



University  
of Glasgow

School of  
Computing Science

Supporting Competent Authorities in  
the Implementation of the NIS  
Directive for Safety-Critical Industries  
(Level M)

Email: [2393558p@student.gla.ac.uk](mailto:2393558p@student.gla.ac.uk)

RASIKA PUROHIT (2393558P)  
AKSHATA BHAT (2361611B)  
2-27-2019

Table of content:

1. Introduction.....	2
1.1 <i>The Network and Information Services</i> .....	2
1.2 <i>National Cyber Security Centre (NCSC) working with NIS</i> .....	2
1.3 <i>NIS Principles</i> .....	2
1.4 <i>Operators of essential services</i> .....	3
1.5 <i>Competent Authorities</i> .....	3
2. Department of Transport .....	4
2.1 <i>Maritime Coastguard Agency</i> .....	4
2.1.1 <i>Vessel Traffic System</i> .....	4
2.2 <i>Maritime Accident Investigation Branch</i> .....	4
3. Method.....	5
3.1 <i>Probability</i> .....	5
3.2 <i>Case study</i> .....s.....	5
3.3 <i>Fault tree analysis</i> .....	5
3.4 <i>Tool for Incident Reporting</i> .....	8
3.5 <i>Failure Mode and Effect Analysis</i> .....	11
4. Evaluation.....	13
5. Conclusion.....	13

## 1. Introduction

### 1.1 The Network and Information Systems Directive (NIS)

The Network and Information Systems Directive (NIS) equip services to the citizens; hence it is essential to take mandatory measures to guard these systems [1]. The NIS are vulnerable to cyber-attacks at a large scale and can cause major obstacles in providing and generating resources such as electricity [1]. The NIS Directive was introduced during the same time as the new General Data Protection Regulations (GDPR) were amended [1].

### 1.2 National Cyber Security Centre (NCSC) working with NIS

The National Cyber Security Centre (NCSC) bestows technical guidance by applying set of cyber security rules, supporting guidance, Cyber assessment framework (CAF) to attest appropriate conventions (good indicators) and support CA by implementing NSCS NIS rules and CAF to interpret the results) [1].

The NSCS has 3 major roles in NIS Directive [1]. They are 1. SPOC: only place where all the decisions are made 2. CSIRT: cyber cell where all the incidents are reported 3. Technical authority on cybercrime: give technical and appropriate solution [1].

### 1.3 NIS Security Principles

There are four main objectives of NIS Principles [1]. These four objectives are categorized into multiple principles [1].

#### Objective A: Managing security risk

A1. Governance	Any organization has the right to set their own security policies
A2. Risk Management	It is analysing the options and their future consequences and presenting that information in an understandable form to improve decision making.
A3. Asset management	Organizations assign weightage to their essential services, staff, software, data, records when planning risk management.
A4. Supply chain	There should be strong security contract between an organization and third-party services.

#### Objective B: Protecting against cyber attack

B1. Service protection policies and processes	All the security related policies and process should be brought into action and ways to validate them.
B2. Identity and access control	Unauthorized users should be exempted from doing certain operations
B3. Data Security	Protection of the data should be handled such that risks are also handled.
B4. System security	An organization should implement the policy and be up to date.
B5. Resilient networks and systems	Building resilience against cyber-attack.

B6. Staff awareness and training	Appropriately supporting staff to ensure they can support essential services' network and information system security
----------------------------------	---

#### Objective C: Detecting cyber security events

C1. Security Monitoring	Monitoring to detect potential security problems and track the effectiveness of existing security measures
C2. Proactive Security Event Discovery	Detecting anomalous events in relevant network and information systems.

#### Objective D: Minimising the impact of cyber security incidents

D1. Response and recovery planning	Putting suitable incident management and mitigation processes in place.
D2. Lessons learned	Learning from incidents and implementing these lessons to make a more resilient service.

### 1.4 Operators for Essential Services (OES)

Operators of essential services (OES) is a public or private body which either (a) provides alimony to essential services as defined in the NIS Directive (b) the service is built upon network and information systems and (c) the service might be affected by events involving those systems [2]. The government chooses OES based on four opinions, namely, the sector and subsector, the type of essential service and lastly the identification of service guideline [2]. Table 1 gives inference to categorization of CA

Sector	Subsector	Essential Service	Identification thresholds
Transport	Maritime		

Table 1: Operators of Essential Services example

### 1.5 Competent Authorities (CA)

The Competent Authorities (CA) are the utmost interface for Operators of Essential Services (OES) and for Digital Service Providers. There are two ways to elect a CA, 1. A single CA for an entire nation. 2. Sector wise nomination of CA [2]. The Government proposes multiple CA approach for wiser distribution of responsibilities [2]. The National Cyber Security Centre (NCSC) aid CA's with technical knowledge [2].

CA's are incumbent to (a) publish measure related to security and risk for network and information systems (b) incident management (c) decision to broadcast the incident (d) prosecute theft of identified NIS Provisions [2]. The CA's have authority to take decisions for OES under the NIS Directive. They can demand information for the security of NIS. The CA's can beseech the OES to report security concerns.

## 2. Department of Transport (DfT)

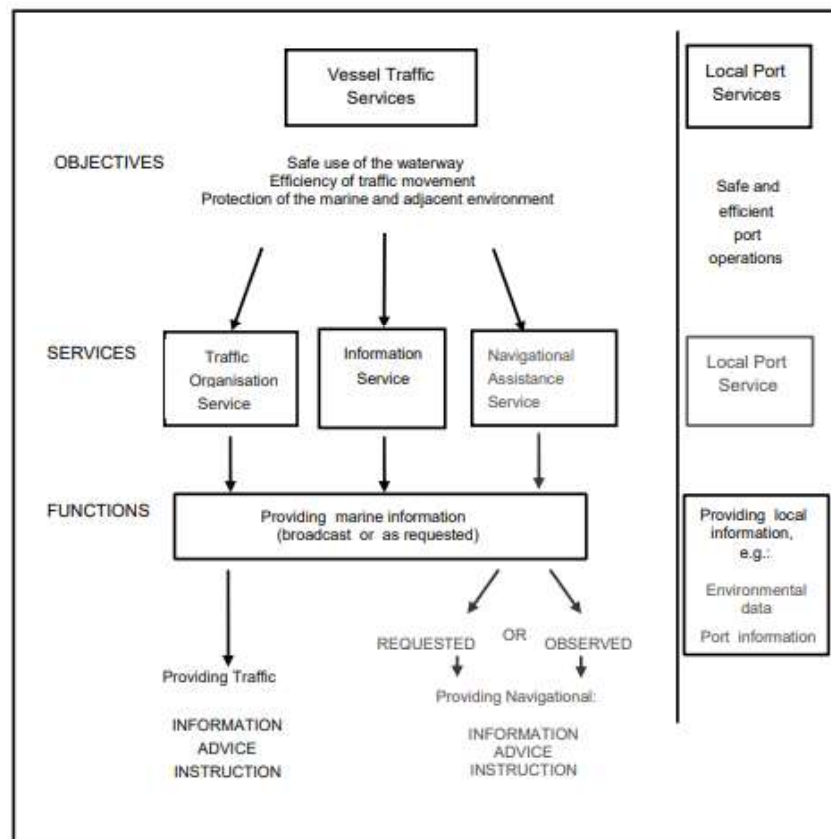
Department of Transport (DfT) is the competent authority (CA) for Maritime Transport [3]. The DfT is responsible for providing right policy, maintaining high standards for safety and security and maintaining pollution caused by transport services [3]. The main objectives and priorities of DfT is to make transport safe and secure, improve transport services and boost economy [3]. DfT has multiple agencies working under them. Maritime Transport has two agencies, namely, Maritime Coastguard Agency (MCA) and Maritime Accident Investigative Branch (MCIB) [3].

### 2.1 Maritime Coastal Agency (MCA)

Maritime Coastguard Agency is a full-time search and rescue service who are responsible for safety of all equipment's and vessels [3].

#### 2.1.1 Vessel Traffic Systems (VTS)

Maritime Coastguard Agency designates Vessel traffic systems (VTS) [3]. VTS should operate within the IALA guidelines. The following chart show function of VTS in the UK [3].



### 2.2. Maritime Accident Investigative Branch (MAIB)

Maritime Accident Investigative Branch (MCIB) carries out all the investigation of an accident. MCIB publishes report of an accident [3]. The report includes casualties, loss of ship, material loss, pollution status [3].

### 3. Method

#### 3.1 Probability

Collision risk assessment at sea is vital for maritime traffic management, crisis management and planning rescue resources and operations [4].

Product of the probability of an event (P), and the consequence (C) associated with the realization of the event [4].

$$R = P C$$

P – Collision probability, C – Consequences of collision:

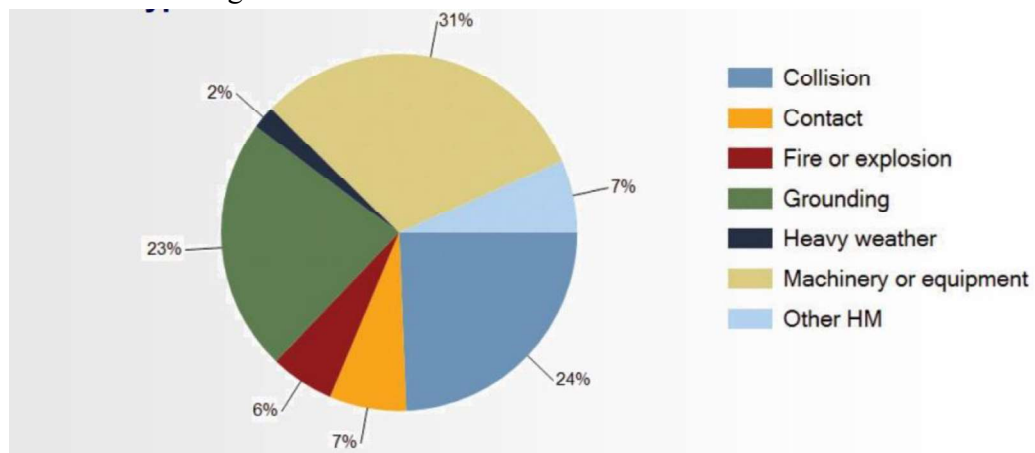
The probability of a collision is defined as

$$P = N_A P_C$$

where  $N_A$  is the number of collision candidates, i.e. ships that are in a collision course

$P_C$  is the causation probability, i.e. the probability of failing to avoid a collision when ships are on a collision course [4].

Probability and statistics can be used to assess risk, mitigate the occurrences and redefine risk assessment techniques [4]. The following is a pie chart which represents different types of ship accidents based on statistics gathered.



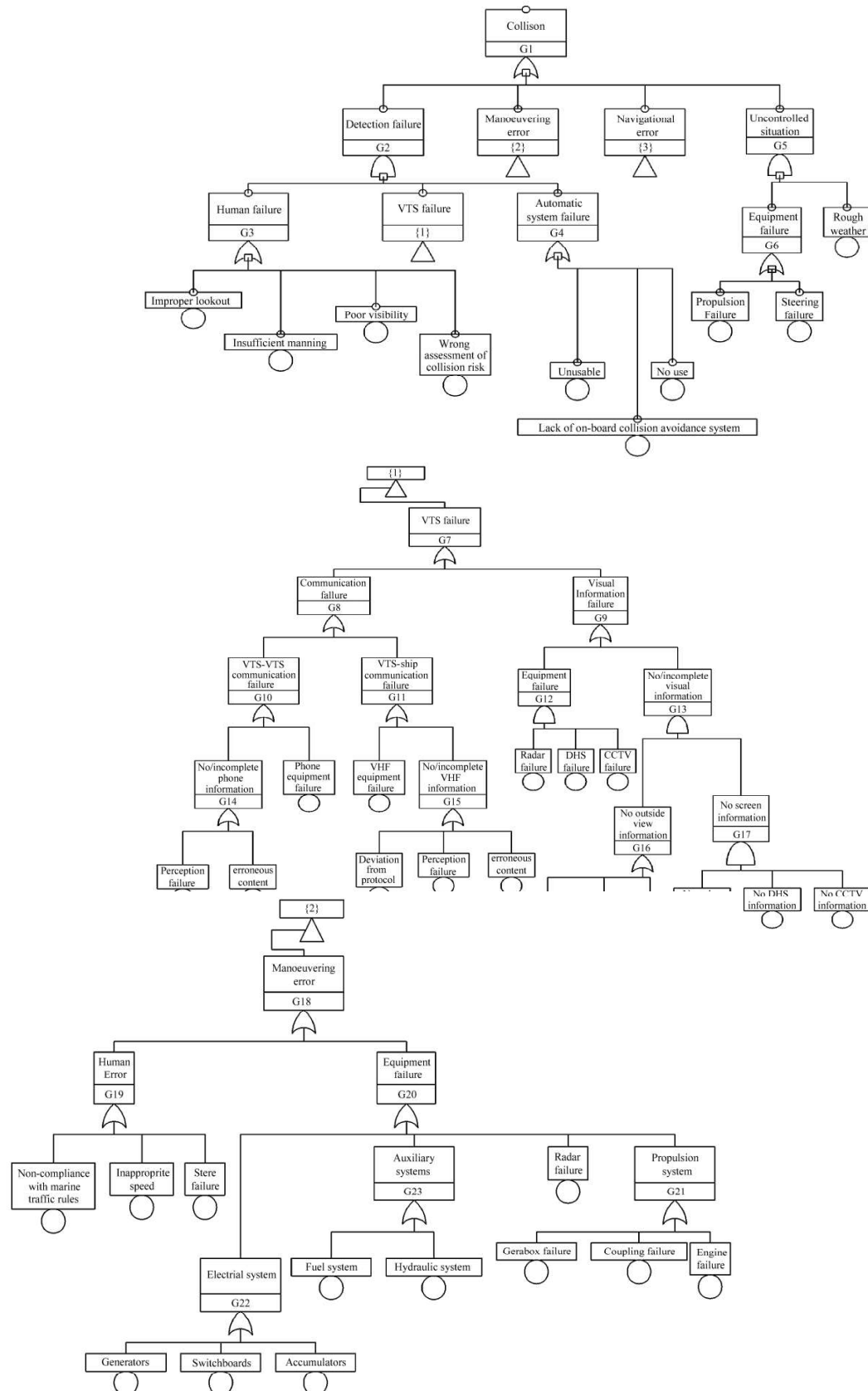
#### 3.2 Case Study

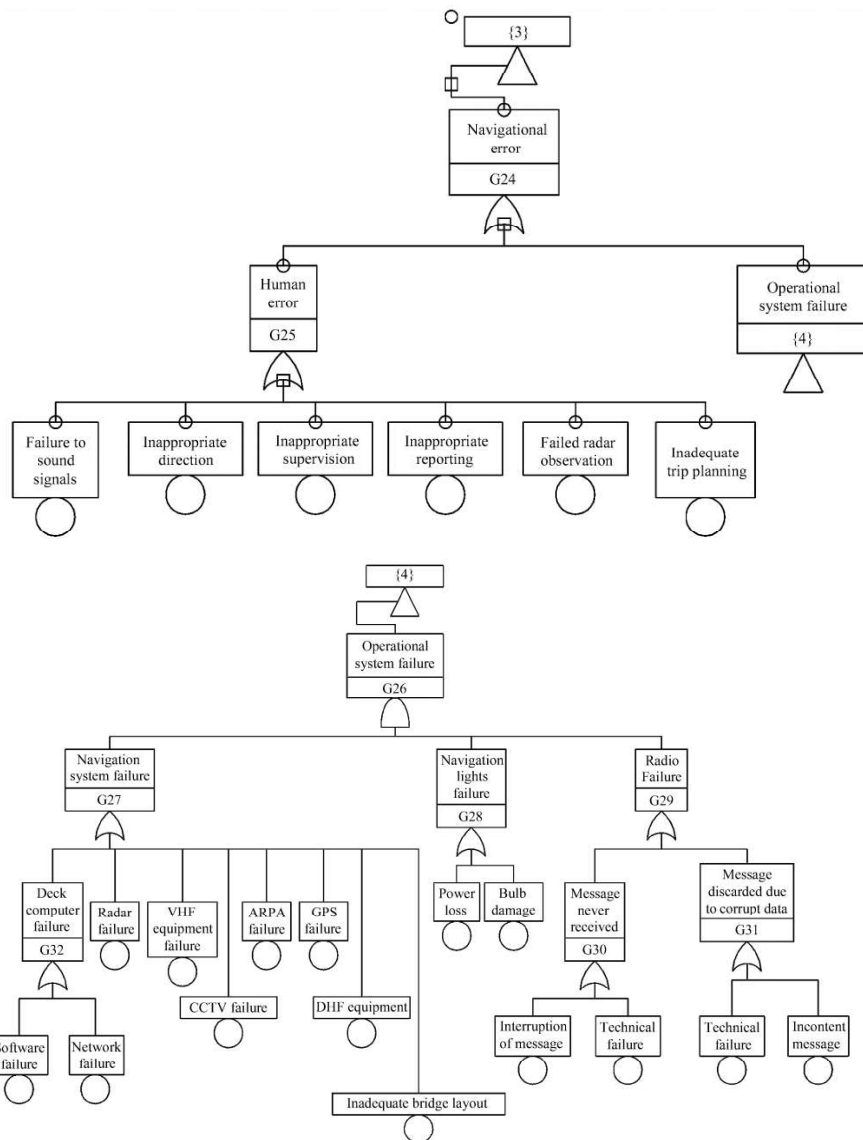
Ballano case study: Two flaws in the AmosConnect 8 web platform, which is used by staff for messaging, web browsing and other internet functions, were found [5]. The software was 10 to 15 years old [5]. The attacker gained access to ships network and gained access to database where credentials were saved in plain text. In the incident report, it was stated that, the ships software versions were degraded in order to avoid this vulnerability [5].

#### 3.3 Fault Tree Analysis (FTA)

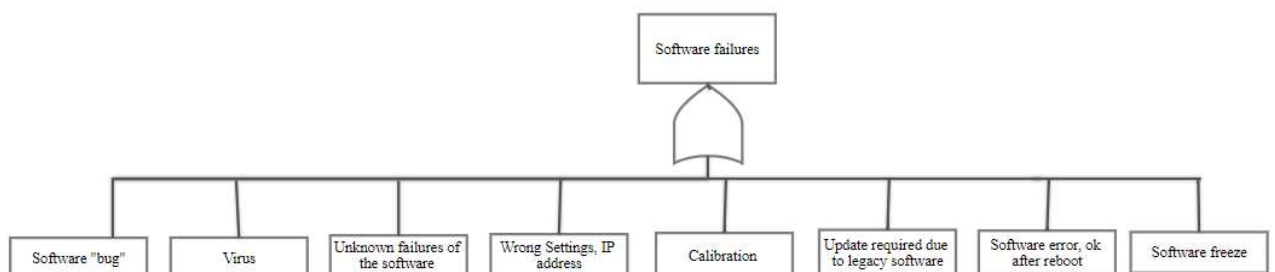
Fault Tree Analysis is used to validate whether the risk is As Low As Reasonably Practicable (ALARP) [6]. There are two main activities in FTA, namely, probability modelling and consequence modelling [6]. Probability modelling exploits FTA and reliability block diagrams [6]. It produces major event and following events which contribute for the major event [6]. The

FTA is a logical and graphical method highly used to calculate the probability of one major event or accident which takes place due to failure of other components[6]. It is a deductive approach, which is used to reach to the root of an event [6]. The following is the fault tree analysis of ship collision developed by Pedro and Carlos to evaluate ship collision.





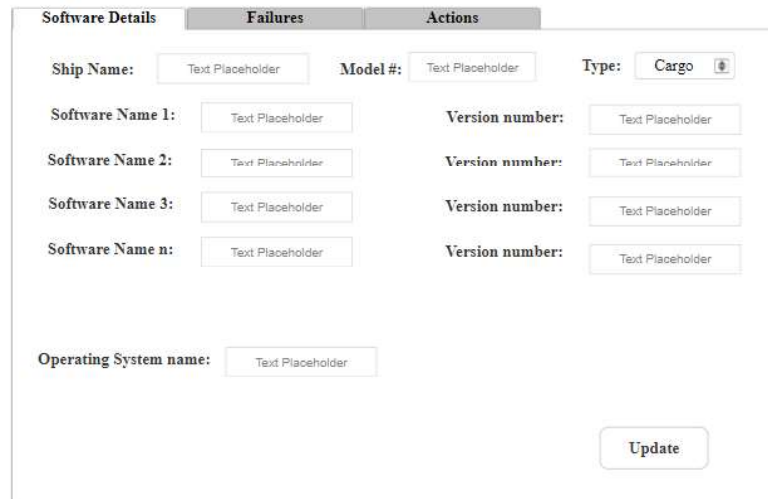
Software failure is one of the causes of ship collision. There are various advancements in types of software failures which have been not included. The following can be used as an extension to the above Fault Tree for ship collision.





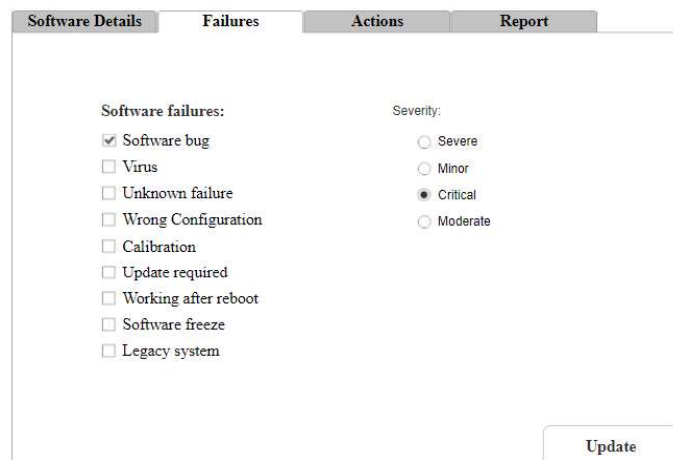
### 3.4 Tool for Incident Reporting

In this assessment, we have attempted to propose a tool. The tool will calculate risk priority number (RPN) for ship collision based on statistics available for ship collisions led by software failures. The first part of the tool report and analyses the software installed for the ship.



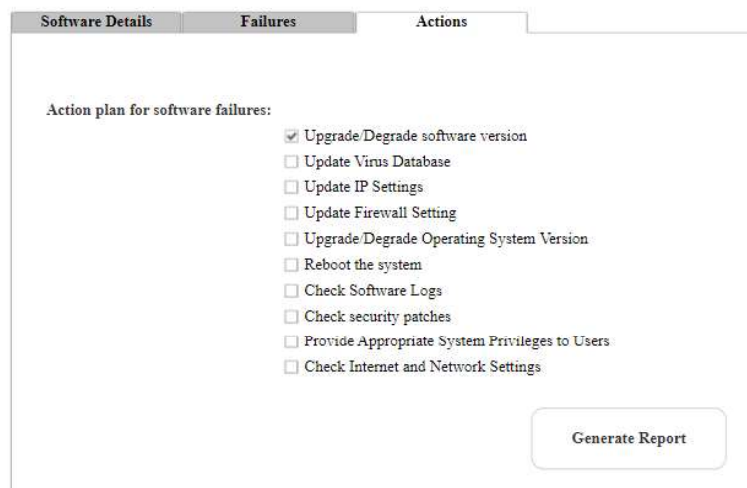
The 'Software Details' form is part of a tabbed interface with 'Failures' and 'Actions' tabs. It contains several input fields: 'Ship Name' (Text Placeholder), 'Model #' (Text Placeholder), 'Type' (a dropdown menu currently showing 'Cargo'), 'Software Name 1' (Text Placeholder), 'Version number' (Text Placeholder), 'Software Name 2' (Text Placeholder), 'Version number' (Text Placeholder), 'Software Name 3' (Text Placeholder), 'Version number' (Text Placeholder), 'Software Name n' (Text Placeholder), 'Version number' (Text Placeholder), and 'Operating System name' (Text Placeholder). An 'Update' button is located at the bottom right of the form.

Failures are the defects incurred and the severity is the level of impact the failure has caused.



The 'Failures' form is part of a tabbed interface with 'Software Details', 'Actions', and 'Report' tabs. It features two sections: 'Software failures' with a list of checkboxes including 'Software bug' (checked), 'Virus', 'Unknown failure', 'Wrong Configuration', 'Calibration', 'Update required', 'Working after reboot', 'Software freeze', and 'Legacy system'; and 'Severity' with radio buttons for 'Severe', 'Minor', 'Critical' (selected), and 'Moderate'. An 'Update' button is positioned at the bottom right.

Actions are the proposed methods to combat the failures incurred.



The 'Actions' form is part of a tabbed interface with 'Software Details' and 'Failures' tabs. It contains an 'Action plan for software failures' section with a list of checkboxes: 'Upgrade/Degrade software version' (checked), 'Update Virus Database', 'Update IP Settings', 'Update Firewall Setting', 'Upgrade/Degrade Operating System Version', 'Reboot the system', 'Check Software Logs', 'Check security patches', 'Provide Appropriate System Privileges to Users', and 'Check Internet and Network Settings'. A 'Generate Report' button is located at the bottom right.

Software Details		Failures		Actions		Report		
Vessel Software Report								
Date	Ship Type	Software Name	Software Version	Last Patch Update	Primary Cause	Impact Level	Action	Status
Nov 2016	Cargo	AmmosConnect	8	October 2016	Software bug	Major	Degrade Software version	In Progress

Download Report

The tool will then ask the information regarding the hardware damages occurred due to failure.

Ship Details		Failures		Actions		Report	
Ship Name:	Text Placeholder						
Ship type:	Text Placeholder						
Ship Model Number:	Text Placeholder						
Ship Size	Length	Width	Height				
Ship Weight:	Text Placeholder						
Ship Speed:	Text Placeholder						
Location:	To	From					

Update

The tool, considering the fault tree analysis for ship collision, will accept the category and sub category(s) as the reason to failure, also it will accept the impact level to calculate the risks.

Ship Details		Failures		Actions		Report	
◀ 183 ▶							
Collision Cause		▼					
Manoeuvring error		▲					
Navigational error		▲					
Uncontrolled situation		▼					
Detection failure							
Subcategory		▼					
Equipment failure							
Rough weather							
Error code		▼					
Propulsion Failure							
Steering failure							
		Impact Level:		<input checked="" type="radio"/> Severe <input type="radio"/> Minor <input type="radio"/> Moderate <input type="radio"/> Critical			

Update

The Action is a list which describes efforts taken to mitigate the failure. The Report tab produces informative report.

Ship Details
Failures
Actions
Report

Action plan for Hardware failure:

- ☐ Obtain the logs
- ☒ Send distress signals
- ☐ Repair/Replace damaged parts
- ☒ Check the alarms
- ☐ Check for spills

Update

Ship Details
Failures
Actions
Report

				Vessel Collision Report			
Date	Location	Ship Type	Operating Circumstances	Primary Cause	Impact Point	Action	Status
Nov 2016	Northern	Cargo	Cargo Transfer	Equipment failure - Electrical Error	Minor	Replaced	Fixed
Feb 2019	Southern	Carrier	Bunkering Operations	Uncontrolled situation - rough weather	Moderate	Dent being fixed	In progress

Download Report

Ship Details
Failures
Actions
Report
Risk Assessment

Failure Type Text Placeholder

Number of occurrences by Severity

Incident Occurrence by Severity			
Minor	Moderate	Severe	Critical
No of occurrences	No of occurrences	No of occurrences	No of occurrences

Likelihood of Detection Text Placeholder

Risk Priority Number Severity \* Occurrence \* Detection

Calculate

Risk assessment tab will calculate the Risk Priority Number (RPN) which will be used to define the Severity Impact level.

### 3.5 Failure Mode and Effect Analysis

Risk Priority Number (RPN) is used to assess risk and help identify critical failure modes. It ranges from 1 to 1000 [4]

$$\begin{aligned} & \blacksquare \text{ Severity (S)} \\ & \blacksquare \text{ Severity X Occurrence (S X O)} \\ & \quad \text{– Criticality} \\ & \blacksquare \text{ Severity X Occurrence X Detection} \\ & \quad \text{(S X O X D) = RPN} \end{aligned}$$

Severity (S) - Severity is the effect which failure has on the system [4].

Occurrence (O) - Occurrence is, number of times, the risk is likely to occur [4].

Detection (D) - Detection is the impact of design control systems to mitigate the chances of failure [4].

The following table is the demonstration of a traditional FMEA for a fishing vessel. The table includes, description of the failure and calculated RPN based on S, O and D. The risk with higher RPN should be given priority to lower the risk i.e. RPN [4].

Descrip.	Comp.	Failure mode	Failure effect (system)	Failure effect (vessel)	Alarm	Provision	$S_f$	S	$S_d$	RPN
Structure	Rudder bearing	Seizure	Rudder jam	No steering ctrl	No	Stop vessel	1	8	3	24
Structure	Rudder bearing	Breakage	Rudder loose	Reduced steering ctrl	No	Stop vessel	1	8	3	24
Structure	Rudder structure	Structural failure	Function loss	Reduced steering	No	Use beams	2	8	4	64
Propulsion	Main engine	Loss of output	Loss of thrust	Loss of speed	Yes	None	8	8	5	320
Propulsion	Main engine	Auto shutdown	M/E stops	Loss of speed	Yes	Anchor	6	8	6	288
Propulsion	Shaft & propeller	Shaft breakage	Loss of thrust	Loss of speed	No	Anchor	2	8	1	16
Propulsion	Shaft & propeller	Shaft seizure	Loss of thrust	Loss of speed	Yes	Anchor	2	9	2	36
Propulsion	Shaft & propeller	Gearbox seizure	Loss of thrust	Loss of speed	Yes	Anchor	1	4	3	12
Propulsion	Shaft & propeller	Hydraulic failure	Cannot reduce thrust	Cannot reduce speed	No	Anchor	3	2	3	18
Propulsion	Shaft & propeller	Prop. blade failure	Loss of thrust	Loss of speed	No	Slow steaming	1	2	4	8
Air services	Air receiver	No start air press.	Cannot start M/E	No propulsion	Yes	Recharge receiver	4	2	3	24
Electrical sys.	Power generation	Generator fail	No elec. power	Some system failures	Yes	Use st-by generators	9	3	7	189
Electrical sys.	Main switch board	Complete loss	Loss of main supply	No battery charging	Yes	Use emergency 24 V	8	3	6	144
Electrical sys.	Emer. S/B	Complete loss	Loss of emer. supp.	No emergency supp.	No	Use normal supply	3	7	4	84
Electrical sys.	Main batteries	Loss of output	Loss of main 24 V	Loss of main low volt	Yes	Use emergency 24 V	3	3	4	36
Electrical sys.	Emer. batteries	Loss of output	Loss of emer. supp.	No emer. supp.	No	Use normal supply	1	8	3	24
Auxiliary sys.	Fuel system	Contamination	M/E and gen. stop	Vessels stops	Yes	Anchor	4	8	5	160
Auxiliary sys.	Fuel system	No fuel to M/E	M/E stops	Vessel stops	No	Anchor	2	7	7	98
Auxiliary sys.	Water system	No cooling water	Engine overheat	M/E auto cut-out	Yes	Use st-by pump	7	2	4	56
Auxiliary sys.	Hydraulic	System loss	No hydraulics	No steering	Yes	Stop vessel	9	8	9	648
Auxiliary sys.	Lube oil system	Loss of pressure	Low pressure cut-off	M/E stops	Yes	Use st-by pump	9	3	6	162

The following is one of the methods to calculate probability using available data.

Table 3. Collision probability based on AIS data at 02.00h

Node	Nm	Ni	$\mu_c$	Dc(m)	L(m)	B(m)	T	Pc	Pan	Pa	Class
1 Ship Head on	12	0.0115287	0.000015				1	0.000015	1.729E-07		
2 Ship Overtaking	15	0.0144108	0.000015	24688	264	32	1	0.000015	2.162E-07	0.0159154	Occasional
3 Ship Crossing	36	0.0951823	0.000015				1	0.000015	1.428E-06		
Total Number of Ship 63									1.817E-06		

Using the probability calculated on the basis of present data the following risk matrix can be generated.

	1	2	3	4	5
A	N	N	N	N	T
B	N	N	N	T	T
C	N	N	T	T(H,C)	I
D	N	T	T	I	I(O)
E	T	T	I	I	I

Figure 4. Risk matrix based on AIS data at 02:00

Based on the tool we proposed, the following matrix can be generated to calculate the severity impact level.

		Severity			
		minor	moderate	severe	critical
Occurance	High				
	Moderate				
	Low				
	Remote				

#### **4. Evaluation**

The tool tries to evaluate risks using Fault tree analysis and FME. According to suggestions we received from fellow classmates/examiners the tool is a minimalist approach towards diminishing the risks which leads to failures. Due to lack of actual data and statistic, since it is not available on public domains, there is a lack of actual probability and statistics. The tool can help evaluate the prime concerns for a selected ship/model.

#### **5. Conclusion**

The NIS has provided certain range of rules to cover cyber security domain for the safety systems [1]. Fault trees and FMEA are convenient methods to carry out risk analysis. Although in our approach, there is a lack of ideal format and data, the tool will help minimize the risk and help the authorities to focus on prime concerns which lead to failures.

#### References:

1. National Cyber Security Center. 2018. Created on 28 Jan 2018  
<https://www.ncsc.gov.uk/guidance/introduction-nis-directive>
2. Security of Network and Information Systems Public Consultation. 2017. FROM  
[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/636207/NIS\\_Directive\\_-\\_Public\\_Consultation\\_\\_1\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf)
3. Department of Transport. From  
<https://www.gov.uk/government/organisations/department-for-transport>
4. FMEA RPN. 2006. From <http://www.fmea-fmeqa.com/fmea-rpn.html>
5. A bug in a popular maritime platform left ships exposed. 2017 from  
<https://www.wired.com/story/bug-in-popular-maritime-platform-isnt-getting-fixed/>
6. Pedro Antão Carlos Guedes. 2006. Fault-tree models of accident scenarios of RoPax vessels.