AFRL-RY-WP-TR-2014-0251

ESTABLISHING AND MAINTAINING TRUST FOR AN AIRBORNE NETWORK

Search and Rescue Enterprise: Security Assessment Report

Djenana Campara

KDM Analytics Inc.

DECEMBER 2014
Final Report

THIS IS A SMALL BUSINESS INNOVATION RESEARCH (SBIR) PHASE II REPORT.

AIR FORCE RESEARCH LABORATORY
SENSORS DIRECTORATE
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433-7320
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the USAF 88th Air Base Wing (88 ABW) Public Affairs Office (PAO) and is available to the general public, including foreign nationals.

Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RY-WP-TR-2014-0251 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH THE ASSIGNED DISTRIBUTION STATEMENT.

*//signature//

KENNETH LITTLEJOHN, PM
Avionics Vulnerability Mitigation Branch

//signature//

DAVID G. HAGSTROM, Chief
Avionics Vulnerability Mitigation Branch

//signature//

TODD A. KASTLE, Chief
Spectrum Warfare Division

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

*Disseminated copies will show "//signature//" stamped or typed above the signature blocks.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
December 2014	Final	30 April 2012 - 28 April 2014

4. TITLE AND SUBTITLE
ESTABLISHING AND MAINTAINING TRUST FOR AN AIRBORNE NETWORK
Search And Rescue Enterprise: Security Assessment Report

5a. CONTRACT NUMBER
FA8650-12-C-1345

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
62204F

6. AUTHOR(S)
Djenana Campara

5d. PROJECT NUMBER
3005

5e. TASK NUMBER
14

5f. WORK UNIT NUMBER
Y0NN

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
KDM Analytics Inc.
1101 Pennsylvania Ave. NW
Suite 600
Washington, DC 20004

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
Sensors Directorate
Wright-Patterson Air Force Base, OH 45433-7320
Air Force Materiel Command
United States Air Force

10. SPONSORING/MONITORING AGENCY ACRONYM(S)
AFRL/RYWA

11. SPONSORING/MONITORING AGENCY REPORT NUMBER(S)
AFRL-RY-WP-TR-2014-0251

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited.

13. SUPPLEMENTARY NOTES
This is a Small Business Innovation Research (SBIR) Phase II report. SBIR data rights have been waived by contractor. Letter on file. PAO Case Number: 88ABW-2014-5093, cleared 04 November 2014. See also AFRL-RY-WP-TR-2014-0159. Report contains color.

14. ABSTRACT

This report was developed under a SBIR contract for topic AF103-165.
This report describes the results a security assessment conducted on the Search and Rescue (SAR) enterprise. The purpose of the security assessment is to identify the operational risks to the SAR enterprise. In particular, those resulting from cyber attacks, identify the corresponding vulnerabilities, assess the criticality of the components, and recommend mitigations. SAR case study is a comprehensive illustration to the Department of Defense Architecture Framework (DoDAF) published as part of the international standard UML Profile for DoDAF and MoDAF (UPDM) by the Object Management Group (OMG). For the purposes of this assessment, the SAR is defined by International Aeronautical and Maritime Search and Rescue Manual (IAMSAR) and Canadian National Search and Rescue Manual. The security assessment described herein was one part of an overall project to develop a generic methodology and technology framework for computing a trustworthiness index (TI). A TI is a measure of confidence that risk is low in a claim about a system component supporting mission objectives.

15. SUBJECT TERMS
SBIR Report, risk analysis, trustworthiness, mission assurance, DoDAF, MoDAF, structured assurance case metamodel, object management group

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT:	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON (Monitor)
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kenneth Littlejohn
Unclassified	Unclassified	Unclassified	SAR	116	19b. TELEPHONE NUMBER *(Include Area Code)* (937) 528-8142

MITCHELL, LOLITA V CIV USAF AFMC AFRL/RYOX

To: MITCHELL, LOLITA V CIV USAF AFMC AFRL/RYOX
Subject: FW: Final Report Change - Search and Rescue Security Assessment

From: J M Schlesselman [mailto:joe@rti.com]
Sent: Wednesday, November 19, 2014 1:16 PM
To: Djenana Campara; LITTLEJOHN, KENNETH CIV USAF AFMC AFRL/RYWA
Cc: Nikolai Mansourov; Rajive Joshi
Subject: RE: Final Report Change - Search and Rescue Security Assessment

Yes, Real-Time Innovations, Inc. concurs with the language below.

Joe Schlesselman

-----Original Message-----
From: Djenana Campara [mailto:djenana@kdmanalytics.com]
Sent: Wednesday, November 19, 2014 7:56 AM
To: LITTLEJOHN, KENNETH CIV USAF AFMC AFRL/RYWA; J M Schlesselman
Cc: Nikolai Mansourov; Rajive Joshi
Subject: Re: Final Report Change - Search and Rescue Security Assessment

Yes from KDM Analytics.

Best regards,
Djenana

On 2014-11-19, 10:45 AM, "LITTLEJOHN, KENNETH CIV USAF AFMC AFRL/RYWA"
<kenneth.littlejohn@us.af.mil> wrote:
Joe / Djenana,

Based on your respective concurrence, is the draft language I provided acceptable to both of you? If so, please concur.

Thanks,

Kenny

"Dear Mr. Littlejohn,

Real-Time Innovations Inc (RTI), together with KDM Analytics, hereby waives its SBIR Data Rights to all contents of the document, "Establishing and Maintaining Trust for an Airborne Network, Search and Rescue Enterprise: Security Assessment Report" for subject contract FA8650-12-C-1345. The Government is granted an unlimited nonexclusive license to use, modify, reproduce, release, perform, and display or disclose this report and the data contained herein."

Rajive Joshi
Real-Time Innovations

Djenana Campara
KDM Analytics

Table of Contents

List of Tables

Section 1

Introduction

This document describes the results a security assessment conducted on the Search and Rescue (SAR) enterprise. The purpose of the assessment is to identify the operational risks to the SAR enterprise in particular those resulting from cyber attacks, identify the corresponding vulnerabilities, assess the criticality of the components and recommend mitigations.

1.1 Background

Search and Rescue (SAR) case study is a comprehensive illustration to the Department of Defense Architecture Framework (DoDAF) published as part of the international standard UML Profile for DoDAF and MoDAF (UPDM) by the Object Management Group (OMG). For the purposes of this assessment, the Search and Rescue is defined by International Aeronautical and Maritime Search and Rescue Manual (IAMSAR) and Canadian National Search and Rescue Manual.

1.2 Purpose

The goal of this assessment is to understand the security posture of the Search and Rescue (SAR) Enterprise. Security posture needs to be clearly stated to system management to ensure acceptance and support of the security program and the compliance with the C&A activities.

This assessment may be used by the C&A Authority, as part of the C&A process, to validate the deployment of the system and to ensure that the security and services of the system do not affect the overall risk rating.

This assessment will provide Senior Management with the security information with which to base informed risk management decisions. This assessment, along with its associated C&A documentation, will contribute to the level of assurance and due diligence being applied to the systems planning, implementation, and operational life-cycle. The assessment may be used as a basis for developing a security policy adapted to the needs of an organization.

1.3 Scope and Assumptions

Security posture of the SAR enterprise is determined by the operational risks originating from the external threats within the intended operational environment, as well as internal threats originating from failures and breakdowns in systems, people and procedures, as well as deliberate malicious activities by the internal threat actors. The purpose of the assessment is to systematically identify all operational risks to the SAR enterprise and identify the corresponding vulnerabilities, in order to identify the critical components. The systematic risk framework for the SAR enterprise is then used to evaluate the overall security posture of the SAR enterprise, and the overall risk of the SAR enterprise. The risk framework is also used to suggest mitigations to reduce the level of risk.

1.3.1 Scope

Operational risks are situations having a negative impact on the organization due to uncertainties related to possible breakdowns in a system or its environment via supply chain, injury to a person or failure of a process resulting from intentional/malicious as well as unintentional/natural operational threats. One of the main impacts of operational risks is inability to conduct operations as planned.

Operational risks involve the uncertainties an organization undertakes when it attempts to operate within a given field or industry. Operational risks are the risks that are not inherent in systemic, financial or market risk. It is the risk remaining after determining systemic, financing and market risk.

The assessment will consist of the following:

- System description from the operational perspective
- A list of assets, including information assets, tangible and intangible assets
- A list of undesired events capturing a statement of sensitivity including impact assessments
- A list of threat scenarios capturing threat analysis
- Risk identification and assessment
- Safeguard analysis
- Vulnerability analysis
- List of recommendations to mitigate the residual risk to the targeted level of risk
- Evidence analysis including identification of vulnerabilities and safeguard effectiveness

1.3.2 Assumptions

This assessment is based upon a snapshot of the current security baseline. The following assumptions have been made in the course of this assessment:

- Medium sensitivity to the confidentiality of the information items
- the scope of the assessment includes physical security situations, safety incidents and cyber attacks
- of particular interest is the identification of cyber attacks that cause physical impacts
- it is outside of the scope of the assessment to perform assessment of mitigation options
- it is outside of the scope of the assessment to recommend complete mitigation options

1.3.3 Methodology

This assessment follows the Fact-Oriented Repeatable Security Assessment (FORSA) methodology developed by KDM Analytics. FORSA methodology is based on Canadian Harmonized Threat and Risk Assessment Methodology (HTRA) and EBIOS (*Expression des besoins et identification des objectifs de sécurité*) Information System Security Risk Assessment methodology. Both methodologies allow systematic identification, assessment and evaluation of risks to systems security, and may be used as a basis for developing a security policy adapted to the needs of an organization.

1.3.4 Information Gathering

This assessment has been developed as an illustration of the systematic risk assessment methodology that uses DoDAF model as the primary input. Any information gathering activities have been restricted to analyzing the input DoDAF model and, whenever was necessary, consulting the Search and Rescue Manuals. SAR DoDAF model and documentation was reviewed to capture an initial baseline of the security requirements, sensitive assets, threats, vulnerabilities and concerns. The intermediate and final results of the assessment have not been validated by the operators, administrative personnel and stakeholders of the SAR Enterprise.

Section 2

Executive Summary

A security assessment was conducted on the Search and Rescue (SAR) enterprise using the reference DoDAF model available as Appendix 1 to the OMG specification "UML Profile for DoDAF and MoDAF" (UPDM).

The mission of the SAR enterprise comprises the search for, and provision of aid to, persons, ships or other craft which are, or are feared to be, in distress or imminent danger. In order to fulfil this mission the combined facilities, equipment and procedures are established in each search and rescue region to provide the response to search and rescue incidents.

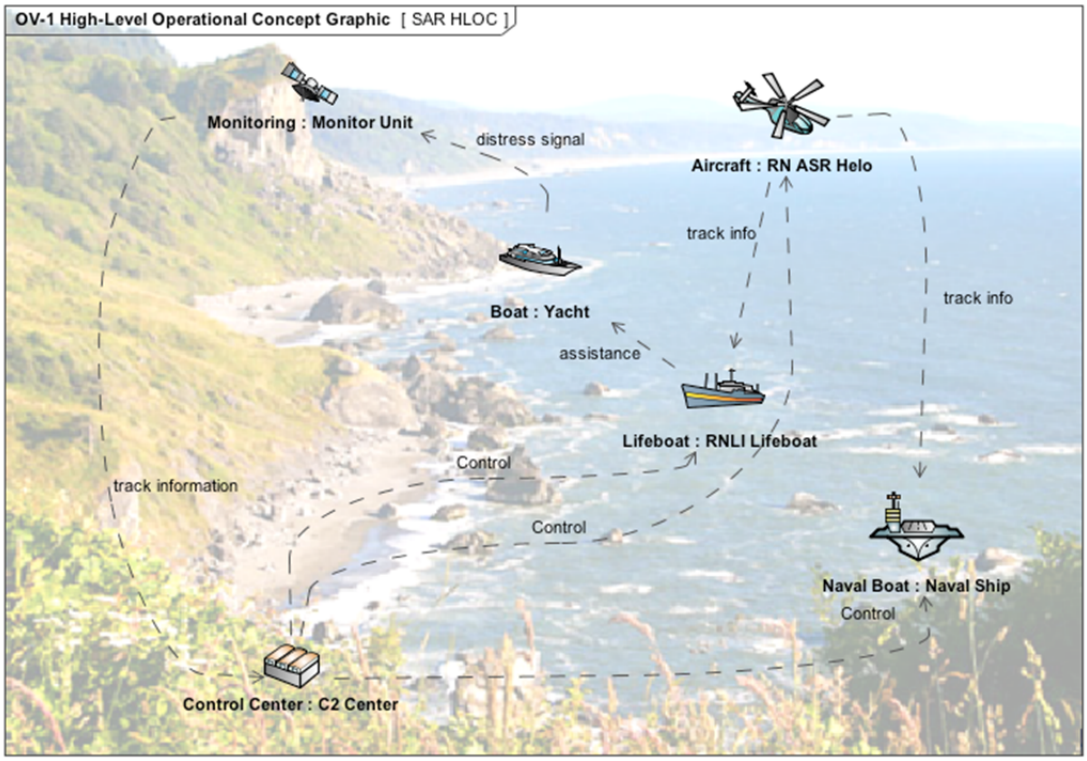

Figure 1. High Level Operational Graphic for the SAR Enterprise

The search and rescue (SAR) objective is to prevent loss of life and injury through search and rescue alerting, responding and aiding activities using public and private resources. Where possible and when directly related thereto, reasonable efforts will be made to minimize damage to or loss of property.

This section provides the key security findings of the security assessment report.

2.1 Overall Risk

The overall risk of the SAR Enterprise is **High**. We have identified 55 risk groups. 7 risks are of High level. Our quantitative risk evaluation ranks the risk of the SAR Enterprise at 254.602 or 0.960064 when normalized into the range of [0..1]. Our analysis shows a single largest risk of catastrophic damage to the person in distress. This risk can occur due to a number of threat scenarios, which involve a combination of a catastrophic of critical failure of the person in distress and a full or partial inability to complete the SAR operation, for example, due to a missed distress signal, failures of the performers involved in the SAR operation, and other situations. We have identified 122 individual threat events and constructed full fault trees for the SAR Enterprise, which correspond to 475 individual threat scenarios. Our analysis indicates that most of the risk to the SAR Enterprise is for natural sources and operator errors. However, we have identified and analyzed several important cyber attack scenarios that also contribute to the overall risk. We performed the criticality analysis of the SAR performers and prioritized them based on their contribution to the overall risk

2.2 Assessment Highlights

- The overall risk of the SAR Enterprise is High
- We have identified 55 risk groups, 7 of them are High, 18 are Serious, 27 are Marginable and 3 are Negligible. Risk categories are based on MIL-STD-882D
- Assessment was based on the formal DoDAF model of the SAR enterprise. The model was captured using NoMagic Cameo Enterprise Architect and saved in standard-compliance UPDM XML format.
- Automated tool Blade Risk Manger developed by KDM Analytics were used to analyze the input DoDAF model to understand its completeness and suitability for automated risk analysis (DoDAF Analytics to validate and certify that the input model provides a coherent operational description and adequately represents causal relationships between operational elements). Blade Risk Manager used the machine-readable format of the DoDAF model to extract the operational elements and build a risk model of the SAR Enterprise. Manual input was used to adjust the likelihoods and severities of the risk elements. Automated tools collected risk metrics and analytics based on the risk model and automatically generated report. The report was further enhanced manually.
- 122 threat events were considered, covering all 6 key performers of the SAR Enterprise. 20 different threat sources were identified.
- The undesired events corresponding to security risks were identified, and full fault tree constructed, linking them to threat events. This resulted in 475 threat scenarios analyzed by the automated tools.

2.3 Summary of Identified Risks

Specific findings related to threat assessment, vulnerability analysis, and risk assessment are captured in dedicated report sections. The following table captures the identified "High" risks for the SAR enterprise.

Table 1: Top Identified Risks

Identified Risk	Risk Level	Likelihood	Severity	Risk
Catastrophic damage to person in distress	High	Frequent	Catastrophic	149.6
Partial loss of capability to rescue	High	Frequent	Critical	14.9
Critical damage to person in distress	High	Frequent-Probable	Critical	10.6
Partial loss of capability to monitor	High	Probable	Critical	10.3
Critical loss of SAR resources	High	Probable	Critical	9.8
Full loss of capability to rescue	High	Probable	Critical-Catastrophic	9.0
Full loss of capability to search	High	Probable	Critical-Catastrophic	8.0

2.4 Summary of the Recommendations

The recommendations presented in this report are intended to provide a course of action to directly mitigate the identified risks by improving the security posture of the system. Recognizing that no environment is completely risk free, implementation of these recommendations will provide the capability to minimize the exposure to the risk and reduce the vulnerabilities, achieving the targeted level of residual risk of

This section is out of the project's scope.

Section 3

System Description

This section defines the system, its boundaries and its operating environment. The definition of the capabilities of the system and its operations is the starting point for gathering the critical assets and identifying the risk to the operations of the system.

3.1 Concept of Operations

This Security Concept of Operations (Con Ops) presents an overall description of the system under assessment emphasizing the system's security considerations and its environment. The mission of the SAR enterprise comprises the search for, and provision of aid to, persons, ships or other craft which are, or are feared to be, in distress or imminent danger. In order to fulfil this mission the combined facilities, equipment and procedures are established in each search and rescue region to provide the response to search and rescue incidents.

The high-level operational graphic for the SAR Enterprise is presented at Figure 1.

The search and rescue (SAR) objective is to prevent loss of life and injury through search and rescue alerting, responding and aiding activities using public and private resources. Where possible and when directly related thereto, reasonable efforts will be made to minimize damage to or loss of property.

3.2 Operational Capabilities

This section describes the operational capabilities of the SAR Enterprise. Search and Rescue service provided by the SAR enterprise comprises performance of distress monitoring, communication, co-ordination, and search and rescue functions, including provision of medical advice, initial medical assistance, or medical evacuation through the use of public and private resources, including cooperating aircraft, vessels and other craft and installations.

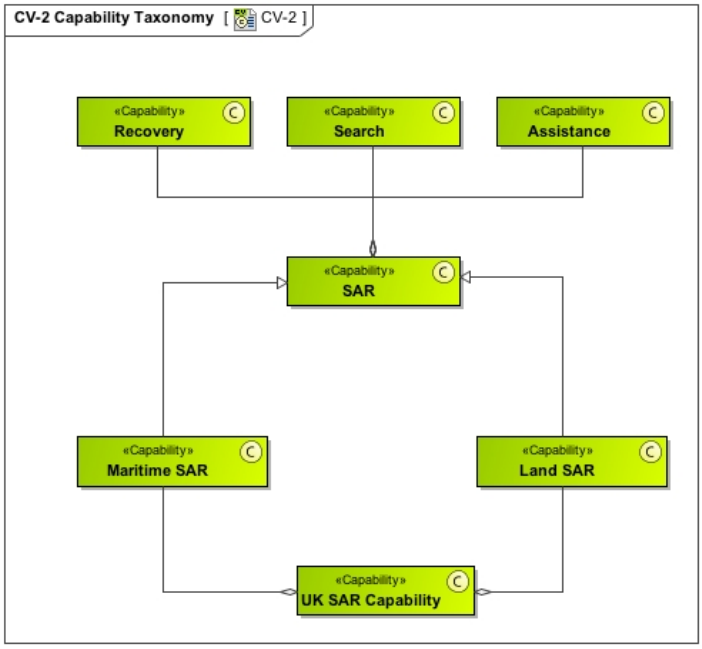

Figure 2: Capabilities Taxonomy

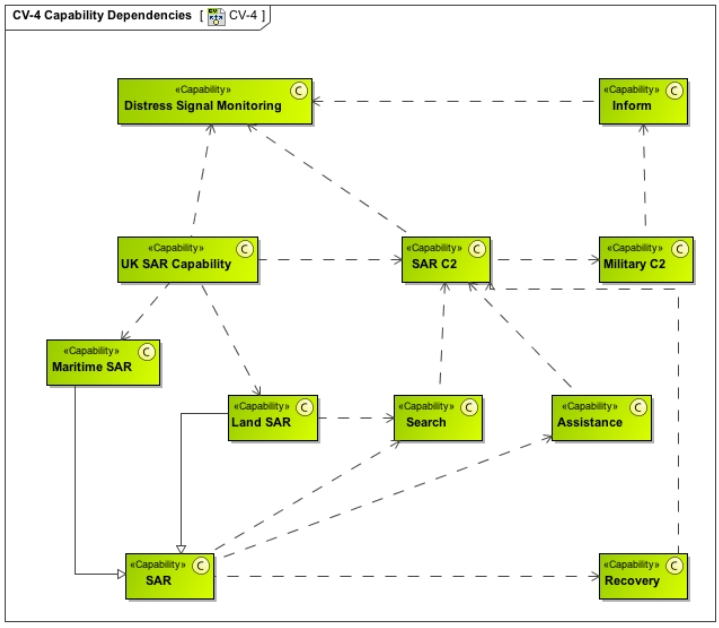

Figure 3: Capabilities Dependencies

Table 2: Operational Capabilities

Operational Capability	Description
C02 - Maritime Assistance	Assistance to a marine vessel in distress. The key capability of the SAR Enterprise
C03 - Distress Signal Monitoring	Monitoring EMF spectrum and providing tracking information to the tactical command and control center
C07 - Maritime Recovery	Extraction of the person in distress and vessel. The key capability of the SAR Enterprise.
C08 - SAR C2	The SAR Tactical Command And Control Center coordinates the search and rescue activities.
C10 - Maritime Search	The SAR Search node locates the vessel in distress based on the tracing information from the monitoring unit and other search nodes.

Observations:

The operational capability items in Table2 are derived directly from the reference DoDAF model of the SAR Enterprise (Capability Views CV-2, CV-4 and CV-6, CV-7) and then filtered based on the scope of the assessment.

For the purpose of the security assessment, we are focusing at unique identifiable capabilities for which the reference model of the SAR Enterprise has defined performers and operational activities. Thus we have dropped any aggregated or generic capabilities, such as SAR, Maritime SAR, Land SAR, and UK SAR Capability; derived detailed names for concrete capabilities, e.g. "Maritime Recovery" for a generic "Recovery" capability that is a subcategory of "Maritime SAR". We have decided to eliminate several capabilities from the scope of this assessment, since the reference DoDAF model does not provide further operational details. The excluded capabilities are any "Land SAR" capabilities (Land Search, Land Recovery, Land Assistance), Military C2, and Inform capabilities.

We have ***High Confidence*** in completeness and correctness of the list of operational capabilities in Table2**Error! Reference source not found.**.

3.3 Stakeholders

The following table describes the Stakeholders for the SAR Enterprise.

Table 3: Stakeholders

Stakeholders	Description
ST01 - SAR Operator	This is the organization responsible for providing SAR services. This corresponds to UK SAR Operator from OV-4 Typical Organizational Relationships Chart, for example Maritime and Coastguard Agency, and the RNLI mentioned in OV-4 Actual Organizational Relationships Chart.
ST02 - C2 Operator	The capability to provide command and control for the SAR operations is internal to the SAR Enterprise.

ST04 - COSPAS-SARSAT operator	This is the organization responsible for running the COSPAS-SARSAT satellite monitoring.

Observations:

The reference DoDAF model for the SAR Enterprise does not provide this information directly; some related information in contained in OV-4 operational views. A typical SAR activity may involve multiple organizations, for example multiple plane operators, boat operators, multiple C2 nodes in different search areas, etc. An important stakeholder in SAR is the regulator (not mentioned in the reference DoDAF model). We assume that the security assessment of the SAR Enterprise is performed for a generic SAR Operator for the purpose of preparing the assurance case justifying the security of the SAR operations and developing additional security controls.

We have ***Medium Confidence*** in completeness and correctness of the list of stakeholders in Table 3.

3.4 Operational Capabilities to Stakeholders

The following table captures the concerns of the stakeholders for the SAR Enterprise. The table represents statements "operational capability A *is the responsibility of* stakeholder B", indicated by an "X" mark in the cells for A-B, while "-" mark in the cell for A-B means that "operational capability A *is not a responsibility of* stakeholder B". A certain capability is a responsibility of a stakeholder when the stakeholder is accountable for the availability, and integrity of the capability as well as confidentiality of the information items involved) by position, law or otherwise. It is possible that two or more stakeholders are accountable for different aspect of the same operational capability.

Table 4: Operational Capability to Stakeholders

From\To	ST01 - SAR Operator	ST02 - C2 Operator	ST04 - COSPAS-SARSAT operator
C02 - Maritime Assistance	X	-	-
C03 - Distress Signal Monitoring	-	-	X
C07 - Maritime Recovery	X	-	-
C08 - SAR C2	-	X	-
C10 - Maritime Search	X	-	-

Observations:

The reference DoDAF model for the SAR Enterprise does not provide this information directly. The above table makes a claim that Distress Signal Monitoring capability is not the responsibility of the SAR Operator, and therefore is outside of the scope of the assessment: we will consider the corresponding threats to the rest of the SAR Enterprise, but will not consider the corresponding vulnerabilities, nor will provide recommendations for the corresponding performers. At the same time, the level of operational activity detail for the Distress Signal Monitoring capability provided by the SAR reference model is quite low.

We have ***High Confidence*** in correctness of the statements in Table 4.

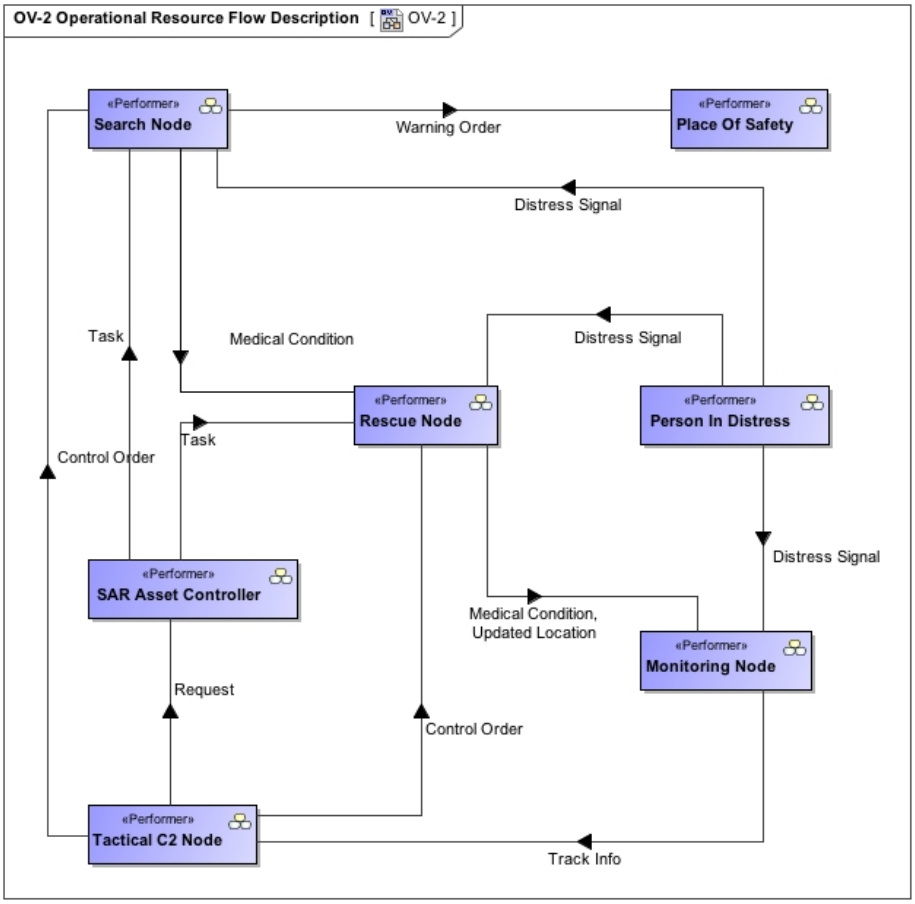

Figure 4. Operational Resource Flow Description

3.5 Performers

The following table captures the list of Performers associated with the SAR Enterprise.

Table 5: Performers

Performer	Description
P01 - Monitoring Node	Satellites of the CONPAS-SARSAT system. They monitor the emergency frequencies in the EMF spectrum to locate marine vessels in distress, or deployed emergency beacons. They perform triangulation to determine the location of the vessel in distress.

P02 - Person In Distress	The operator of the marine vessel in distress, including crew members and passengers on board, or any other people involved in a marine accident
P03 - Place of Safety	For example, a port, a land hospital, a naval vessel with medical facilities on board, etc. Victims of a marine accident are delivered to the Place of Safety for further assistance.
P04 - Rescue Node	For example, a helicopter, or a boat. Rescue node that is deployed to recover the victims of the marine accident, and to provide assistance.
P05 - SAR Asset Controller	Asset Controller identifies search and rescue assets to be used in a given SAR operation
P07 - Search Node	For example, a fixed wing aircraft, a helicopter or a UAV. Search node is deployed to locate the marine vessel in distress and provide accurate information for the search and rescue operation, to establish contact with the person in distress, and to monitor the situation
P08 - Tactical C2 Node	The command and control center of the SAR enterprise.

Observations:

This list of performers in the above table is derived directly from the reference DoDAF model for the SAR Enterprise, namely the Operational View OV-2. The reference model provides operational detail for the Person in Distress, Search Node and Rescue Node. The level of operational detail for Monitoring Node and Place of Safety is low. The reference model does not provide any operational detail for Tactical C2 Node and Asset Controller Node.

We have ***High Confidence*** in completeness and correctness of the list of performers.

3.6 Operational Activities

The following table captures the list of Operational Activities associated with the SAR Enterprise.

Table 6: Operational Activities

Operational Activity	Description
OA01 - Find Victim	The key activity for the Search Capability. Use ESM tracking, visuals and radio systems to locate the object of a SAR operation. This activity is guided by the control orders from the C2 center, based on other sources tracking information.
OA02 - Monitor Health	Monitoring EMF spectrum and providing tracking information to the tactical command and control center
OA03 - Process Warning Order	A Place Of Safety prepares for the arrival of victims of the SAR operation
OA04 - Provide Medical Assistance	Rescue personnel provide medical assistance to victims if needed. More comprehensive medical treatment is provided in the Place of Safety
OA05 - Receive Distress Signal	Monitor the appropriate frequencies of the EMF spectrum to receive the distress signal and compute tracking information
OA06 - Recover Victim	The victim of the vessel in distress is transferred to the Rescue node to be delivered to the Place Of Safety

OA07 - Rescue	General activities of the SAR Rescue node.
OA08 - Search	The SAR Search node locates the vessel in distress based on the tracing information from the monitoring unit and other search nodes.
OA09 - Search And Rescue	General activities involved in a SAR operation.
OA10 - Send Distress Signal	The vessel in distress broadcasts the distress signal using the appropriate EMF frequencies
OA11 - Send Warning Order	Once the SAR Node has located the vessel in distress and assessed the situation it communicates to the Place of Safety to inform about required assistance to the victim that will be delivered to the Place Of Safety upon successful completion of the SAR operation
OA12 - Transit to SAR Operation	Wrap-up of the on-going SAR operation

Observations:

The list of operational activities is derived directly from the reference DoDAF model of the SAR Enterprise, namely from the Operational Views OV-5a and OV-5b. Operational activities OA07, OA08 and OA09 are rather generic and do not provide operational detail for Monitoring Node, Place of Safety, Tactical C2 Node and Asset Controller.

We have ***Medium Confidence*** in completeness of the list of operational activities and ***High Confidence*** in its correctness.

3.7 Operational Activity to Performers Dependency

The following table captures the dependency from the Operational Activity to the Performers for the SAR Enterprise. The table represents statements "operational activity A *is carried out by* performer B", indicated by an "X" mark in the cell for A-B. This means that a failures of the performer causes failure of the corresponding operational activity. The mark "-" in the cell for A-B indicates a statement "operational activity A *is not carried out by* performer B". It is possible that two or more performers carry out an operational activity.

Lightly shaded cells indicate claims based on partial evidence in the reference SAR model.

Table 7: Operational Activity to Performers

From\To	P01 - Monitoring Node	P02 - Person In Distress	P03 - Place of Safety	P04 - Rescue Node	P05 - SAR Asset Controller	P07 - Search Node	P08 - Tactical C2 Node
OA01 - Find Victim	-	X	-	-	-	X	X
OA02 - Monitor Health	-	X	-	-	-	X	-
OA03 - Process Warning Order	-	-	X	-	-		-

OA04 - Provide Medical Assistance	-	X	-	X	-	-	X
OA05 - Receive Distress Signal	X	-	-	X	-	X	-
OA06 - Recover Victim	-	X	-	X	-	-	-
OA07 - Rescue	-	X	X	X	-	-	X
OA08 - Search	X	X	-	-	-	X	X
OA09 - Search And Rescue	X	X	X	X	X	X	X
OA10 - Send Distress Signal	-	X	-	-	-	-	-
OA11 - Send Warning Order	-	-	-	-	-	X	-
OA12 - Transit to SAR Operation	-	-	X	X	-	X	X

Observations:

The statements in the above table are derived from Operational View OV-5b Operational Activity Model as well as from OV-5a Operational Activity Decomposition Tree.

We have ***High Confidence*** in the correctness of the operational activity to performers statements, commensurate with the granularity of the reference model for SAR, even though some of the statements are based on less explicit evidence than others.

3.8 Operational Capability to Operational Activity Dependency

The following table captures the dependency from the Operational Capability to the Operational Activity for the SAR Enterprise. The table represents statements "operational capability A *depends on* operational activity B", indicated by mark "X" in the cell A-B. This statement means that a failure in the operational activity causes failure in the corresponding operational capability. The dependencies are therefore transitive in nature. Mark "-" in a cell A-B indicates a statement "operational capability A *does not depend on* operational activity B".

Table 8: Operational Capability to Operational Activity

From\To	OA01 - Find Victim	OA02 - Monitor Health	OA03 - Process Warning Order	OA04 - Provide Medical Assistance	OA05 - Receive Distress Signal	OA06 - Recover Victim	OA07 - Rescue	OA08 - Search	OA09 - Search And Rescue	OA10 - Send Distress Signal	OA11 - Send Warning Order	OA12 - Transit to SAR Operation
C02 - Maritime Assistance	X	X	-	X	X	-	-	X	X	X	-	-
C03 - Distress Signal Monitoring	-	-	-	-	X	-	-	-	X	X	-	-
C07 - Maritime Recovery	X	-	X	-	X	X	X	X	X	X	X	X
C08 - SAR C2	-	-	-	-	-	-	-	-	X	-	-	-
C10 - Maritime Search	X	-	-	-	X	-	-	X	X	X	-	-

Observations:

The statements in the above table are based on the analysis of the reference SAR model, in particular the Capability Views CV-2, CV-4 and the OV-5a Operational Activity Decomposition Tree.

We have ***High Confidence*** in the operational capability to operational activity dependency statements.

3.9 Operational Exchange Items

The following table summarizes the Operational Exchange Items for the SAR Enterprise. This step focuses at identification of information assets of the SAR Enterprise.

Table 9: Operational Exchange Items

Operational Exchange Item	Description
Distress Signal	Distress Signal sent by a Person in Distress and picked up by the Monitoring Node and then by the Search Node and Rescue Node
Track Info	Information sent by the Monitoring Node to the Tactical C2 Node; presumably the triangulated location of the person in distress

Request	Asset allocation request sent by the Tactical C2 Node to Asset Controller when a SAR Operation is launched. We assume that some information about the allocated assets is sent back to the Tactical C2 Node. It is also important that the Tactical C2 Node has rules to handle the situation when there are no available assets.
Control Order	Tactical information sent by the Tactical C2 Node to Search Node and Rescue Node. This includes the designated search area, commands to return to base, weather updates, etc. We assume that the Tactical C2 Node receives a confirmation (or a status update) in response to the control order.
Task	Allocation order sent by the Asset Controller to one of the assets (Search Node or Rescue Node) to join a particular SAR Operation and receive control orders from a designated Tactical C2 Node. We assume that the Asset Controller receives a confirmation from the asset (a status update).
Task Response	Response to Task from Search Node or Rescue Node
Allocation	Response to the Allocation Request with the list of assets allocated to the SAR Operation.
Control Order Response	Response to Control Order from a Search Node or a Rescue Node
Medical Condition	Information originating from "Monitor Health" activity sent by the Search Node to the Rescue Node and information originating from "Provide Medical Assistance" activity sent by Rescue Node to the Monitoring Node. We assume that this information is further sent to the Tactical C2 Node, and also to the Place of Safety.
Warning Order	Information related to the ongoing SAR operation sent by Search Node to the Place of Safety.
Updated Location	Information originating from "Recover Victim" activity sent by Rescue Node to the Monitoring Node. We assume that this information is further sent to the Tactical C2 Node. We assume that the Search Node also provides an update on the location of the Person In Distress as the result of "Find Victim" activity.
Victim	Victim delivered to the place of safety. We assume that this exchange leads to the successful wrap-up of the SAR Operation.

Observations:

This information is derived directly from the Operational Views, in particular from the OV-2 Operational Resource Flow Description. Some additional items are provided as the result of the causal analysis of the exchanges and operational activity flow based on OV-5b Operational Activity Model.

We have ***High Confidence*** in the list of exchange elements.

3.10 Operational Exchanges

The following table summarizes the Operational Exchanges of the SAR Enterprise.

Table 10: Operational Exchanges

Operational Exchange Item	Originating Performer	Originating Operational Activity	Receiving Performer	Receiving Operational Activity
Distress Signal	P02 - Person In Distress	OA10 - Send Distress Signal	P01 - Monitoring Node	OA05 - Receive Distress Signal
Distress Signal	P02 - Person In Distress	OA10 - Send Distress Signal	P07 - Search Node	OA05 - Receive Distress Signal
Distress Signal	P02 - Person In Distress	OA10 - Send Distress Signal	P04 - Rescue Node	OA05 - Receive Distress Signal
Track Info	P01 - Monitoring Node	OA09 - Search and Rescue	P08 - Tactical C2 Node	OA09 - Search and Rescue
Request	P08 - Tactical C2 Node	OA09 - Search and Rescue	P05 - SAR Asset Controller	OA09 - Search and Rescue
Task	P05 SAR Asset Controller	OA09 - Search and Rescue	P07 - Search Node	OA09 - Search and Rescue
Task Response	P07 - Search Node	OA09 - Search and Rescue	P05 SAR Asset Controller	OA09 - Search and Rescue
Task	P05 SAR Asset Controller	OA09 - Search and Rescue	P04 - Rescue Node	OA09 - Search and Rescue
Task Response	P04 - Rescue Node	OA09 - Search and Rescue	P05 SAR Asset Controller	OA09 - Search and Rescue
Allocation	P05 SAR Asset Controller	OA09 - Search and Rescue	P08 - Tactical C2 Node	OA09 - Search and Rescue
Control Order	P08 - Tactical C2 Node	OA08 - Search	P07 - Search Node	OA08 - Search
Control Order Response	P07 - Search Node	OA08 - Search	P08 - Tactical C2 Node	OA08 - Search
Control Order	P08 - Tactical C2 Node	OA07 - Rescue	P04 - Rescue Node	OA07 - Rescue
Control Order Response	P04 - Rescue Node	OA07 - Rescue	P08 - Tactical C2 Node	OA07 - Rescue
Medical Condition	P07 - Search Node	OA02 - Monitor Health	P04 - Rescue Node	OA04 - Provide Medical Assistance, OA06 - Recover Victim
Warning Order	P07 - Search Node	OA11 - Send Warning Order	P03 - Place of Safety	OA03 - Process Warning Order

Updated Location	P04 - Rescue Node	OA06 - Recover Victim	P01 - Monitoring Node	OA07 - Rescue
Medical Condition	P04 - Rescue Node	OA04 - Provide Medical Assistance	P01 - Monitoring Node	OA07 - Rescue
Victim	P02 - Person In Distress	OA07 - Rescue	P04 - Rescue Node	OA06 - Recover Victim
Victim	P04 - Rescue Node	OA06 - Recover Victim	P03 - Place of Safety	OA12 - Transit to SAR Operation

Observations:

This information is derived directly from the Operational Views, in particular from the OV-2 Operational Resource Flow Description and OV-3 Operational Exchange Matrix. Some additional items are provided as the result of the causal analysis of the exchanges and operational activity flow based on OV-5b Operational Activity Model.

We have ***High Confidence*** in the operational exchange statements.

3.11 Performer Dependencies

The following table summarizes dependencies between performers.

Table 11: Performers to Performers

From\To	P01 - Monitoring Node	P02 - Person In Distress	P03 - Place of Safety	P04 - Rescue Node	P05 - SAR Asset Controller	P07 - Search Node	P08 - Tactical C2 Node
P01 - Monitoring Node	X	X	-	X	-	-	-
P02 - Person In Distress	-	X			-	-	-
P03 - Place of Safety	-	-	X	X	-	X	-
P04 - Rescue Node	-	X	-	X	X	X	X
P05 - SAR Asset Controller	-	-	-	X	X	X	X
P07 - Search Node	-	X	-	-	X	X	X
P08 - Tactical C2 Node	X	-	-	X	X	X	X

Observations:

Performer dependencies are derived directly from the OV-2 Operational Resource Flow Description. Some additional items are provided as the result of the causal analysis of the exchanges and operational activity flow based on OV-5b Operational Activity Model.

We have ***High Confidence*** in performer dependency statements.

Section 4

Security Criteria and Metrics

This section captures the security requirements of the Stakeholders of the SAR Enterprise within the selected scope of the security assessment.

4.1 Security Criteria

The following table captures the security criteria selected for the security assessment of the SAR Enterprise. We are making an assumption that the following security criteria define the concerns of the Stakeholders with respect to the product and its environment. For example, Stakeholders may be concerned about the compromise to availability, confidentiality, or integrity. The levels for each criterion are defined by security metrics in the next section.

Table 12: Security Criteria

Security Criteria	Description
Availability	Related to the availability of assets and their associated capabilities.
Confidentiality	Related to disclosures of sensitive information, credentials, etc.
Integrity	Related to loss, corruption or subversion of assets.
Environment	Related to maritime and land pollution
Health	Related to safety of the SAR personnel

4.2 Security Metrics

The security metrics define different levels of injury arising from the compromise of one of these security criteria. For example, confidentiality, availability, integrity, value, damage to health, or damage to the environment. Currently a uniform set of metrics is used for all security criteria identified in the previous section.

Table 13: Security Metrics

Security Level
High
Medium
Negligible
Not Set

Table 14. Severity Categories

Severity Categories	Mil-Std-882D Category	Environmental, Safety and Health Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Table 15: Likelihood Categories

Likelihood Categories	Mil-Std-882D Level	Specific Individual Item	Fleet or inventory
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10-1 in that life.	Continuously experienced
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10-1 but greater than 10-2 in that life.	Will occur frequently
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10-2 but greater than 10-3 in that life.	Will occur several times
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10-3 but greater than 10-6 in that life.	Unlikely, but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10-6 in that life.	Unlikely to occur, but possible

Table 16. Risk Categories

Risk Categories		Severity			
		Catastrophic	Critical	Marginal	Negligible
Likelihood	Frequent	High	High	Serious	Medium
	Probable	High	High	Serious	Medium
	Occasional	High	Serious	Medium	Low
	Remote	Serious	Medium	Medium	Low
	Improbable	Medium	Medium	Medium	Low

4.3 Impacts

Although the consequences of compromise can vary considerably, depending upon the threat and the assets affected, the actual outcome can be reduced to one or more possible impacts/injuries according to a number of categories. For example physical or psychological harm to human beings or a financial loss.

The following table captures the Impacts and their categories selected within the scope of the security assessment of the SAR Enterprise. This assessment uses a best-practices taxonomy of impacts and impact categories including the following:

- impacts on mission
- impacts on decision-making capability
- impacts on safety
- impacts on morale
- impacts on intellectual property
- financial impacts
- impacts on the image of the organization
- impacts of non-compliance to regulations
- legal impacts
- environmental impacts
- security impacts

Table 17: Impacts

Impact	Description	Category
Impacts on mission	Direct or indirect impact on the successful accomplishment of the mission (such as the production of goods or services).	Impacts on mission
I01.01 - Inability to provide a service		Impacts on mission
I01.02 - Loss of expertise		Impacts on mission
I01.03 - Change of strategy		Impacts on mission
I01.04 - Inability to assure a service		Impacts on mission
I01.05 - Impact on production of goods and services		Impacts on mission
I01.06 - Possible inability to provide a service	impact on production or distribution of goods or services which in extreme case may affect satisfaction of basic human needs, exercise of the state authority, functioning of the economy, maintaining the potential of defense, national security.	Impacts on mission
Impacts on decision-making capacity	Direct or indirect impact on the freedom to decide and control the enterprise.	Impacts on decision-making capacity
I02.01 - Loss of sovereignty		Impacts on decision-making capacity
I02.02 - Loss or limitation of independence of judgment or decision		Impacts on decision-making capacity
I02.03 - Limiting the room for negotiation		Impacts on decision-making capacity
I02.04 - Loss of ability to influence		Impacts on decision-making capacity
I02.05 - Taking control over the organization		Impacts on decision-making capacity
Impacts on safety	Direct or indirect effects on the physical integrity of individuals. Examples include accident, occupational disease, loss of life, endangerment.	Impacts on safety
I03.01 - Accident		Impacts on safety
I03.02 - Illness		Impacts on safety

I03.03 - Loss of human lives		Impacts on safety
I03.04 - Endangerment		Impacts on safety
Impacts on morale	Direct or indirect impact on the quality of social relationships within the organization.	Impacts on morale
I04.01 - Loss of employee confidence	Loss of employee confidence in the sustainability of the company	Impacts on morale
I04.02 - Tensions between social groups	Exacerbation of resentment and tension between social groups (including national / international management / employees, officials / non-officials, youth / seniors),	Impacts on morale
I04.03 - Weakening of commitment of employees towards the organization	Weakening of the commitment of the employees towards the company	Impacts on morale
I04.04 - Weakening of shared ethical values of the employees	Weakening of shared ethical values to employees (humanitarian, public service for all social progress, contribution to health in the world, etc.)	Impacts on morale
Impacts on intellectual property	Direct or indirect effects on non-explicit knowledge accumulated by the organization with the expertise, capacity for innovation, on common cultural references.	Impacts on intellectual property
I05.01 - Loss of corporate memory	Loss of corporate memory (old projects, successes and failures, etc.)	Impacts on intellectual property
I05.02 - Loss of tacit knowledge	Loss of tacit knowledge (know-how transmitted between generations, optimizations in the execution of tasks or processes, capture innovative ideas,	Impacts on intellectual property
I05.03 - Cultural loss	Loss of cultural knowledge (aesthetic references, models, styles, etc.)	Impacts on intellectual property
I05.03 - Scientific loss	Scientific loss (rare or extinct biological species, etc.).	Impacts on intellectual property
Financial impacts	Financial consequences, direct or indirect. Examples include loss of revenue, unexpected expenses, loss of stock value, loss of income, penalties.	Financial impacts
I06.01 - Loss of revenue		Financial impacts
I06.02 - Unexpected expenses		Financial impacts
I06.03 - Loss of stock value		Financial impacts
I06.04 - Loss of income		Financial impacts
I06.05 - Penalties		Financial impacts

I06.06 - Damage to property		Financial impacts
Impacts on the image	Direct or indirect impact on the brand image, reputation, fame, influence the ability of the organization (lobby, relationship with actors and political and economic decision-makers) or ethics (transparency, non-corruption, respect for human dignity, clean money, etc.). Examples include publication of a satirical article in the press, loss of credibility in the eyes of the customers, shareholder discontent, loss of competitive advance, loss of reputation.	Impacts on the image
I07.01 - Loss of credibility		Impacts on the image
I07.02 - Shareholders dissatisfaction		Impacts on the image
I07.03 - Loss of competitive advantage		Impacts on the image
I07.04 - Loss of reputation		Impacts on the image
I07.05 - Satirical publication in the press		Impacts on the image
Impacts of non-compliance	Direct or indirect consequences of obtaining or maintaining compliance standards (license, certification, qualification, etc.). Examples include refusal of a license or loss of certification due to non-compliance with ISO 27001, Sarbanes-Oxley.	Impacts of non-compliance
I08.01 - Loss of certification or license		Impacts of non-compliance
I08.02 - Loss of compliance		Impacts of non-compliance
Legal impacts	Procedural consequences, criminal, civil or administrative, direct or indirect. Examples include trial, fine, conviction of a leader, bankruptcy, amendment, and amendments to contracts.	Legal impacts
I09.01 - Trial		Legal impacts
I09.02 - Fine		Legal impacts
I09.03 - Conviction of a leader		Legal impacts
I09.04 - Bankruptcy		Legal impacts
I09.05 - Amendments to contracts		Legal impacts
I09.06 - Civil litigation		Legal impacts

Environmental impacts	Ecological consequences in the short or long term, direct or indirect. Examples include pollution due to waste discharges or sources of pollution (chemical, biological, radiological, audio, visual, olfactory, etc.) generated by the organization within its perimeter, neighborhood or area.	Environmental impacts
I10.01 - Pollution		Environmental impacts
Security impacts		Security impacts
I11.01 - Outside knowledge gain of network	Attackers gain information about the network, its vulnerabilities, including the identify and versions of the system software and COTS packages (for example, through software fingerprinting)	Security impacts
I11.02 - Outside knowledge gain of other assets and targets	Attacker gains access to some information assets and exfiltrates information that may facilitate planning further attacks.	Security impacts
I11.03 - Possible loss of confidentiality to other nodes and assets	Attacker gains access to some information assets and exfiltrates information that may facilitate further attacks.	Security impacts
I11.04 - Exfiltration of confidential information	Attacker gains access to exfiltrate confidential information.	Security impacts

Observations:

The enumeration of the impacts is obtained from our standard taxonomy of impacts, adjusted to the operational context of the SAR Enterprise.

4.4 Internal Actors

The following table captures the list of internal actors (roles) in the SAR Enterprise.

Table 18: Internal Actors

Internal Actors	Description
IA01 - Driver	Driver may abuse the rescue node, damage the rescue node, do mischief, or be motivated to do harm to a person in distress, to the environment, or to other property, or people.
IA02 - Operator	Operator may abuse the resources of the C2 Node, damage the C2 node (sabotage), do mischief, or be motivated to do harm to the person in distress.
IA03 - Pilot	Pilot may abuse the Search Node, damage the Search Node (sabotage), do mischief, or be motivated to do harm to a person in distress, to the environment, or to other property
IA4 - Swimmer	Swimmer may be motivated to do harm to person in distress
IA05 - Yacht operator	Yacht operator may be motivated to do mischief, abuse the emergency equipment, or be motivated to do harm to the SAR enterprise.

IA06 - Maintenance contractor	Maintenance contractor has access to equipment and facilities and may be motivated to sabotage or do harm to the personnel or to the property or environment.
IA07 - Supplier	Someone within the supply chain motivated to do harm

Observations:

Internal actors are derived directly from the OV-4 Typical Organizational Relationships Charts and other views of the reference SAR Enterprise DoDAF model.

We have ***High Confidence*** in internal actor statements.

4.5 Threat Sources

Threats are categorized according to the root cause, either by human beings or by forces of nature. The following table captures the list of Threat Sources within the scope of the security assessment for the SAR Enterprise. This assessment uses a standard taxonomy of threat source categories.

Table 19: Threat Sources

Threat Source	Description	Category
ThrS1.1 - Malicious driver	Driver may abuse the rescue node, damage the rescue node, do mischief, or be motivated to do harm to a person in distress, to the environment, or to other property, or people.	Human Malicious Internal High Capability
ThrS1.2 - Malicious operator	Operator may abuse the resources of the C2 Node, damage the C2 node (sabotage), do mischief, or be motivated to do harm to the person in distress.	Human Malicious Internal Limited Capability
ThrS1.3 - Malicious pilot	Pilot may abuse the Search Node, damage the Search Node (sabotage), do mischief, or be motivated to do harm to a person in distress, to the environment, or to other property	Human Malicious Internal Limited Capability
ThrS1.4 - Malicious swimmer	Swimmer may be motivated to do harm to person in distress	Human Malicious Internal Limited Capability
ThrS2.1 - Mischievous yacht operator	Yacht operator may be motivated to do mischief, abuse the emergency equipment, or be motivated to do harm to the SAR enterprise.	Human Malicious External Limited Capability
ThrS2.10 - Targeted virus	Malware developed to do harm to specific target, or to collect information from that target. Development and operation of such malware involves someone motivated to do harm to the target, or obtain information from the target.	Human Malicious External Unlimited Capability
ThrS2.11 - Competition	In general, some organizations may be motivated to do harm to their competitors (probably not in the SAR case)	Human Malicious External High Capability

ThrS2.2 - Script kiddy	Person who is motivated to explore attack capabilities, often without understanding of their consequences. Existence of script kiddies is the consequence of weaponized attack tools.	Human Malicious External Limited Capability
ThrS2.3 - Vandal	Person who is motivated to sabotage the enterprise.	Human Malicious External Limited Capability
ThrS2.4 - Thief	Motivated to steal fuel or parts	Human Malicious External Limited Capability
ThrS2.5 - Avenger	High capability individual who is not part of internal personnel and who has a personal grudge against someone within the enterprise context. Can be highly motivated to do harm to a specific person	Human Malicious External High Capability
ThrS2.6 - Hacker	Person who is developing attack capabilities	Human Malicious External High Capability
ThrS2.7 - Malicious supplier	Someone within the supply chain motivated to do harm	Human Malicious External High Capability
ThrS2.8 - Malicious maintenance contractor	Maintenance contractor has access to equipment and facilities and may be motivated to sabotage or do harm to the personnel or to the property or environment.	Human Malicious External High Capability
ThrS2.9 - Terrorist	Motivate to do extended damage	Human Malicious External Unlimited Capability
ThrS3.1 - Operator acting by mistake		Human Non-malicious Internal Limited Capability
ThrS3.2 - Driver acting by mistake		Human Non-malicious Internal High Capability
ThrS3.3 - Pilot acting by mistake		Human Non-malicious Internal High Capability
ThrS3.4 - Swimmer acting by mistake		Human Non-malicious Internal Limited Capability
ThrS4.1 - Victim acting by mistake	Victim is the operator of the yacht in distress, a crew member, or one of the passengers on board.	Human Non-malicious External Limited Capability
ThrS4.2 - Journalist	A journalist may be motivated to obtain information about current operations	Human Non-malicious Internal Limited Capability
ThrS4.3 - Maintenance contractor acting by mistake		Human Non-malicious External High Capability
ThrS4.4 - Supplier acting by mistake		Human Non-malicious External High Capability
ThrS5.1 - Non-targeted virus	A non-targeted virus is developed to exploit vulnerabilities in known software.	Non-human Malicious

ThrS5.2 - Botnet	A botnet is malware that exploits vulnerabilities in known software and establishes control over the computing nodes, making them exercise commands of the botnet master.	Non-human Malicious
ThrS6.1 - Bad weather		Non-human Non-malicious
ThrS6.2 - Solar flare		Non-human Non-malicious
ThrS6.3 - Fire		Non-human Non-malicious
ThrS6.4 - Earthquake		Non-human Non-malicious
ThrS6.5 - Tornado		Non-human Non-malicious
ThrS6.6 - Tsunami		Non-human Non-malicious
ThrS6.7 - Shark attack		Non-human Non-malicious
ThrS6.8 - Equipment failure		Non-human Non-malicious
ThrS6.9 - Hurricane		Non-human Non-malicious

Observations:

The enumeration of threat sources is obtained from our standard taxonomy of threat sources, adjusted to the operational context of the SAR Enterprise. The information on internal human threat sources is derived from the list of internal actors.

Section 5

Asset Identification

The proper management of assets is vital to the success of the organization and is a major responsibility of all management levels. From a security perspective a successful security program is driven by the identification of the assets of the organization. Assets can be divided into two categories:

- Primary Assets are defined as an intangible asset (information or service) provided by the enterprise to its environment and therefore requiring protection; primary assets are a responsibility of a stakeholder; primary assets are the goals of the attacks. Proper identification of the sensitivities of the stakeholders helps scope the effort of the security assessment project. Primary assets determine the set of undesired events considered by the assessment. Primary assets are instrumental in systematically identifying the effects of the security incidents.
- System Assets are defined as assets that support operational activities. These are tangible items that are attacked and that fail such as hardware, software, networks, and people. System assets are the entry points of the attacks. System assets determine the locations for the system vulnerabilities. System assets are instrumental in systematically identifying the causes of security incidents.

This section captures the Assets of the SAR Enterprise.

5.1 System Assets

The following table captures the System Assets associated with the SAR Enterprise. The list of System Assets involves all tangible things as well as personnel within the scope and at the level of detail of the reference SAR Enterprise model.

Table 20: System Assets

System Asset	Category	Performer	Description
SS01 - Distress Signal Network	network	Person in Distress, Monitoring Node, Search Node, Rescue Node, Tactical C2 Node	Aggregate of the deployed equipment to use EMF to broadcast distress signal and to receive it in such a way that tracking information can be provided. We assume that the track information from the Monitoring Node to the Tactical C2 Node is sent through this network rather than the Tactical Network
SS02 - Tactical Network	network	Search Node, Rescue Node, Tactical C2 Node	Link 16 Network. Aggregate of the deployed Link-16 terminals and other equipment so that tactical information can be exchanged between participating nodes.
SS03 - C2 Node and Asset Controller Facility	facility	Tactical C2 Node, Asset Controller	Aggregate of building and essential mechanical systems.

SS04 - Rescue Node Facility	facility	Rescue Node	This is ship/boat element; It includes engine, fuel supply electrical power supply, life support, etc. Equipment is addressed separately; software is addressed separately; communications equipment is addressed separately.
SS05 - Place of Safety Facility	facility	Place of Safety	This includes medical equipment, facility, e.g. boat, medical personnel, etc.
SS06 - Monitoring Node Facility	facility	Monitoring Node	This includes satellite, engines, fuel, communication equipment, ground control station, etc. We do not consider any further differentiation, since this performer is outside of the scope of the assessment.
SS07 - Person In Distress Facility	facility	Person in Distress	Likely, ship/boat subcategory. This includes yacht, engine, fuel, etc. The emergency equipment is considered separately.
SS09 - C2 Node sw	software/ application	Tactical C2 Node	This includes custom application c2 software, communications software, etc. COTS software is addressed separately
SS10 - Asset Control sw	software	Asset Controller	This includes custom asset management sw, communications software, etc. COTS software is addressed separately
SS11 - C2 Node COTS sw	software/ COTS	Tactical C2 Node	This includes operating systems, communications software, etc.
SS12 - Search Node sw	software	Search Node	This includes operating systems, c2 software, communications software, flight control sw, etc.
SS13 - Rescue Node sw	software	Rescue Node	This includes operating systems, c2 software, communications software, boat control sw, etc.
SS14 - Place of Safety sw	software	Place of Safety	This includes operating systems, c2 software, communications software, etc.
SS15 - Emergency Equipment	hardware	Person in Distress	This includes emergency radio as well as any other broadcasting equipment for distress signal
SS17 - Rescue Node equipment	hardware	Rescue Node	This includes equipment for rescue mission such as communications equipment;
SS18 - Search Node equipment	hardware	Search Node	This includes equipment for the search mission other than the aircraft itself or communications equipment
SS19 - C2 Node equipment	hardware	Tactical C2 Node	This includes computing equipment. This includes the local network, the computing equipment, etc.
SS20 - Asset Controller equipment	hardware	Asset Controller	This includes computing equipment, network, etc.

SS26 - Search Node facility	facility	Search Node	This an aircraft or a helicopter; This includes engine, fuel supply electrical power equipment is addressed separately; software is addressed separately; communications equipment is addressed separately
SS27 - Victim	people	Person in Distress	The distressed person, victim of the emergency
SS28 - C2 Operator	people	Tactical C2 Node	operator of the Tactical C2 Node
SS29 - Asset Controller Operator	people	Asset Controller	operator of the Asset Controller Node
SS30 - Pilot	people	Search Node	pilot of the search node
SS31 - Driver	people	Rescue Node	driver of the rescue node
SS32 - Swimmer	people	Rescue Node	swimmer of the rescue node
SS33 - Place of Safety Operator	people	Place of Safety	operator of the place of safety node
SS34 - C2 Procedure	procedure	Tactical C2 Node	The set of rules that determines the operations of the C2 node, including normal procedures and contingencies
SS35 - Asset Control Procedure	procedure	Asset Controller	The set of rules that determines the operations of the Asset Controller node, including normal procedures and contingencies
SS36 - Rescue Procedure	procedure	Rescue Node	The set of rules that determines the operations of the Rescue node, including normal procedures and contingencies
SS37 - Search Procedure	procedure	Search Node	The set of rules that determines the operations of the Search node, including normal procedures and contingencies
SS38 - Place of Safety Procedure	procedure	Place of Safety	The set of rules that determines the operations of the Place of Safety node, including normal procedures and contingencies
SS40 - Distress Signal	information	Monitoring Node, C2 Node	see exchange elements
SS41 - Track Info	information	C2 Node	see exchange elements
SS42 - Request	information	Asset Controller	see exchange elements
SS43 - Control Order	information	Search Node, Rescue Node	see exchange elements
SS44 - Task	information	Search Node, Rescue Node	see exchange elements
SS45 - Task Response	information	Asset Controller	see exchange elements
SS46 - Allocation	information	C2 Node	see exchange elements

SS47 -Control Order Response	information	C2 Node	see exchange elements
SS48 - Medical Condition	information	Rescue Node	see exchange elements
SS49 - Warning Order	information	Place of Safety	see exchange elements

Observations:

The list of system assets is identified as the result of analysis of the Operational Views of the reference SAR Enterprise model. The information on people assets is derived from the OV-4 Typical Organizational Relationships Chart. The validation of the list involves making sure that there is at least one system asset for each performer and each operational exchange needline within the scope of assessment, and that each element of the asset category has been considered.

We have ***High Confidence*** in the list of system assets. We believe that the granularity of the system asset identification (which largely determines the granularity of the threat model) is commensurate with the purpose of this assessment and the level of detail in the reference SAR model.

5.2 Primary Assets

The following table captures the list of Primary Assets associated with the SAR Enterprise.

Table 21: Primary Assets

Primary Asset	Category	Description
A01 - Person In Distress	People	The operator of the yacht in distress as well as any crew members and passengers on board.
A02 - SAR Personnel	People	The employees of the SAR enterprise.
A03 - Location of Person In Distress	Information	If the bad guys come there first they can cause harm.
A04 - Location of the Search Node	Information	If the bad guys know where the Search Node is going to be, they can cause damage to it. Also they may know where the Person In Distress might be.
A05 - Location of the Rescue Node	Information	If the bad guys know where the Rescue Node is going to be, they can cause damage to it. Also they may know where the Person In Distress might be.
A06 - SAR Capacity	Information	The assets and resources available for SAR. If the bad guys have this information they can predict what the SAR operator will do. They can plan to exceed the capacity of the SAR operator.
A07 - Land Environment	Environment	Search Nodes are involved in SAR operations, and they are also hazards that can pollute the environment.

A08 - Maritime Environment	Environment	Rescue nodes are involved in SAR operations, and they are also hazards that can pollute the environment.
A10 - SAR Resources	Other	For example, fuel, money, medical supplies, emergency equipment, spare parts, hours available on engines before maintenance, personnel available for operations.
A11 - Maritime Assistance Capability	Capability	This involves assets, people and resources to perform maritime assistance
A12 - Distress Signal Monitoring Capability	Capability	This involves assets, people and resources to perform distress signal monitoring. The only part that is within the scope of the responsibility of the SAR stakeholders is the Track Info interface. The rest is the responsibility of the Satellite Operator.
A13 - Maritime Rescue Capability	Capability	This involves assets, people and resources to perform maritime rescue
A14 - SAR C2 Capability	Capability	This involves assets, people and resources to perform tactical C2 for SAR operations
A15 - Maritime Search Capability	Capability	This involves assets, people and resources to perform maritime search
A16 - SAR operator image	Other	This involves reputation and image of the SAR operator
A17 - Other persons	People	bystanders, civilians

5.3 Primary Asset to Stakeholder

The following table captures the Stakeholders associated with the Primary Assets for the SAR Enterprise.

Table 22: Primary Asset to Stakeholder

Primary Asset	Stakeholder
A01 - Person In Distress	ST01 - SAR Operator
A02 - SAR Personnel	ST01 - SAR Operator
A03 - Location of Person In Distress	ST01 - SAR Operator, ST02 - C2 Operator
A04 - Location of the Search Node	ST01 - SAR Operator, ST02 - C2 Operator
A05 - Location of the Rescue Node	ST01 - SAR Operator, ST02 - C2 Operator
A06 - SAR Capacity	ST01 - SAR Operator
A07 - Land Environment	ST01 - SAR Operator
A08 - Maritime Environment	ST01 - SAR Operator
A10 - SAR Resources	ST01 - SAR Operator

A11 - Maritime Assistance Capability	ST01 - SAR Operator, ST02 - C2 Operator
A12 - Distress Signal Monitoring Capability	ST02 - C2 Operator
A13 - Maritime Rescue Capability	ST01 - SAR Operator, ST02 - C2 Operator
A14 - SAR C2 Capability	ST02 - C2 Operator
A15 - Maritime Search Capability	ST01 - SAR Operator, ST02 - C2 Operator
A16 - SAR operator image	ST01 - SAR Operator
A17 - Other persons	ST01- SAR Operator

5.4 Statement of Sensitivity

The following table captures the sensitivity of the Primary Assets associated with the SAR Enterprise with respect to the security criteria identified in the scope of the assessment.

Table 23: Primary Assets to Sensitivity Levels

Primary Asset	Sensitivity	Security Criterion	Sensitivity Level
A07 - Land Environment	SE07 - Pollution to the land environment	Environment	High
A08 - Maritime Environment	SE08 - Pollution to the maritime environment	Environment	High
A01 - Person In Distress	SE01 - person in distress health is compromised	Health	High
A02 - SAR Personnel	SE02 - SAR personnel health is compromised	Health	High
A03 - Location of Person In Distress	SE03 - Location of person in distress is disclosed	Confidentiality	Medium
A03 - Location of Person In Distress	SE11 - Location of person in distress is lost	Availability	Medium
A03 - Location of Person In Distress	SE12 - Location of person in distress is inaccurate	Integrity	Medium
A04 - Location of the Search Node	SE04 - Location of the search node is disclosed	Confidentiality	Medium
A05 - Location of the Rescue Node	SE05 - Location of the rescue node is disclosed	Confidentiality	Medium
A06 - SAR Capacity	SE06 - SAR capacity is disclosed	Confidentiality	Medium
A10 - SAR Resources	SE10 - SAR resource is not available	Availability	Medium
A11 - Maritime Assistance Capability	SE12 - Maritime assistance capability is not available (fully or partially/delayed)	Availability	Medium

A12 - Distress Signal Monitoring Capability	SE13 - Distress signal monitoring capability is not available (fully or partially/delayed)	Availability	High
A13 - Maritime Rescue Capability	SE14 - Maritime rescue capability is not available (fully or partially/delayed)	Availability	Medium
A14 - SAR C2 Capability	SE16 - SAR C2 capability is not available (fully or partially/delayed)	Availability	High
A15 - Maritime Search Capability	SE17 - Maritime search capability is not available (fully or partially/delayed)	Availability	High
A16 - SAR operator image	SE18 - Loss of reputation of the SAR operator	Availability	Medium

Section 6

Undesired Events Identification

Undesired events are the elements of the risk analysis framework that focus on the systematic identification of threats and risks based on their outcome and impact.

6.1 Risk Categories

Based on the security criteria considered in the previous section, we are going to consider the following 5 categories of risk:

- Category "Risks to Personnel"
- Category "Risks to Environment"
- Category "Risks to Information"
- Category "Risks to Capabilities"
- Category "Risks to Other Assets"

6.2 Risk Groups

Each risk category can be further expanded based on the operational information related to the SAR Enterprise into one or more risk groups. Further, each risk group includes one or more risks based on the severity. This produces the following top-down framework comprised of 50 risks based entirely on the outcome and impact.

Category "Risks to Personnel"
- Group “Risks to Person In Distress"
  - Risk "Catastrophic damage to person in distress", severity: Catastrophic
  - Risk "Critical damage to person in distress", severity: Critical
  - Risk "Marginal damage to person in distress", severity: Marginal
  - Risk "Negligible damage to person in distress", severity: Negligible
- Group "Risks to Search personnel"
  - Risk "Catastrophic damage to search personnel", severity: Catastrophic
  - Risk "Critical damage to search personnel", severity: Critical
  - Risk "Marginal damage to search personnel", severity: Critical
  - Risk "Negligible damage to search personnel", severity: Negligible
- Group "Risks to Rescue personnel"
  - Risk "Catastrophic damage to rescue personnel", severity: Catastrophic
  - Risk "Critical damage to rescue personnel", severity: Critical
  - Risk "Marginal damage to rescue personnel", severity: Marginal
  - Risk "Negligible damage to rescue personnel", severity: Negligible
- Group "Risks to C2 personnel"

Risk "Catastrophic damage to control personnel", severity: Catastrophic
Risk "Critical damage to control personnel", severity: Critical
Risk "Marginal damage to control personnel", severity: Marginal
Risk "Negligible damage to control personnel", severity: Negligible
Group "Risks to POS personnel"
Risk "Catastrophic damage to POS personnel", severity: Catastrophic
Risk "Critical damage to POS personnel", severity: Critical
Risk "Marginal damage to POS personnel", severity: Marginal
Risk "Negligible damage to POS personnel", severity: Negligible
Group "Risks to Other Persons"
Risk "Catastrophic damage to other persons", severity: Catastrophic
Risk "Critical damage to other persons", severity: Critical
Risk "Marginal damage to other persons", severity: Marginal
Risk "Negligible damage to other persons", severity: Negligible

Category "Risks to Environment"
Group "Risks of Maritime Pollution"
Risk “Catastrophic maritime pollution", severity: Catastrophic
Risk “Critical maritime pollution", severity: Critical
Risk “Marginal maritime pollution", severity: Marginal
Risk “Negligible maritime pollution", severity: Negligible
Group "Risks of Land Pollution"
Risk “Marginal land pollution", severity: Marginal
Risk “Negligible land pollution", severity: Negligible

Category "Risks to Information"
Group "Risks to Confidentiality of Location of Person In Distress"
Risk “Disclosure of location of person in distress", severity: Critical
Group "Risks to Confidentiality of Location of Search Node"
Risk “Disclosure of location of search node", severity: Negligible
Group "Risks to Confidentiality of Location of Rescue Node"
Risk “Disclosure of location of rescue node", severity: Negligible
Group "Risks to Confidentiality of SAR Capacity"
Risk “Disclosure of SAR capacity", severity: Critical
Group "Risks to Integrity of C2 Node"
Risk “Full subversion of C2 node", severity: Critical

Category "Risks to Capabilities"
Group "Risks to Monitoring Capability"
Risk “Full loss of capability to monitor", severity: Critical
Risk “Partial loss of capability to monitor", severity: Marginal
Group "Risks to Search Capability"
Risk “Full loss of capability to search", severity: Critical
Risk “Partial loss of capability to search", severity: Marginal
Group "Risks to Rescue Capability"
Risk “Full loss of capability to rescue", severity: Critical
Risk “Partial loss of capability to rescue", severity: Marginal

Category "Risks to Other Assets"
Group "Risks to SAR Resources"
Risk “Catastrophic loss of SAR resources", severity: Catastrophic

Risk “Critical loss of SAR resources", severity: Critical
Risk “Marginal loss of SAR resources", severity: Marginal
Risk “Negligible loss of SAR resources", severity: Negligible

Group "Risks to Third Party Property"
Risk “Catastrophic loss of property", severity: Catastrophic
Risk “Critical loss of property", severity: Critical

Group "Risks to Navigation in the area"
Risk “Critical loss of navigation", severity: Critical
Risk “Marginal loss of navigation", severity: Marginal
Risk “Negligible loss of navigation", severity: Negligible

Additional risks may involve risks to intangible assets, for example risk to the reputation of the SAR enterprise and risk to compliance. These risks were considered out of scope because the reference DoDAF model for the SAR Enterprise does not provide enough detail in this area.

6.3 Undesired Events

The following section captures the undesired events of the SAR Enterprise based on the identified risk categories and groups, and connects risks to primary assets.

The following table captures the list of Undesired Events associated with the SAR Enterprise.

Table 24: Undesired Events

Undesired Event	Severity	Sensitivity	Primary Asset	Stakeholder
UE01 - Damage to health of person in distress	High	SE01 - person in distress health compromised	A01 - Person In Distress	ST01 - SAR Operator
UE02 - Damage to Health of SAR personnel	High	SE02 - SAR personnel health compromised	A02 - SAR Personnel	ST01 - SAR Operator
UE03 - Damage to rescue node	High	SE02 - SAR personnel health compromised	A02 - SAR Personnel	ST01 - SAR Operator
UE03 - Damage to rescue node	High	SE08 - Pollution to the Maritime Environment	A08 - Rescue Node	ST01 - SAR Operator
UE04 - Damage to search node	Medium	SE02 - SAR personnel health compromised	A02 - SAR Personnel	ST01 - SAR Operator
UE04 - Damage to search node	Medium	SE07 - Pollution to the Land Environment, SE08 - Pollution to the Maritime Environment	A07 - Search Node	ST01 - SAR Operator
UE05 - loss of confidentiality of search node location	Medium	SE04 - Location of the search node disclosed	A04 - Location of the Search Node	ST01 - SAR Operator
UE06 - loss of confidentiality of person in distress location	High	SE03 - Location of person in distress disclosed	A03 - Location of Person In Distress	ST01 - SAR Operator

UE07 - loss of confidentiality of rescue node location	Medium	SE05 - Location of the rescue node disclosed	A05 - Location of the Rescue Node	ST01 - SAR Operator
UE08 - loss of confidentiality of SAR capacity	Medium	SE06 - SAR capacity disclosed	A06 - SAR Capacity	ST01 - SAR Operator
UE09 - loss of integrity of C2 node	High	SE09 - Integrity of the C2 node compromised	A09 - C2 Node	ST01 - SAR Operator
UE10 - loss of SAR resources	High	SE10 - SAR resources are depleted	A10 - SAR Resources	ST01 - SAR Operator

6.4 Undesired Events and Associated Impacts

The following table captures the list of Impacts associated with Undesired Events for the SAR Enterprise.

Table 25: Undesired Events and Impacts

Undesired Event	Severity	Impact
UE01 - Damage to health of person in distress	High	I03.01 - Accident
UE01 - Damage to health of person in distress	High	I03.03 - Loss of human lives
UE01 - Damage to health of person in distress	High	I03.04 - Endangerment
UE01 - Damage to health of person in distress	High	I06.02 - Unexpected expenses
UE01 - Damage to health of person in distress	High	I07.04 - Loss of reputation
UE01 - Damage to health of person in distress	High	I09.01 - Trial
UE01 - Damage to health of person in distress	High	I09.06 - Civil litigation
UE02 - Damage to Health of SAR personnel	High	I01.01 - Inability to provide a service
UE02 - Damage to Health of SAR personnel	High	I01.02 - Loss of expertize
UE02 - Damage to Health of SAR personnel	High	I03.01 - Accident
UE02 - Damage to Health of SAR personnel	High	I03.03 - Loss of human lives
UE02 - Damage to Health of SAR personnel	High	I04.01 - Loss of employee confidence
UE02 - Damage to Health of SAR personnel	High	I06.02 - Unexpected expenses
UE02 - Damage to Health of SAR personnel	High	I07.04 - Loss of reputation
UE02 - Damage to Health of SAR personnel	High	I09.01 - Trial
UE02 - Damage to Health of SAR personnel	High	I09.06 - Civil litigation
UE03 - Damage to rescue node	High	I01.01 - Inability to provide a service
UE03 - Damage to rescue node	High	I03.01 - Accident

UE03 - Damage to rescue node	High	I03.03 - Loss of human lives
UE03 - Damage to rescue node	High	I03.04 - Endangerment
UE03 - Damage to rescue node	High	I06.02 - Unexpected expenses
UE03 - Damage to rescue node	High	I06.06 - Damage to property
UE03 - Damage to rescue node	High	I07.04 - Loss of reputation
UE03 - Damage to rescue node	High	I08.01 - Loss of certification or license
UE03 - Damage to rescue node	High	I09.01 - Trial
UE03 - Damage to rescue node	High	I09.06 - Civil litigation
UE03 - Damage to rescue node	High	I10.01 - Pollution
UE04 - Damage to search node	Medium	I01.01 - Inability to provide a service
UE04 - Damage to search node	Medium	I03.01 - Accident
UE04 - Damage to search node	Medium	I03.03 - Loss of human lives
UE04 - Damage to search node	Medium	I03.04 - Endangerment
UE04 - Damage to search node	Medium	I06.02 - Unexpected expenses
UE04 - Damage to search node	Medium	I06.06 - Damage to property
UE04 - Damage to search node	Medium	I07.04 - Loss of reputation
UE04 - Damage to search node	Medium	I08.01 - Loss of certification or license
UE04 - Damage to search node	Medium	I09.01 - Trial
UE04 - Damage to search node	Medium	I09.06 - Civil litigation
UE04 - Damage to search node	Medium	I10.01 - Pollution
UE05 - loss of confidentiality of search node location	Medium	I03.04 - Endangerment
UE05 - loss of confidentiality of search node location	Medium	I06.06 - Damage to property
UE05 - loss of confidentiality of search node location	Medium	I08.02 - Loss of compliance
UE05 - loss of confidentiality of search node location	Medium	I09.01 - Trial
UE05 - loss of confidentiality of search node location	Medium	I11.04 - Exfiltration of confidential information
UE06 - loss of confidentiality of person in distress location	High	I03.04 - Endangerment
UE06 - loss of confidentiality of person in distress location	High	I08.02 - Loss of compliance
UE06 - loss of confidentiality of person in distress location	High	I09.01 - Trial
UE06 - loss of confidentiality of person in distress location	High	I09.06 - Civil litigation
UE06 - loss of confidentiality of person in distress location	High	I11.04 - Exfiltration of confidential information
UE07 - loss of confidentiality of rescue node location	Medium	I03.04 - Endangerment

UE07 - loss of confidentiality of rescue node location	Medium	I06.06 - Damage to property
UE07 - loss of confidentiality of rescue node location	Medium	I09.01 - Trial
UE07 - loss of confidentiality of rescue node location	Medium	I11.04 - Exfiltration of confidential information
UE08 - loss of confidentiality of SAR capacity	Medium	I02.02 - Loss or limitation of independence of judgment or decision
UE08 - loss of confidentiality of SAR capacity	Medium	I08.02 - Loss of compliance
UE08 - loss of confidentiality of SAR capacity	Medium	I09.01 - Trial
UE08 - loss of confidentiality of SAR capacity	Medium	I11.04 - Exfiltration of confidential information
UE09 - loss of integrity of C2 node	High	I01.01 - Inability to provide a service
UE09 - loss of integrity of C2 node	High	I02.02 - Loss or limitation of independence of judgment or decision
UE09 - loss of integrity of C2 node	High	I03.04 - Endangerment
UE09 - loss of integrity of C2 node	High	I06.02 - Unexpected expenses
UE09 - loss of integrity of C2 node	High	I06.06 - Damage to property
UE09 - loss of integrity of C2 node	High	I07.04 - Loss of reputation
UE09 - loss of integrity of C2 node	High	I08.01 - Loss of certification or license
UE09 - loss of integrity of C2 node	High	I08.02 - Loss of compliance
UE09 - loss of integrity of C2 node	High	I09.01 - Trial
UE09 - loss of integrity of C2 node	High	I09.02 - Fine
UE10 - loss of SAR resources	High	I01.01 - Inability to provide a service
UE10 - loss of SAR resources	High	I02.02 - Loss or limitation of independence of judgment or decision
UE10 - loss of SAR resources	High	I03.04 - Endangerment
UE10 - loss of SAR resources	High	I06.02 - Unexpected expenses
UE10 - loss of SAR resources	High	I07.04 - Loss of reputation

6.5 Evaluation of Undesired Events

The following table describes the prioritization of the Undesired Events based on the severity for the SAR Enterprise.

Table 26: Evaluation of Undesired Events

Undesired Event	Severity
UE01 - Damage to health of person in distress	High
UE02 - Damage to Health of SAR personnel	High
UE03 - Damage to rescue node	High
UE04 - Damage to search node	Medium
UE05 - loss of confidentiality of search node location	Medium
UE06 - loss of confidentiality of person in distress location	High
UE07 - loss of confidentiality of rescue node location	Medium
UE08 - loss of confidentiality of SAR capacity	Medium
UE09 - loss of integrity of C2 node	High
UE10 - loss of SAR resources	High

Section 7

Threat Scenario Identification

Threat Scenarios systematically describe attacks on the system. Threat Scenarios are based on the cause and effect sequences of activities initiated by an attack involving a certain entry point of the system, which then causes a sequence of events that (eventually) cause one of the undesired events. In order to systematically identify attacks

7.1 Attack Modes

Attack modes are categories of injury describing a specific kind of compromise to assets as an outcome of attack especially resulting from deliberate threats but also covering accidental threats and natural hazards. Attack modes are used to systematically and objectively identify threats. The following table captures the attack modes selected within the scope of the security assessment of the SAR Enterprise.

Table 27: Attack Modes

Attack Mode	Description
Abuse	System assets are used for purposes other than those intended; without being altered or damaged. Abuse of hardware or equipment causes depletion of resources and unavailability. Abuse of software may result in unauthorized access to information, improper removal or modification of information. Abuse of communication channels may result in the flow of information being altered, slowed of blocked. Abuse of personnel may result in decreased performance or unavailability. Abuse of business process may affect the flow of information which can be altered, slowed down, or blocked
Damage	System assets are damaged, partially or completely, temporarily or permanently, inside or outside the premises. As the result, the system assets can fail, or break down and can no longer be used.
Exceeding Limits of Operation	System assets are overloaded or used beyond their operating limits. Exceeding limits of operation of hardware may result in failures or temporary malfunction. In case of software this attack may cause malfunction, interrupts, delays, breaking down or subversion. Overloading communication channels may result in the flow of information being slowed down or blocked. Overloading personnel or business processes may result in decreased performance.
Information Gathering	System assets are being observed, with or without additional equipment; without being damaged.
Loss	system assets are absent (lost, stolen, sold, given away...) without being altered or damaged, so that they are no longer be available for normal operation and be available for others, for example for information gathering or abuse.

Modification	System assets are modified; by the removal, addition, substitution or disabling an item inside or outside the premises. As the result the modified asset may fail, malfunction or operate differently than its normal operation. Examples include improper handling during the update, configuration or maintenance. Modification of assets may enable information gathering, for example via wiretapping. A person can be coerced, inside or outside the premises and thus be brought to act inappropriately or disclose information. Examples include pressure, corruption or manipulation (via money, ideology, blackmail, ego boosts ...), phishing, social engineering, harassment, torture, misinformation, indoctrination, rumor.

7.2 Entry Points

The following table captures the Entry Points for the SAR Enterprise.

Table 28: Entry Points

Entry Point	Performer	Description	Category
Ep01 - Yacht equipment	Person In Distress	Yacht equipment can malfunction, can be sabotaged, modified, abused or damaged; physical damage to the yacht itself is considered to be outside of the scope of the assessment	Local Access
Ep03 - Distress Signal	Monitoring Node	Distress signal can be jammed, intercepted or spoofed	Remote Access
Ep04 - Monitoring Node equipment	Monitoring Node	Monitoring node equipment can malfunction or be damaged, for example due to operator error	Local Access
Ep05 - Track Info	Tactical C2 Node	Track info can be jammed, intercepted or spoofed	Remote Access
Ep06 - Control Order Response	Tactical C2 Node	Control order response can be jammed, intercepted or spoofed	Remote Access
Ep07 - Asset Allocation	Tactical C2 Node	Asset Allocation response can be jammed, intercepted or spoofed	Remote Access
Ep08 - C2 Node software Remote	Tactical C2 Node	Remotely accessible entry points into the software (e.g. open ports) can be used for attacks	Remote Access
Ep09 - C2 Node software Local	Tactical C2 Node	Locally accessible entry points (e.g. local files, configuration files) can be used for insider attacks	Local Access
Ep10 - Request	Asset Controller	Request can be jammed, intercepted or spoofed	Remote Access
Ep11 - Asset Controller software Remote	Asset Controller	Remotely accessible entry points into the asset controller software can be exploited by attackers	Remote Access
Ep12 - Asset Controller software Local	Asset Controller	Locally accessible entry points into the asset controller software can be used by malicious insiders	Local Access

Ep13 - Search Node Task	Search Node	Search Node Task can be jammed, intercepted or spoofed	Remote Access
Ep14 - Search Control Order	Search Node	Search Control Order can be jammed, intercepted or spoofed	Remote Access
Ep15 - Search Node Distress Signal	Search Node	Search Node Distress Signal can be jammed, intercepted or spoofed/faked	Remote Access
Ep16 - Search Node equipment	Search Node	Search Node equipment can malfunction, can be sabotaged, damaged or modified	Local Access
Ep17 - Rescue Node Task	Rescue Node	Rescue Node Task can be jammed, intercepted or spoofed	Remote Access
Ep18 - Rescue Control Order	Rescue Node	Rescue Control Order can be jammed, intercepted or spoofed	Remote Access
Ep19 - Rescue Node Distress Signal	Rescue Node	Rescue Node Distress Signal can be jammed, intercepted or spoofed/faked	Remote Access
Ep20 - Rescue Node equipment	Rescue Node	Rescue Node equipment can malfunction, can be damaged	Local Access
Ep21 - Warning Order	Place of Safety	Warning Order can be jammed, intercepted or spoofed	Remote Access
Ep22 - Victim	Rescue Node		Local Access
Ep23 - Place of Safety equipment	Place of Safety	Place of Safety equipment can malfunction, can be damaged	Local Access
Ep24 - C2 node equipment	Tactical C2 Node	C2 Node equipment can malfunction, can be sabotaged, modified or damaged	Local Access
Ep25 - C2 node facility	Tactical C2 Node	C2 Node facility can malfunction, can be damaged or modified	Local Access

7.3 Exit Points

The following table captures the Exit Points for the SAR Enterprise.

Table 29: Exit Points

Exit Point	Performer	Description	Category
Exp01 - Distress Signal	Person In Distress	Distress Signal can reveal the fact of the distress and the location of the person in distress, as well as potential future location of the rescue node.	Message

Exp02 - Track Info	Monitoring Node, Tactical C2 Node	Track Info signal can reveal the fact of the distress and the location of the person in distress as well the future location of the rescue node	Message
Exp03 - Request	Tactical C2 Node, Asset Controller	Asset Allocation Request can reveal the fact of the distress	Message
Exp04 - Control Order	Tactical C2 Node, Search Node or Rescue Node	Control Order can reveal the fact of the ongoing SAR operation and the location of the rescue node	Message
Exp05 - Task	Asset Controller, Search Node or Rescue Node	Task signal can reveal the fact of the ongoing SAR operation	Message
Exp06 - Allocation	Asset Controller, Tactical C2 Node	Response to the Allocation Request can reveal the SAR capacity	Message
Exp07 - Control Order Response	Search Node, Tactical C2 Node	Response to the Control Order from the search node can reveal the fact of the ongoing SAR operation and potentially the location of the person in distress	Message
Exp08 - Medical Condition	Search Node, Rescue Node	Response to the Control Order can reveal the fact of the distress, the status of the person in distress and possibly the location of the person in distress	Message
Exp09 - Warning Order	Search Node, Place of Safety	Warning Order can reveal the fact of the ongoing SAR operation and the location of the rescue node	Message
Exp10 - Control Order Response	Rescue Node, Tactical C2 Node	Response to the Control Order from the rescue node can reveal the fact of the ongoing SAR operation and potentially the location of the rescue node	Message
Exp12 - Operational Data Local	Tactical C2 Node	Operational Data Accessible Locally to the C2 Node, e.g. on the operator's display; can reveal the location of the person in distress, rescue node, SAR capacity	Local Access
Exp13 - Operational Data Remote	Tactical C2 Node	Operational Data Accessible Remotely, e.g. by remote access to a database, or through an api. can reveal the location of the person in distress, rescue node, SAR capacity	Remote Access

7.4 Attack Groups

The following table captures the list of Attack Groups identified for the SAR Enterprise. Attack Groups provide a systematic framework for identification of individual Threat Events and combined Threat Scenarios.

Table 30: Attack Groups

Attack Group	Performer	Attack Mode
TS1.1 - Abuse of Person In Distress	P02 - Person In Distress	Abuse
TS1.2 - Exceeding the limits of Person In Distress	P02 - Person In Distress	Exceeding Limits of Operation
TS1.3 - Damage to Person In Distress	P02 - Person In Distress	Damage
TS1.4 - Modification of Person In Distress	P02 - Person In Distress	Modification
TS1.5 - Loss of Person In Distress	P02 - Person In Distress	Loss
TS1.6 - Information gathering on Person In Distress	P02 - Person In Distress	Information Gathering
TS2.1 - Abuse of Monitoring Node	P01 - Monitoring Node	Abuse
TS2.2 - Exceeding the limits of the Monitoring Node	P01 - Monitoring Node	Exceeding Limits of Operation
TS2.3 - Damage to Monitoring Node	P01 - Monitoring Node	Damage
TS2.4 - Modification of Monitoring Node	P01 - Monitoring Node	Modification
TS2.5 - Loss of Monitoring Node	P01 - Monitoring Node	Loss
TS2.6 - Information gathering on Monitoring Node	P01 - Monitoring Node	Information Gathering
TS3.1 - Abuse of C2 Node	P08 - Tactical C2 Node	Abuse
TS3.2 - Exceeding the limits of the C2 Node	P08 - Tactical C2 Node	Exceeding Limits of Operation
TS3.3 - Damage to C2 Node	P08 - Tactical C2 Node	Damage
TS3.4 - Loss of C2 Node	P08 - Tactical C2 Node	Loss
TS3.5 - Modification of C2 Node	P08 - Tactical C2 Node	Modification
TS3.6 - Information gathering on C2 Node	P08 - Tactical C2 Node	Information Gathering
TS4.1 - Abuse of Asset Controller	P05 - SAR Asset Controller	Abuse
TS4.2 - Exceeding the limits of the Asset Controller	P05 - SAR Asset Controller	Exceeding Limits of Operation
TS4.3 - Damage to Asset Controller	P05 - SAR Asset Controller	Damage

TS4.4 - Loss of Asset Controller	P05 - SAR Asset Controller	Loss
TS4.5 - Modification of Asset Controller	P05 - SAR Asset Controller	Modification
TS4.6 - Information gathering on Asset Controller	P05 - SAR Asset Controller	Information Gathering
TS5.1 - Abuse of Search Node	P07 - Search Node	Abuse
TS5.2 - Exceeding the limits of the Search Node	P07 - Search Node	Exceeding Limits of Operation
TS5.3 - Damage to Search Node	P07 - Search Node	Damage
TS5.4 - Loss of Search Node	P07 - Search Node	Loss
TS5.5 - Modification of Search Node	P07 - Search Node	Modification
TS5.6 - Information gathering on Search Node	P07 - Search Node	Information Gathering
TS6.1 - Abuse of Rescue Node	P04 - Rescue Node	Abuse
TS6.2 - Exceeding the limits of the Rescue Node	P04 - Rescue Node	Exceeding Limits of Operation
TS6.3 - Damage to Rescue Node	P04 - Rescue Node	Damage
TS6.4 - Loss of Rescue Node	P04 - Rescue Node	Loss
TS6.5 - Modification of Rescue Node	P04 - Rescue Node	Modification
TS6.6 - Information gathering on Rescue Node	P04 - Rescue Node	Information Gathering
TS7.1 - Abuse of Place of Safety	P03 - Place of Safety	Abuse
TS7.2 - Exceeding the limits of the Place of Safety	P03 - Place of Safety	Exceeding Limits of Operation
TS7.3 - Damage to Place of Safety	P03 - Place of Safety	Damage
TS7.4 - Loss of Place of Safety	P03 - Place of Safety	Loss
TS7.5 - Modification of Place of Safety	P03 - Place of Safety	Modification
TS7.6 - Information gathering on Place of Safety	P03 - Place of Safety	Information Gathering

7.5 Threat Events and Threat Sources

This section captures individual Threat Events with associated Attack Modes and Threat Sources for the SAR Enterprise. Threat Events are grouped by Performers and by Attack Modes. The next section describes how combinations of Threat Events are combined into Threat Scenarios and cause the Undesired Events. In order to provide better resolution to the Threat Events, we are considering 4 distinct failure events for each performer:

Catastrophic failure, Critical failure, Marginal failure and Negligible failure. This allows us to give different estimates to these events and to separately track their causal relationships to the Undesired Events of different severity. This decision has inflated the number of identified risks.

Performer Person in Distress
- Event "Catastrophic failure of Person in Distress"
  - Damage by
    - Fire : Probable
    - Maritime conditions : Probable
    - Terrorist : Remote
  - Modification by
    - Terrorist : Improbable
    - Criminal : Remote

- Event "Critical failure of Person in Distress"
  - Abuse by
    - Person in distress error : Probable
  - Exceeding Limits by
    - Person in distress error : Probable
  - Damage by
    - Fire: Probable
    - Maritime conditions : Probable
    - Terrorist: Remote
    - Maintenance error : Occasional
    - Malicious maintenance : Improbable
    - Supplier error : Occasional
    - Operator error : Remote
  - Modification by
    - Terrorist : Improbable
    - Criminal : Remote

- Event "Marginal failure of Person in Distress"
  - Abuse by
    - Person in distress error : Probable
  - Exceeding Limits by
    - Person in distress error : Probable
  - Damage by
    - Fire : Occasional
    - Equipment failure : Probable
    - Maritime conditions : Probable
    - Maintenance error : Remote
    - Malicious maintenance : Improbable
    - Supplier error : Remote
    - Operator error : Occasional

- Event "Negligible failure of Person in Distress"
  - Abuse
    - Person in distress error : Frequent
  - Exceeding Limits
    - Person in distress error : Probable
    - Maritime conditions : Probable

Damage
Maritime conditions : Occasional
Equipment failure : Probable
Operator error : Occasional
Loss
Criminal : Occasional

###

Event "Person in distress is unable to send distress signal"
Damage
Equipment failure : Probable
Maintenance error : Probable
Person in distress error : Occasional
Modification
Maintenance error : Occasional
Supplier error : Remote
Malicious maintenance : Improbable
Criminal : Remote

Event "Person in distress is unable to communicate to search node"
Abuse
Terrorist : Remote
Damage
Equipment failure : Probable

Event "Person in distress is unable to communicate to rescue node"
Abuse
Terrorist : Remote
Person in distress error : Probable
Damage
Equipment failure : Probable

Event "Rescue node damages person in distress"
Abuse
Operator error : Remote
Person in distress error : Probable
Damage
Equipment failure : Remote

Event "Incorrect information is sent to search node"
Abuse
Malicious person in distress : Improbable
Person in distress error : Occasional
Terrorist : Remote

Event "Incorrect information is sent to rescue node"
Abuse
Malicious person in distress : Improbable
Person in distress error : Occasional
Terrorist : Remote

information events

```
        Event "Person in distress discloses location"
                Abuse
                        Person in distress error :Occasional
                Spying
                        Terrorist : Remote
                        Hacker :Remote
                Modification
                        Hacker :Improbable
                        Equipment failure :Improbable

        Event "Person in distress discloses location of search node"
                Abuse
                        Person in distress error :Remote
                Spying
                        Terrorist : Improbable
                        Hacker :Improbable

        Event "Person in distress discloses location of rescue node"
                Abuse
                        Person in distress error :Remote
                Spying
                        Terrorist :Improbable
                        Hacker :Improbable

#
#####################################################
#
Performer MonitoringNode
        Event "Catastrophic failure of monitoring node"
                Damage
                         Space conditions :Remote
                         Equipment failure  :Remote
                Modification
                        Operator error :Remote

        Event "Critical failure of monitoring node"
                Abuse
                        Operator error :Occasional
                Damage
                         Space conditions :Remote
                         Equipment failure  :Occasional
                Modification
                        Operator error :Occasional

        Event "Marginal failure of monitoring node"
                Abuse
                        Hacker :Remote
                        Operator error : Occasional
                Damage
                        Space conditions :Remote
                        Equipment failure :Probable
```

Modification
Operator error : Occasional

Event "Negligible failure of monitoring node"
Abuse
Hacker :Occasional
Operator error :Probable
Damage
Space conditions :Occasional
Equipment failure :Occasional
Modification
Operator error :Occasional

###
Event "Monitoring node is unable to receive distress signal"
Abuse
Hacker :Occasional
Operator error :Remote
Damage
Space conditions : Remote
Equipment failure :Occasional
Modification
Operator error :Remote

Event "Monitoring node receives incorrect location"
Damage
Space conditions : Remote
Equipment failure : Remote
Modification
Operator error :Remote

Event "Monitoring node is unable to send track info"
Abuse
Hacker : Occasional
Damage
Space conditions : Remote
Equipment failure : Occasional
Modification
Maintenance error : Occasional

Event "Monitoring node sends incorrect track info"
Abuse
Hacker : Remote
Operator error : Remote
Damage
Space conditions : Remote
Equipment failure : Occasional
Modification
Operator error : Remote
Targeted virus : Improbable

```
        Event "Monitoring node delays track info"
                Abuse
                        Hacker :Remote
                        Operator error: Remote
                Damage
                        Space conditions : Improbable
                        Equipment failure : Probable
                Modification
                        Operator error : Occasional
                        Targeted virus : Remote
#
### information events ####
#
        Event "Monitoring node discloses location of person in distress"
                Abuse
                        Operator error : Occasional
                Spying
                        Terrorist : Remote
                        Hacker : Occasional

        Event "Monitoring node discloses location of search node"
                Spying
                        Terrorist : Improbable
                        Hacker : Improbable

        Event "Monitoring node discloses location of rescue node"
                Spying
                        Terrorist : Improbable
                        Hacker : Improbable

#
#######################################################
#

Performer C2Node
        Event "Catastrophic failure of C2 node"
                Damage
                        Land conditions :Improbable
                        Fire :Occasional
                        Terrorist : Improbable

        Event "Critical failure of C2 node"
                Damage
                        Land conditions :Occasional
                        Fire :Occasional
                        Terrorist : Improbable
                        Maintenance error: Improbable
                        Equipment failure: Remote

        Event "Marginal failure of C2 node"
                Abuse
```

Operator error : Occasional
Damage
Land conditions :Remote
Fire :Occasional
Terrorist : Improbable
Equipment failure : Occasional
Non-targeted virus: Occasional

Event "Negligible failure of C2 node"
Abuse
Operator error : Probable
Damage
Land conditions : Occasional
Fire : Occasional
Electrical failure : Probable
Equipment failure : Probable
Terrorist : Remote
Non-targeted virus: Occasional

###

Event "C2 node is unable to receive track info"
Abuse
Terrorist :Improbable
Operator error: Remote
Damage
Equipment failure :Occasional
Land conditions :Remote

Event "C2 node receives incorrect track info"
Abuse
Terrorist :Improbable
Operator error: Remote
Damage
Equipment failure :Remote

Event "C2 node is unable to communicate to search node"
Abuse
Terrorist :Improbable
Operator error :Remote
Damage
Equipment failure :Occasional
Land conditions :Remote
Exceeding Limits
Operator error :Remote

Event "C2 node is unable to communicate to rescue node"
Abuse
Terrorist :Improbable
Operator error :Remote
Damage
Equipment failure :Occasional

Land conditions :Remote
Maritime conditions :Remote
Exceeding Limits
Operator error :Remote

Event "C2 node is unable to communicate to POS"
Abuse
Terrorist :Improbable
Operator error :Remote
Damage
Equipment failure :Occasional
Land conditions :Remote
Maritime conditions :Remote

Event "C2 node sends incorrect control order to search node"
Abuse
Operator error :Probable
Terrorist :Improbable
Modification
Targeted virus :Improbable

Event "C2 node sends incorrect control order to rescue node"
Abuse
Operator error :Probable
Terrorist :Improbable
Modification
Targeted virus :Improbable

Event "C2 node loses data for the SAR operation"
Abuse
Hacker: Occasional
Operator error :Occasional
Damage
Equipment failure :Probable
Fire :Probable
Electrical failure :Probable
Land conditions :Remote
Non-targeted virus :Occasional
Targeted virus :Remote
Supplier error :Remote

Event "C2 delays launching SAR operation"
Abuse
Operator error :Probable
Damage
Non-targeted virus :Occasional
Targeted virus :Remote
Land conditions :Occasional
Maritime conditions :Probable
Electrical failure :Occasional

Event "C2 fails to launch SAR operation"
- Abuse
  - Operator error :Occasional

Event "C2 launches inappropriate SAR operation"
- Abuse
  - Operator error :Probable

Event "C2 delays control order to search node"
- Abuse
  - Operator error :Probable
- Damage
  - Non-targeted virus :Occasional
  - Targeted virus :Remote
  - Fire :Remote
  - Electrical failure :Occasional
  - Land conditions :Remote
  - Maritime conditions :Remote

Event "C2 delays control order to rescue node"
- Abuse
  - Operator error :Probable
- Damage
  - Non-targeted virus :Occasional
  - Targeted virus :Remote
  - Fire :Remote
  - Electrical failure :Occasional
  - Land conditions :Remote
  - Maritime conditions :Occasional

Event "C2 incorrectly cancels SAR operation"
- Abuse
  - Operator error :Probable
  - Criminal :Remote

Event "C2 aborts SAR operation"
- Abuse
  - Operator error :Probable
  - Criminal :Remote
- Exceeding Limits
  - Land conditions : Occasional
  - Maritime conditions :Occasional
  - Insufficient resources :Remote

Event "C2 restarts search"
- Abuse
  - Operator error : Probable
- Exceeding capacity
  - Land conditions : Occasional
  - Maritime conditions : Probable
  - Insufficient resources : Probable

```
        Event "C2 restarts rescue"
                Abuse
                        Operator error : Probable
                Exceeding capacity
                        Land conditions :Occasional
                        Maritime conditions :Probable
                        Insufficient resources :Probable

        Event "C2 restarts transfer"
                Abuse
                        Operator error : Occasional
                Exceeding Limits
                        Land conditions :Remote
                        Maritime conditions :Probable
                        Insufficient resources :Occasional

#
### information events ####
#
        Event "C2 node discloses location of person in distress"
                Abuse
                        Operator error :Remote
                Spying
                        Terrorist :Remote

        Event "C2 node discloses location of search node"
                Abuse
                        Operator error :Remote
                Spying
                        Terrorist :Remote

        Event "C2 node discloses location of rescue node"
                Abuse
                        Operator error :Remote
                Spying
                        Terrorist :Remote

        Event "C2 node discloses SAR capacity"
                Abuse
                        Operator error :Occasional
                Spying
                        Terrorist :Occasional

        Event "Full subversion of C2 node"
                Abuse
                        Hacker :Occasional
                Modification
                        Targeted virus :Remote
                        Botnet :Occasional
```

```
#
#####################################################
#

Performer SearchNode
        Event "Catastrophic failure of search node"
                Abuse
                        Operator error : Remote
                Damage
                        Weather conditions : Occasional
                        Equipment failure : Remote
                        Fire       : Remote
                        Terrorist : Improbable
                Exceeding capacity
                        Operator error : Remote
                Modification
                        Maintenance error : Remote
                        Malicious maintenance : Improbable
                        Supplier error : Improbable

        Event "Critical failure of search node"
                Abuse
                        Operator error : Occasional
                Damage
                        Weather conditions : Occasional
                        Equipment failure : Occasional
                        Fire       : Occasional
                        Terrorist : Improbable
                Exceeding Limits
                        Operator error : Occasional
                Modification
                        Maintenance error : Occasional
                        Malicious maintenance : Improbable
                        Supplier error : Remote

        Event "Marginal failure of search node"
                Abuse
                        Operator error : Probable
                Damage
                        Weather conditions : Probable
                        Equipment failure : Occasional
                        Fire       : Occasional
                        Terrorist : Improbable
                Exceeding Limits
                        Operator error : Occasional
                Modification
                        Maintenance error : Remote
                        Malicious maintenance : Improbable
                        Supplier error : Remote

        Event "Negligible failure of search node"
```

Abuse
Operator error : Probable
Damage
Weather conditions : Probable
Equipment failure : Occasional
Fire : Occasional
Terrorist : Improbable
Exceeding Limits
Operator error : Probable
Modification
Maintenance error : Remote
Malicious maintenance : Improbable
Supplier error : Remote

###

Event "Search node fails to find person in distress"
Damage
Equipment failure: Occasional
Exceeding capacity
Weather conditions: Probable
Equipment failure: Occasional
Operator error: Occasional

Event "Search node delays SAR operation"
Abuse
Operator error: Occasional
Damage
Non-targeted virus: Remote
Equipment failure: Occasional
Weather conditions: Probable

Event "Search node is unable to communicate to person in distress"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Occasional

Event "Search node is unable to communicate to C2 node"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Remote

Event "Search node is unable to communicate to rescue node"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Remote

```
        Event "Search node is unable to communicate to POS"
                Damage
                        Operator error: Occasional
                        Maintenance error: Remote
                        Supplier error: Improbable
                        Weather conditions: Remote

        Event "Search node sends incorrect track info to C2 node"
                Abuse
                        Terrorist: Improbable
                        Operator error: Occasional

        Event "Search node sends incorrect warning order to POS"
                Abuse
                        Terrorist: Improbable
                        Operator error: Occasional

        Event "Search node sends incorrect status to rescue node"
                Abuse
                        Terrorist: Improbable
                        Operator error: Occasional

        Event "Search node receives incorrect control order"
                Abuse
                        Terrorist: Improbable
                        Operator error: Occasional

#
### information events ####
#
        Event "Search node discloses location of person in distress"
                Abuse
                        Operator error :Remote
                Spying
                        Terrorist :Improbable

        Event "Search node discloses location of search node"
                Abuse
                        Operator error :Remote
                Spying
                        Terrorist :Improbable

        Event "Search node discloses location of rescue node"
                Abuse
                        Operator error :Improbable
                Spying
                        Terrorist :Improbable

#
#######################################################
```

```
#

Performer RescueNode
        Event "Catastrophic failure of rescue node"
                Abuse
                        Operator error : Remote
                Damage
                        Weather conditions : Occasional
                        Equipment failure : Remote
                        Fire       : Remote
                        Terrorist : Improbable
                Exceeding Limits
                        Operator error : Remote
                Modification
                        Maintenance error : Remote
                        Malicious maintenance : Improbable
                        Supplier error : Improbable

        Event "Critical failure of rescue node"
                Abuse
                        Operator error : Occasional
                Damage
                        Weather conditions : Occasional
                        Equipment failure : Occasional
                        Fire       : Occasional
                        Terrorist : Improbable
                Exceeding Limits
                        Operator error : Occasional
                Modification
                        Maintenance error : Occasional
                        Malicious maintenance : Improbable
                        Supplier error : Remote

        Event "Marginal failure of rescue node"
                Abuse
                        Operator error : Probable
                Damage
                        Weather conditions : Probable
                        Equipment failure : Occasional
                        Fire       : Occasional
                        Terrorist : Improbable
                Exceeding Limits
                        Operator error : Occasional
                Modification
                        Maintenance error : Remote
                        Malicious maintenance : Improbable
                        Supplier error : Remote

        Event "Negligible failure of rescue node"
                Abuse
                        Operator error : Probable
```

Damage
Weather conditions : Probable
Equipment failure : Occasional
Fire : Occasional
Terrorist : Improbable
Exceeding Limits
Operator error : Probable
Modification
Maintenance error : Remote
Malicious maintenance : Improbable
Supplier error : Remote

####

Event "Rescue node fails to find person in distress"
Damage
Equipment failure: Occasional
Exceeding capacity
Weather conditions: Probable
Equipment failure: Occasional
Operator error: Occasional

Event "Rescue node fails to rescue person in distress"
Damage
Equipment failure: Occasional
Exceeding Limits
Weather conditions: Probable
Equipment failure: Occasional
Operator error: Occasional

Event "Rescue node fails to find place of safety"
Damage
Equipment failure: Occasional
Exceeding Limits
Weather conditions: Probable
Equipment failure: Occasional
Operator error: Occasional

Event "Rescue node fails to transfer person in distress"
Damage
Equipment failure: Occasional
Exceeding Limits
Weather conditions: Probable
Equipment failure: Occasional
Operator error: Occasional

Event "Rescue node delays SAR operation"
Abuse
Operator error: Occasional
Damage
Non-targeted virus: Remote

Equipment failure: Occasional
Weather conditions: Probable

Event "Rescue node is unable to communicate to person in distress"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Occasional

Event "Rescue node is unable to communicate to C2 node"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Remote

Event "Rescue node is unable to communicate to search node"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Remote

Event "Rescue node is unable to communicate to POS"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Remote

Event "Rescue node sends incorrect track info to C2 node"
Abuse
Terrorist: Improbable
Operator error: Occasional

Event "Rescue node sends incorrect warning order to place of safety"
Abuse
Terrorist: Improbable
Operator error: Occasional

Event "Rescue node receives incorrect control order"
Abuse
Terrorist: Improbable
Operator error: Occasional

Event "Rescue node damages person in distress"
Abuse
Terrorist: Improbable
Operator error: Remote
Damage

```
                        Equipment failure: Remote
                        Maritime conditions: Occasional
                        Weather conditions: Occasional

        Event "Rescue node damages POS"
                Abuse
                        Terrorist: Improbable
                        Operator error: Remote
                Damage
                        Equipment failure: Remote
                        Maritime conditions: Occasional
                        Weather conditions: Occasional
#
### information events ####
#
        Event "Rescue node discloses location of person in distress"
                Abuse
                        Operator error :Remote
                Spying
                        Terrorist :Improbable

        Event "Rescue node discloses location of search node"
                Abuse
                        Operator error :Remote
                Spying
                        Terrorist :Improbable

        Event "Rescue node discloses location of rescue node"
                Abuse
                        Operator error :Occasional
                Spying
                        Terrorist :Remote

#
#####################################################
#

Performer PlaceOfSafety
        Event "Catastrophic failure of place of safety"
                Abuse
                        Operator error : Remote
                Damage
                        Weather conditions : Remote
                        Equipment failure : Remote
                        Fire       : Remote
                        Terrorist: Improbable
                Exceeding Limits
                        Operator error : Remote
                Modification
                        Maintenance error : Remote
                        Malicious maintenance : Improbable
```

Supplier error : Improbable

Event "Critical failure of place of safety"
Abuse
Operator error : Remote
Damage
Weather conditions : Occasional
Equipment failure : Remote
Fire : Remote
Terrorist : Improbable
Exceeding Limits
Operator error : Remote
Modification
Maintenance error : Remote
Malicious maintenance : Improbable
Supplier error : Remote

Event "Marginal failure of place of safety"
Abuse
Operator error : Occasional
Damage
Weather conditions : Occasional
Equipment failure : Occasional
Fire : Occasional
Terrorist : Improbable
Exceeding Limits
Operator error : Occasional
Modification
Maintenance error : Remote
Malicious maintenance : Improbable
Supplier error : Remote

Event "Negligible failure of place of safety"
Abuse
Operator error : Probable
Damage
Weather conditions : Probable
Equipment failure : Occasional
Fire : Occasional
Terrorist : Improbable
Exceeding Limits
Operator error : Probable
Modification
Maintenance error : Remote
Malicious maintenance : Improbable
Supplier error : Remote

###

Event "POS delays SAR operation"
Abuse
Operator error: Occasional
Damage

Non-targeted virus: Remote
Equipment failure: Occasional
Weather conditions: Probable

Event "POS is unable to communicate to search node"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Remote

Event "POS is unable to communicate to rescue node"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Remote

Event "POS is unable to communicate to C2 node"
Damage
Operator error: Occasional
Maintenance error: Remote
Supplier error: Improbable
Weather conditions: Remote

Event "POS sends incorrect status to C2 node"
Abuse
Terrorist: Improbable
Operator error: Occasional

Event "POS receives incorrect warning order"
Abuse
Terrorist: Improbable
Operator error: Occasional

Event "POS damages person in distress"
Abuse
Terrorist: Improbable
Operator error: Improbable
Damage
Equipment failure: Remote
Maritime conditions: Remote
Weather conditions: Remote

Event "POS damages rescue node"
Abuse
Terrorist: Improbable
Operator error: Remote
Damage
Equipment failure: Remote
Maritime conditions: Occasional

```
                    Weather conditions: Occasional
#
### information events ###
#
        Event "POS discloses location of person in distress"
                Abuse
                        Operator error :Remote
                Spying
                        Terrorist :Improbable

        Event "POS discloses location of rescue node"
                Abuse
                        Operator error :Remote
                Spying
                        Terrorist :Improbable
```

7.6 Threat Scenarios to Undesired Events

The following table captures the list of Threat Scenarios and associated Undesired Events for the SAR Enterprise.

```
 Category "Risks to Personnel"

  Group  "Risks to Person In Distress"
                Risk "Catastrophic damage to person in distress", severity: Catastrophic - 1000
                        Event "Catastrophic failure of Person in distress" &
                        Fault "Minor delay in SAR operation" ;

                        Event "Catastrophic failure of person in distress" &
                        Fault "Major delay in SAR operation";

                        Event "Catastrophic failure of person in distress" &
                        Fault "SAR operation not accomplished";

                        Event "Critical failure of person in distress" &
                        Fault "Major delay in SAR operation";

                        Event "Critical failure of person in distress" &
                        Fault "SAR operation not accomplished";

                        Event "Marginal failure of person in distress" &
                        Fault "SAR operation not accomplished";

                        Fault "Highjacking of the person in distress";


                Risk "Critical damage to person in distress", severity: Critical - 100
                        Event "Critical failure of person in distress" &
                        Fault "Minor delay in SAR operation";
```

```
                Event "Marginal failure of person in distress" &
                Fault "Major delay in SAR operation";

                Event "Rescue node damages person in distress";
                Event "POS damages person in distress";

        Risk "Marginal damage to person in distress", severity: Marginal - 10

                Event "Marginal failure of person in distress" &
                Fault "Minor delay in SAR operation";

                Event "Negligible failure of person in distress" &
                 Fault "Major delay in SAR operation";

                 Event "Rescue node damages person in distress";
                Event "POS damages person in distress";

        Risk "Negligible damage to person in distress", severity: Negligible - 1
                 Event "Negligible failure of person in distress" &
                 Fault "Minor delay in SAR operation";

                 Event "Rescue node damages person in distress";
                Event "POS damages person in distress";

Group "Risks to Search personnel"
        Risk "Catastrophic damage to search personnel", severity: Catastrophic - 1000
                Event "Catastrophic failure of search node";

        Risk "Critical damage to search personnel", severity: Critical - 100
                Event "Critical failure of search node";

        Risk "Marginal damage to search personnel", severity: Marginal - 10
                Event "Marginal failure of search node";

        Risk "Negligible damage to search personnel", severity: Negligible - 1
                Event "Negligible failure of search node";


Group "Risks to Rescue personnel"
        Risk "Catastrophic damage to rescue personnel", severity: Catastrophic - 1000
                Event "Catastrophic failure of rescue node";
                Fault "Highjacking of the person in distress";
                Fault "Highjacking of the rescue node";

        Risk "Critical damage to rescue personnel", severity: Critical - 100
                Event "Critical failure of rescue node";

        Risk "Marginal damage to rescue personnel", severity: Marginal - 10
                Event "Marginal failure of rescue node";
                Event "POS damages rescue node";
```

```
        Risk "Negligible damage to rescue personnel", severity: Negligible - 1
            Event "Negligible failure of rescue node";

Group "Risks to C2 personnel"
        Risk "Catastrophic damage to control personnel", severity: Catastrophic - 1000
            Event "Catastrophic failure of C2 node";

        Risk "Critical damage to control personnel", severity: Critical - 100
            Event "Critical failure of C2 node";

        Risk "Marginal damage to control personnel", severity: Marginal - 10
            Event "Marginal failure of C2 node";

        Risk "Negligible damage to control personnel", severity: Negligible - 1
            Event "Negligible failure of C2 node";


Group "Risks to POS personnel"
        Risk "Catastrophic damage to POS personnel", severity: Catastrophic - 1000
            Event "Catastrophic failure of place of safety";
            Fault "Highjacking of the rescue node";
            Fault "Highjacking of the person in distress";

        Risk "Critical damage to POS personnel", severity: Critical - 100
            Event "Critical failure of place of safety";

        Risk "Marginal damage to POS personnel", severity: Marginal - 10
            Event "Marginal failure of place of safety";

        Risk "Negligible damage to POS personnel", severity: Negligible - 1
             Event "Negligible failure of place of safety";
             Event "Rescue node damages POS";

Group "Risks to Other Persons"
        Risk "Catastrophic damage to other persons", severity: Catastrophic - 1000
            Event "Catastrophic failure of search node" &
            Condition "Search node over populated area";

            Event "Catastrophic failure of rescue node" &
            Condition "Rescue node in populated area";

            Event "Highjacking of the person in distress";

        Risk "Critical damage to other persons", severity: Critical - 100
            Event "Critical failure of search node" &
            Condition "Search node over populated area";

            Event "Catastrophic failure of rescue node" &
            Condition "Rescue node in populated area";
```

```
                Risk "Marginal damage to other persons", severity: Marginal - 10
                        Event "Marginal failure of search node";

                Risk "Negligible damage to other persons", severity: Negligible - 1
                        Event "Negligible failure of search node";


Category "Risks to Environment"

  Group "Risks of Maritime Pollution"
          Risk  "Catastrophic maritime pollution", severity: Catastrophic - 1000
                  Event "Catastrophic failure of person in distress" &
                  Condition "Yacht is a major hazard";

          Risk  "Critical maritime pollution", severity: Critical - 100
                  Event "Catastrophic failure of person in distress";

                   Event "Catastrophic failure of search node" &
                   Condition "Search node in maritime area";

                  Event "Catastrophic failure of rescue node";

          Risk  "Marginal maritime pollution", severity: Marginal - 10
                  Event "Critical failure of person in distress";

                  Event "Critical failure of search node" &
                   Condition "Search node in maritime area";

                  Event "Critical failure of rescue node";

          Risk  "Negligible maritime pollution", severity: Negligible - 1
                      Event "Marginal failure of person in distress";

                  Event "Marginal failure of rescue node";

  Group "Risks of Land Pollution"
                  Risk  "Marginal land pollution", severity: Marginal - 10
                          Event "Catastrophic failure of search node" &
                          Condition "Search node in land area";

                  Risk  "Negligible land pollution", severity: Negligible - 1
                          Event "Critical failure of search node" &
                          Condition "Search node in land area";


Category "Risks to Information"
 Group "Risks to Confidentiality of Location of Person In Distress"
                  Risk  " Disclosure of location of person in distress", severity: Critical - 30
                          Fault "Disclosure of location of person in distress";

  Group "Risks to Confidentiality of Location of Search Node"
```

```
            Risk  " Disclosure of location of search node", severity: Negligible - 20
                  Fault " Disclosure of location of search node";

   Group "Risks to Confidentiality of Location of Rescue Node"
            Risk  " Disclosure of location of rescue node", severity: Negligible - 50
                  Fault "Disclosure of location of rescue node";

   Group "Risks to Confidentiality of SAR Capacity"
            Risk  "Disclosure of SAR capacity", severity: Critical - 100
                  Fault "Disclosure of SAR capacity";

   Group "Risks to Integrity of C2 Node"
            Risk  "Full subversion of C2 node", severity: Critical - 100
                  Event "Full subversion of C2 node";

Category "Risks to Capabilities"
Group "Risks to Monitoring Capability"
            Risk  "Full loss of capability to monitor", severity: Critical - 500
                  Event "Catastrophic failure of monitoring node";
                  Event "Critical failure of monitoring node";

            Risk  "Partial loss of capability to monitor", severity: Marginal - 200
                  Event "Marginal failure of monitoring node";
                  Event "Negligible failure of monitoring node";

   Group "Risks to Search Capability"
            Risk  "Full loss of capability to search", severity: Critical - 500
                  Event "Catastrophic failure of search node";
                  Event "Critical failure of search node";
                  Event "Catastrophic failure of C2 node";

            Risk  "Partial loss of capability to search", severity: Marginal - 100
                  Event "Marginal failure of search node";
                  Event "Critical failure of C2 node";
                  Event "Marginal failure of C2 node";

   Group "Risks to Rescue Capability"
            Risk  "Full loss of capability to rescue", severity: Critical - 500
                  Event "Catastrophic failure of rescue node";
                  Event "Critical failure of rescue node";
                  Event "Catastrophic failure of C2 node";
                  Event "Catastrophic failure of place of safety";
                  Event "Critical failure of place of safety";

            Risk  "Partial loss of capability to rescue", severity: Marginal - 200
                  Event "Marginal failure of rescue node";
                  Event "Critical failure of C2 node";
                  Event "Marginal failure of C2 node";
                  Event "Marginal failure of place of safety";
                  Event "POS damages rescue node";
                  Event "Rescue node damages POS";
```

```
Category "Risks to Other Assets"
 Group "Risks to SAR Resources"
                Risk  "Catastrophic loss of SAR resources", severity: Catastrophic - 800
                                Event "Catastrophic failure of C2 node";

                                Event "Catastrophic failure of search node",
                                Event "Catastrophic failure of rescue node";

                                Event "Catastrophic failure of place of safety";

                Risk  "Critical loss of SAR resources", severity: Critical - 200
                                Event "Critical failure of C2 node";

                                Event "Critical failure of search node";
                                Event "Critical failure of rescue node";

                                Event "Critical failure of place of safety";
                                Fault "Major Fake distress signal";

                Risk  "Marginal loss of SAR resources", severity: Marginal - 10
                                Fault "Minor Fake distress signal";
                                Fault "Major delay in SAR operation";
                                Fault "Incorrectly initiated SAR operation";
                                Fault "Inadequate use of SAR resources";

                Risk  "Negligible loss of SAR resources", severity: Negligible - 5
                                Fault "Minor delay in SAR operation";

 Group "Risks to Third Party Property"
                Risk  "Catastrophic loss of property", severity: Catastrophic - 700
                        Event "Catastrophic failure of search node" &
                        Condition "Search node over populated area";

                        Event "Catastrophic failure of rescue node" &
                        Condition "Rescue node in populated area";

                Risk  "Critical loss of property", severity: Critical - 300
                        Event "Critical failure of search node" &
                        Condition "Search node over populated area";

                        Event "Catastrophic failure of rescue node" &
                        Condition "Rescue node in populated area";

 Group "Risks to Navigation in the area"

                Risk  "Critical loss of navigation", severity: Critical - 800
                        Event "Catastrophic failure of person in distress" &
                        Condition "Yacht in restricted area";

                        Event "Catastrophic failure of rescue node" &
```

Condition "Rescue in restricted area";

Risk "Marginal loss of navigation", severity: Marginal - 200
Event "Critical failure of person in distress" &
Condition "Yacht in restricted area";

Event "Critical failure of rescue node" &
Condition "Rescue in restricted area";

Risk "Negligible loss of navigation", severity: Negligible - 20
Event "Marginal failure of person in distress" &
Condition "Yacht in restricted area";

Event "Marginal failure of rescue node" &
Condition "Rescue in restricted area";

Additional risks may involve risks to intangible assets, for example risk to the reputation of the SAR enterprise and risk to compliance. These risks were considered out of scope because the reference DoDAF model for the SAR Enterprise does not provide enough detail in this area.

The description of the faults (middle elements of the fault tree connecting Threat Events to Undesired Events, is provided in Section 14 of this document.

7.7 Evaluation of Attack Groups

The following table describes the prioritization of Attack Groups based on the Likelihood for the SAR Enterprise[1].

Table 31: Evaluation of Attack Groups by Likelihood

Rank	Attack Group	Likelihood
1	Damage to C2Node	0.42265
2	Abuse of Person in Distress	0.39036
3	Damage to Person in Distress	0.36083
4	Abuse of C2Node	0.34223
5	Damage to RescueNode	0.23776
6	Damage to SearchNode	0.23166
7	Abuse of SearchNode	0.16512
8	Abuse of RescueNode	0.14714
9	Exceeding Limits of C2Node	0.14022
10	Exceeding Limits of Person in Distress	0.12273

[1] Risk calculation method correctly handles AND-OR fault trees to calculate the combined likelihood of multiple events. However, when relative contribution of an individual risk factor is computed, the sum of all likelihoods is usually slightly higher than 1, because of the overlaps when multiple factors contribute to the same risk.

11	Damage to PlaceOfSafety	0.11348
12	Exceeding Limits of RescueNode	0.11204
13	Exceeding Limits of SearchNode	0.10262
14	Abuse of PlaceOfSafety	0.05530
15	Damage to MonitoringNode	0.04941
16	Exceeding Limits of PlaceOfSafety	0.04907
17	Abuse of MonitoringNode	0.03006
18	Modification of C2Node	0.02401
19	Modification of MonitoringNode	0.00821
20	Modification of RescueNode	0.00820
21	Modification of SearchNode	0.00625
22	Spying on MonitoringNode	0.00406
23	Spying on C2Node	0.00406
24	Modification of Person in Distress	0.00245
25	Loss of Person in Distress	0.00222
26	Modification of PlaceOfSafety	0.00020
27	Spying on Person in Distress	0.00004
28	Spying on RescueNode	0.00003
29	Spying on SearchNode	0.00002
30	Spying on PlaceOfSafety	0.0000004

Table 32: Evaluation of Attacks on Performers by Likelihood

Rank	Performer	Likelihood
1	Person in distress	0.858
2	C2Node	0.855
3	SearchNode	0.501
4	RescueNode	0.498
5	PlaceOfSafety	0.217
6	MonitoringNode	0.091

Table 33: Evaluation of Attack by Threat Sources by Likelihood

Rank	Threat Source	Likelihood
1	"Operator error	0.89338
2	"Person in distress error	0.48889
3	"Weather conditions	0.48668
4	"Equipment failure	0.37017
5	"Maritime conditions	0.26547
6	"Fire	0.23447
7	"Electrical failure	0.12141
8	"Insufficient resources	0.04965
9	"Maintenance error	0.04476
10	"Hacker	0.03503

11	"Non-targeted virus	0.03414
12	"Land conditions	0.02550
13	"Botnet	0.02200
14	"Supplier error	0.00432
15	"Terrorist	0.00428
16	"Criminal	0.00227
17	"Targeted virus	0.00211
18	"Space conditions	0.00205
19	"Malicious maintenance	0.000004
20	"Malicious person in distress	0.0000002

Section 8

Safeguard Identification

Safeguards (countermeasures, controls) are practices, procedures, or mechanisms that may deter the threat, reduce vulnerability, limit the impact of undesired events, detect undesired events, and facilitate recovery.

Safeguards may be considered to perform one or more of the following functions:

- Prevention
- Deterrence
- Detection
- Limitation
- Correction
- Recovery
- Monitoring
- Awareness

An appropriate selection of safeguards is essential for a properly implemented security program. Many safeguards can serve multiple functions. It is often more cost effective to select safeguards that will satisfy multiple functions.

This section captures the safeguards of the SAR Enterprise.

8.1 Safeguards

The following table captures the safeguards and their categories selected within the scope of the security assessment of the SAR Enterprise. This assessment uses a standard taxonomy of safeguards and safeguards categories. Any deviations from the standard taxonomy are clearly marked in the Description column.

Table 34: Safeguards

Safeguard	Description	Performer	Category
SG01 - Authentication mechanism	This safeguard can ensure that only legitimate users perform exchanges and access systems related to the Tactical C2 Node, Asset Controller Node, The tactical communication network (ControlOrder exchanges) and asset allocation network (Task exchanges)	Asset Controler, Tactical C2 Node, Search Node, Rescue Node	Technical
SG02 - User identity management	This safeguard can ensure that only legitimate users perform exchanges and access systems related to the Tactical C2 Node, Asset Controller Node, The tactical communication network (ControlOrder exchanges) and asset allocation network (Task exchanges)	Asset Controler, Tactical C2 Node, Search Node, Rescue Node	Technical

SG03 - Access control mechanism	This safeguard can ensure that only legitimate users perform exchanges and access systems related to Tactical C2 Node, Asset Controller Node, The tactical communication network (ControlOrder exchanges) and asset allocation network (Task exchanges)	Asset Controler, Tactical C2 Node, Search Node, Rescue Node	Technical
SG04 - Encryption mechanism	Encryption of the Information at the Tactical C2 node, Asset Controller Node, and messages at the tactical network and asset allocation network can ensure integrity and protect information from unauthorised access	Asset Controler, Tactical C2 Node, Search Node, Rescue Node	Technical
SG05 - Administrative safeguards	to protect access to tactical C2 Node systems and asset controller systems	Asset Controler, Tactical C2 Node	Administrative
SG05 - Procedure against fake distress calls	Procedure for the tactical C2 node to diligently deploy SAR resources in the situations that may turn to be fake distress calls	Tactical C2 Node	Administrative
SG06 - Security awareness training for rescue node	To prevent ambush of rescue node during victim recovery.	Rescue Node	Administrative
SG07 - Procedure against ignored distress calls	For example, filing a flight/journey plan with a SAR timeout and reporting to SAR authority at closing the flight/journey plan so that the SAR can be triggered even unable to send distress signal.	Tactical C2 Node, Person in distress	Administrative
SG08 - Alternative ways to communicate to SAR party	For example, training in smoke signals, signs, etc.	Person in distress	Administrative
SG09 - Emergency procedure training	emergency procedure training can improve performance during emergency	Person in distress	Administrative
SG10 - Mandatory certification of the emergency equipment	this safeguard ensures integrity of the emergency equipment to send the distress signal, communicate with SAR	Person in distress	Administrative
SG11 - Mandatory periodic maintenance of equipment	this safeguard ensures that equipment of the yacht does not fail, which increases the survival time during emergency	Person in distress	Administrative
SG12 - Certification of the equipment	certification of the SAR equipment can ensure that it will not fail during the SAR operation	Rescue node, search node, Tactical C2 node	Administrative
SG13 - Anti-tamper mechanism on emergency equipment	A mechanism that visibly alerts for modification of emergency equipment	person in distress	Technical
SG14 - Protection of the Monitoring Node control channel	This safeguard protects against unauthorised modification and access to the monitoring node	Monitoring node	Technical
SG15 - Restricted Access to Monitoring Node control	This safeguard protects against unauthorised modification and access to the monitoring node	Monitoring Node	Administrative
SG16 - Periodic inspection of the monitoring node	This safeguard allows timely detection of the malfunctions of the monitoring node which can prevent it from receiving distress signals	Monitoring node	Administrative
SG17 - Remote diagnostics of the monitoring node	This capability allows timely diagnostics of the monitoring node	Monitoring node	Technical

SG18 - Capability to check integrity of the monitoring node	This capability allows timely detection of the integrity of the monitoring node, such as unauthorised access and modifications	Monitoring node	Technical
SG19 - Restricted access to the source code and operational procedures of the monitoring node	This safeguard makes it more difficult to exploit the monitoring node	Monitoring node	Administrative
SG20 - Procedure for Search Node to limit exposure on C2 node failures	For example, alternative communication channel to the C2 node to clarify control orders, weather checks, fuel checks, alternative landings, etc. to ensure that the search node does not fail in the situation when the C2 node is unavailable, tactical network is down or damaged or jammed, or when search node receives fake control orders	Search node	Administrative
SG21 - Procedure for Rescue Node to limit exposure on C2 node failures	For example, alternative communication channel to the C2 node to clarify control orders, weather checks, fuel checks, alternative ports, etc. to ensure that the search node does not fail in the situation when the C2 node is unavailable, tactical network is down or damaged or jammed, or when search node receives fake control orders	Rescue node	Administrative
SG22 - Restricted access to C2 node facility	security clearance, personnel screening, etc. to restrict access to C2 node facility	tactical c2 node	Administrative
SG23 - Up-to-date anti-virus software for C2 node	to ensure integrity of the C2 node software	tactical c2 node	Administrative
SG24 - Physical security for C2 node	to prevent unauthorized access to the C2 node systems	tactical c2 node	Administrative
SG25 - Firewall for C2 network	to prevent unauthorised remote access to C2 node systems	tactical c2 node	Technical
SG26 - Intrusion detection system for C2 network	to protect integrity of the c2 node systems by timely detecting intrusions	tactical c2 node	Technical
SG27 - Logging security events on C2 network	to protect integrity of the c2 node systems by timely detecting intrusions	tactical c2 node	Technical
SG28 - Inspecting C2 system logs	to protect integrity of the c2 node systems by timely detecting intrusions	tactical c2 node	Administrative
SG29 - Cyber Incident Response Team	to monitor cyber operations of the C2 node and ensure its integrity and provide timely response to cyber attacks	tactical c2 node	Administrative
SG30 - Power backup	to ensure uninterrupted service of the C2 node systems	tactical c2 node	Technical
SG31 - Fire protection system	to ensure uninterrupted service of the C2 node systems	tactical c2 node	Technical
SG32 - Data backup	to enable recovery from incidents	tactical c2 node	Technical
SG33 - Backup facility	to ensure uninterrupted service of the C2 node systems in situations such as severe weather emergency	tactical c2 node	both
SG33 - Business Continuity Plan	to ensure uninterrupted service of the C2 node systems and plan recovery	tactical c2 node	administrative
SG34 - Training for the C2 node personnel	to ensure optimal performance during emergencies; to reduce operator error during SAR operations	tactical c2 node	administrative

SG35 - Simulation capability	to facilitate training, simulating inputs from monitoring node, tactical situations	tactical c2 node	technical
SG36 - Security training	to ensure optimal performance	tactical c2 node	administrative
SG37 - Supplier chain assurance	to ensure security of the supply chain	tactical c2 node, search node, rescue node	administrative
SG38 - Assurance for the maintenance personnel	to protect from tampering, unauthorised modifications of the equipment, and maintenance errors	search node, rescue node	administrative
SG39 - Public communication channels	tactical node should establish public communication channels to exchange information related to the ongoing SAR operations, for example, with police, coast guard, military, hospitals, etc.	tactical c2 node	administrative
SG40 - Verification procedures for the information exchanges in tactical node	tactical node should have verification procedure for the information, e.g. leading to the cancelation of the SAR operation to prevent fake cancellation calls	tactical c2 node	administrative
SG41 - Monitoring of the Search node	tactical node should have procedure and technical capability to monitor search node to ensure its integrity, for example a radar service	tactical c2 node	both
SG42 - Monitoring of the Rescue node	tactical node should have procedure and technical capability to monitor rescue node to ensure its integrity	tactical c2 node	both
SG43 - Stand-by capacity for search	the SAR enterprise should have search node capacity on stand by to ensure rapid response to distress signal	SAR enterprise	both
SG44 - Reserve capacity for search	the SAR enterprise should have reserve search node capacity to ensure response to distress signals	SAR enterprise	both
SG45 - Stand-by capacity for rescue	the SAR enterprise should have rescue node capacity on stand by to ensure rapid response to distress signal	SAR enterprise	both
SG46 - Reserve capacity for rescue	the SAR enterprise should have reserve search node capacity to ensure response to distress signals	SAR enterprise	both
SG47 - Weather information	the SAR enterprise should have access to up-to-date weather information in the SAR area	SAR enterprise	both
SG48 - Alternative communication channels to Place of Safety	The SAR enterprise should involve alternative communication channels to Place of Safety to ensure that the warning order is delivered when the Search node is malfunctioning, or when the channel between the Search node and the Place of Safety node is malfunctioning. The same safeguard contributes to mitigation of fake warning order exchanges	Place of Safety	both
SG49 - Procedure to verity warning order	Place of Safety should use procedure to verify the integrity of the warning order exchanges, for example by using an alternative channel to the tactical C2 node	Place of Safety	administrative
SG50 - Procedure to verify updates	Tactical C2 node should use procedure to verify the updates from the Rescue Node to mitigate from fake update exchanges, or situations where Rescue Node is malfunctioning	Tactical C2 node	administrative

SG51 - Route planning	Tactical C2 node should plan typical routes for search nodes and rescue nodes to the locations of frequent incidents to avoid impact on populated areas	Tactical C2 node	administrative
SG52 - Positioning	SAR assets should be positioned close to the locations of frequent incidents to ensure rapid response and optimal usage of SAR resources, e.g. fuel, maintenance resource, personnel time, etc.	Asset controlled	administrative
SG53 - Navigation hazard planning	Tactical C2 node should plan to understand which incidents may pose threat to navigation in the SAR domain, and use this information when conducting SAR operation	Tactical C2 node	administrative

Section 9

Vulnerabilities

The following table captures the safeguards and their categories selected within the scope of the security assessment of the SAR Enterprise. This assessment uses a standard taxonomy of safeguards and safeguards categories. Any deviations from the standard taxonomy are clearly marked in the Description column.

Table 35: Vulnerabilities

Vulnerability	Description	Performer
V01 - Inadequate decision procedure to initiate SAR operation		C2
V02 - Inadequate procedure to cancel a false SAR operation		C2
V03 - Unauthorized access to C2 equipment		C2
V04 - Inability to distinguish fake distress signal from a real one		C2, Monitoring Node
V05 - Inadequate feedback that emergency signal is deployed		Yacht
V06 Inadequate protection of the uplink of the monitoring node		Monitoring Node
V07 - Inadequate safety mechanism of emergency equipment		Yacht
V08 - Remote access to C2 equipment		C2
V09 - Faulty equipment of the yacht		Yacht
V10 - Easy access to the yacht		Yacht
V11 - Maritime characteristics of the yacht are inadequate for the particular environment		Yacht
V12 - Inadequate training of the yacht operator		Yacht
V13 - Lack of fire protection of the yacht		Yacht
V14 - Inadequate security screening of the yacht maintenance		Yacht
V15 - Inadequate storage conditions for the yacht		Yacht
V16 - Possibility to jam radio communication channel		Yacht
V17 - Access to voyage planning data		Yacht
V18 - Sharing voyage planning data		Yacht
V19 - Inadequate procedure for satellite control		Monitoring node
V20 - Access to satellite uplink		Monitoring node

V21 - Access to satellite downlink		Monitoring node
V22 - Inadequate screening of the satellite operators		Monitoring node
V23 - Faulty equipment on satellite		Monitoring node
V24 - Inadequate training of the satellite operator		Monitoring node
V25 - Software vulnerabilities in satellite		Monitoring node
V25 - Remote access to satellite control software		Monitoring node
V26 - Access to the C2 facility		C2
V27 - Software vulnerabilities in C2 software		C2
V28 - Inadequate training of C2 personnel		C2
V29 - Faulty C2 equipment		C2

Section 10

Risk Identification

Identified risks is the potential that a given threat source will exploit vulnerabilities of an asset thereby causing one of the events identified as undesired because they describe situations where a compromise to the asset caused injury to the organization which leads to further consequences characterized as impact. The level of risk is determined as the combination of the likelihood of the undesired event occurring and the severity of its impact. The risk is further characterized by one or more threat scenarios.

This section will focus on identified risks of the SAR Enterprise.

10.1 Identified Risk

The total risk of SAR Enterprise is 254.602. The normalized value of risk in the range of [0..1] is 0.960064.

Calculation of risk is based on the analysis of the full fault tree. For each undesired event with assigned severity level (1000 for catastrophic events, 100 for critical, 10 for marginal and 1 for negligible, and possibly some intermediate levels), all threat scenarios are constructed, which at the end comprise of sequences of threat events with likelihoods (0.2 for frequent, 0.02 for probable, 0.002 for occasional, 0.00001 for remote and 0.0000001 for improbable). Risk calculation uses the formula Risk=Severity*Likelihood. Risk calculation method correctly handles AND-OR fault trees to calculate the combined likelihood of multiple events.

The following table captures the Identified Risks for the SAR Enterprise.

Table 36: Identified Risk

Identified Risk	Risk Level	Likelihood	Severity	Risk
Catastrophic damage to person in distress	High	Frequent	Catastrophic	149.6
Partial loss of capability to rescue	High	Frequent	Critical	14.9
Critical damage to person in distress	High	Frequent-Probable	Critical	10.6
Partial loss of capability to monitor	High	Probable	Critical	10.3
Critical loss of SAR resources	High	Probable	Critical	9.8
Full loss of capability to rescue	High	Probable	Critical-Catastrophic	9.0
Full loss of capability to search	High	Probable	Critical-Catastrophic	8.0
Marginal loss of SAR resources	Serious	Frequent	Marginal	6.3
Partial loss of capability to search	Serious	Probable	Critical	5.7
Critical maritime pollution	Serious	Probable	Critical	4.3
Partial subversion of C2 node	Serious	Occasional	Critical-Marginal	3.4

Full loss of capability to monitor	Serious	Occasional	Critical-Catastrophic	3.0
Marginal damage to person in distress	Serious	Frequent	Marginal	2.5
Catastrophic damage to rescue personnel	Serious	Occasional	Catastrophic	2.1
Catastrophic damage to search personnel	Serious	Occasional	Catastrophic	2.1
Catastrophic damage to control personnel	Serious	Occasional	Catastrophic	2.0
Catastrophic loss of SAR resources	Serious	Occasional	Catastrophic	1.7
Negligible loss of SAR resources	Marginal	Frequent	Negligible-Marginal	1.5
Critical damage to search personnel	Serious	Probable	Critical	1.2
Critical damage to rescue personnel	Serious	Probable	Critical	1.2
Marginal maritime pollution	Serious	Frequent	Marginal	1.0
Marginal damage to rescue personnel	Serious	Occasional	Marginal	0.5
Marginal damage to other persons	Serious	Probable	Marginal	0.5
Marginal damage to search personnel	Serious	Probable	Marginal	0.5
Critical damage to control personnel	Serious	Occasional	Critical	0.4
Full subversion of C2 node	Serious	Occasional	Critical	0.4
Full disclosure of SAR capacity	Marginal	Occasional	Critical	0.4
Critical damage to POS personnel	Marginal	Occasional	Critical	0.2
Partial disclosure of SAR capacity	Marginal	Occasional	Marginal-Critical	0.2
Full disclosure of location of person in distress	Marginal	Occasional	Marginal-Critical	0.2
Partial disclosure of location of person in distress	Marginal	Probable	Negligible-Marginal	0.1
Negligible maritime pollution	Marginal	Frequent	Negligible	0.1
Full disclosure of location of rescue node	Marginal	Remote	Marginal-Critical	0.1
Marginal damage to POS personnel	Marginal	Occasional	Marginal	0.1
Negligible damage to person in distress	Marginal	Probable	Negligible	0.1
Marginal damage to control personnel	Marginal	Occasional	Marginal	0.1
Negligible damage to POS personnel	Marginal	Probable	Negligible	0.1
Negligible damage to control personnel	Marginal	Probable	Negligible	0.1
Negligible damage to rescue personnel	Marginal	Probable	Negligible	0.1
Negligible damage to search personnel	Marginal	Probable	Negligible	0.1
Negligible damage to other persons	Marginal	Probable	Negligible	0.1

Catastrophic damage to POS personnel	Marginal	Remote	Catastrophic	0.1
Critical loss of navigation	Marginal	Remote	Catastrophic-Critical	0.03
Partial disclosure of location of rescue node	Marginal	Occasional	Marginal	0.02
Marginal loss of navigation	Marginal	Remote	Critical-Catastrophic	0.02
Partial disclosure of location of search node	Negligible	Occasional	Negligible-Marginal	0.01
Marginal land pollution	Marginal	Remote	Marginal	0.01
Critical loss of property	Marginal	Remote	Critical-Catastrophic	0.004
Catastrophic damage to other persons	Marginal	Remote-Improbable	Catastrophic	0.004
Catastrophic maritime pollution	Marginal	Remote-Improbable	Catastrophic-Critical	0.004
Negligible land pollution	Negligible	Occasional	Negligible	0.004
Catastrophic loss of property	Marginal	Remote-Improbable	Catastrophic-Critical	0.003
Negligible loss of navigation	Marginal	Remote	Marginal-Critical	0.003
Critical damage to other persons	Marginal	Remote	Critical	0.001
Full disclosure of location of search node	Negligible	Occasional	Marginal-Critical	0.001

Section 11

Risk Assessment

This section provides assessment of the risks for the SAR Enterprise.

11.1 Risk Assessment

The following table summarizes the risk contribution of various components to overall risk.

Table 37: Contribution of individual Performers to Identified Risk

Rank	Performer	Risk
1	Yacht	119.7
2	C2Node	55.6
3	RescueNode	37.8
4	SearchNode	28.0
5	MonitoringNode	14.6
6	PlaceOfSafety	10.5

Table 38: Contribution of individual Threat Sources to Identified Risk

Rank	Threat Source	Risk
1	Operator error	51.6
2	Fire	49.5
3	Person in distress error	42.0
4	Maritime conditions	41.7
5	Weather conditions	32.6
6	Equipment failure	26.2
7	Maintenance error	8.0
8	Electrical failure	5.6
9	Insufficient resources	3.1
10	Hacker	2.8
11	Land conditions	1.9
12	Botnet	1.8
13	Non-targeted virus	1.6
14	Supplier error	1.6
15	Space conditions	0.4
16	Terrorist	0.3
17	Targeted virus	0.2
18	Criminal	0.03
19	Malicious maintenance	0.001
20	Malicious person in distress	0

Table 39: Contribution of Individual Attack Modes to Identified Risk

Rank	Attack Mode	Risk
1	Damage	151.6
2	Abuse	65.2
3	Exceeding capacity	41.7
4	Modification	7.5
5	Spying	0.4
6	Loss	0.02

Table 40: Contribution of individual Attack Groups to Identified Risk

Rank	Attack Group	Risk
1	Damage of Yacht	80.1
2	Damage of C2Node	27.6
3	Abuse of Yacht	23.2
4	Exceeding of Yacht	19.1
5	Abuse of C2Node	18.8
6	Damage of RescueNode	18.7
7	Damage of SearchNode	14.8
8	Abuse of RescueNode	8.9
9	Exceeding of RescueNode	8.6
10	Exceeding of C2Node	7.9
11	Abuse of SearchNode	7.0
12	Damage of MonitoringNode	6.8
13	Damage of PlaceOfSafety	6.3
14	Abuse of MonitoringNode	5.9
15	Exceeding of SearchNode	4.7
16	Abuse of PlaceOfSafety	2.1
17	Exceeding of PlaceOfSafety	2.0
18	Modification of C2Node	2.0
19	Modification of MonitoringNode	1.9
20	Modification of RescueNode	1.7
21	Modification of SearchNode	1.6
22	Modification of Yacht	0.3
23	Spying of C2Node	0.3
24	Spying of MonitoringNode	0.1
25	Modification of PlaceOfSafety	0.05
26	Loss of Yacht	0.02
27	Spying of Yacht	0.0007
28	Spying of RescueNode	0.0007
29	Spying of SearchNode	0.0001
30	Spying of PlaceOfSafety	0

Table 41: Contribution of Attacks be a particular Threat Source to a Performer

Rank	Performer attacked by Threat Source	Risk
1	Yacht by Person in distress error	42.0
2	Yacht by Maritime conditions	35.6
3	Yacht by Fire	32.3
4	RescueNode by Weather conditions	17.0
5	C2Node by Operator error	16.5
6	RescueNode by Operator error	13.1
7	C2Node by Fire	12.3
8	SearchNode by Weather conditions	11.2
9	SearchNode by Operator error	10.7
10	Yacht by Equipment failure	7.5
11	MonitoringNode by Operator error	7.3
12	MonitoringNode by Equipment failure	6.4
13	C2Node by Equipment failure	6.1
14	C2Node by Electrical failure	5.6
15	C2Node by Maritime conditions	5.1
16	Yacht by Maintenance error	4.6
17	PlaceOfSafety by Weather conditions	4.5
18	PlaceOfSafety by Operator error	4.2
19	RescueNode by Equipment failure	3.2
20	C2Node by Insufficient resources	3.1
21	SearchNode by Equipment failure	2.4
22	RescueNode by Fire	2.3
23	C2Node by Hacker	2.3
24	SearchNode by Fire	2.1
25	C2Node by Land conditions	1.8
26	C2Node by Botnet	1.8
27	RescueNode by Maintenance error	1.6
28	C2Node by Non-targeted virus	1.6
29	SearchNode by Maintenance error	1.6
30	Yacht by Supplier error	1.5
31	PlaceOfSafety by Equipment failure	0.7
32	PlaceOfSafety by Fire	0.7
33	RescueNode by Maritime conditions	0.6
34	MonitoringNode by Hacker	0.5
35	PlaceOfSafety by Maritime conditions	0.4
36	MonitoringNode by Space conditions	0.4
37	Yacht by Operator error	0.4
38	C2Node by Terrorist	0.3
39	C2Node by Targeted virus	0.2
40	PlaceOfSafety by Maintenance error	0.03
41	Yacht by Criminal	0.03
42	MonitoringNode by Maintenance error	0.03
43	Yacht by Terrorist	0.02
44	RescueNode by Supplier error	0.01

45	PlaceOfSafety by Supplier error	0.01
46	SearchNode by Supplier error	0.01
47	C2Node by Supplier error	0.002
48	C2Node by Criminal	0.001
49	RescueNode by Terrorist	0.001
50	MonitoringNode by Terrorist	0.001
51	MonitoringNode by Targeted virus	0.0004
52	PlaceOfSafety by Terrorist	0.0004
53	SearchNode by Terrorist	0.0004
54	Yacht by Hacker	0.0004
55	PlaceOfSafety by Malicious maintenance	0.0003
56	RescueNode by Malicious maintenance	0.0003
57	SearchNode by Malicious maintenance	0.0003
58	SearchNode by Non-targeted virus	0.0002
59	RescueNode by Non-targeted virus	0.0002
60	PlaceOfSafety by Non-targeted virus	0.00022
61	Yacht by Malicious maintenance	0.00011
62	C2Node by Maintenance error	0.00007
63	Yacht by Malicious person in distress	0.000003

Section 12

Recommendations

This section is out of the project's scope.

Section 13

Risk Assessment Tools

We used 3 tools integrated into a technical Evidence-driven TI Framework:

- Cameo Enterprise Architecture from NoMagic
- ASCE from Adelard
- Blade Risk Manager from KDM Analytics

Cameo Enterprise Architecture from NoMagic

The Cameo Enterprise Architecture product, based on the NoMagic core product Magic Draw, offers the standards compliant DoDAF 2.0, MODAF and NAF 3 via a UPDM standardized solution. **UPDM** is Unified Profile for DoDAF, MODAF and NAF developed and maintained by international specification organization Object Management Group (OMG). In other words UPDM is a standardized way of expressing DoDAF, MODAF and NAF artifacts using UML, SysML and SoaML.

ASCE from Adelard

The ASCE product from Adelard is a software tool designed to simplify the creation and management of your assurance case, helping to reduce project and system risk through effective and straightforward communication of the safety/security and other types of argument and its associated evidence. It is an industry standard, used by hundreds of organizations world-wide.

ASCE lets you build robust arguments using recognized notations such as Claims-Arguments-Evidence (CAE) and Goal Structuring Notation (GSN).

It targets problems with a proven approach to help you deliver robust safety/security and other assurance cases. ASCE manages information complexity and communicates your argument to your stakeholders.

The KDM Analytics team extended the ASCE tool by developing a plug-in for Trustworthiness Index computation. This enabled the team to visualize methodology and calibrate computation parameters.

Blade Risk Manager from KDM Analytics

The **Blade Risk Manager** product from KDM Analytics is a Threat Risk Assessment Platform that provides a systematic, comprehensive and automated validation of a system's security posture. It operates by using information that is extracted directly from the system, its architecture models (e.g. UPDM) and operational environment, converted into an open standards representation and is semantically integrated into a high fidelity model. The model includes formal artifacts such as software elements and relationships, system build elements, system resource (e.g. database), architecture models, COTS/GOTS interface elements and relationships, as well as information from the national vulnerability database and code weakness information from code scanners.

The generated model is used as an evidence repository for threat risk analysis and to automatically produce a fact-based Threat Risk Assessment report.

Section 14

Faults and Conditions for SAR Enterprise

This section completes the description of the fault trees for SAR Enterprise by describing the fault elements (the middle elements describing cause and effect relationships between individual Threat Events and Undesired Events). This section also describes several situational conditions used in the risk model for the SAR Enterprise.

Faults

Fault "Minor delay in SAR operation" caused by

Fault "Minor C2 node delay to initiate SAR operation";

Event "C2 delays control order to search node" ;

Event "C2 delays control order to rescue node" ";

Event "Search node delays SAR operation";

Event "Rescue node delays SAR operation";

Event "Search node is unable to communicate to rescue node";

Event "Rescue node is unable to communicate to search node";

Event "Search node is unable to communicate to person in distress";

Event "Person in distress is unable to communicate to search node";

Event "Search node sends incorrect status to rescue node";

Event "Search node is unable to communicate to POS";

Event "Search node sends incorrect warning order to POS";

Event "Rescue node sends incorrect warning order to place of safety";

Event "C2 node is unable to communicate to POS";

Event "POS is unable to communicate to search node";

Event "POS receives incorrect warning order";

Event "POS is unable to communicate to rescue node";

Event "Rescue node is unable to communicate to POS";

Event "Rescue node is unable to communicate to person in distress";

Event "Person in distress is unable to communicate to rescue node";

Event "POS sends incorrect status to C2 node";

Event "POS delays SAR operation";

Event "C2 restarts transfer";

Fault "Minor C2 node delay to initiate SAR operation" caused by

Event "C2 delays launching SAR operation";

Event "Negligible failure of C2 node";

Fault "Major delay in SAR operation" caused by

Event "Monitoring node delays track info";

Fault "Major C2 node delay to initiate SAR operation";

Fault "Major C2 node delay to control search node";

Fault “Major C2 node delay to control rescue node";

Fault "Major search node delay";

Fault "Major rescue node delay";

Fault "Major place of safety delay";

Fault "Major C2 node delay to initiate SAR operation" caused by

Event "Critical failure of C2 node";

Event "Marginal failure of C2 node";

Event "C2 node is unable to receive track info";

Event "C2 node loses data for the SAR operation";

Event "Person in distress is unable to send distress signal";

Fault "Major C2 node delay to control search node" caused by

Event "Monitoring node receives incorrect location";

Event "Monitoring node sends incorrect track info";

Event "C2 node receives incorrect track info";

Event "Incorrect information is sent to search node";

Event "Critical failure of C2 node";

Event "Marginal failure of C2 node";

Event "C2 node is unable to communicate to search node";

Event "C2 node sends incorrect control order to search node";

Event "Search node receives incorrect control order";

Event "C2 node loses data for the SAR operation";

Event "C2 delays control order to search node";

Event "C2 restarts search";

Fault "Major C2 node delay to control rescue node" caused by

Event "Critical failure of C2 node";

Event "Marginal failure of C2 node";

Event "C2 node is unable to communicate to rescue node";

Event "Rescue node is unable to communicate to C2 node";

Event "Search node sends incorrect track info to C2 node";

Event "Rescue node sends incorrect track info to C2 node";

Event "C2 node sends incorrect control order to rescue node";

Event "Incorrect information is sent to rescue node";

Event "C2 node loses data for the SAR operation";

Event "C2 delays control order to rescue node";

Event "C2 restarts rescue";

Event "C2 restarts transfer";

Fault "Major search node delay" caused by

Event "Negligible failure of search node";

Event "Marginal failure of search node";

Event "Search node fails to find person in distress";

Event "Search node is unable to communicate to C2 node";

Fault "Major rescue node delay" caused by

Event "Negligible failure of rescue node";

Event "Marginal failure of rescue node";

Event "Rescue node fails to find person in distress";

Event "Rescue node receives incorrect control order";

Event "Rescue node fails to find place of safety";

Fault "Major place of safety delay" caused by

Event "Negligible failure of place of safety";

Event "Marginal failure of place of safety";

Event "POS is unable to communicate to C2 node";

```
# also yacht is out of range will cause delay of the SAR operation and waste of resources

Fault "SAR operation not accomplished"
        Event "C2 fails to launch SAR operation";
        Event "C2 incorrectly cancels SAR operation";
        Event "C2 aborts SAR operation";
        Event "Person in distress is unable to send distress signal";
        Event "Monitoring node is unable to receive distress signal";
        Event "Monitoring node is unable to send track info";
        Event "Rescue node fails to rescue person in distress";
        Event "Rescue node fails to transfer person in distress";

Fault "Major Fake distress signal"
        Event "C2 launches inappropriate SAR operation";

Fault "Minor Fake distress signal"
        Event "C2 launches inappropriate SAR operation",
        Event "C2 aborts SAR operation";

Fault "Inadequate use of SAR resources"
        Event "C2 launches inappropriate SAR operation";

Fault "Incorrectly initiated SAR operation"
        Event "C2 launches inappropriate SAR operation";
#
############## information faults ###############
#

Fault "Full disclosure of location of person in distress"
        Event "Person in distress fully discloses location";
        Event "C2 node fully discloses location of person in distress";
        Event "Search node fully discloses location of person in distress";
        Event "Monitoring node fully discloses location of person in distress";
```

Event "Rescue node fully discloses location of person in distress";

Event "POS fully discloses location of person in distress";

Fault "Partial disclosure of location of person in distress"

Event "Person in distress partially discloses location";

Event "C2 node partially discloses location of person in distress";

Event "Search node partially discloses location of person in distress";

Event "Monitoring node partially discloses location of person in distress";

Event "Rescue node partially discloses location of person in distress";

Event "POS partially discloses location of person in distress";

Fault "Full disclosure of location of search node"

Event "Person in distress fully discloses location of search node";

Event "C2 node fully discloses location of search node";

Event "Search node fully discloses location of search node";

Event "Monitoring node fully discloses location of search node";

Event "Rescue node fully discloses location of search node";

Fault "Partial disclosure of location of search node"

Event "Person in distress partially discloses location of search node";

Event "C2 node partially discloses location of search node";

Event "Search node partially discloses location of search node";

Event "Monitoring node partially discloses location of search node";

Event "Rescue node partially discloses location of search node";

Fault "Full disclosure of location of rescue node"

Event "Person in distress fully discloses location of rescue node";

Event "C2 node fully discloses location of rescue node";

Event "Search node fully discloses location of rescue node";

Event "Monitoring node fully discloses location of rescue node";

Event "Rescue node fully discloses location of rescue node";

Event "POS fully discloses location of rescue node";

Fault "Partial disclosure of location of rescue node"

```
        Event "Person in distress partially discloses location of rescue node";
        Event "C2 node partially discloses location of rescue node";
        Event "Search node partially discloses location of rescue node";
        Event "Monitoring node partially discloses location of rescue node";
        Event "Rescue node partially discloses location of rescue node";
        Event "POS partially discloses location of rescue node";

Fault "Full disclosure of SAR capacity"
        Event "C2 node fully discloses SAR capacity";

Fault "Partial disclosure of SAR capacity"
        Event "C2 node partially discloses SAR capacity";


##########################################################
################## Conditions ##########################
##########################################################

Conditions

        Condition "Search node over populated area"  0.001
        Condition "Rescue node in populated area"  0.001
        Condition "Yacht is a major hazard"  0.0001
        Condition "Search node in maritime area"   0.7
        Condition "Search node in land area"   0.3
        Condition "Yacht in restricted area"  0.001
        Condition "Rescue in restricted area"  0.001
```

Glossary of Terms

A

Activity

Work, not specific to a single organization, weapon system or individual that transforms inputs (Resources) into outputs (Resources) or changes their state.

Application Specific Vulnerability Patters (avp)

Application Specific Vulnerability Patterns (AVP) describe the necessary conditions for the identified undesired events and lead to the discovery of their corresponding points in the code.

C

Capability

The ability to achieve a Desired Effect under specified [performance] standards and conditions through combinations of ways and means [activities and resources] to perform a set of activities.

Concept of Operations (CONOPS)

Concept of Operations (CONOPS) is a general idea derived or inferred from specific instances or occurrences of major planning and operating functions.

Common Platform Enumeration (CPE)

Common Platform Enumeration (CPE™[1]) provides a standard machine-readable format for encoding names of IT products and platforms, set of procedures for comparing names, language for constructing "applicability statements" that combine CPE names with simple logical operators and a standard notion of a CPE Dictionary.

Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE®[2]) is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities.

CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools.

Common Weakness Enumeration (CWE)

Common Weakness Enumeration (CWE) is a formal list of software weakness types created to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code
- Serve as a standard measuring stick for software security tools targeting these weaknesses
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts

F

Fact Oriented Repeatable Security Assessment (FORSA)

Fact Oriented Repeatable Security Assessment (FORSA) is a systematic methodology used to perform security assessments of software applications with a focus on threat risk identification, architecture risk analysis, and vulnerability detection.

I

Impact

This is the consequence of an unwanted incident, caused either deliberately or accidentally, that affects the assets. For example, the impact of Loss of availability/integrity of network may be loss of

reputation or possible loss of compliance or possible financial loss.

N

National Vulnerability Database repository (NVD)

National Vulnerability Database repository (NVD) is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

O

Operational Activity

An activity is an action performed in conducting the business of an enterprise. It is a general term that does not imply a placement in a hierarchy (e.g., it could be a process or a task as defined in other documents and it could be at any level of the hierarchy of the Operational Activity Model). It is used to portray operational actions not hardware/software system functions.

Operational Capability

Operational capability is one or more sequences of activities.

Organization

A specific real-world assemblage of people and other resources organized for an on-going purpose.

P

Performer

Any entity that is human, automated, or any aggregation of human and/or automated that performs an activity and provides a capability.

Primary Asset

Primary Asset is usually an intangible asset (information or service) provided by the enterprise to its environment and therefore is a responsibility of a stakeholder.

R

Resource

Data, Information, Performers, Materiel, or Personnel Types that are produced or consumed.

S

Safeguard

Safeguards (counter measures, controls) are practices, procedures, or mechanisms that may deter the threat, reduce vulnerability, limit the impact of an undesired events, detect undesired events, and facilitate recovery.

Security Content Automation

Security Content Automation Protocol (SCAP)

Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. Community participation is a great strength for SCAP, because the security automation community ensures the broadest possible range of use cases is reflected in SCAP functionality.

System Assets

System Assets are defined as assets that support operational activities. These are tangible things that are attacked and that fail such as hardware, software, networks, and people.

Software Fault Pattern (SFP)

Software Fault Patterns (SFP) is a generalized description of a family of faulty computations in the software. SFPs map to multiple elements of the CWE in such a way that each individual CWE element in the family can be defined as a specialization of the SFP.

System

A functionally, physically, and/or behaviourally related group of regularly interacting or interdependent elements.

T

Task

An action, activity, or undertaking enabling missions, activities or functions to be performed or accomplished.

Threat Scenarios

A detailed chronological and functional description of an actual or hypothetical threat intended to facilitate risk analysis by creating a confirmed relationship between an asset of value and a threat agent having motivation toward that asset and having the capability to exploit a vulnerability found in the same asset. For example, a threat scenario could be a local or remote availability attack on system software.

Threat Source

The point of origin of a threat, where a threat is an indication that an unwanted incident may result in harm to a system or organization and its assets. For example, a threat source could be a supplier acting without malice (bug) or malicious supplier (backdoor, time bomb).

U

Undesired Event

Undesired events are the elements of the risk analysis framework that focus on the systematic identification of threats based on their outcome and impact.

V

Vulnerability

A certain unit of knowledge about a fault in the system that allows exploiting this system in unauthorized and possibly even malicious ways.

1CPE is a registered trademark of The MITRE Corporation.

2CVE is registered trademarks of The MITRE Corporation.

Index

T

U

V