-30 Guide for conducting Risk Assessments. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- NIST SP800-39 Managing information security risks. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
- ENISA Risk management tools. http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-tools?b_start:int=0
- ISO 27000 Information security management systems, Overview and vocabulary.
- ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements.
- ISO 27002 Code of practice for information security controls.
- ISO/IEC 27005, Information technology – Security techniques – Information security risk management systems.
- ISO/IEC 31000, Risk management – Principles and guidelines.
- ISO/IEC 31010, Risk management – Risk assessment techniques.