Security Risk Assessment in Systems of Systems

by

Duncan Ki-Aries

Doctor of Philosophy

August 2020

Bournemouth University

The Defence Science and Technology Laboratory

Department of Computing and Informatics
Faculty of Science and Technology

Per la mia famiglia

Declaration

Confidentiality

I confirm that this dissertation does not contain information of a commercial or confidential nature or include personal information other than that which would normally be in the public domain unless the relevant permissions have been obtained.

In particular any information which identifies a particular individual's religious or political beliefs, information relating to their health, ethnicity, criminal history or sex life has been anonymised unless permission has been granted for its publication from the person to whom it relates.

Original Work Declaration

This dissertation and the project that it is based on are my own work, except where stated, in accordance with University regulations.

Signed:

Duncan Ki-Aries
August 2020

Acknowledgements

The research described in this thesis was funded by Bournemouth University (BU) studentship DSTLX1000104780R_BOURNEMOUTH_PhD_RASOS, in partnership with Dstl. Therefore, I offer my sincerest gratitude to all the Doctoral College and Sci-Tech / Computing and Informatics Staff at BU and Dstl for their support, assistance, and sponsorship of this work. Thanks also to Naomi Bailey for co-ordinating this.

I would like to acknowledge my absolute thanks to Dr Christopher Williams from Dstl for keeping me grounded along the journey, and always providing brilliant support. As too with Dr Huseyin Dogan from BU, for his guidance and support, in particular towards SoSs and Human Factors. Dr Shamal Faily also from BU, is simply a special shade of awesome. He is a genius, a Jedi master, he is - *The Sensei*. Actually, they're all Jedi masters, and incredibly passionate and dedicated towards their work, and students. Many many thanks to you all for this opportunity, your time, patience, and belief; you are such amazing people and an inspiration.

I also owe my gratitude to Prof. Vasilis Katos and his team for their support and collaboration with certain security related projects. Furthermore, Dr Edward Apeh and Prof. Angelos Stefanidis have always extended their faith and continued support in an organisational context, for which I am truly thankful.

My absolute gratitude also goes to my Ph.D buddies, Dr Andrew M'manga and Dr Jane Henriksen-Bulmer for helping to keep each other sane through the crazy hardwork and sacrifice behind achieving a Ph.D. I also thank the Mo's for their fun and inspiration, and reminding me what's important along this journey.

My greatest thanks is reserved for the family, as this Ph.D is for them. They too have travelled this journey, and it is with their continued support, patience, and understanding, providing the freedom in which to enable the necessary focus, that this could be achieved. They have been the Yin to this Yang throughout, and an amazing one too! Grazie a tutti!

Abstract

A System of Systems (SoS) is a set of independent systems that interoperate to achieve capabilities that none of the separate systems can achieve independently. The component systems may be independently operated or managed, and this may cause control problems. An area of particular concern is managing security of the large complex system that is the SoS, because development and operation of component systems may be done independently. Security vulnerabilities may arise at the SoS level that are not present or cannot be determined at the component system level. Security design and management processes typically operate only at component system level.

Within this thesis, the problem of security risk assessment at the SoS level is examined by identifying factors specific to SoSs, formulating a framework through which it can be managed, and creating a process with visualisation to support risk managers and security experts in making assessment of security risks for a SoS. Humans must be considered as part of the SoS and feature in risks associated with security.

A broadly qualitative methodology has been adopted using interviews, case studies, and a scenario method in which prototype framework elements were tested. Two SoS examples, including the Afghan Mission Network (AMN) as a SoS, and a SmartPowerchair SoS were used to identify, combine, and apply relevant elements in a SoS context towards addressing the research problem. For the AMN, this included interviews and focus groups with stakeholders experienced in NATO security, risk, and network-based roles. Whereas, the SmartPowerchair SoS was based on interviews and on-going communication with a single stakeholder representative as the owner and user of the SoS.

Based on the findings, OASoSIS has been developed as a framework combining the use of OCTAVE Allegro and CAIRIS to model and assess Information Security risk in the SoS context. The process for applying OASoSIS is detailed within the thesis. The first contribution of OASoSIS introduces a SoS characterisation process to support a SoS security risk assessment. The second contribution modifies a version of the OCTAVE Allegro Information Security risk assessment process to align with the SoS context. Risk data captured during a first-stage assessment then provides input for a third contribution that integrates concepts, models, and techniques with tool-support from CAIRIS to model the SoS information security risks.

Two case studies relating to a Military Medical Evacuation SoS and a Canadian Emergency Response SoS were used to apply and validate the contributions. These were validated through input from expert Military Medical stakeholders experienced in NATO operations, and key Emergency Response SoS stakeholders with further input from an expert Emergency Management stakeholder. To further strengthen the validity of the end-to-end application of OASoSIS in future work, it would benefit from being implemented within the SoS design process for other SoS scenarios.

Table of Contents

List of Figures

List of Tables

List of Acronyms

ACO	Allied Command Operations
ACT	Allied Command Transformation
AEMA	Alberta Emergency Management Agency
ALE	Annual Loss Expectancy
AMN	Afghan Mission Network
AMN AWG	The AMN Architecture Working Group
AMNOC	Afghan Mission Network Operations Centre
ANSF	Afghan National Security Force
ASF	Afghan Security Forces
ATRS	Automated Transport and Retrieval System
A&V	Assurance & Validation
BPMN	The Business Process Model and Notation
C2	Command & Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
C5ISR	Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance
CAIRIS	Computer Aided Integration of Requirements and Information Security
CCIS	(German Armed Forces FüInfoSysSK) Command and Control Information System
CEMA	Calgary Emergency Management Agency
CENTRIXS	The Combined Enterprise Regional Information Exchange System
CFBLNet	The Combined Federated Battle Laboratories Network

CIA	Confidentiality, Integrity, Availability
CIAV	Coalition Interoperability Assurance and Validation
CIAV MG	CIAV Management Group
CIAV WG	CIAV Working Group
CIS	Communication and Information Systems
CJOA-A	Combined Joint Operations Area
CM	Configuration Management
CMT	Coalition Mission Thread
CoCo	Code of Connection
COIN	Counter-Insurgency
COMISAF	ISAF General in Command
COMIJC	ISAF Joint Command General
COTS/OTS	Commercial Off-The-Shelf
COP	Common Operational Picture
CPS	Cyber-Physical System
CTE2	Coalition Test and Evaluation Environment
CTTP	Coalition Tactics, Techniques, and Procedures
CWIX	Coalition Warrior Interoperability Exercise
CWIX SMG	CWIX Senior Management Group
DEU Milnet	A German Military Network
DFD	Data Flow Diagram
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DPIA	Data Protection Impact Assessment
Dstl	Defence Science and Technology Laboratory
EHR	Electronic Health Record
EMS	Emergency Medical Services
EMS	Emergency Management System
EMSoS	Emergency Management SoS
EMT	Emergency Medical Technician
ERSoS	Emergency Response SoS
FMC	Field Medical Card
FMN	Federated Mission Network

FMN	Future Mission Network
FOB	Forward Operating Base
FR	Functional Requirements
FSB	Forward Support Base
FST	Forward Surgical Team
GAISP	The Generally Accepted System Security Principles
GDPR	The General Data Protection Regulation
GRL	Goal-oriented Requirements Language
HCD	Human-Centred Design
HCI	Human Computer Interaction
HFE	Human Factors Engineering
HFI	Human Factors Integration
HFSI	Human Factors System Integration
HIPAA	The Health Insurance Portability and Accountability Act
HMG	Her Majesty’s Government
HQ	Headquarters
HSCIC	Health and Social Care Information Centre
HSI	Human Systems Integration
IA	Information Assurance
ICS	Incident Command System
IG	Information Governance
IJC	ISAF Joint Command
IM	Information Management
IoT	Internet of Things
IP	Internet Protocol
ISAB	ISAF Security Accreditation Board
ISAF	International Security Assistance Force
ISR	Intelligence, Surveillance, and Reconnaissance
JMeWS	Joint Medical Workstation
JMT	Joint Mission Thread
JITC	Joint Interoperability Test Command
JOC	Joint Operations Centre
LiDAR	Light Detection and Ranging

MAA	Mutual Aid Alberta
MEDEVAC	Medical Evacuation
MMN	MEDEVAC Mission Network
MoD	Ministry of Defence
MoDAF	Ministry of Defence Architecture Framework
MPE	Mission Partner Environment
MPV	Multi-Purpose Vehicle
MSAB	Multi-National Security Accreditation Board
NATO	The North Atlantic Treaty Organisation
NC3A	The NATO Consultation, Command and Control Agency
NCDMA	NATO Cyber Defence Management Authority
NCIRC	NATO Computer Incident Response Capability
NCOP	NATO Common Operational Picture
NCSA	The NATO Communication and Information Systems Services Agency
NCSC	The National Cyber Security Centre
NGO	Non-Governmental Organisation
NIST	National Institute of Standards and Technology
NMD-I	NCSA Mission Detachment of ISAF
NFR	Non-Functional Requirements
NIP	Network Interconnection Points
NNEC	Network Enabled Capabilities
OA	OCTAVE Allegro
OASoSIS	OCTAVE Allegro for SoS Information Security with CAIRIS
OCTAVE	The Operationally Critical Threat, Asset, and Vulnerability Evaluation
PECC	Patient Evacuation Co-ordination Cell
PIA	Privacy Impact Assessment
PMR	Patient Movement Request
PNG	Personae non Gratae
PoI	Point of Injury
PoP	Points of Presence
PRT	Provincial Reconstruction Team

RACI	Responsible, Accountable, Consulted, Informed
RBDM	Risk-Based Decision Making
RC	Regional Command
RDT&A	Research, Development, Trials, and Assessments
RE	Requirements Engineering
RFC	Request For Comments
RIDM	Risk-Informed Decision Making
RM	Risk Management
RMADS	Risk Management Accreditation Document Set
RQ	Research Question
RSM	Resolute Support Mission
SA	Situational Awareness
SABSA	Sherwood Applied Business Security Architecture
SCR	(NATO) Senior Civilian Representative
SDLC	The Systems Development Life-Cycle
SFA	Security Force Assistance
SHAPE	Supreme Headquarters Allied Powers, Europe
SLE	Single Loss Expectancy
SMF	Service Management Framework
SoA	Service Orientated Architecture
SoS	System of Systems
SoSs	Systems of Systems (*Plural*)
SoSE	SoS Engineering
SoSRE	SoS Requirements Engineering
SoI	System-of-Interest
SQUARE	Security Quality Requirements Engineering
STANAGS	Standard Operating Agreements
STRIDE	Spoofing, Tampering, Information Disclosure, Denial of Service, and Elevation of Privilege
SVTC	Video-based Secure Video Teleconferencing
SysML	Systems Modeling Language
TCN	Troop Contributing Nation
TDMS	Theatre Medical Data Store

TM	Trust Management
TMIP-J	Theater Medical Information Program-Joint applications
TOC	Tactical Operations Centre
UML	Unified Modelling Language
USCENTCOM	United States Central Command
UN	United Nations
UX	User Experience
VoIP	Voice-over-Internet-Protocol
WAN	Wide Area Network
WPA2	Wi-Fi Protected Access II
XML	eXtensible Markup Language

Chapter 1

Introduction

In this Chapter, the research problem, motivation, and objectives towards addressing certain research gaps are introduced. Three research questions are presented as a means to address problem areas. These aimed to identify the needs and requirements towards the problem situated within a *System of Systems* (SoS) context, and the identification of elements, concepts, and techniques suitable for application towards assessing information security risks and related human factor concerns within the problem domain. In support of the thesis claim, an integrated approach is proposed towards addressing the problem and research gaps. The thesis structure to address the research gaps is summarised to detail the related research applied towards this problem.

1.1 Thesis Motivation

Throughout society and industry, technological evolution has increased the reliance placed upon the inter-connected worldwide networks to facilitate diverse technical and social system integrations, thus creating challenges and opportunities towards meeting these socio-technical needs. These may arise due the continuing supply and demand needs of consumers, businesses, critical infrastructure, or military and defence, who themselves are in a constant state of evolution exploring new ways of interacting to achieve new and different purposes. However, whilst integrating people with evolving processes and emerging technologies, a number of risks are created by related challenges associated with these socio-technical systems, for example, accounting for security needs and its related human factors within the context of the System-of-Interest (SoI) - The system whose life cycle is under consideration (International Council of Systems Engineering 2007).

There are many different types of systems that are designed and created by people, then used or exploited by people in varying contexts of application. People and culture becomes more applicable when traversing across geographical and environmental boundaries. Regulatory and legal requirements also play a factor in determining operational requirements, trust boundaries, and potential risks when integrating technology with people and a process of activities. Human factors therefore play a central role in most systems where there is a joining of social and technical interaction, and thus there is a need towards identifying those dependencies and implications.

In some scenarios, systems may choose to collaborate in new ways, in addition to or extending from their originally designed purpose, or what could be considered as their *day-job*. This creates and interdependency between independent systems to achieve a common goal, meaning a reliance and dependency is placed upon the collaborative activities for the ability to achieve the goal. For example, in a disaster scenario, an emergency response unit has a need to interoperate with the police, fire, ambulance, coastguard, or other critical services. Each of these entities may be considered as an independent system with its own purpose, operational capacity, and systems integrating people, processes, and technology. Each of these independent systems collaborates and interoperates with other emergency response unit stakeholders to collectively meet the emergency response mission objectives.

This example of systems, with a day-job, coming together for a greater interaction collaborating with the emergency response unit could, therefore, be described as being a SoS. Many examples of SoSs exist, but the term has become a source of confusion across domains. Moreover, there are few illustrative SoS examples demonstrating their initial classification and structure. Different examples of independent system collaborations converging to form a SoS may be less or more complex, or have different needs and goals, with differing levels of management and oversight. Many examples of SoSs are further challenged by geographical, organisational, safety, security, and human factors considerations affecting risk within the SoS as a whole.

Previous emergency and disaster scenarios such as the July 7th attacks in London have shown the potential need for independent systems coming together in a SoS context, and the challenges experienced between emergency services in which to efficiently interoperate with each other as a whole (Dogan et al. 2011). In addition to failings related to interoperability and the ability for services to communicate and co-ordinate with each other, there was a further failure to explicitly address the needs and priorities of the people involved, including responders, casualties, and the general public affected by the events that unfolded (London Assembly 2006).

Because these considerations are typically greater than that of a single system, the interactions and interdependencies between entities can increase risks for independent systems, and the SoS as a whole. Therefore, the required interactions and interdependencies to achieve SoS goals that would inherently bring greater risks for independent systems, need to be accounted for to identify the impact to the SoS as a whole. Threats in a SoS are also likely to differ at different system levels, some of which are likely to posses different degrees of dependency and control compared to that of a SoS level.

Security risks are exacerbated by the differing requirements needs of independent systems, their goals, trust boundaries, and overall levels of assurance provided. Furthermore, security goals at one level, may be greater or lesser at the SoS level, presenting obstacles that need to be identified at an early stage. This further implies a need for SoSs to integrate ongoing feedback-loops to promote situational awareness and real-time information in which to evaluate and apply applicable security risk mitigation towards areas of uncertainty in a SoS context.

However, assessing security risk would be challenged by the level of centralised management and control within the SoS, specifically towards risk-based decision making, and from what or whose view within the SoS risk is being assessed. The emergency response unit could, for example, provide management towards the SoS interaction, but may have limited operational control of independent systems, and therefore an ability to assess its operations. The SoS may be assessed from the emergency response unit point of view to form the SoS with independent systems. Alternatively, the police may assess SoS integration with other systems and the emergency response unit, independently or as a whole.

In either case, a challenge for SoSs is where each entity may only know or have access to limited amounts of information about each system in which to assess security risk as a whole. In which case, security and risk should still be assessed at a SoS level, but may need to be done at a system level if there is a weak collaboration with limited or no useful information to support security risk assessment. Moreover, some risk may be unknown or may not exist until the coming together of the SoS, and can be created from emergent behaviour occurring through the evolution of the SoS.

The dynamics of SoSs often depend upon the type and level of management and collaboration from independent systems, their sub-systems, with varying degrees and dynamics of trust. Identifying the SoS context is, therefore, vital to security risk assessment if we are to appreciate the SoS mission and complexities. In some scenarios, there may be a weak collaboration from decentralised control, thus providing limited information. Having detailed information of the SoS interactions as a whole may, therefore, not be available or achievable in some SoS scenarios, yet we need to understand the given SoS scenario if we are to identify security risks and mitigating requirements. Therefore, identifying the minimum level of detail to adequately assess SoS security risk is a challenge, certainly towards bridging operational needs of independent systems to SoS Requirements Engineering (SoSRE), meeting the criticality of the independent requirements accurately reflecting interdependent users' needs crucial to the success of RE for the SoS (Ncube et al. 2013, AlhajHassan et al. 2016).

Despite this motivation towards the needs of SoSRE, research covering the broad topic of SoSs exists, but appears to lack in relevant approaches towards assessing security risk, and its human factors concerns within a SoS context, with suitable case studies to support the ideation of security risk assessment in SoSs. While there are many approaches for engineering of systems, less exist for SoSRE. Although some engineering methods are applied towards SoS engineering, e.g. Office of the Deputy Under Secretary of Defense, for Acquisition and Technology, Systems and Software Engineering (2008), International Council of Systems Engineering (2007), Ross et al. (2016), research indicates that further work is required towards how we may assess and model information security risk whilst capturing related human factors concerns in the context of a SoS. In particular, aligning the assessment of security risk to the

SoS under consideration, and identifying suitable concepts, models, and techniques that can be applied within a risk assessment and modelling process to inform SoSRE and risk-based decision making stakeholders.

There appears to be no SoS focused security risk approach or tool-support that demonstrates modelling and visualisation of risks, people, process and technology in a SoS context. Current approaches tend to focus on a single system or organisation, its operations and impacts, but not the wider impacts from the bottom-up collaboration in a SoS, and the resulting effects towards interoperability and the satisfaction of SoS goals. Most current tools or approaches appear to be designed with a single system or organisation in mind, or there is no clear guidance provided to inform how different approaches may be integrated towards capturing and assessing a SoS in context.

A method of assessing, modelling, and visualising SoS information security risks whilst capturing related human factor concerns could, however, increase consistency to this process across the SoS as a whole, helping to bridge the communication gap between operational needs and SoSRE. This should extend to the identification of new approaches towards formulating an information security risk assessment for SoSs, applying research to consider the challenges associated with SoSs, such as the dependency towards interoperability of systems, sub-systems and components, assurance and accountability, integrated with human and system interactions to achieve their SoS goals.

It is therefore argued, that identifying suitable techniques appropriate to help with modelling and visualising these interactions would be useful as a means for assessing and demonstrating the wider risks in a SoS context. This would be applied towards the SoS operational needs, informing the RE of security, system and software engineering needs to meet the operational mission goals of a SoS. A tool-supported framework to assist the modelling of risk would explore available and accessible tools for visualising security risk in SoSs. Furthermore, identify an alignment of SoS factors and concepts suitable for eliciting, analysing, validating risks within the SoS context to support the process of risk-based decision making.

However, where tools exist and appear to be designed with a single system context or organisation in mind, scaling-up to a SoS context and scenario, sometimes of which could be quite complex requiring many designs, is a challenge. It may require combinations of tools, techniques, and models, or an integrated design tool with the ability to combine different concepts to approach this challenge. Therefore, identifying and testing a combination of these approaches would provide useful research contributions towards closing the research gaps. When combined, these contributions would aim to support an end-to-end information security risk assessment and modelling process to assist risk-based decision making in SoSRE.

1.2 Research Questions

SoS decision making often consists of independent decisions, meaning there is a multiplicity of decision making processes with varying degrees of coupling. Because of this, it is argued that when assessing then modelling information security risks with associated human factors concerns, tools need a common way of working to model, visualise and analyse the impacts of security risks in a SoS context. The output should help to inform decision makers by providing a better understanding of risks to the SoS, and required mitigations towards the SoS achieving its goals. Moreover, the end-point for integrated tools is to realise how the output of a first-stage risk assessment can support or feed into tool-support for security, risk, design and operational decision making, and what type of information is useful to support this process for modelling and visualising the SoS in context.

Taking account of the motivations towards the research problem, the aim of the research is focused towards identifying challenges for SoSs and how information security risk and associated human factor concerns may be assessed in this context. Furthermore, how the security risk assessment process can align SoS factors and concepts suitable for eliciting, analysing, and validating risks with the use of tool-support. This would aim to provide a means for assessing SoS information security risks, whilst capturing human factors concerns in the SoS context, the output of which would support risk-based decision makers and SoSRE activities. To achieve this, research questions were devised to focus on three core areas of consideration.

The following indicates each research question (RQ) considered to address three main areas of focus:

RQ1 What SoSs factors contribute to challenges of security risk assessment of SoSs?

RQ2 What concepts are suitable to support a framework for security risk assessment with requirements elicitation in SoSs?

RQ3 How can the newly developed SoS security risk assessment framework be extended using modelling and visualisation software tools to assist the SoS security risk and requirements process?

Based on findings from addressing the RQs, three contributions were provided to address the research gaps and formulated into an end-to-end process. In particular, research indicated a need for a SoS characterisation process that could then inform an information security risk assessment process suitable for addressing a SoS context. Its output is aligned and integrated with tool-support for modelling, visualisation, and analysis in the SoS context.

Therefore, in support of the thesis, OASoSIS *(Oasis)* provides an alignment of SoS factors and modelling concepts suitable for eliciting, analysing, and validating SoS information security risks and associated human factors. Although parts of OASoSIS can be used in a standalone nature, as a whole, the thesis claims *OASoSIS represents an end-to-end information security risk assessment and modelling process to assist risk-based decision making in SoSRE*.

The scope of the research problem to be addressed has, therefore, provided a focus for research to first understand how the coming together as a SoS presents challenges and opportunities towards system interactions. Accounting for the context of the SoS then provides a focus towards identifying related challenges towards security risk assessment in SoSs, and the different degrees of ownership, trust, and dependency upon assets and interoperability within a SoS. This includes the identification of processes required to capture then model important SoS goals, activities, and interactions to inform related information security considerations. The output would aim to support risk-based decision making towards the secure design and operation of a SoS, informing towards risk mitigating controls and requirements for SoSRE.

The intended users of OASoSIS would therefore be aimed towards roles related to SoSRE and organisational system entities responsible for assessing risk within the SoS. Typical roles applying OASoSIS would, for example, be risk assessors or security analysts, requirements, systems, software, and security engineers, or a combination of these roles supported by input from other SoS stakeholders and subject-matter experts. The output would then be aimed towards supporting stakeholder roles of SoSRE and organisational system entities with risk-based decision making responsibilities towards the assessed SoS.

1.3 Thesis Structure

When considering the research problem, motivation, and aims, the derived RQ's are explored in Chapters 4 and 5, whilst grounded in literature detailed in Chapter 2. Chapter 6 introduces *OASoSIS* representing an end-to-end information security risk assessment and modelling process, whilst Chapters 7 an 8 demonstrate its contributions and application, further supporting RQs. This concludes with Chapter 9 and discusses future directions towards related work.

In Chapter 2, the review of related literature considers the concept of Information Security and risk-based decision making processes towards managing and assessing information security risk. The concept of SoSs is reviewed considering the different aspects and challenges of SoSs that sets them apart from single systems and related approaches, whilst considering the role of RE for SoS to ensure SoS needs have been considered to satisfy its goals. Related modelling techniques are identified, whilst considering the benefits or drawbacks of model integration using tool-support to help model and visualise information security risks and their associated human factors concerns in SoSs.

In Chapter 3, research methods are considered towards addressing the RQs detailed, with examples of how methods would be applied to achieve elements of the research contributing to the thesis. This begins in Chapter 4 where research considers a means of characterising the candidate SoS towards formulating a SoS characterisation process to support a SoS security risk assessment. The SoS example is also used to identify its SoS challenges, concepts, and factors applicable for consideration within a SoS security risk assessment framework.

Chapter 5 continues to identify challenges, concepts, and factors applicable for consideration within a SoS. This chapter introduces an existing example of a SoS, with a primary focus of considering implications towards security, risk, and human factors within the example SoS, and how this may be assessed and modelled in a SoS context.

Building upon the findings of Chapters 4 and 5, related literature reviews, and stakeholder feedback and validation, Chapter 6 introduces the three contributions towards *OASoSIS* representing an end-to-end information security risk assessment and modelling process to assist risk-based decision making in SoSRE.

These contributions include:

> A SoS characterisation process to support the information security risk assessment process by providing the relevant SoS context.
>
> This aligns with a modified information security risk assessment approach using OCTAVE Allegro in the SoS context.
>
> The output of this first-stage assessment would then be modelled in tool-support for further analysis using a goal-driven approach towards SoS information security risk, capturing related human factors.

Details of the steps to be taken within the refined process in Chapter 6, provide direction and considerations for each step to be taken throughout the process.

How the three contributing components of OASoSIS have been applied, tested, and validated with a SoS case study and related stakeholders is discussed in Chapter 7. Then, Chapter 8 presents a final SoS case study, addressing a real-world problem and intervention. Building upon previous findings, this chapter applies a refined process of OASoSIS to test the end-to-end information security risk assessment and modelling process to assist risk-based decision making in SoSRE. Based on lessons learned from this application, models were also enhanced to close an identified gap within the modelling process towards accountability. The application of OASoSIS described in this chapter received further stakeholder validation towards the contributions, concepts, models, and techniques that represents an end-to-end information security risk assessment and modelling process to assist risk-based decision making in SoSRE.

Chapter 9 draws on overall findings, challenges, and observations from research reviewed. Then, concludes with continuing areas of focus towards future work. For example, this would continue to consider the implications of information security risks, whilst capturing their related human factor concerns in SoSs, and further applying OASoSIS to different types of SoSs. Moreover, considering how models may be further enhanced in tool-support adding clarity to a model's context to support analysts, engineers, and risk-based decision makers in SoSs and RE.

1.4 Related Publications

Overview

In support of this research project, four conference and workshop papers were published, and work introducing the research areas of focus was published and presented at a Doctoral Symposium. How these are applicable to related research and peer review is indicated within Chapter Summaries of Chapters 4, 5, and 7.

Conference / Workshop Proceedings

1. Ki-Aries, D., Faily, S., Dogan, H., and Williams, C. Assessing System of Systems Security Risk and Requirements with OASoSIS. *Proceedings of 5th International Workshop on Evolving Security & Privacy Requirements Engineering* at 26th International Requirements Engineering Conference 20-24 August 2018, Banff, Canada. IEEE.

2. Ki-Aries, D., Faily, S., Dogan, H., and Williams, C. System of Systems Characterisation assisting Security Risk Assessment. *IEEE 13th System of Systems Engineering Conference* 19-22 June 2018, Paris, France. IEEE.

3. Ki-Aries, D., Dogan, H., Faily, S., Whittington, P.,and Williams, C. From Requirements to Operation: Components for Risk Assessment in a Pervasive System of Systems. *Proceedings of 4th International Workshop on Evolving Security & Privacy Requirements Engineering* at 25th International Requirements Engineering Conference 4-8 September 2017 Lisbon, Portugal.

4. Ki-Aries, D., Faily, S., Dogan, H., and Williams, C. Re-framing “The AMN”: A Case Study Eliciting and Modelling a System of Systems using the Afghan

Mission Network. *11th IEEE International Conference on Research Challenges in Information Science* 10-12 May 2017 Brighton, UK.

Doctoral Symposium

1. Ki-Aries, D. Assessing Security Risk and Requirements for Systems of Systems. *26th International Requirements Engineering Conference (RE'18) Doctoral Symposium* 20-24 August 2018, Banff, Canada. IEEE.

Chapter 2

Literature Review

In this Chapter, the review of related literature first explores the concept of Information Security and how related risk may be assessed, with an early indication of how approaches may be considered towards the SoS context. The concept of SoSs is reviewed considering the different aspects and challenges of SoSs that sets them apart from single systems and related approaches. This includes the dependence on available and interoperable systems, where emergent behaviours may also occur.

Further challenges for SoSs are explored by considering the role of SoS engineering and the criticality of the requirements engineering process to ensure SoS needs have been considered to satisfy its goals. How this may translate into a range of typical engineering models is reviewed, whilst considering related benefits or drawbacks, including the integration of models using tool-support that would aim to help model and visualise security risk and human factors in a SoS context.

2.1 Risk and Security

The meaning and definitions of risk have evolved through different concepts and explanations, often relating to a decision making process and a propensity to take a risk towards a possibility of reward over the uncertainty of loss (Bernstein 1996, Adams 1999). Risk and uncertainty can be attributed to a number of contexts that could include examples such as weather and environmental concerns, stock markets and financial systems, or safety related cases. Risk in a security context can be defined as "*the effect of uncertainty on objectives*" (British Standards Institution

2011). For example, this can relate to assets being used securely to achieve a purpose to meet objectives.

Risk in security combines various elements in which to account for risks to security. These include:

- *An Asset* is anything that has value to the organisation (British Standards Institution 2011);
- *A Vulnerability* is a weakness in system security procedures, design, implementation, or internal controls that could result in a security breach or a violation (Kissel 2013);
- *A Threat* is a potential for a threat-source to accidentally trigger or intentionally exploit a specific vulnerability (Kissel 2013);
- *A Threat Source*, synonymous with *Threat Agent*, has the intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability (Kissel 2013);
- *Security* is a condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach (Kissel 2013).

Security is primarily concerned about the protection of these assets from potential threats and vulnerabilities, and the application of security controls to reduce or mitigate the risks (Von Solms and Van Niekerk 2013). To understand the related elements and estimate the level of risk towards security, the probability and impact of a threat-source intentionally or accidentally exploiting a system or information asset vulnerability is considered (Stoneburner et al. 2002).

The risks presented are likely to have an impact in different ways. For example, immediate impacts may be towards the Confidentiality, Integrity, and Availability. This would be due to unauthorised disclosure, modification, or destruction of information, resulting from unintentional errors, omissions, a failure to exercise due care and diligence in the implementation and operation, or disruptions due to natural or man-made disasters (Stoneburner et al. 2002). The effects of these impacts usually result in further consequential impacts, for example, where customer data may be disclosed to unauthorised entities, causing further customer and business related impacts, losses, or fines because of the data breach.

Accounting for people, their asset interactions and dependencies are an important aspect of the risk equation, given the potential impacts to people resulting from the effect uncertainty, or the risk-based decisions made in relation to risk. Systems and processes are designed by and for people, creating a dependency towards a need where a loss may create a negative effect to people, businesses, society, and continents. Security is, therefore, an important aspect to ensure the continued protection of assets to support functional ability where there is a dependency and reliance by people, groups, and organisations to achieve a positive outcome.

2.1.1 Information Security

Information Security takes a broad approach to security, considering the protection of information assets and the related systems and people responsible for the storage, processing, and transportation or transmission of data or information. The aim of Information Security is to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorised access, use, disclosure, disruption, modification, or destruction in order to achieve security goals of confidentiality, integrity, and availability, accountability, and assurance (Stoneburner et al. 2002, Kissel 2013, SANS 2015).

The term *Cyber Security* is often used in place of *Information Security*. However, cyber security has a particular focus towards the electronic and digital domain (British Standards Institution 2012), whereas information security also considers people and physical security elements, such as the use of paper-based information, or knowledge held and verbally communicated. Information security is therefore the whole within which cyber security aims to protect or defend the use of cyberspace from cyber-attacks, where *Cyberspace* refers to a global information environment consisting of the interdependent network of information systems infrastructures and their data flows. For example, the Internet, telecommunications networks, computer systems, and embedded processors and controllers (Kissel 2013).

As a whole, information security encapsulates the concepts of physical, computer, application, network, and data security, where the primary focus is towards the use and protection of information assets. The focus towards data and security is critically important in most contexts where entities such as people, groups, or organisations are dependent upon the information flows of which the entities and their operations are built around. This would include accounting for the different needs of data-related stakeholders, e.g. data owners, custodians, and users, and the individual security goals and requirements for where data may be at rest, in process, or in transit between these entities (Whitman and Mattord 2011).

Given the different layers in which information security may be concerned, this drives the need for more holistic approaches towards managing and assessing security and risk, taking into account the user, analyst, defender, and attacker, and the impacts beyond the system itself (Henshel et al. 2015). For example, the concept of *Defense in Depth* is a widely recognised holistic approach towards asset protection, interconnections, dependencies, and available resources, providing strategic layers of defence supporting the monitoring, protection, and decision making processes to manage and reduce security risks (Bass and Robichaux 2001, Coole et al. 2012, Homeland Security 2016a). The important aspect of this focus is, however, ensuring security risks and controls are considered and applied at different levels, rather than relying upon a single line of analysis and defence.

2.1.2 Managing Information Security Risk

Risk Management (RM) is defined as being "*co-ordinated activities to direct and control an organisation with regard to risk*" (British Standards Institution 2011). RM for information security is the process of identifying, controlling, and mitigating information system risks. A common RM approach such as ISO 31000 (International Organization for Standardization 2018) is designed to provide a basic framework and process for risk management as illustrated in Figure 2.1. This approach is also adopted in the ISO 27005 standard for Information technology - Security techniques - Information security risk management (British Standards Institution 2011), and is a point-of-reference for RM and security related approaches.

Approaches may include standards and guidelines for information security risk management in an organisation, such as from the ISO 27001 to 27005 (British Standards Institution 2011 2013), or could include a range of NIST security related Special Publications from the SP 800 collection (NIST 2017). Examples such as these provide a wide range of security techniques, controls, and considerations

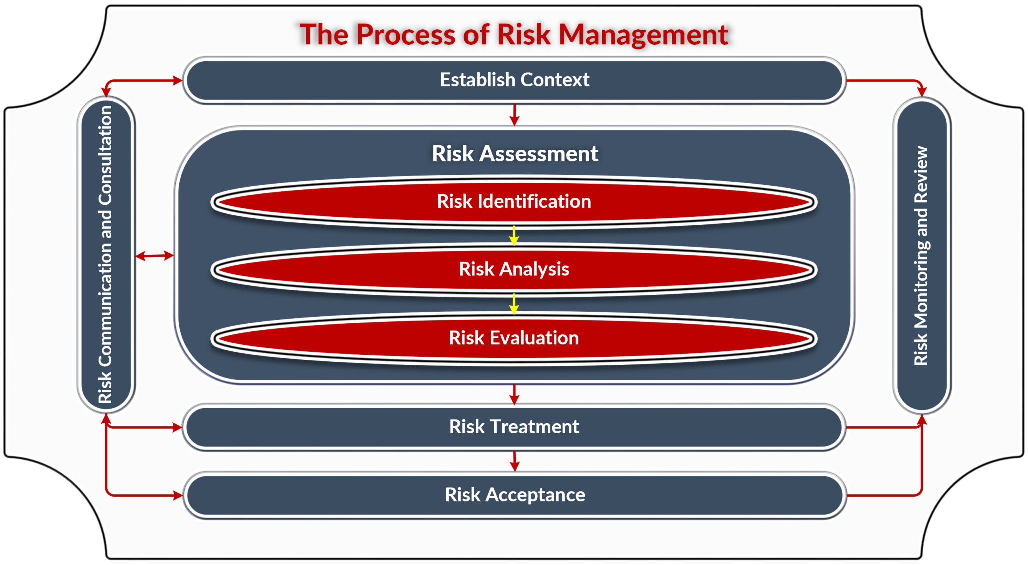


Fig. 2.1 The Process of Risk Management (British Standards Institution 2011)

towards approaching and applying information security risk management and assessment.

Risk-based Decision Making (RBDM) is defined as "*a process that organises information about the possibility for one or more unwanted outcomes into a broad, orderly structure that helps decision makers make more informed management choices*". It is a process that should aim to be simple and practical, whilst considering a range of factors that combined, provide necessary information helping decision makers to make more informed decisions (Myers 2002). RBDM as a process may be supported by Risk-informed Decision Making (RIDM) that focuses towards performance measures and the human element of decision making, acknowledging that reliance on technical information alone cannot be the sole basis for decision making (Dezfuli et al. 2010). Together, these play an intrinsic role towards the process of Risk Management.

2.1.3 Assessing Information Security Risk

Before any risk assessment begins, it must be supported with information pertaining to the context of use, mission goals, boundaries, relevant stakeholders, scope, and considerations to the risk criteria parameters. Critical resources must be identified to gain an accurate account of the potential for risks propagating from compromised resources and functional dependencies (Shameli-Sendi et al. 2016). This includes the effectiveness and efficiency of resources, and the impact upon the goals and constraints towards policy, regulatory and legal requirements (Stoneburner et al. 2002).

To achieve this, a range of risk approaches may be used for a given context. A chosen approach should be repeatable, measureable, auditable, and integrate the use of modelling (Jones 2007) for traceability and accountability that is important for a robust end-to-end risk process. These elements should be incorporated within the risk assessment to ensure a clear and consistent articulation of risk that helps risk-based decision makers to identify possible adverse effects (Böröcz 2016).

Literature demonstrates that risk assessment generally entails three key process steps, as illustrated in Figure 2.1. As described by ISO 27005 (British Standards Institution 2011), these process steps are:

> *Risk Identification* develops an in-depth understanding of the system structure and assets. To identify the risks present within the system environment, it then identifies threat-sources and vulnerable system elements, controls and potential consequences;
>
> *Risk Analysis* determines the likelihood and severity of consequences from identified risks impacting on the system element, and individual systems;
>
> *Risk Evaluation* considers the risk criteria and context, controls, and regulatory requirements to make risk-based decisions for future operation. High or unacceptable risks identified are prioritised with potential risk reduction controls considered ahead of risk treatment.

2.1.4 Approaching Information Security Risk and Assessment

There are many differing approaches to risk and how it can be managed and assessed, some of which extend security with other concepts. For example, towards, privacy, safety, or specific legal and regulatory requirements. In an organisational context, addressing security risk is often considered as a technical responsibility residing in the IT department. However, security needs are also linked with privacy needs, despite privacy being a topic that usually resides with legal and compliance functions (O'Brien 2016).

Approaches may apply different methods towards risk estimation, for example, some identify all possible attack scenarios and estimate all their risks, but this can be costly. Alternatively, some use a set of factors for estimating the risks of the threats grouped into classes using specific logic, such as those found within the OCTAVE family of risk approaches. However, most would benefit from ensuring analysis of potential attacker capabilities is considered to help reduce the uncertainty in estimating the potential ease in which an attacker is actually likely exploit a weakness, and therefore the risk exposure estimates (ben Othmane et al. 2015, The CERT Division 2017).

In a typical scenario, it is likely owners will be assigned within other departments to manage risk for which they are associated with, e.g. people and processes, but an organisation's owners and senior managers would be accountable and responsible for driving their risk management activities and setting the risk criteria, given their legal and regulatory obligations amongst others. Successful risk and cost-benefit estimation is reliant upon transparency, and experts providing a knowledge base of known misuse cases and countermeasures applicable to the organisational system and context of operation (Herrmann and Paech 2009).

Performing a risk assessment is therefore dependent upon a level of expertise towards risk, and an understanding of the environmental context to which the assessment would be conducted. In some cases, this responsibility may fall upon the roles of a Risk or Security Manager, or Security and Requirements engineers. In either case, the role would be required to possess sufficient skills to identify potential concerns, analyse and evaluate the potential threats, vulnerabilities, and their potential impacts using quantitative or qualitative means independently and with other stakeholders where required. These roles may provide some level of expert opinion, and rely on other roles to provide input and expert opinion towards the analysis, evaluation, and other subsequent RBDM.

Consequently, opinions may be subjective, and could be open to bias. For example, Rhee et al. (2012) argues that executives who perform risk assessments are more likely to exhibit optimism bias in comparison to other roles considered. Executives perceive their information security risk to be significantly lower, indicating an understanding towards the actual reality of 'information security risk'. However, they can be overly optimistic in their analysis, evaluation, or subsequent RBDM, as they do not seem to associate that same reality with themselves.

Although the inputs of a risk assessment are dependent upon it's quality and quantity, the output can be dependent upon the applied level of expertise and subjectivity. Moreover, consistency of how risk assessments are performed, in particular, across the different systems of a SoS becomes an important factor. In the context of a SoS, there would be a dependency between each of the organisational systems in which to manage and communicate their risks, specifically risks that would directly or indirectly impact upon the SoS achieving its goals.

Towards the SoS context, there is a need for a robust approach for managing, assessing, and communicating the implications towards information security and risk, not simply to a system or organisation, but in relation to a SoS as a whole. To address the research problem, it would also be useful if an assessment process had the ability to align with further modelling and analysis of security risks and related human factor concerns in greater detail, to better inform RBDM towards related information security risk mitigation requirements for the SoS.

Quantitative and Qualitative Risk Assessment

Approaches to RM may be classified as being asset or service driven, quantitative, qualitative or a combination of either. A quantitative approach may, for example, consider factors such as Single Loss Expectancy (SLE) and Annual Loss Expectancy (ALE), whereas a qualitative approach may use risk matrices to categorise and prioritise levels of risk, e.g. high, medium, low (Shameli-Sendi et al. 2016).

Comparative research, e.g. (Syalim et al. 2009, Behnia et al. 2012, Shameli-Sendi et al. 2016), has detailed the advantages and disadvantages of different approaches. In most scenarios though, it is the context to which they are to be applied that is the important decision making factor for the type of approach required.

Component-driven or System-driven Risk Assessment

Risk approaches may also be considered as being component-driven or system-driven, and therefore address different aspects of security and risk. The National Cyber Security Centre (NCSC) (NCSC 2018) consider the main differences as:

Component-Driven Methods

- Analysing the risks faced by individual technical components;
- De-constructing less complex systems, with well understood connections between component parts;
- Working at levels of abstraction where a system's physical function has already been agreed amongst stakeholders.

System-Driven Methods

- Exploring security breaches that emerge out of the complex interaction of many parts of the system;
- Establishing system security requirements before it is decided on the systems exact physical design;
- Bringing together multiple stakeholders' views of what a system should and should not do (e.g. safety, security, legal views);
- Analysing security breaches that cannot be tracked back to a single point of failure.

The distinctions between component-driven and system-driven are also aligned with an abstraction hierarchy representing the many interactions and relationships at different levels of complex systems. This provides reasoning for decision makers towards functional and component properties across several levels of abstraction along the means-end dimension (Rasmussen 1985). For example system-driven assessments are conceptual, considering goals of the system, balances, flows, governing principles, processes, and interaction of components. Whereas component-driven assessment focuses towards dimensions, locations, physical properties, capabilities, equipment, and components (NCSC 2018).

Best Practices and Industry Standards

It is not uncommon to only rely upon the use of best practices (Laracy and Leveson 2007), certainly for smaller organisations, groups, or independent entities. At a basic organisational level, Cyber Essentials and the Ten Steps to Cyber Security may also be considered. These encourage a focus towards cyber risks of information risk management, secure configuration, network security, managing user privileges, malware prevention, monitoring, removable media controls, home and mobile working

(Gov.UK 2015). Other larger more established organisations may need to implement standards and guides such as from the ISO 27001 to 27005 (British Standards Institution 2011 2013) or NIST Special Publications from the SP 800 collection (NIST 2017).

For some, implementing these controls and approaches is mandatory, as a minimum, suggesting more controls may be required given the context. However, for others, the costs and expertise required towards implementing these approaches or controls are aspirational. Security approaches and protection mechanisms should be proportionately affordable, be reasonably easy to integrate, use, access, and maintain, whilst providing user convenience without sacrificing security (Strawser and Joy Jr 2015). This should also consider needs of training and awareness, physical security, and due diligence on third parties and contractual management, and data privacy requirements (O'Brien 2016).

As a further consideration, given the range of stakeholders involved in a typical process of risk management and assessment, the communication and documentation of risk should be written in business-friendly language rather than endless detail of overly complex technical jargon, and clearly note potential impacts on operations (Everett 2011). The detail and traceability should still be captured, although it is likely certain audiences and in particular, risk-based decision makers, may require different levels of detail in which to base decisions upon. By clearly illustrating and communicating elements of risk and its effects, this output should aim to minimise negative impact upon the organisation, supported by robust decision-making when implementing a risk management process (Unuakhalu 2014).

The Generally Accepted System Security Principles (GAISP) has historically been adopted throughout many sectors, focusing towards the premise of accountability, awareness, ethics, multidisciplinary interaction, proportionality, integration, timeliness, reassessment, and democracy (Swanson and Guttman 1996). In an engineering or architectural context, integrated business RM frameworks such as the Sherwood Applied Business Security Architecture (SABSA) approach is said to be useful for large-scale systems (Szwed and Skrzyński 2014).

Government, Critical Infrastructures, and Defence

As identified through related interviews and research, British Government, military and defence adopt the Risk Management Accreditation Document Set (RMADS) within their security policy framework, originally using the now deprecated HMG Information Assurance Standard 1 & 2 for Information Risk Management (CESG 2012) that still serves a useful purpose. These standards may also assist national healthcare environments, although historically healthcare are likely to implement the Information Governance (IG) toolkit. Developed by the Health and Social Care Information Centre (HSCIC), this provides a means to assess how organisations process or handle their information, and a single standard set of information governance requirements aligned with certain standards and regulations (NHS 2017). This may incorporate the need for Data Protection Impact Assessments (DPIA) required under various data protection regulations, including the General Data Protection Regulation (GDPR), captured as part of the organisational and security risk management processes (Böröcz 2016).

RM approaches are also supported by different processes towards risk assessment, ranging across a number of areas and contexts, e.g. organisations, Customs, Critical Infrastructure, or developmental areas including the NATO acquisition process (Howard and Lipner 2006, Giannopoulos et al. 2012, Karabacak and Sogukpinar 2005, Dillard et al. 2006, CESG 2012, U.S. Customs and Border Protection 2014, North Atlantic Treaty Organization 2012). A benefit of many of these approaches is that they generally relate to a specific area or context, however, none directly address the SoS context. Moreover, some approaches are likely to require area or sector-specific knowledge and training for use, or may require a number of stakeholder interactions to complete the assessment of security and risk. Therefore, this means they may not be compatible with the needs of a SoS focused security risk assessment, where system information and stakeholder interaction may be limited.

The US Customs five-step approach did, however, provide an interesting approach towards different perspectives of typical stakeholder views that would need to account for risk. For example, importers, brokers, consolidators, highway carriers, foreign manufacturers, and US exporters. Considering stakeholder types and views could be a useful concept for SoSs, but would likely be difficult to implement given the many different types of system configurations and stakeholders interacting as SoSs.

An assessment process would however need to align with a range of stakeholder needs from an operational perspective, as well as security design and requirements engineering.

Elements applied in the Microsoft Security Development Life-cycle (Howard and Lipner 2006) approach that is applicable in many sectors, do however align with security design and requirements engineering, and support the elaboration of modelling data flows and performing threat assessments to capture and consider the potential for risks from a more technical perspective. Although, in a SoS context, other models would need to be introduced to account for other organisational and socio-technical perspectives, data for which would also need to be captured within the security risk assessment, which is beyond the current scope in Howard and Lipner (2006).

Considering OCTAVE

Considering there are a number of approaches available, this becomes a challenge for different organisations or during stages of the development life-cycle, where differing risk assessment approaches may be used to achieve the same goal. Many of these approaches are also designed and specified towards a single system or organisational context, and therefore when applied in a SoS context, will potentially scale poorly given the collaborative complexities of SoSs. RM should also consider factors such as program complexity and available resources for all systems and interactions (Rebovich Jr. and Authors 2014).

Moreover, asset identification is rarely performed reliably and consistently (Stephenson 2004) at a system level, which could then create further issues at a SoS level when accounting for risk. Assets are, however, central to a security risks assessment, meaning it is important to capture the human and system interactions with resulting dependencies to account for potential risks to assets, and the resulting effect towards the SoS reliance placed upon assets and interoperability to achieve its SoS goals. How these approaches may be aligned and applied in a SoS context therefore requires further consideration and testing.

An approach that has been used across many areas supporting RM is the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) risk assessment approach that caters for differing levels of skill and application. For example, OCTAVE has been developed in three stages. OCTAVE was originally designed for large organisations, whereas OCTAVE-S was developed as a focused version to support smaller businesses (The CERT Division 2017). OCTAVE Allegro (OA) is further refined and is perhaps the most flexible version that is specifically suitable for assessing information security risk (Caralli et al. 2007).

In comparison to other versions, OA reduces the need for workshops calling for participation by employees from all organisational levels, producing more robust results without the need for extensive risk assessment knowledge (Alberts and Dorofee 2002, Caralli et al. 2007), which would suit some of the challenges towards stakeholder interactions during a SoS security risk assessment. Some larger-scaled assessments introduced in previous sections including OCTAVE may also require a deeper focus towards vulnerability scanning and penetration testing to identify weaknesses, e.g. in software systems or networks. This expectation is unlikely to be effective or even applicable in an information security risk assessment for different types of SoSs, and would instead be encouraged as part of independent systems' ongoing risk monitoring activities, if applicable, but should nevertheless inform a SoS information security risk assessment when performed.

2.2 Systems of Systems

The term *System of Systems* is used to describe an arrangement of independent and interdependent systems, collectively coming together to deliver higher capabilities and performance (Baldwin and Sauser 2009). According to Maier (1996), to be defined as a SoS, it must have a majority presence of five characteristics present within its formulation. These are considered to be operational independence, managerial independence, geographical distribution, evolutionary development, and emergent behaviour (Maier 1996) from combined system interactions in ways not intended by the original single system designers. The coming together provides a set of systems for a task that none of the systems can accomplish on their own (Director of Systems Engineering 2010), and thus drives the need for a SoS collaboration, different to that of a traditional single monolithic system.

Boardman and Sauser (2006) believe the difference between a system and SoS lies in its composition, and is based on how the parts and relationships are gathered together, and therefore in the nature of the emergent whole. A system may be defined as being a functionally, physically, and behaviourally related group of regularly interacting or interdependent elements; that group of elements forming a unified whole (Office of the Deputy Under Secretary of Defense, for Acquisition and Technology, Systems and Software Engineering 2008).

Systems are composed of parts or elements with relationships between other elements of the system (Sommerville 2015). However, the arrangement of the whole must be understood to appreciate how it forms as a system (Staker 2001). For example, a system within a SoS can be considered as an organisation or its sub-division, a group, or social system, people networks, digital networks, manual or physical systems, computerised systems, or as is often perceived some form of software and hardware combination.

Each SoS can be composed of these different socio-technical combinations resulting from the collaborative interactions between independent systems and related sub-systems. The systems integrate to achieve new SoS goals under complex situations with intrinsic social and technical components (Kovacic et al. 2008). This intrinsic complexity is created by the multi-dimensional interactions between components, adding to the challenges posed by SoS configurations under different ownership and control (Sommerville et al. 2012). A SoS can, therefore, be considered as being a socio-technical system, involving both complex physical-technical systems, and networks of interdependent stakeholders (De Bruijn and Herder 2009) integrating directly and indirectly with other organisational systems, processes, and people to achieve the SoS goals.

2.2.1 Examples of Systems of Systems

Research has found that the context, application, or general concept of SoSs often means different things to different people. For example, when considering a military and defence context, SoSs will likely include configurable sets of constituent-systems in dynamic communication infrastructures (Lane and Epstein 2013). In a typical organisational context, the SoS may be considered as the enterprise-wide sharing of core business services and information with other geographically distributed organisational systems. This is again quite different to a typical stakeholder interacting with a cyber-physical system or an Internet of Things (IoT) set of systems. Nevertheless, in each of these contexts, there is a continued need for SoS techniques to be aligned to the design and operation of these increasingly complex systems (Henshaw 2016).

Many IoT systems are likely to be considered as SoSs (Maia et al. 2014, Alkhabbas et al. 2016), where strategic principles are required for design and operation (Homeland Security 2016b). The Internet, which IoT is based around, can be considered as being a global computer-to-computer network of a Collaborative SoS, where its elements are themselves computer networks and major computer sites (Maier 1996). Making further use of the Internet are software applications on smartphones and smart devices connecting to other smart systems such as home security, communications systems, or assistive technology (Whittington and Dogan 2016).

Other examples could include a combination of general business information systems, sensor networks, space and earth observation systems, defense and national security systems (Baldwin et al. 2011, Lane and Epstein 2013). Emergency response systems are considered as SoSs with their independently owned and managed systems and services such as fire, police, ambulance, hospitals and other facilities collaborating to deliver a service on which reliance is placed to achieve the SoS level objective or mission (Dogan et al. 2011, Nielsen et al. 2015).

Further reliance is placed upon the over-arching role of Critical Infrastructure. For example, where the health infrastructure on a national level has a operational and managerial dependence upon hospitals, medical centres, communication systems, power systems and networks, transportation, health insurance and finance networks to operate as a complex inter-connected infrastructure (Branagan et al. 2006). Moreover, supporting power grid technology, transport systems, and production systems (Nielsen et al. 2015), highlighting the criticality of stakeholders understanding how these systems who have their own objectives and risks, also need to come together at differing levels, thus evolving into SoSs for a new purpose, goal or objective.

2.2.2 Characteristics of Systems of Systems

A SoS is a system that contains two or more independently managed elements (Sommerville 2015), regardless of scale. When analysing a SoS, focus toward the SoI frames the SoS and its aspects of interest, and considers the life-cycle dimensions that contribute to emergent behaviour from the combined interactions (Kinder et al. 2012). In a SoS, the SoI elements are themselves systems interacting to achieve one or more purposes, although, a system in one context can also be a SoS in another. Therefore, in a SoS context and where other SoSs may exist, there is a further consideration towards the SoS SoI, which is defined as being "*The system of systems whose life cycle is under consideration described by all dimensions that contribute to the resultant emergent behaviour*" (Kinder et al. 2012).

Many SoSs consist of multiple, heterogeneous, operationally, distributed systems, embedded into multi-level networks of complex systems with different degrees of autonomy and which evolve over time (DeLaurentis 2007, Chiprianov et al. 2014, Harvey and Stanton 2014). Independent systems of the SoS generally retain their own identities. For example, in addition to the SoS interaction, they have a *day-job*, along with their own authorities, responsibilities, goals, and resources, whilst adapting to meet SoS goals to support its current and evolving user needs, design, engineering, and operational needs (Director of Systems Engineering 2010, Baldwin et al. 2011).

As a result, this suggests that accounting for interoperability needs and required actions to achieve SoS goals can only be predicted through analysis considering the SoS as a whole (Dyson 2012). This is because all system components and their relationships need to be thoroughly and continually understood as the complexity increases throughout the system evolution (Sommerville et al. 2012), and thus becomes important to the success of the SoS and its process of systems' integration. This can, for example, be defined as "*a process that combines system elements to form complete or partial system configurations in order to create a product specified in the system requirements*" International Organization for Standardization (2008).

Interoperability is defined as being "*the ability of two or more systems or components to exchange information and to use the information that has been exchanged*" (International Organization for Standardization 2010). Where Interoperability relies upon the ability of two or more systems or elements to use and exchange information (Institute of Electrical and Electronics Engineers (IEEE) 1990), overcoming the complexity resulting from interoperability needs across systems towards information sharing becomes a critical success factor for a SoS (Dogan et al. 2011). Point-to-point interoperability can be directed towards specific systems, but may fail to fully facilitate interoperation between other systems, e.g. legacy systems with compatibility issues or new systems added during the SoS evolution (Morris et al. 2004).

Interoperability is the key to a system's success, yet fully achieving interoperability can often be problematic for component systems, and consequently presents challenges towards safety and security in the SoS (Kinder et al. 2012, Harvey and Stanton 2014). Moreover, the Network Centric Operations Industry Consortium (NCOIC) indicates that interoperability within and across domains is better achieved when considering and addressing all dimensions, including technology, mission, business value, policies and regulations, culture and people (NCOIC 2019b). However, there is a need for better decisions taking a wider perspective in order to achieve cross-domain interoperability (NCOIC 2019a).

Interoperation between constituent systems requires stakeholders at system and SoS levels to play a greater role in determining policies that make goals of the SoS and the constituent systems achievable (AlhajHassan et al. 2016). It is important for stakeholders to determine the amount of effort required to improve and expand SoS capabilities (Lane and Valerdi 2007). Although, it should be considered that sole reliance upon standards, architectural frameworks, or striving for compatible technology does not always guarantee achievement of required interoperability, as technology, people, and organisational integration all need to be aligned to achieve interoperability (Chiprianov et al. 2014, Homeland Security 2017). However, where a SoS may have been dynamically composed through rapid evolution, and may quickly dissolve, the overall governance policy will be difficult to implement, yet there will be a continued need to demonstrate ownership and accountability towards the SoS (Morris et al. 2006).

Boardman and Sauser (2006) identified characteristics in Table 2.1 showing a comparison between the focus towards a system and a SoS context, distinguishing some of the specific characteristics found in SoSs. A distinction from the term *gathering together* is derived by two opposing forces, which are said to be present in a SoS but entirely lacking for a system. *Legacy* is a driving force from the parts perspective, and *Mystery* acts upon the whole (Boardman and Sauser 2006).

Because SoSs are composed of independent systems and sub-systems, coming together in ways elements may not have originally been designed for, this can increase the possibility of emergence, and thus increase risks for independent

Table 2.1 Differentiating a System from a System of Systems (Boardman and Sauser 2006)

Element	**System**	**SoS**
Autonomy	Autonomy is ceded by parts in order to grant autonomy to the system.	Autonomy is exercised by constituent systems in order to fulfil the purpose of the SoS.
Belonging	Parts are akin to family members; they did not choose themselves but came from parents. Belonging of parts is in their nature.	Constituent systems choose to belong on a cost/benefits basis; also in order to cause greater fulfilment of their own purposes, and because of belief in the SoS supra purpose.
Connectivity	Prescient design, along with parts, with high connectivity hidden in elements, and minimum connectivity among major subsystems.	Dynamically supplied by constituent systems with every possibility of myriad connections between constituent systems, possibly via a net-centric architecture, to enhance SoS capability.
Diversity	Managed, reduced or minimised by modular hierarchy; parts' diversity encapsulated to create a known discrete module whose nature is to project simplicity into the next level of the hierarchy.	Increased diversity in SoS capability achieved by released autonomy, committed belonging, and open connectivity.
Emergence	Foreseen, both good and bad behaviour, and designed in or tested out as appropriate.	Enhanced by deliberately not being foreseen, though its crucial importance is, and by creating an emergence capability climate, that will support early detection and elimination of bad behaviours.

systems and the SoS as a whole if left unaccounted for. *Emergence* is defined as being "*the principle that entities exhibit properties which are meaningful only when attributed to the whole, not to its parts*" (Checkland 1999). Emergence can be described as relating to the formation of new behaviours due to development or evolutionary processes and coming together (Chiprianov et al. 2014).

When designing for the SoS, it is suggested that emergent behaviours must be carefully planned, tested, and managed (Office of the Deputy Under Secretary of Defense, for Acquisition and Technology, Systems and Software Engineering 2008). Emergence may occur at different levels, however, emergent behaviour is consequently often an unplanned occurrence, evolving through the interactions and collaborations within the SoS (Maier 1996). This occurrence is described as being strong emergence, where unexpected emergence is not observed until the system is simulated, tested, or implemented into operation a situation that was not anticipated during design and development (SEBoK Authors 2019). This would include the varied interactions between sub-systems, groups and individuals contributing to emergent behaviour that in most cases cannot be predicted due to individual sub-systems isolation (Harvey and Stanton 2014). The challenge, therefore, is to learn how to maintain interoperability and systems' availability as the SoS evolves, allowing emergence to flourish, whilst retaining the agility to quickly detect and defend against unintended behaviours (Boardman and Sauser 2006).

2.2.3 Classification of System of Systems Types

Maier (2005) argues that interconnected systems are formed of substantially independently operated elements. These elements do not solely contribute to an overall purpose or set of functions, but rather individually fulfil useful purposes. Therefore, in order to be classified as being a SoS, the system should correspond with the following parameters described by Maier (2005):

- The elements of the system are themselves sufficiently complex to be considered systems;
- Operating together, the elements produce functions and fulfil purposes not produced or fulfilled by the elements alone;
- Each element possess operational independence and fulfils useful purposes whether or not connected to the assemblage. If disconnected, the element continues to fulfil useful purposes;
- Each element possess managerial independence, and managed, at least in part, for its own purposes rather than the purposes of the collective;
- A SoS is typically geographically distributed such that its elements exchange only information rather than mass or energy;
- A SoS typically evolves over time and space. It does not have a unique configuration, but rather evolves and changes.

There are many different combinations where independent systems with multiple stakeholders have a dependency towards other systems, driving a need for a SoS collaboration. A broad definition of the SoS objective should be provided and framed in terms of improved capabilities and not a well specified technical performance objective (Dahmann and Baldwin 2008). The level of interaction is also dependent upon the collaborative nature of the system stakeholders, where loose coupling becomes a requirement for systems over tight coupling and inflexibility.

Nevertheless, stakeholder interaction is likely to be driven by the design and purpose as a SoS, and its needs for interoperable interactions. For example, when considering design and SoS Engineering (SoSE) needs, identifying the characteristics, type, and classification of SoS becomes important step towards understanding the correct context of the SoS, its needs, owners, and conflicts. Stakeholder interaction therefore becomes essential to the SoS and its collaborative interoperation.

To support the classification of SoSs, Maier (2005) describes the levels of system interactions as being:

> Closed - Where the collaborative nature of the assemblage is under central design control. This is the typical situation where a single agency acquires the SoS and there is a lead system integrator, but the designers make a conscious choice to design with operational and managerial independence. That is, the designers choose to distribute control to the elements of the system;
>
> Open - Where a central design group exists, but does not have full control. The design choices of the central group are advisory on the elements. All integrated operation of the integrated SoS is a voluntary act on the part of the elements, but a central body exists to coordinate purposes and design choices;
>
> Virtual - Where no central governing body exists. The assemblage's purposes and configuration emerge from the undirected interactions of the elements.

Given these differences, it becomes evident that centralised control of SoSs is not always possible, presenting wider challenges for SoSs where the degrees of decentralisation are greater, which creates limitations towards assessing and managing SoS security risks as a whole. Maier (1996) further defines SoSs by certain combinations related to managerial and operational independence and control within the SoS. These are defined as being *Directed*, *Collaborative* and *Virtual* (Maier 1996).

However, Sommerville (2015) claims these classifications fail to reflect the distinctions between different types of SoSs. For example, when considering systems as Virtual, this is confusing given the term is also used to describe something that is usually implemented by software, e.g. virtual machines (Sommerville 2015). The term Directed could also be misleading as this may imply a top-down authority, whereas a single organisation still has the need to maintain good working relationships between the people involved, which means that governance is agreed rather than imposed (Sommerville 2015).

Additionally, Dahmann and Baldwin (2008) introduce a fourth definition of an *Acknowledged* SoS. These have an amount of increased centralised management control and resources to support the SoS, possessing qualities of Directed and Collaborative SoSs (Dahmann and Baldwin 2008).

The difference in all cases is that independent systems of a SoS have a day-job and were designed for a different purpose, that as a result will collectively have ensuing conflicts and limitations towards the SoS collaboration that must be accounted for to assist the success and dependability of the SoS. Each SoS collaboration integrates within rapidly evolving contexts in continuous and often disconnected execution of multiple life-cycle phases (Software Engineering Institute 2016). Who has managerial and operational control of the SoS is, however, the most important aspect of the SoS. This is particularly important towards to understanding the ensuing risks and complexities of shared control between different owners, whilst ensuring adequate authority is in place to manage and mitigate risks across the SoS.

The differences between the four main types of SoSs can be described as:

Directed SoSs

These are built and managed to fulfil specific purposes; they are centrally managed during long-term operation to continue to fulfil and evolve those purposes. Component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose (Maier 1996).

Acknowledged SoSs

These have recognised objectives, a designated manager, and resources for the SoS, but constituent systems retain their independent ownership, objectives, funding, as well as development and sustainment approaches. Changes to systems are based on collaboration between the SoS and systems (Dahmann and Baldwin 2008).

Collaborative SoSs

These are distinct from Directed SoSs in that the central management organisation does not have coercive power to run the system. The component systems must, more or less, voluntarily collaborate to fulfil the agreed upon central purposes (Maier 1996).

Virtual SoSs

These lack both central management authority and centrally agreed upon purposes, may exist deliberately or accidentally, and large-scale behaviour emerges, which may be desirable (Maier 1996). Participants informally collaborate and manage their own systems to maintain the system as a whole (Sommerville 2015).

While SoSs generally align with one of these categories, the distinction is not always clear. For example, a Collaborative SoS may need to formulate into an Acknowledged SoS due to the importance or complexities of the missions supported by the SoS (Lane and Epstein 2013), or an Acknowledged SoS with very little or ineffective managerial control may be regarded as a Collaborative SoS. Moreover, since much of the early SoS research began, the context of SoSs has changed considerably. For example, early research (Ackoff 1971, Jackson and Keys 1984) focused on more mechanical-based machines, or machines with low computational capabilities. As researched progressed with Maier, Dahmann and Baldwin (Maier 1996, Dahmann and Baldwin 2008) who provide the main four SoS categories that hold today, the concept of *Smart* internet-connected everything, rapid evolution, and now common place geographical distribution of technology and people was not as prevalent of a factor as it is today.

The four types of SoSs are still applicable, however, the lines between types of SoSs become wider and more blurred, with an increasing potential for different SoSs existing within a SoS. Nevertheless, a Directed SoS is the strongest formulation, whereas the interactions within Acknowledged and Collaborative begin to depend more on the collaboration and trust equations to achieve its goals. Virtual coalitions of SoSs are considered to be where there are no formal governance mechanisms, but where the organisations involved informally collaborate and manage their own systems to maintain the system as a whole. This also means there is no governance at the organisational level, but informal collaboration at the management level (Sommerville 2015). National economies can be thought of as Virtual SoSs where there are conscious attempts to architect these systems through politics. Although, the long-term nature is determined by highly distributed, partially invisible mechanisms, and the purposes expressed by the system emerge only through the collective actions of the systems participants (Maier 1996).

Virtual SoS are therefore perhaps the greatest challenge in terms of control, but the most likely to take a single system approach where an independent system is at least in control of their own destiny, and where reliance upon trust mechanisms may not be an option. Furthermore, a Directed SoS could at least in part take a single system approach with a greater reliance on trusted mechanisms, given the centralised control of most aspects that make it a Directed SoS. For a Directed SoS, the centralised control would also provide for more co-ordinated decision making towards the SoS's risks, and the implementation of unified processes and risk mitigations towards achieving its goals. However, where centralised governance and control is reduced across other types of SoS, although there is a sense of unity towards achieving a common goal, co-ordinating stakeholders with differing degrees of authority, accountability, and conflicting goals creates challenges for the RBDM as a whole.

2.2.4 Stakeholders in Systems of Systems

It is imperative to consider all stakeholders, needs, boundaries, and resulting challenges between inter-connections of the SoS. This includes, the ownership and operation of constituent systems and related assets within a SoS by independent stakeholders to overcome limitations on the exchange of information (Nielsen et al. 2015). Socio-technical systems combine different actors each with differing success criteria for the SoS design or integration (Ottens et al. 2005). However, when stakeholders contribute data towards risk activities, they are likely to value particular assets over others (Faily et al. 2012), meaning conflicts may arise between their own independent needs, or with other independent systems of the SoS. Security risks will likely increase where stakeholders are not always recognised across the SoS, or stakeholders of individual systems provide minimal input and interaction, or conflicts are not addressed (Office of the Deputy Under Secretary of Defense, for Acquisition and Technology, Systems and Software Engineering 2008).

Success can only be achieved if the stakeholder engagement is conducted correctly with all relevant stakeholders (Böröcz 2016) throughout the SoS life-cycle. A concise knowledge of stakeholders' needs, preferences, and alternative solutions is required, and subject matter experts may be consulted when knowledge gathering (Staker 2001). SoS projects, large and small, may engage a diverse group of stakeholders, with limited expertise in specific areas. However, all stakeholders should be valued and recognised as being unique individuals assisting in the discovery of socio-technical and psychological factors relevant to project requirements (Cleland-Huang 2016).

Stakeholder interactions would be considered throughout the system life-cycle stages of engineering, development, transfer for production or use, logistics and maintenance, operation, and disposal (SEBoK Authors 2016). The Systems Security Engineering Guide (Ross et al. 2016) in the context of identifying the stakeholders who have a security interest in the system throughout its life-cycle, define stakeholders as being:

> Stakeholders include persons, groups, and organisations (or a designated delegate thereof) that impact the system or are impacted by the system, including the protection aspects of the system;
>
> Key stakeholders are those stakeholders that have decision-making responsibility associated with life-cycle concepts, program planning, control, and execution; acquisition and life-cycle milestones, engineering trades, risk management, system acceptance, and trustworthiness;
>
> Key stakeholders and their associated decision-making authority are correlated to each of the engineering activities performed in each life-cycle stage;
>
> Stakeholders are identified, including their security interest and specific roles and responsibilities relative to the systems engineering effort.

The design, engineering, and operation of SoSs is largely driven by stakeholders' goals and needs, and involves more stakeholders than typical single-system focused systems engineering activity. For example, stakeholders at the system and SoS level each have their own needs and objectives, and competing stakeholders' interests and goals (AlhajHassan et al. 2016). However, it is also true that through limited interaction, some stakeholders needs or specific technicalities for secure interoperability may not be available and captured as part of a security risk assessment or engineering activities.

2.3 Engineering for Systems of Systems

Systems Engineering is an integration of disciplines, e.g. software and security engineering, design and testing, forming a structured development process from concept to production, back to operation where the need and requirements began. As an interdisciplinary process, systems engineering has a focus towards managing the design of the complex engineering project life-cycles, that addresses business and technical needs of customers, with the goal of meeting user needs (Sommerville et al. 2012, Frank 2014).

Because usual engineering methods are applied towards a single system context, these rarely scale reliably when applied to the context of SoSs (Henson et al. 2013). This creates a continuing need for the SoSE community to grow and understand the discipline and approaches required to engineer SoSs, extending beyond a single system framework towards a class of complex systems whose constituents are themselves complex (Valerdi et al. 2007, Dahmann and Baldwin 2008, Jamshidi 2011). Systems are becoming more complex and closely interconnected with the human social environment, therefore understanding organisational and environmental goals is a necessity (AlhajHassan et al. 2016).

Capability suppliers must integrate many new technical and organisational systems with older legacy systems, within and beyond their own organisational boundary (Dogan et al. 2011). Each individual system's technical and organisational context and constraints should be considered when identifying viable options to address SoSs needs and objectives (Dahmann et al. 2008a). Difficulty may increase with the ensuing complexity of multiple independently managed systems and requirements that need to be co-ordinated in order to achieve the SoS objectives (Chiprianov et al. 2014).

Requirements applicable to the design and engineering of the SoS are important aspects that also need to evolve from a single system context. There is a need to identify the essential characteristics of systems which ensures established objectives can be achieved (Keating et al. 2008) within the context of a SoS as a whole towards achieving its goals, rather than each independent system's alone. RE communities have motivated the need for a greater focus towards engineering for SoSs and their security needs. New approaches for SoSRE should continue to evolve existing RE capabilities to align with SoSs, taking into account their complex collaborative interactions. For example, this should include multi-level modelling techniques and security requirements frameworks for SoSs (Ncube 2011, Ncube et al. 2013, Ncube and Lim 2018).

When eliciting SoS requirements, we cannot simply focus on elements such as software or network architecture. The context of the SoS and how it comes together as a whole should be identified, and how each type of system along with their interrelated SoS roles, responsibilities, processes, and information flows are dependent upon each other to achieve SoS goals. This includes manual or physical interactions, as well as computerised activities, and perhaps most importantly the related humans activities, needs, and dependencies. This becomes a complex task to ensure security risks are addressed with applicable requirements and related implementation and communication strategies. Requirements may therefore need to support a number of stakeholder needs at different stages of the life-cycle.

For example, early requirements should support and inform the SoS design and architecture stages to address the operation of systems, internal and external functions, relationships and dependencies, and end-to-end functionality, data flow and communications requirements critical to the SoS (Dahmann et al. 2008a). Architectural design involves selecting the systems to be included in the SoS, assessing how these systems will interoperate, and designing mechanisms that facilitate interaction, considering data management, redundancy and communications (Sommerville 2015). Therefore, identifying how and why systems and people would need to interoperate at different levels would be critical towards the assessment and reduction of security risks within the SoS and its life-cycle.

Other engineering life-cycle stages include integration, verification, validation, and building on the processes and activities of the systems operation, where risks relating to the SoS and its mission and objectives are identified. It is key for the systems engineer to understand the individual systems and their technical and organisational context, constraints, boundaries and interfaces. The behaviour and performance of constituent systems is critical to the SoS achieving its processes and data flow through combined interactions (Dahmann et al. 2008a).

Open systems and loose coupling provides advantages to SoS design, providing for maximum flexibility to address changing needs and technology opportunities. One example that adopts this concept is Service Orientated Architecture (SoA) that is said to offer a technical approach to address some of the organisational and governance issues, responding to the loosely coupled architectural needs of a SoS (Dahmann et al. 2009).

Engineering models include the various iterations of the V-Model for requirements and systems engineering, or the Double-V model for SoSE, providing means in which to apply the development life-cycle with various stages of verification, validation and testing (Clark 2009, Dahmann et al. 2008b, Weilkiens et al. 2015). The Ministry of Defence and Department of Defense Architectural Frameworks DODAF and MODAF can also be applied within these approaches. For example, MODAF is framework providing a means to model, understand, analyse and specify capabilities, systems, SoS and related business processes of an enterprise architecture (MODAF Partners 2005).

Other useful examples may include those detailed within the Systems and SoS engineering guides (International Council of Systems Engineering 2007, International Organization for Standardization 2006, Director of Systems Engineering 2010), security and requirements engineering approaches (Dahmann et al. 2013, Ross et al. 2016, Mead and Stehney 2005, Firesmith 2003) or a range of other context-specific engineering and operational approaches. For example, the Wave model addresses major steps in the application of SoS security engineering where SoS risks and required mitigations are addressed throughout the process, focusing on desired capabilities and undesirable emergent behaviours (Dahmann et al. 2013).

2.3.1 Systems of Systems Security and Risk

Research suggests the bridge between operational and engineering environments is essential for the analysis and communication of security and other critical aspects to increase end-to-end SoS security, reducing risk to mission outcomes. Security risk mitigations are addressed throughout the evolution of the SoS as a result of the interactions between constituent systems (Dahmann et al. 2014). Directed SoSs are more likely to apply an amount of top-down identification of security risk, whereas Collaborative SoSs who voluntarily collaborate to fulfil the agreed upon central purposes act in a more bottom-up capacity. However, given there is a need to achieve combined SoS goals, capturing security risks from the bottom up could be considered a benefit towards the understanding of how risks at different parts or levels of the SoS can affect different systems' goals, thus ultimately affecting the SoS as a whole and beyond.

It becomes imperative that these interactions between systems, data flows, and people are accounted for early in the development life-cycle and carried through to meet operational needs. Yet, for SoSs with reduced centralised governance and control, this can be a challenge to account for all interactions and stakeholder needs at different levels, and therefore required protections towards the secure operation of the SoS. Nevertheless, a fundamental principle of engineering is that systems should be built to withstand failure. However, SoSs with independently managed elements and negotiated requirements, it is increasingly impractical to completely avoid failure (Sommerville et al. 2012), but strengthens the need to engage stakeholders and reduce bounded rationality by capturing suitable detail of the SoS interactions in which to adequately assess and mitigate the SoS risks throughout its life-cycle.

The Systems Development Life-cycle (SDLC) has five main phases of initiation, development or acquisition, implementation, operation or maintenance, and disposal. Tending to risk is an iterative process that can be performed during each major phase of the SDLC (Stoneburner et al. 2002). Information security and the assessment of risks must be integrated throughout the SDLC to ensure the required security protection needs are integrated towards the information, and the systems and people that store, process, or transport the information. Furthermore, there is a need to consider how people may be accessing, using or sharing data outside of the original scope of the system or SoS (Lee 2012), including any other security-related aspects of communications between systems and the external world (Zhou et al. 2010).

Supply chain risk is also considered an area of concern towards business continuity and should be accounted for throughout risk management (Christopher and Peck 2004). For example, this is evident where military, civil, and intelligence capabilities have increased software assurance concerns, such as emergent behaviour of the integrated components or defects sufficient enough to compromise a system (Ellison et al. 2010). Supply chain risks and assurance of security must therefore begin to be addressed during acquisition of the development life-cycle (Boyson 2014).

Critical infrastructures and complex systems present a major challenge to risk analysis, often from tight coupling. Identifying threat sources is complicated by system complexities and the barriers to sensitive security information data flows between autonomous managed systems (Branagan et al. 2006). Context-based policy often drives data sharing while the number of recipients or their identities may not be known in advance. Independent systems may also be reluctant to disclose sensitive data to other entities, requiring extra measures such as policy-based data encryption techniques in some scenarios (Chiprianov et al. 2014).

When a security risk assessment is performed with an operational focus, this should inform the needs and requirements to be carried through to the development life-cycle, therefore capturing required security requirements should begin with asset analysis and the context in which they are in (Firesmith 2003). This should be supported by a continual focus on related human factors and interoperability critical for the SoS operation. Context of interaction among the socio-technical elements and surrounding objects should be identified and analysed to anticipate possible emerging activities, properties, and behaviours (Boy 2017).

This should account for roles critical to the interoperation of systems, assets, and people, where processes, tasks, and goals need to be performed, achieved, or maintained. For example, identifying who is accountable, responsible, or should be consulted or informed (RACI). The RACI approach may be considered by risk-based decision makers to understand where elements of risk may be present, and which roles are required to make decisions with an aim of mitigating the risk and maximising opportunities. Although, it is suggested that where high trust relationships are in place with a good understanding towards the organisational interactions, needs, and goals, the decision making process may have less barriers and be more rapid by comparison to rigidly relying upon RACI matrices (Kesler et al. 2016). Assigning roles of responsibility is an important factor for the process of RE towards the system-to-be achieving its objectives, whilst accounting for constraints related to the systems, software, and people (Van Lamsweerde 2009).

The output of the RBDM process should ensure socio-technical protective measures have been considered and deployed across the SoS to protect against external adversaries, and to secure the human vulnerabilities associated with system use. Early identification of these types of security threats, vulnerabilities and appropriate mitigations can lower the long-term cost of security control and mitigation (Lee 2012, Unuakhalu 2014). Security protection mechanisms should be proportionately affordable, be reasonably easy to integrate, use, access, and maintain, whilst providing user convenience without sacrificing security (Strawser and Joy Jr 2015). This should also consider needs of training and awareness, physical security, and due diligence on third parties and contractual management, and data privacy requirements (O'Brien 2016).

A positive security risk posture provides the initial characterisation of the threat environment and security risk tolerance, supported by ongoing analysis to identify emergent properties of the SoS (Dahmann et al. 2013). A challenge to achieving this results from the likelihood that many systems within SoS may not have gone through the same risk or security engineering processes, presenting the potential for new vulnerabilities and threats, and thus new risks to the end-to-end SoS (Chiprianov et al. 2014).

SoSs risks and mitigations focus on desired capabilities and undesirable emergent behaviours of the SoS. Capabilities provide resources for technical and organisational elements, although may have dependences with other capabilities (Lock and Sommerville 2010). SoS capability security may be impacted by operational use or change over time. Independent system changes to meet individual needs of constituent system stakeholders may change risk equations that might go unidentified unless specific focus is given to detect a threats or vulnerabilities susceptible within inter-system relationships (Dahmann et al. 2013).

Applying security to systems in isolation or applying inconsistent security policies may also lead to incorrect areas of focus for effective security, potentially consuming needed resources, and can lead to unidentified areas of threat (Baldwin et al. 2011, O'Brien 2016). An incorrect process or flaw in one system may result in severe consequences for the entire composed system (Zhou et al. 2010), or indeed SoS. Security must, therefore, be designed into the systems with a concious aspect towards how it is operated in the system and SoS context (Laracy and Leveson 2007). Cyber resilience should also be built-in to cyber resources to enable the SoS to anticipate, withstand, recover and evolve its business missions, functions and supporting cyber capabilities to minimise adverse impacts from attacks (Bodeau and Graubart 2011).

Additional risks are likely to arise from the complex human interaction across the collaborating services in addition to other process, technology or interoperability constraints (Dogan et al. 2011). With a greater interaction between technology, organisational and working environments, and human behaviour, security is also challenged by feedback, temporal change, time delays, soft factors, and interdisciplinary aspects (Gonzalez and Sawicka 2002). Human behaviour tends to conform to certain patterns, therefore understanding these patterns can signify where further protective measures should be deployed (Lee 2012).

Considering Ownership and Authority

An Owner is someone or something that owns a something that belongs to or is carried out by someone or something. An owner may be a person or a larger entity such as a group or an organisation with the authority for control, but is the single entity accountable for its level of authority to what is owned. Ownership therefore refers to the agency with authority over the system elements and its evolution. This includes the different levels of possession, authority, and control that exist over systems and processes necessary for the interoperation between those systems. For example, an asset that is physically owned and used by someone, a document or process that needs to be maintained, or a goal to be achieved.

Users and stakeholders may be attributed to an owner, but may themselves not be considered owned, and are instead likely to be regarded as accountable and responsible to the owner. They can also be associated as the owners of risks, systems, goals, tasks, processes, information, hardware, and software (Carney et al. 2005). Although, where a copy of the software may be considered bought and paid for, and therefore owned as an asset by an organisation or person, it is more likely the case that organisation or person is instead only granted a license for use of the software.

This is also similar to the perception of information ownership, whereby a business may own their information, but where personal information is concerned, a data subject is theoretically the owner of that information. However, when a data subject provides personal data for business use with consent, the business will often become the owner permitted to use the information, in accordance with data protection regulations. Therefore, the owner may not always have full property rights to the asset e.g. software or information, but has responsibility and accountability for its production, development, maintenance, use, and security. The owners, including risk owners holding accountability and authority to manage risk must therefore be identified as part of the SoS governance in accordance with supporting Risk Management frameworks (British Standards Institution 2011, International Organization for Standardization 2018).

In a SoS, the perception or understanding regarding ownership of each relationship between all systems may be ambiguous, or become implicit rather than explicit. This presents challenges for SoSs where co-operation by mutual understanding is required to understand what the others are doing, why, when and how, in order to anticipate their own actions (Boy and Grote 2011) if the SoS is to achieve its goals, securely.

Where ownership in the context of interoperability requires an understanding and agreement between individual owners about applicable authority, relationships, and accountability between independent systems, the challenge becomes much greater due to the complexity of SoSs. For example, where certain degrees of authority may not be clear due to a lack of centralised collaboration or control, in particular within a Virtual SoS, potentially leading to perceptions of apparent authority, rather than clear actual authority. Without this clear line of authority and responsibility, security risks may therefore increase or be perceived as greater given the uncertainty from reduced information and assurances towards the secure, dependable and interoperable systems and interactions between entities.

Considering Responsibility and Authority

Consequential responsibility is usually assigned to an organisation, a role, or a person, and is aligned towards who gets the blame in a negative event, and is therefore primarily accountable. Different strategies for responsibility discharge are applied, e.g. rule-based, experience-based, and knowledge-based. Whereas, a casual responsibility which has an obligation to its related authority has a different focus towards actions, e.g. doing, monitoring, avoiding. Both responsibilities do however remain accountable to their authority, but in different capacities (Sommerville 2007a).

For example, a person or role may be trusted and accountable to their authority for ensuring data is secured during their work, but if this was not achieved, this could amount to a data breach. This means there would likely be consequences for the person who was accountable and responsible for performing the task, but the organisation as the principal authority would ultimately be accountable for the data, and subsequent fines and losses. However, where accountability for the level of authority extends to blameworthiness towards consequences as a result of the data breach, liability and culpability would represent both a legal element towards their responsibility and to the extent blame may be applied towards a negative effect of the responsibility, e.g. not being achieved or maintained.

Where SoSs are built upon collaboration, understanding where accountability resides across all systems and stakeholders becomes a challenge, but is important for maintaining the resilience, dependability, and continued interoperability of the SoS. It is therefore important for stakeholders to address and maintain interoperability at different levels, e.g. people, process/procedures, software/hardware, to ensure operability and availability across each of the levels depended upon within the SoS, which is important towards meeting its security needs.

When discharging responsibilities, these may be framed based on defined process and procedures, or the agent assigned the responsibility may have the flexibility to decide how to discharge that responsibility based on their knowledge and experience of the environment and scenario. Having a degree of authority involves both control over humans and system elements, and the consequent responsibility and accountability for fulfilment, where transparency, predictability, and sufficient ability to fulfil responsibilities are a prerequisite (Boy and Grote 2011). The agent holding the responsibility is accountable to some authority for their actions (Sommerville et al. 2009), but should themselves be provided adequate authority in which to assist the ability to perform those actions.

Ability can also be considered towards the independent system's day-job and its originally designed purpose against its ability to meet the SoS needs and goals. When an independent system owner delegates an element of control and authority, this should not exceed the independent system's level of ability, control, or authority, but this may increase the delegatee's ability, control, or authority, and accountability in the SoS context. The assigned level of control afforded to a responsibility should not, however, exceed the level of control for which authority is granted towards sufficient ability to fulfil the responsibility, e.g. necessary competence, skills, resources, time, tools or personnel to execute control (Flemisch et al. 2012).

2.3.2 Human Factors in Systems of Systems

An important aspect for SoSRE are the people central to SoS activities, decision making processes, design, and operation of the SoS, providing varied input and output to its needs and dependencies. Human-Computer Interaction (HCI) and Human-Centred Design (HCD) approaches consider human factors in organisations, computing systems, software and hardware, and people's activities (Boy 2017). Accounting for the human factor at different stages can be addressed using a range of different approaches to address human factors in systems (Neumann 2007).

How this may be achieved for SoSs requires the human factors community to identify new ways of addressing information overload resulting from the complex interaction between SoSs, and provide ways to ensure a flow of interoperability and situational awareness (SA) (Dogan et al. 2011). This reliance on ensuring human factors are accounted for is demonstrated in emergency scenarios (Dogan et al. 2011). Moreover, in military operations where the lives of end-users in-theatre were dependent upon user-friendly designed systems that were easy to administer and operate, whilst providing reliable and timely communication information systems and SA in emergency scenarios (Veit 2011).

Further encapsulating human factors is the Human Systems Integration (HSI) approach that can be implemented early in the design stage and maintained at operational level. HSI considers relevant roles, responsibilities and relationships of manpower and personnel, ownership, stakeholder interaction, training, safety and other factors (National Research Council and others 2007). For example, NASA use HSI early in system development and acquisition to acknowledge hardware, software, and human interactions and elements needed to operate and maintain the system within an environment. However, successful HSI depends upon integration and collaboration of multiple domains (Zumbado 2015).

Similarly, Human Factors Integration (HFI) considers similar factors identifying and managing human-related risk, but considers other social and organisational factors. HFI can be integrated at an operational level, or included within RE or other elements of systems engineering to address the underlying philosophy and application of the human views throughout the development life-cycle into operations (Bruseberg 2008, Tadros 2013). HFI has, for example, been widely incorporated into defence and healthcare environments where safety is a priority (Hignett et al. 2017).

As SoSs come together combining new technology in different ways, enabling the integration of new systems performing new tasks, there is a lack of user and design experience or knowledge, meaning these systems will occasionally fail in ways designers failed to predict (Lee 2012). Given both the complexity of SoSs and the socio-technical interactions that may impact upon security, there is a need to incorporate HCD into approaches when engineering SoSs. Accounting for human factors is an important aspect that can reduce unwarranted assumptions or preconceptions about the human activities applicable to the system design, or to minimise latent errors from occurring, potentially from conflicting requirements, such as those that may be captured as part of CONOPS - the Concept of Operations documentation, as detailed by Rebovich Jr. and Authors (2014). CONOPS would generally be applied in a systems engineering context, but also accounts for other business and software engineering requirements, inputs, and outputs.

Supporting these approaches, graphical representations such as the Business Process Model and Notation (BPMN) or others can be used to account for the business processes of technical and human interactions (Altuhhova et al. 2012), or Responsibility and Capability modelling can be used to focus on a relatively abstract model of the socio-technical system (Lock and Sommerville 2010). People interaction within or across systems and sub-systems works on many different levels, each of which enables varied opportunities of interaction (Faily and Fléchais 2010b), but may create greater areas of risk that needs to be accounted for. Task analysis is a common technique for understanding how people should use the system under design or evaluation (Diaper and Stanton 2004), and could be related with use cases and misuse cases to capture elements of steps performed or that may be at risk (Sindre and Opdahl 2005).

A suitable approach for SoSRE towards task analysis can incorporate the use of scenarios to describe a shared story that puts the system in context (Go and Carroll 2004). User research on the participants within the narratives can be used to provide grounded human descriptions with scenario-based tasks. HCD tools such as *personas* can be used for a range analysis needs to identify user needs and goals. Personas represent archetypical descriptions of users that can, for example, embody the goals of business users offering insights into threats, vulnerabilities and likely areas of risk that may otherwise be overlooked (Cooper 1999, Faily and Fléchais 2010a, Atzeni et al. 2011, Cooper et al. 2014, Ki-Aries and Faily 2017). The integration of personas at the start of a project has been shown to be useful towards RE, assisting with user stories, and scenarios in which personas are situated within (Cleland-Huang 2013). In the same way that misuse cases can be used to behavioural model attacks,

Attacker Personas (Atzeni et al. 2011) or Personae non Gratae (PnG) (Cleland-Huang 2014) can also be used to analyse the negative intentions of a bad actor. Through analysis, sometimes aligned with misuse cases, this can inform risk-based decision making towards suitable requirements to address the identified threats (Mead et al. 2017). Personas may also assist assessors to identify potential security risk perceptions based on important human aspects, e.g. heuristics, biases, mental models, and distributed cognition models (Parsons et al. 2010, M'manga et al. 2017b a).

Also of consideration towards the human element, is where people have differing perceptions towards understanding security threats or risks, and users are often seen as the weakest link (Schneier 2011, Öğütçü et al. 2016). Security and usability is a factor that considers perceived usefulness and the ease of use against the propensity to take risks, for example with smart device application's data and communication security (Yoon and Occeña 2014, Lee et al. 2015). Perceptions towards security and risk become a learned experience, but perceptions could also become highly engrained and difficult to change (Workman et al. 2012).

When two entities have different levels of knowledge or understanding towards risk, their perceptions of risk are likely to differ. This would be applicable both during the assessment of risk with bias and subjectivity, and towards changing security behaviours to reduce risks. For example, it was found that IT personnel were more confident towards security, and therefore were more security risk tolerant in comparison to general staff who were more adverse of taking risks, yet presented better less risky behaviours by comparison to the IT personnel (Ki-Aries and Faily 2017). In addition to other controls, communication and awareness can address this disparity to some degree, but must use clear jargon-free user friendly language (Harkins 2012), tailored to the audience and context. When implementing security functions for the human interaction, they need to be meaningful, understandable, and should not reduce performance, but should make the user feel more protected (Furnell 2005).

Schneier (2011) believes that when people believe technology can solve all of their security problems, then they don't understand the problems. It is also a people problem. For example, there is a natural assumption information security is a technological problem, derived from a reliance on interconnecting with systems. However, most data and security breaches are a result of human error, sometimes due to lack of training or awareness (O'Brien 2016).

A distinction can, however, be made between violations and human error. Violations are usually considered to be intentional and sometimes malicious. These are usually performed by disgruntled insiders, former employees, contractors, or business partners. This may incorporate the misuse of authorised levels of access with the intention of harming a specific individual, the organisation, its data, systems, network, and business operations (Cappelli et al. 2009). Privacy breach incidents due to both slips and mistakes have steadily increased relative to malicious attacks in public firms (Liginlal et al. 2009). Human error may lead to mistakes from inadequate planning, or something not going to plan through slips and lapses at an execution stage (Reason 1990). Studies demonstrate the inherent risks in computer and information system security from accidental and intentional causes, or internal and external threats with related consequences (Kraemer and Carayon 2007).

Design principles from Saltzer and Schroeder (1975) continue to remain applicable to the modern day of computing and its users to help alleviate potential security concerns. Saltzer and Schroeder (1975) state that when designing for protection, this should apply:

- Economy of mechanism: Keep the design as simple and small as possible;
- Fail-safe defaults: Base access decisions on permission rather than exclusion;
- Complete mediation: Every access to every object must be checked for authority. This principle, when systematically applied, is the primary underpinning of the protection system;
- Open design: The design should not be secret. The mechanisms should not depend on the ignorance of potential attackers;
- Separation of privilege: Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key;
- Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job.

Although it is generally assumed systems rely on people behaving securely, assurance mechanisms still need to be applied (Fléchais et al. 2005), but should balance realistic needs and goals for design and operation in the context of the socio-technical SoS. Therefore, the people interaction factor needs focused consideration, along with other cultural and environmental factors, risk and security.

Where people can accurately perceive and identify risks that may impact towards information security, they are more likely to act appropriately. It is therefore necessary to identify and analyse those factors creating barriers preventing an accurate risk perception (Parsons et al. 2010). Trade-off's, social norms and internal interactions may also influence an individuals understanding of risks and requirements (Albrechtsen 2007).

2.3.3 Systems of Systems and Trust

At human and system levels, the notion of trust and assurance are important factors for stakeholders towards achieving SoS goals, and play a continuing role when addressing security, risk, and mitigating requirements as SoSs evolve (Ncube and

Lim 2018). This need and its challenges are exacerbated by the complexities of SoSs and their differing degrees of ownership and control. In order for the SoS to remain dependable, technical and social countermeasures are necessary for risk reduction that depend on a level of attained trust between entities, signalled and verified through a trust relationship (Fléchais et al. 2005).

Different assumptions, perceptions, expectations, and risk appetite will be present across systems, and requires active participation of transparency and trust focused towards related systems of the SoS as a whole to achieve its mission (Dahmann et al. 2009). Moreover, in security risk assessment and design, assumptions about the trust assumptions may need to be made by the analyst to explicitly limit the scope of the analysis to the context of the domain being analysed. This also means any security requirements to be satisfied depends on the design and trust assumptions identified by the requirements engineer in the context of the problem (Haley et al. 2004).

Capturing requirements that accurately reflect users' needs is crucial to the success of software engineering and its role in the system development process (AlhajHassan et al. 2016), and its success towards reducing the potential of security-related risk and its level of impact across a SoS. Unfortunately, where the notion of trust is an important factor for society, safety, privacy, and security, it is often a target area of exploitation from threat actors. However, although the notion of trust can be considered as a vulnerability, achieving and maintaining trust can under certain conditions reduce risks, but increase dependencies.

Trust is nevertheless something that can be hard to gain and require time, but can be quickly and easily lost. *Trust* is a belief by a *Trustor* that a *Trustee* will perform to an acceptable level as expected in a given scenario as depended upon. This *Trustum* is the encapsulating cycle in which the trust relationship is formed, thus trust can be considered as the willingness to be vulnerable, based on the positive expectations about the actions of others (Zand 1972).

Where there is an interaction or potential for interaction between two or more entities, a *Trust Relationship* is formed, implicitly then explicitly through verification or acceptance enabling the interaction with a degree of trust. This may range from no or low trust, to a higher more bounded level of trust that may increase or decrease overtime, thus increasing or decreasing the potential of a risk. Trust is, however, a

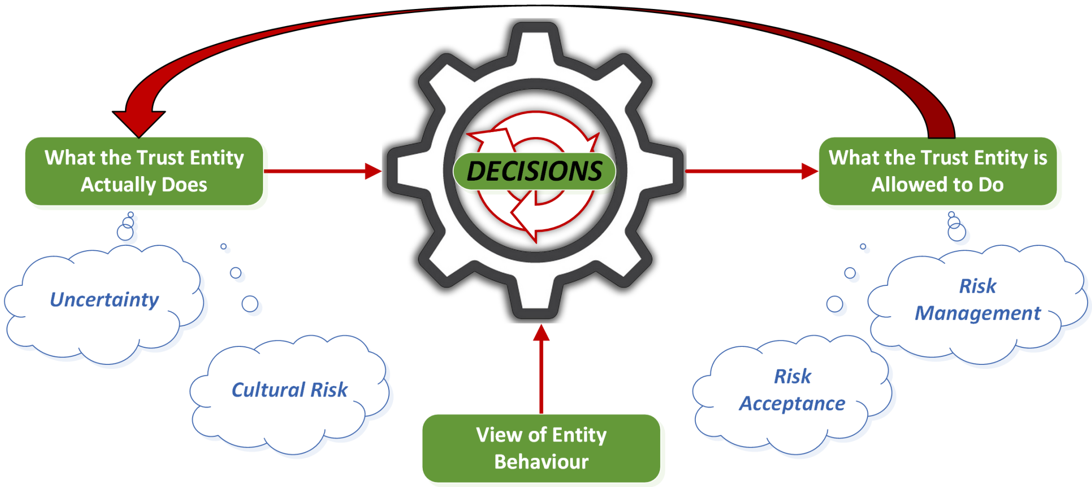


Fig. 2.2 Simple Trust Decision

two-way relationship where there will likely be more than one objective. For example, the (User) Trustor trusts the Trustee (Service Provider) to provide access to a system, but equally an expectation by the trustee is that the user/trustor will use the system correctly, meaning the roles of trust can be asymmetric.

Where trust is the likelihood of a positive action being performed, e.g. within a task, it is from the input and output of this belief that a decision making process considers whether a risk of the interaction should be accepted to achieve the desired goal. As in Figure 2.2, this continues with a further decision made to permit the expected action by others - or not, and re-evaluated based on continued interactions, and consistency of overall behaviour with positive outcomes aligning with risks.

Establishing trust relies on and number of direct and indirect approaches, policy, and protocols by which the parties negotiate and exchange the evidence and credentials, which are needed for evaluating trust in order to define a trust relationship (Grandison and Sloman 2003). There have been many ways identified towards how we may compare and determine different levels of trust and context (McKnight and Chervany 1996). In most cases, this relates to where an individual has reliance on another party under conditions of dependency and risk (Currall and Judge 1995), and therefore require measures in which to attribute degrees of trust warranting properties to determine and maintain trust. For example, this may consider the competence, honesty, security and dependability of a trustee (Haley et al. 2004), and be supported by policy to assess reputation, recommendation, and competence to be considered trusted in a related context (Alcalde et al. 2009).

The trust warranting properties within a relationship shown in Figure 2.3 extends the Riegelsberger et al. (2005) trust model considering this instead as a two-way interaction. This relationship and interactions can be described as having *Contextual* and *Intrinsic* properties, where Intrinsic properties are attributes of a trustee that lead to trustworthy behaviour. For example, internal factors to the trustor and trustee, such as the propensity to take risks, versus the benefits or drawbacks of the interaction. Contextual properties are attributes of the context or scenario that provide motivation for trustworthy behaviour, such as external actors, law enforcement, expectations of future interactions or reputation.

Moreover, contextual properties align with temporal, social, and institutional embeddedness, and intrinsic properties align with ability, and motivation by internalised norms and benevolence (Riegelsberger et al. 2005). Trust trade-off's may be observed from the context and distinction between these properties. Trust relationships are dynamic, may change over time, and can span across multiple systems, locations, boundaries, organisations, and people, meaning the frequency of change within a SoS is a critical factor (Sommerville et al. 2012, Kinder et al. 2012), yet identifying the changes is critical towards reducing risks and maintaining the SoS's security needs at different levels.

Trust can therefore be considered holistically where at the most common level, trust interactions between a trustor and trustee are at a human-to-human level, although in human-to-machine interactions, the belief or sense of trust is different and may require alternative signals and cues. Trust may be arrived at through informal exchanges, however, technology changes the interaction, perceptions, and trust variables, meaning traditional trust elements or signals through the trustor-trustee relationship may not exist when required (Riegelsberger et al. 2005).

Trust can also be considered as a confidence towards interacting with software and hardware systems or services that will function as expected (Henshel et al. 2015). Lack of confidence in the understanding, usability, or application of human-to-machine interactions may not create a sense of trust, but may lead to human error consequently increasing risk. That said, error detection and prevention for users could potentially reduce risk and increase trust.

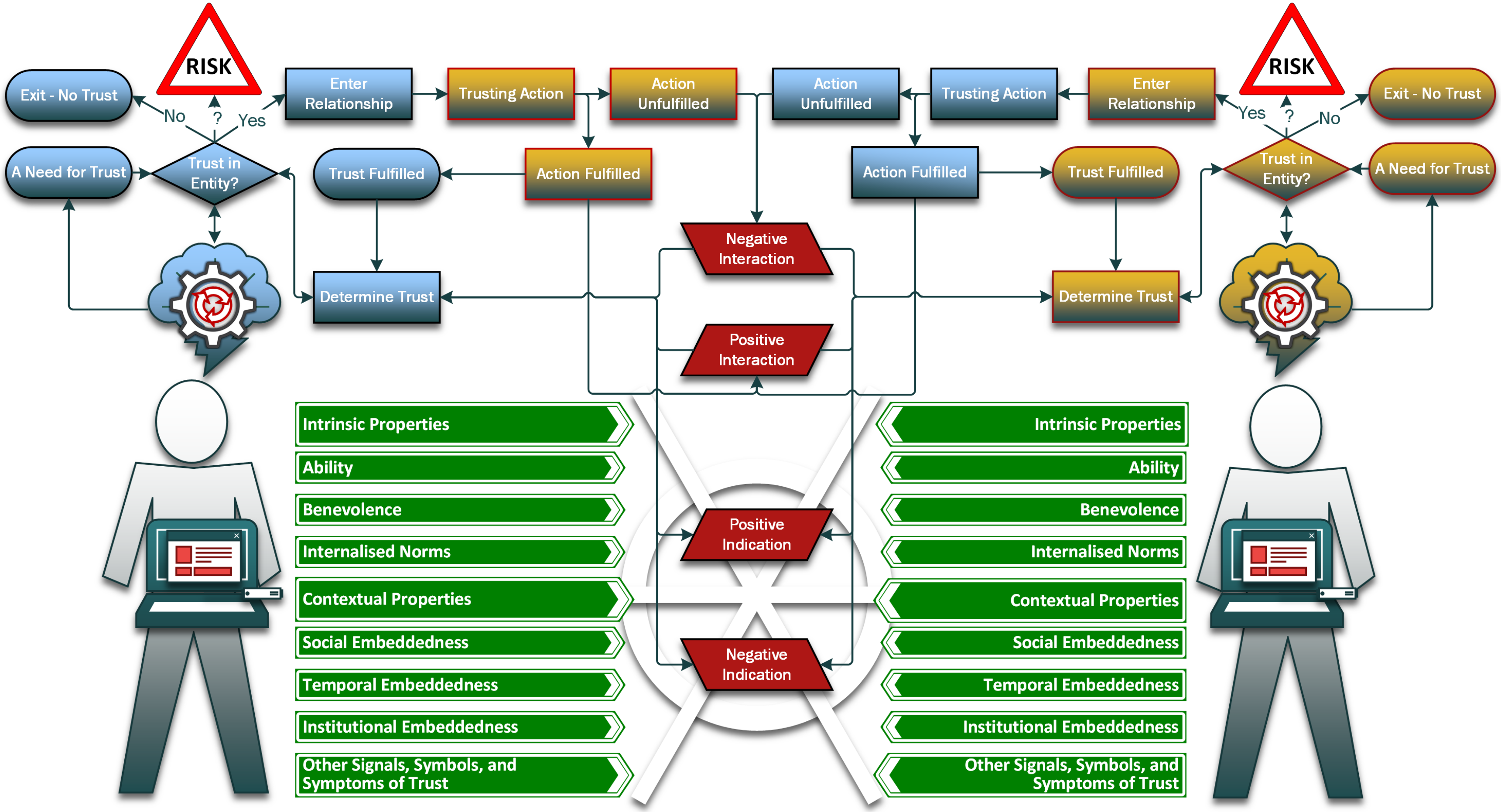


Fig. 2.3 Trustor and Trustee - Simple Two-Way Trust Equation, extended from Riegelsberger et al. (2005)

User interactions are also dependent upon machine-to-machine interactions outside of their control, for example, background services or networks working together in the process of sending and receiving data. However, it is likely humans-in-the-loop are dependent upon this trust and interaction, relying upon the output to be returned through the machine-to-human interaction, and that the trustum was as expected.

In this example alone, we can consider an overall trust relationship, with multiple sub-relations to fulfil individual interactions between trust relations. Descending from the top level, the trust relationship is formed between two organisations, who each have trust relationships with their accountable employees to carry out functions. These functions include human and machine trust-based interactions that are performed to send and receive data, which is itself trusted towards the data's integrity, availability, and confidentiality.

Across each of these trust levels, a trust relationship becomes a dependency relationship, but the level of determined trust is one measure, and level of dependency on the interaction is another. In this context, a level of trust may be similar to the level in which we determine how much an entity may be depended upon to fulfil as expected. Whereas, the level in which the relationship interaction is depended upon to achieve its goal is a separate measure. In both cases, an increase in dependencies could, however, contribute to the increase of security risks across the SoS. For example, where there are weaknesses towards the performance of the expected dependability, in particular, where issues go unidentified or communicated across less-centrally managed and controlled SoSs, and which could potentially have a knock-on effect towards the SoS achieving and maintaining its goals securely.

This would suggest that when considering risk and mitigations in a SoS context, based on trust assumptions with an expectation to achieve required goals, we must then consider what obstacles may cause this trust relationship to change. These changes could bring positive or negative effects towards the dependency, thus potentially increasing or decreasing risks if an interaction is not fulfilled as expected, e.g. when performing tasks and processes with assets, contributing to the satisfaction of goals – which other tasks and goals may also be dependent upon for their success, all of which contribute to the overarching SoS purpose and goal.

Different needs, expectations, and requirements make trust preservation difficult to achieve and maintain, yet easy to lose, adding challenges towards the criticality of the trust relationship and dependencies. There is a need to determine how the trusted entities are depended upon within each trust relationship. Each relationship can relate to different contexts, where some may be more likely to change and evolve, and dependencies may increase, or levels of trust may reduce. For example, a third-party may claim to have data security processes and controls in place, but lack of availability to data, perhaps as a result of an expired 'trust' certificate in vital communication services exposes the lack of controls in place to prevent the issue. Despite this, there is still a dependency for the goal of the trust relationship to be fulfilled, either continuing with the third-party, or withdrawing and interacting with another. In a SoS context, at an independent system level, this could be critical towards a SoS achieving its goals.

Actual trustworthiness within a trust relationship is established following one or more interactions between entities, whereas perceived trustworthiness may have been derived based on assumptions towards prior reputation or other trust signals. Trustworthiness is defined from the trustor and trustee perspectives as an objective quality governing the degree to which transactional obligations will be fulfilled in situations characterised by risk or uncertainty (Bailey et al. 2003).

Trustworthiness can also be considered in relation to the flow of information, the security and service provisions to protect systems and data used by supporting systems of the SoS (Richardson 2012). Trust assurance for data requires the data to be accurate, precise, available, and uncorrupted (Miller et al. 2010) and thus a dependency is created between the trustor and trustee to maintain this trustworthiness for continued interaction and risk reduction, despite the risk still being present.

As interactions increase, trustors are likely to develop an expectation that the trustee is reliable (Fléchais et al. 2005) if the trustum has been fulfilled as expected, and therefore the potential for security risks may be reduced where interactions would be considered 'trusted'. If the trustum has not been fulfilled as expected, this may lead to a quantified belief by a trustor that a trustee is incompetent, dishonest, not secure, or dependable (Grandison and Sloman 2003), and thus the potential for risk, impact, and required countermeasures and controls would be increased.

Distrust, therefore becomes a measure of the trustor's belief towards the unlikelihood that the trustee will fulfil as expected. This may be as a result of misplaced trust creating *Mistrust*, leading to *Untrust* that becomes a measure of how little the trustee is actually trusted (Marsh and Dibben 2005).

2.4 Towards Modelling System of Systems Security and Risk

Throughout the engineering and decision making processes, modelling is used at different stages to represent system and human elements for different purposes related to the context in which modelling is used. This may include the design of a system, its data flows, and activities related to required interactions. To support the modelling process, it is necessary to identify what the systems does, its purpose, mission and goals, and to explore the interactions of different decisions in a security context.

Capturing the design of systems and interactions through the use of models can help decision makers to reflect upon the system's social-technical characteristics, and are effective instruments to reason about the integration of people with systems and software, whilst accounting for multiple stakeholder needs, costs, and risks (Al-hajHassan et al. 2016, Salvaneschi 2016). However, it can also be time-consuming and expensive to maintain model consistency as changes are made to the systems' architecture or interactions (Sommerville 2015). A particular challenge in the SoS context is a potential for limitations within the communication flow capturing all changes to the SoS. Despite this challenge, ongoing monitoring by independent systems should at very least aim to account for areas of change towards risk equations to support the necessary risk-based decision making for the SoS.

Design principles, heuristics, best practices, and patterns are all similar terms for the idea that soft rules correlated with success can be inducted from observing system development (Maier 1996). Models can be a descriptive abstraction of reality, representing the decomposition of systems, sub-systems, and their inter-relationships, inputs and outputs, functions, and performance indicators. However, given the complexities of SoSs, as the models and their elements of the decomposed SoS increases, it may become impossible to understand all elements of the SoS and related risk in its entirety, indicating the unlikelihood of single model successfully capturing the multiple dimensions and perspectives of a SoS (De Bruijn and Herder 2009, Haimes 2017).

2.4.1 Modelling for SoSRE

The scale, complexities and challenges presented by SoSs require us to go beyond traditional RE approaches (Ncube et al. 2013). When modelling systems and SoSs, a combination of top-down and bottom-up processes can be used within SoSRE, but would require modelling of goals in the system and SoS context (AlhajHassan et al. 2016). Using reductionism in the SoS context as a form of decomposition is challenged due to the inherent complexity of SoSs. Reductionism assumes clear system boundaries, rational decision making, and well-defined problems, whereas in the SoS context, these assumptions do not always align to the context (Sommerville 2015). Moreover, researchers in software engineering generally adopt this reductionist assumption, but for large-scale complex systems, these assumptions are never true and can attribute to failures (Sommerville et al. 2012).

Nevertheless, model decomposition is a natural approach to systems analysis and design, therefore, acknowledging the strengths and limitations of using the approach is important when decomposing the SoS. Incorporating the concept of abstraction stacks within the process of decomposing the SoS provides a simple means towards modelling different levels of abstraction of the SoS (Simpson and Dagli 2008). For example, a decomposition may involve different levels of abstraction to define the SoS and its independent systems and associations, decomposed into associated sub-systems. This should factor-in their security features and services that are meaningful, e.g. addressing accountability, non-repudiation, or authentication (Bodeau 1994). This could be applied to the concepts of asset, goals, task, and process modelling, where security and risk-related elements can be incorporated during different parts of the modelling processes.

When modelling security aspects in particular, there is already a call for better models visualising how various people approach a security task, their mental models, or security-related skills and knowledge. Current informal and implicit models that aim to capture the human element are not always robust enough, or rarely focus on how people make security decisions (Shostack 2014). Therefore, when modelling security and human elements, the supporting risk assessment inputs and outputs must assist the process of risk-based decision making to help make more informed decisions to mitigate risk in the SoS.

However, in the SoS context, given there are likely to be a range of stakeholders with different needs or expertise, and systems with varying degrees of coupling, the data gathering, modelling, and communication of model aspects can be a challenge. Some current methods for modelling security in a single system context are said to fall short for the average user, as some may require special coding practices or require significant training and interaction with the modelling tool. Moreover, given the small community of security engineers and researchers, there appears little motivation for creating tools (Ardi et al. 2007). This challenge therefore extends into the field of SoSRE that is still relatively unexplored towards security.

UML Modelling Approaches

Standard design and engineering approaches usually incorporate various types of UML models or Class diagrams to represent elements such as assets, systems, structures, or software functions. Capturing the SoS structure and related associations under consideration would be useful towards aligning with the assessment of security risk, but should also align with other concepts and models. Use cases and descriptions are also useful for capturing related actors interacting with elements of a systems, thus indicating the process for interaction with specified functions and dependencies of the systems.

Other typical modelling techniques or languages include the Systems Modeling Language (SysML) based on UML that is a graphical modelling language for analysing and specifying the design, verification and validation of complex systems, and can be tailored to support SoS capability engineering, and cost estimation (Lane and Bohn 2013, Lane and Epstein 2013, Friedenthal et al. 2014). Aligning with SysML, CML is language specifically designed for modelling and reasoning about system interactions and the architecture needed for composing them into a SoS (Woodcock et al. 2012).

Some approaches have also been extended to factor security within its process. For example, SysML-Sec supports the assessment towards the impact of security through a three-phase approach of system analysis, software design, and system verification and validation from safety and security perspectives (Apvrille and Roudier 2013, Roudier and Apvrille 2015). UMLSec or SecureUML are also used at the design stage, although are both used in differing ways to model security risks and access control (Matulevičius and Dumas 2010, Chowdhury 2014). SecureUML could be applied for security risk management, although some limitations of modelling security risk using SecureUML were found (Chowdhury 2014). Moreover, Secure Tropos extends the i* and Tropos approaches and can be used to model stakeholders, along with risk-related concepts towards the system and social goals (Mouratidis 2011).

Security and Threat Modelling Modelling

Security modelling should bring together techniques used for identifying threats, vulnerabilities and countermeasures to prevent security problems early in development (Baadshaug et al. 2010). To provide assurance that countermeasures are applied to target vulnerabilities correctly, a full understanding is required towards areas of weakness, threats, and behaviours of attackers against the software and SoI (Ardi et al. 2007).

There are a number of approaches with a particular focus towards threats. This could incorporate the internet threat model described in RFC 3552 (Rescorla and Korver 2003), or security and privacy considerations from RFC 6973 as another means supporting threat modelling by describing threat areas for consideration against protecting from vulnerabilities (Cooper et al. 2013). Determining threats, potential areas of weakness, and modelling of such instances may incorporate threat models such as OWASP Top Ten, Trike, DREAD, or STRIDE (OWASP 2017). STRIDE can also be aligned with Data Flow diagrams (DFDs) to identify areas of concern towards information assets and their related information flows (Shostack 2014).

However, where OWASP provides focused considerations towards application security, and STRIDE is useful for capturing perhaps more cyber perspectives through its threat model approach, neither really account for other human or environmental threats and vulnerabilities that may be associated both from a wider information security perspective, and a SoS context, for example, as introduced within OA.

Obstacle and Goal Modelling

Architectural and contextualised attack patterns can assist architectural risk analysis (Faily et al. 2012), or fault tree analysis is another useful technique (Aitken et al. 2011). The use of Attack Trees is another common approach (Moore et al. 2001), and Obstacle modelling can be used in a similar way. As a consequence of security threats or vulnerabilities under consideration in a SoSRE process, obstructions may occur towards a goal being achieved resulting from the affected performance of a task and its related processes. Obstacles can be introduced into the KAOS Goal modelling approach to anticipate exceptional behaviours in order to identify realistic goals, requirements, and assumptions towards the satisfaction of goals (Van Lamsweerde and Letier 2000). In a SoS context, modelling of SoS goals and their obstacles with KAOS would play a central role aligning with risks towards security and human factor concerns of the SoS, and would therefore be a chosen approach for application within the research contribution.

The KAOS approach considers what a system needs in order to achieve each goal, and includes different model elements such as a Responsibility model indicating goal related responsibilities. Goals and their descriptive elements used within KAOS are considered to be a prescriptive statement of intent that a system must satisfy (Van Lamsweerde 2009). These may be refined using leaf goals with AND/OR relationships to support the satisfaction of the root goal being achieved, and provide alternative methods to achieve the goal where applicable.

This concept would align with the high-level goal refinement in a SoS context, where independent systems interoperate to achieve the SoS goals. Sub-goals support the satisfaction of root goals and could operationalise processes, supporting the completion of tasks operationalised by the goal and their associated roles, related to activities performed by human users. Moreover, using this approach may be more straight-forward towards capturing system goals in a SoS context, providing more flexibility by comparison to i* and Tropos-based approaches.

Taking a different approach to KAOS, the Goal-oriented Requirement Language (GRL) models may be effective towards considering interoperability between systems to examine the impact of changing system assets, goals, or user processes (Faily and Fléchais 2014) or towards conflicting security and regulatory requirements (Ghanavati et al. 2014). GRL takes a similar approach to that of the i* and Tropos approaches that implements a Strategic Rationale model mapping organisational relationships, and a Strategic Dependency model. The processes applied for social goal modelling are versatile, and useful for capturing the social rationale for requirements. However, the modelling notation can appear complex, and large models can be difficult to scale (Moody et al. 2010, Maiden et al. 2011), which may become a challenge when modelling a SoS where scale and complexity is inevitable. Another RE approach for modelling and specifying goals implements anti-goals and anti-requirements similar to that of use and misuse cases (Van Lamsweerde et al. 2003), although this approach is likely to require further research and testing before being considered for use with SoSs security and risk.

Modelling Responsibilities and Dependencies

Modelling responsibilities and dependencies between systems, roles, and people is not a new concept, but my be applied differently using different approaches. Responsibility models can be used dynamically to represent evolving socio-technical scenarios and the interaction between humans and machines, highlighting areas of mitigation towards risk, whilst providing support for the analysis of potential process change (Lock et al. 2010).

A common point of reference is within the Tropos approach that adopts the i* model and implements a Strategic Dependency model that relates to a Strategic Rationale model. These are used to support early requirements analysis (Giorgini et al. 2004), and are to some degree adopted within the GRL approach to goal modelling (Amyot et al. 2009).

When modelling dependencies, the basic premise is that You as the *Depender* depends upon Me the *Dependee* for something, the *Dependum*. For goal modelling, the dependum may be to achieve a goal or sub-goal, or as i* and Tropos begins to explore, dependencies towards tasks being performed and the availability or creation of related resources.

Goals may be used to capture the dependencies and rationale relationships between system ‘hard’ goals, and human ‘soft’ goals, where soft goals may also be captured and analysed by other means. Modelling in a systems or software context, non-functional requirements (NFR) including security considerations are often represented as soft goals. These can be described as goals where there is possible ambiguity in its description, without a clear measure of satisfaction to achieve the goal or not, whereas a goal is quantifiable and more concrete (Amyot et al. 2009).

Although, in a security context, it could be argued that a goal to achieve a security need is likely to be considered a hard goal, something that needs to be achieved for the system to function as required. For example, where a user may access online banking, and some form of authorisation and authentication mechanism is required in order to provide access to the user.

The KAOS Goal and Responsibility modelling approach integrates this concept which is slightly different to GRL, and takes a different direction to i* and Tropos by implementing a Responsibility model, generated from its other models that support goals, objects, and operations (Lapouchnian 2005). Root or main goals can be supported by leaf or sub-goals where they could be applied as functional or NFR, and may concern resources, e.g assets.

It is also possible to represent a risk-based obstruction towards goals being achieved with Obstacles, which are not explicitly defined in i* and Tropos, but are useful towards expressing where security risks may impact upon tasks and goal completion and related dependencies. However, by comparison to i* that considers actors as agents, roles, and positions within its dependency model linking to the rationale model, the KAOS Responsibility model does not directly show the relationships between all actors' dependencies in the same way (Werneck et al. 2009).

When modelling these dependencies in a SoS context, it would be useful to draw upon the benefits of these approaches and further consider the SoS relationships and dependencies, making clear who is accountable. This would relate to the owner and subsequent authorities, e.g of an asset or the goal, where there is delegated authority to a role, e.g to achieve a goal, and therefore a chain of accountability for its operation and control, for which the SoS as a whole is dependent upon. This could potentially be adapted within the KAOS Responsibility model, with elements that considers where accountability at each level resides, e.g. between an owner and delegated role, thus highlighting other dependencies in addition to the currently captured elements, specifically where there is a risk to assets associated to other assets used in tasks and processes to achieve a goal.

Although Sommerville (2007b) goes some way towards drawing a degree of accountability with the causal and consequential responsibility model elements and notation, greater dependencies are not clear. The i*, Tropos, and GRL approaches also have slightly different notation related to the links between dependencies, which again is different to KAOS Goal modelling. When integrating models, this may become confusing if different independent systems' stakeholders of a SoS are familiar with one approach over another, which may again be different to other approaches e.g. UML. For example, in each of these cases, arrow head types may have a meaning, but are not consistent across approaches.

Consistency in models would therefore be desirable, but should aim to reduce cognitive load, certainly if there is an expectation to share these models with non-technical stakeholders as part of RBDM. Models should capture and clearly illustrate each of the dependencies reliant upon the input or output by each accountable entity to achieve the task or goal, or specifically in the context of security, achieve and maintain risk reduction towards the SoS interaction.

2.4.2 Integrating Tool-support

It is evident there are a number of approaches to modelling with different types of models, each capturing different elements of systems. Given that these are usually used in a single system context, combining models is already a challenge as tools may be limited, or multiple model generating tools may need to be used in parallel. Sharing modelling results with others can contribute to greater awareness of security issues, but models must be illustrated in such a way that they can be understood.

A current tool often used for a variety or purposes is Microsoft Visio that offers a range of flowcharts, diagrams and model types for graphical illustration (Microsoft 2017). However, for some users it was found tools such as Rational Rose and Poseidon could take 60% less time to create a security model compared to modelling with Visio (Baadshaug et al. 2010). Visual Paradigm (Visual Paradigm 2017) also offers a range of flowcharts, but is a slightly more powerful tool, with some model alignment, although understanding different model elements can become complicated.

There are a range of other off-the-shelf tools available, but some may have more of a HCD focus, or others may specifically focus on systems threats, but not model its goals. The GRL approach to goal modelling is also tool-supported with jUCMNav

(Amyot et al. 2009), but doesn't combine other elements to capture security and risk holistically to consider the tasks, processes, and asset interactions. The CORAS method does, however, provide risk analysis as a model-driven approach using a computerised tool designed to support documenting, maintaining and reporting security analysis, using UML based threat and risk modelling to capture and model relevant information (Lund et al. 2010, Stølen and Solhaug 2015).

Many of these approaches offer value in their specific areas, but do not align directly with other model types and concepts.To enhance security during development, good tool-support is required that can integrate with other current development tools or be used by other stakeholders (Meland and Jensen 2008). Moreover, as security modelling usually incorporates a variety of general purpose drawing tools, standardised modelling methods and tools with data repositories would be greatly beneficial towards the production of security related models (Ardi et al. 2007), and potentially increase the efficiency of producing and updating integrated models.

However, there appears limited tool-support integrating some of these different modelling elements specifically with a focus towards security and human factors to visualise and assess the interactions and consequences of risk in greater detail. Identifying the combinations of model elements to suitably visualise these concerns would be useful for illustrating systems design and security risks related to the independent and interdependent socio-technical system interactions of a SoS.

The open-source Computer Aided Integration of Requirements and Information Security (CAIRIS) requirements management tool (Faily 2018a) does attempt to address and integrate a number of these important elements and models. CAIRIS and its automatic analysis and visualisation capabilities can assist when modelling the socio-technical interaction of the SoS and the usability, security, and requirements engineering activities (Faily et al. 2012, Faily and Iacob 2017). This provides a current view on security risks and associated assets, roles, goals, tasks, and other security and usability concepts, thus providing an ideal combination of model opportunities in which to explore.

In addition to CAIRIS already integrating a number of useful elements and tools helpful towards assessing security risk, a further motivation for using this type of a tool considers the benefits of CAIRIS being an open-source tool, which could enable a potential for further development. The tool is also in constant development, meaning new features and enhancements continue to be implemented, thus adding to its value of an integrated tool. CAIRIS could, potentially incorporate SoS specific modifications to the tool, further aligning towards a tool-supported framework for security risk assessment in the SoS context. CAIRIS was, therefore, adopted for application within a research contribution towards integrating concepts, models, and techniques for assessing and modelling information security risk and human factors concerns with tool-support.

CAIRIS and IRIS

Many of these security requirements engineering and human factors ingredients necessary for SoS analysis have been incorporated into the IRIS framework (Faily 2018b). The IRIS framework was created to illustrate how design concepts and techniques in Security, Usability, and Requirements Engineering can be integrated when devising processes for designing usable and secure software.

IRIS is underpinned by a meta-model stipulating the conceptual alignment between these areas of engineering, and are supported by the CAIRIS platform (Faily 2018a), which implements this meta-model. Because CAIRIS uses a relational database to implement the IRIS meta-model, we can reason about CAIRIS models to highlight areas of potential concern. For example, related work (Coles et al. 2018) implemented validation checks of privacy elements, where goals can be related to the processing of personal data.

The different IRIS model elements provide aligned perspectives of a secure system's context of use, many of which are specific to the modelled environment. The IRIS concepts captured within the environment meta-model are illustrated in Figure 2.4. An *environment* is used to represent the context of use for the physical, social, or cultural environs within which the system is situated. This may include goals, or tasks, and related roles and dependencies that may affect the satisfaction of goals.

The use of environments could be particularly useful towards capturing the view of independent systems of the SoS. Each environment or view, would therefore capture the direct interactions of systems with other systems, that combined would account for the SoS to be modelled using selected concepts of the IRIS meta-model. Separate environments can be used to represent a view from specific independent

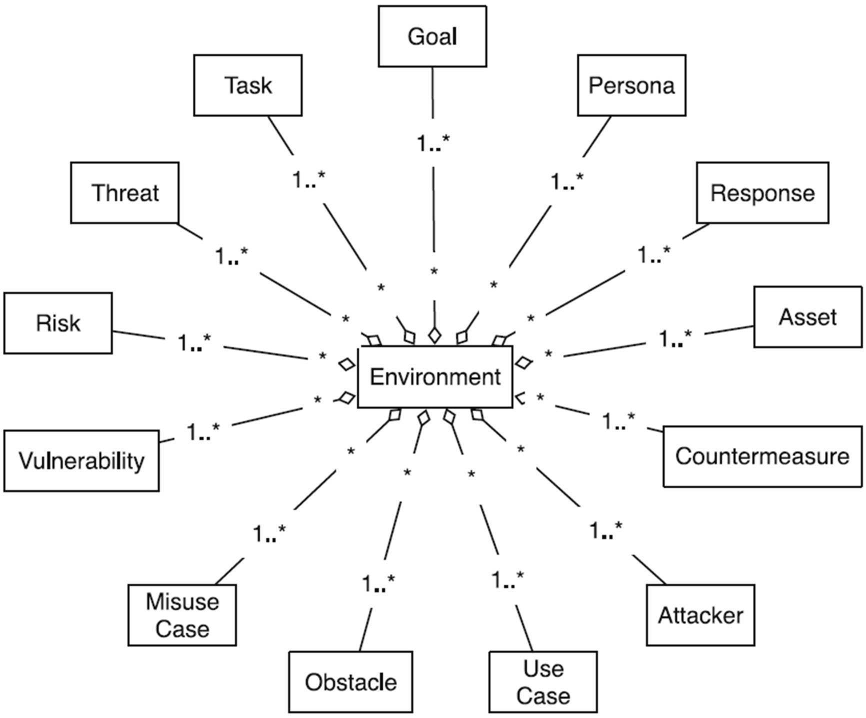


Fig. 2.4 IRIS Environment Meta-model (Faily 2018b)

system of the SoS to capture the contexts of use within which a system specification needs to be situated for. This would be favoured over the box within a box approach to modelling or swimlanes, given there could be many boxes or swimlanes to account for representing different levels and views of the SoS and for each model type.

To address the bounded rationality (Simon 1979) problems that occur that make creating, managing and visualising SoS models difficult due to its size and complexity, CAIRIS can automatically generate several types of system models. These are based on requirements, security, and usability model elements. CAIRIS also has the flexibility to facilitate collaboration between different types of systems stakeholder to explore the impact of a threat on different systems, while its API can be used to facilitate integration with complementary tools.

2.5 Chapter Summary

There is a continuing need for the SoSRE community to grow and understand the discipline and approaches required to engineer SoSs, whilst accounting for their constraints on geographical, environmental, evolutionary and emergent behaviour, risks, human interaction and culture that add to SoSs complexities. Moreover, a gap is evident towards a formal process to support a security risk assessment for defining and characterising a SoS. In particular, where the distinction between types of SoSs' authority and control is not always clear, leading to ambiguity towards how a SoS may be represented and its security concerns assessed.

Although there are many differing approaches to risk and how it may be managed and assessed, there has been little research focusing on Information Security risk assessment in SoSs that combines modelling and visualisation of related interactions using tool-support to integrate different models, concepts, and techniques within analysis. Different approaches and models elements may be considered towards assessing security risk in a SoS context, capturing the stakeholder needs, goals, activities, assets, ownership and accountability, multiple responsibilities, human factors and perspectives of a SoS to assess the interactions and consequences of risk in greater detail.

Security modelling should bring together techniques used for identifying threats, vulnerabilities and countermeasures to prevent security problems early in development, whilst accounting for human factors to reduce unwarranted assumptions or pre-conceptions about the activities applicable to the system design, yet there is no clear guidance provided to inform how they may be integrated towards a SoS context. Therefore, the identification and testing of suitable approaches would be a useful research contribution to support an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE.

Chapter 3

Research Methodology

In this Chapter, a range of research methods were considered that could be adopted to address the RQs detailed in Section 1.2. The chosen methods for the research strategy applicable to the research context are indicated, with examples of how methods would be applied to achieve elements of the research contributing to the thesis.

3.1 Research Methods

A paradigm can be considered as relating to the concepts of ontology, epistemology, and methodology with related methods that presents a worldview providing differing assumptions of reality and knowledge underpinning the related research approach (Scotland 2012). A methodology can be considered as to provide a combination of research design methods, approaches, processes and procedures used in an investigation that is well planned to find out something (Keeves 1997).

Paradigms are often regarded as being philosophical in nature, and may, for example, align towards positivism, constructivism, realism, and pragmatism, each taking a different stance towards the research focus (Maxwell 2012). For example, the positivist ontology and epistemology aims to discover absolute knowledge or truth about an objective reality, although the subsequent generalisations may not be fully understood as they do not take into account the intentionality of human-centred activity (Scotland 2012). The post-positivist paradigm may instead provide a worldview more suited towards research than considers human behaviour, as post-positivism accepts that reality is imperfect and that truth is not absolute, but probable (Kivunja and Kuyini 2017).

Other approaches that take a more qualitative role may include interpretivsim, critical theory, post-modernism, and phenomenology, providing further options towards combining well developed methods within a research approach (Maxwell 2012). However, interpretivism rejects the positivism approach by arguing that the effects of human behaviour are intrinsically aligned with the environment in which they are in, and the associated subjective perceptions about the environmental conditions (Willis et al. 2007). Therefore, when research has a focus towards information system and human interaction, capturing these elements becomes critical for the researcher. The interpretive paradigm does not question ideologies; it accepts them, whilst focusing upon the interactions that are culturally derived and historically situated, striving for legitimacy and trustworthiness of the research without claiming uncontested certainty (Scotland 2012).

Research design methods are constructed, combined, and applied in different ways, but should be relevant to the scientific demands for a given domain, e.g. where a broad or deep and narrow focus may be required through quantitative and qualitative approaches. Quantitative research methods usually involve a quantity of statistics from counting, measuring, and analysing a range of data inputs, such as surveys and questionnaires. These may also take a positivism approach where assumptions towards objective measurements may be made from observations and fact-based analysis (Hennink et al. 2010). Whereas, qualitative research approaches are considered descriptive, inferential, investigative, and evidence-based (Gillham 2000). Qualitative approaches seek to embrace and understand the contextual influences taking an interpretative approach, where the researcher must be open and empathic with a curiosity for discovery and understanding (Hennink et al. 2010).

When undertaking qualitative research, there is a need for researchers to set aside their own perspectives, beliefs, and unwarranted assumptions of a problem domain. There is a tendency for researchers to identify with aspects of human activity to appreciate different perspectives, behaviours, and cultural needs of users and stakeholders, whilst gathering and analysing related data to make research decisions (Taylor et al. 2015). An exception and addition to this may be where a researcher introduces personal reflexivity to consider how their personal background and experience may influence the elements of the research and findings (Hennink et al. 2010).

Another method of integration may take an inductive approach that can be used in a qualitative way with consecutive research findings, leading to inductive inferences towards a deeper understanding of the domain. Alternatively, a deductive approach can be used with quantitative research methods, relying on existing literature and theory to deduce a conceptual framework for data collection (Hennink et al. 2010).

Action research could be used to provide focused observation towards a specific agenda, with a reflective period evaluating multiple inputs aiming to achieve a specified output. It provides a theory and practical knowledge contributing to a more equitable and sustainable impact towards the ecological context of society through observation, reflection, and intervention (Ivankova 2014). It is a systematic investigative approach enabling discovery of effective solutions to every day problems (Stringer 2013).

Where specified research questions have a focus towards information systems and the environments in which they are situated in, applying a case study approach provides a useful means to capture the organisational context and knowledge of practitioners, then developing theories from it. This enables the researcher to examine "how" and "why" questions to unravel the complexity of the questions posed (Benbasat et al. 1987).

As case studies are implemented, the long-term value of a study, its processes, and findings would need to be considered. The quality of case studies possess certain characteristics that are desired. For example, these would relate to the trustworthiness, credibility, confirmability, and data dependability of a study that can be tested in four areas to determine validity and reliability of a case study (Yin 2013). A case study approach can help generate a more holistic representation of a particular problem domain, allowing for generalisations of findings that can be enhanced by use of replication with multiple case studies to improve the accuracy, validity, and reliability of results (Noor 2008).

These can be supported by interviews, observations, focus groups. Focus groups can be useful to gain different perspectives, whilst maximising stakeholders' time and availability, sometimes in addition to supporting fact-finding or validation interviews, or as an alternative. However, based on other research activities, it is acknowledged that identifying and securing candidate organisations for projects as case studies providing interviews, observations, focus groups or other data gathering for modelling and analysis is difficult. This seems more apparent when the topic is security and risk related, even with basic research requests.

This has a direct impact when applying certain methodological approaches, but can still be addressed by using exemplars or case studies, or other means of data capture and analysis to reduce participant interaction time and resource requirements. Furthermore, where interviews are undertaken, within the bounds of research ethics, it is common for research data to apply anonymisation to remove the identities of the interviewees to provide a level of confidentiality, whilst affording the ability to share and publish research analysis and findings. Researchers should, however, adopt oversight to maintain the verifiability of the data, and ensure ethical requirements are adhered to.

Nevertheless, semi-structured interviews can be used with pre-prepared simple and open questions, prompting responses of concrete descriptions of the respondent's knowledge and experiences (Given 2008). Semi-structured interviews can be applied and tailored to the context of the expertise, but also allows the interviewees the freedom to limit or elaborate upon the content being discussed. Where two or more interviews use consistent questions, triangulation of analysis of data can be applied to compare and contrast between the given answers to help strengthen the validity of the findings (Griffee 2005).

Grounded theory is considered as another qualitative approach used to systematically analyse data, forming a theory from its output. The concept is often linked back to the work of Glaser et al. (1968), although most common day approaches follow a more updated version (Corbin and Strauss 2008). Grounded theory can be described as a process of two steps forward, one back through data analysis (Glaser 1978).

The specific aim of grounded theory is to investigate the real world, discovering concepts grounded in the data and uses the derived concepts to build theory around the data in context (Allan 2003). It is an analytical process using coding strategies, splitting data into distinct units of meaning, clustered into interrelated descriptive concept categories (Goulding 2002), which can then be analysed and modelled to support research findings. Persona Cases based on grounded theory is a method of data analysis that can, for example, be applied to analyse interview transcripts and factoids represented in affinity diagrams, and lead to new insights of users, behaviours, and their environments (Faily 2018b).

Findings of research may also inform the design and prototyping of certain research outputs. Prototypes act as a means of inquiring into a context of use through experimentation to generate research data and conceptual arguments for reflection towards the design (Wensveen and Matthews 2015). McElroy (2016) considers prototyping to be a manifestation of an idea into a format that communicates the idea to others or is tested with users, with an intention to improve over time, and is therefore useful for stakeholder decision making. The use of prototyping can provide a generative and balanced structure, that can potentially save time, effort, and money whilst reducing risk by identifying problems early in the process and throughout the development life-cycle (Warfel 2009).

Effective prototyping is demonstrated through repeatable processes with a range of prototyping methods available to elevate the creation of systems and software being designed with tangible representations of the design interactions. Examples of prototyping can include card sorting, wireframes, storyboards, paper or digital prototypes, and others (Arnowitz et al. 2010).

3.2 Application of Adopted Methods

Because the scope of the research project is part agenda-driven with a multi-disciplinary crossover between the different elements contributing to its subject area, the research strategy chosen to address the research problem applies a selection of methods in combination with design, engineering, security, risk, and human factors techniques. From the methods introduced in Section 3.1, a qualitative research approach has predominately been applied as a main research methodology.

This further applies mixed-methods for exploration and discovery in a SoS context, incorporating examples of SoSs and case studies for the purpose of combining, applying, and validating the research contributions. Kumar (2019) argues that combining or mixing different methods within a research approach can take advantage of strengths from different paradigms to enhance the accuracy, validity, and reliability of findings towards the theory and application of the related research (Kumar 2019).

Figure 3.1 illustrates how each of the selected methods and approaches were combined and applied in research presented throughout related chapters, whilst demonstrating their relation towards addressing each of the RQs. Each research method or approach was chosen for use to address parts of a particular RQ, or combination of RQs. For example, the focus of RQ1 was to consider "*What SoSs factors contribute to challenges of security risk assessment of SoSs*". A review of literature suggested there was a common theme in SoSs whereby the notions of decentralised control, different owners, conflicting requirements, and a dependability upon interoperability are critical. To explore these notions further, a literature-based SoS example would be constructed, supported by interviews and a focus group to help test and validate theories with related stakeholders, helping to address the RQ, whilst informing other RQs towards a clearer understanding of the SoS context required to support the security risk assessment process.

As indicated in Figure 3.1, the output related to RQs would lead to a SoS characterisation process in Chapter 4, providing context to support the information security risk assessment process. Other SoS security, risk, and human factor considerations and challenges would be identified whilst addressing RQs 2 and 3 in Chapter 5. Together, these outputs from exploring RQs provided a focus and foundations towards the three contributions of OASoSIS for addressing the research gaps discussed in Chapter 6. OASoSIS blends a component-driven and system-driven SoS assessment for information security risk capturing related human factors concerns, aligned with a SoS goal-driven modelling approach applied with tool-support from CAIRIS.

3.2.1 An Inductive and Deductive approach

A combined inductive and deductive approach would be applied towards process design, testing, and validation of an approach, and its suitability towards assessing information security risks and associated human factors in a SoS, and which integrates tool-support for modelling and visualising risks in the SoS. Considering different examples of SoSs would help to provide a view of who the different owners are, who controls what, and what these challenges and impacts may actually look like, thus informing other RQs and thesis contributions.

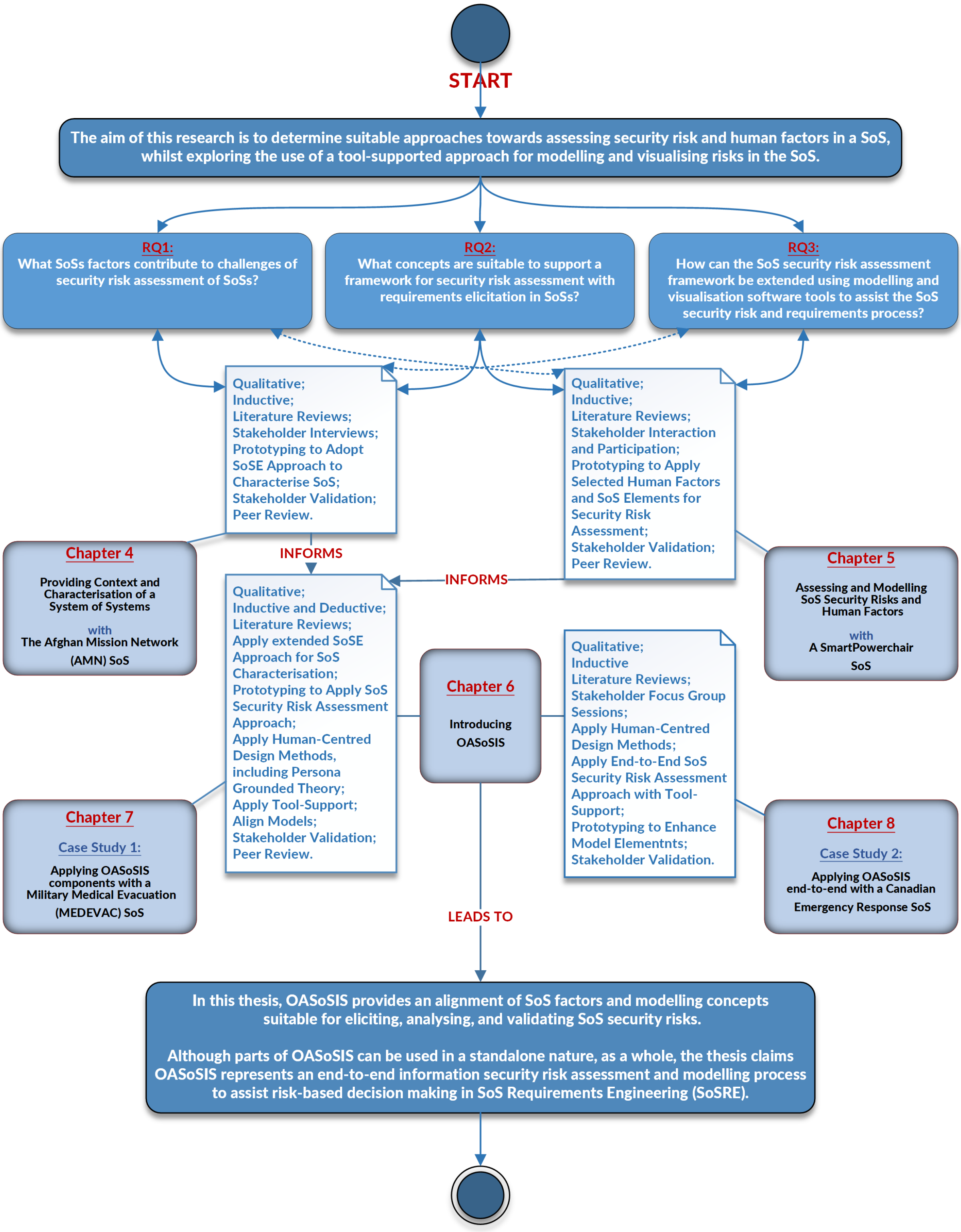

START
The aim of this research is to determine suitable approaches towards assessing security risk and human factors in a SoS, whilst exploring the use of a tool-supported approach for modelling and visualising risks in the SoS.
RQ1:
What SoSs factors contribute to challenges of security risk assessment of SoSs?
RQ2:
What concepts are suitable to support a framework for security risk assessment with requirements elicitation in SoSs?
RQ3:
How can the SoS security risk assessment framework be extended using modelling and visualisation software tools to assist the SoS security risk and requirements process?
Qualitative; Inductive; Literature Reviews; Stakeholder Interviews; Prototyping to Adopt SoSE Approach to Characterise SoS; Stakeholder Validation; Peer Review.
Qualitative; Inductive; Literature Reviews; Stakeholder Interaction and Participation; Prototyping to Apply Selected Human Factors and SoS Elements for Security Risk Assessment; Stakeholder Validation; Peer Review.
Chapter 4
Providing Context and Characterisation of a System of Systems
with
The Afghan Mission Network (AMN) SoS
INFORMS
INFORMS
Chapter 5
Assessing and Modelling SoS Security Risks and Human Factors
with
A SmartPowerchair SoS
Qualitative; Inductive and Deductive; Literature Reviews; Apply extended SoSE Approach for SoS Characterisation; Prototyping to Apply SoS Security Risk Assessment Approach; Apply Human-Centred Design Methods, including Persona Grounded Theory; Apply Tool-Support; Align Models; Stakeholder Validation; Peer Review.
Chapter 6
Introducing OASoSIS
Qualitative; Inductive Literature Reviews; Stakeholder Focus Group Sessions; Apply Human-Centred Design Methods; Apply End-to-End SoS Security Risk Assessment Approach with Tool-Support; Prototyping to Enhance Model Elementnts; Stakeholder Validation.
Chapter 7
Case Study 1:
Applying OASoSIS components with a Military Medical Evacuation (MEDEVAC) SoS
Chapter 8
Case Study 2:
Applying OASoSIS end-to-end with a Canadian Emergency Response SoS
LEADS TO
In this thesis, OASoSIS provides an alignment of SoS factors and modelling concepts suitable for eliciting, analysing, and validating SoS security risks.
Although parts of OASoSIS can be used in a standalone nature, as a whole, the thesis claims OASoSIS represents an end-to-end information security risk assessment and modelling process to assist risk-based decision making in SoS Requirements Engineering (SoSRE).

Fig. 3.1 Combining Research Design Methods

For example, informed by inductive research and the SoS examples in Chapters 4 and 5, a shift to deductive research would be used to identify a suitable process for assessing risk in the SoS context. After prototyping an approach for assessing SoS information security risk, inductive research then continues in later Chapters with more interviews and focus group activities with two case studies to apply, test, and validate the approach. These activities apply elements of interpretive design, taking a model-driven approach in a SoS context with the use of tool-support to assist the research process of assessing SoS information security risk and related human factors for RBDM and SoSRE.

3.2.2 SoS Examples and Cases studies

Each of the SoS examples that were implemented in Chapters 4 and 5 were applied to help explore the problem domain, leading to the testing, validation, and formalisation of the OASoSIS framework. The three contributions of OASoSIS would be applied using *Case Study 1* in Chapter 7, including the processes for SoS characterisation and context, an information security risk assessment aligned towards a SoS, integrated with other concepts, models, and techniques, then re-applied as an end-to-end process in *Case Study 2* in Chapter 8.

Supported by stakeholder feedback and validation, the case studies and example SoSs were the main supporting methods applied, along with other largely qualitative methods as a structured approach to address RQs, and to explore the different perspectives, inputs, outputs, and activities related to the problem domain, specifically towards assessing and modelling information security risks and their related human factors concerns in a SoS. A potential for using action research was considered for *Case Study 2*, but would not be applied in full due to changes in the on-going availability of the original stakeholders.

3.2.3 Interviews and Focus Groups

Supporting literature reviews and document analysis, followed by verbal or electronic communications with relevant stakeholders would be used to ground the theory based on the empirical study, whilst gaining expert feedback and validation through interviews and focus groups. Semi-structured interviews and focus groups would be used to place the SoSs under consideration into context with stakeholders and other experts, and to provide stakeholder validation towards the adopted approach and elements within it, as applied in the case studies and example SoSs. Semi-structured interviews as a qualitative method was chosen to allow for an initial set of interview questions to be applied, but still afford the flexibility to explore answers in different ways. For example, stakeholders from a variety of roles and sectors would provide different expertise and input in relation to a particular context, but specifically related to their area of expertise, thus covering different topics or aspects.

It is, however, acknowledged that a challenge to the research community is where interview candidates are difficult to secure in a SoS context and towards security and risk, where even when conducted, many decline an audio recording of the interview, which instead relies upon hand-written note taking. Some instead prefer an informal short discussion to provide context towards specific scenarios or environments without giving specific detail. At times, there is a reluctance or resistance towards giving access to a company and its potentially private or confidential information, internal processes, some of which may warrant security clearances in order to access or observe, in particular government, or military and defence. Nevertheless, for research-based projects, an amount of information captured must be publishable, and may therefore be duly limited by stakeholders, which presents challenges for research evolution adopted in real-world and organisational scenarios. This is a challenge for SoSs, certainly at a time where there is an industry appetite towards data and information security to defend and mitigate against the ongoing information and cyber security conundrum.

3.2.4 Prototyping

Prototyping would be used in differing scenarios, for example, for the SoS characterisation approach, or where SoS and HFSI elements are implemented into a suitable information security risk assessment process identified through a deductive approach. As the chosen information security risk assessment method, OCTAVE Allegro by Caralli et al. (2007), would then be modified and tested towards the SoS context and used in conjunction with tool-support.

Prototypes of model enhancements and model validation checks within the tool-support was a further option. One example, is where CAIRIS source code was modified to display a new symbol within certain models, e.g. the responsibility model, to represent accountable owners, similar to that representing a role of responsibility. The benefit of this enhancement also gained stakeholder validation, demonstrating its use towards risk-based decision making identifying the dependencies between those responsible, and accountable for the satisfaction of SoS goals, tasks, processes, associated assets, and the mitigation of related risks.

3.2.5 Grounded Theory and Personas

Grounded theory could be used to systematically analyse research data supported by literature reviews, interviews, and case studies forming a theory from its output. However, an element of grounded theory would be used when creating personas, representative of archetypical users identified as being central within the SoS examples and case studies. Data collection, coding and categorising of elements of data as factoids would be captured and grouped using an affinity diagramming process. Moreover, in one case study this was integrated with the Toulmin based argumentation model to support the validity of assumptions in persona models generated within the CAIRIS tool-support.

3.3 Chapter Summary

In this chapter, a number of approaches to research were considered and selected to align with the research project type and its multi-disciplinary nature. This research would aim to integrate a selection of methods in combination with design, engineering, security, risk, and human factors techniques applied within OASoSIS. Research methods were adopted to address the RQs detailed in Section 1.2, and applied to achieve elements of the research contributing to the thesis, as illustrated in Figure 3.1. A qualitative approach was predominately selected as a research methodology, incorporating example SoSs and case studies towards validating the research contributions and OASoSIS.

Methods applied would lead to the formulation of a SoS characterisation process providing context to support the information security risk assessment process in Chapter 4. SoS security, risk, and human factor considerations and challenges towards addressing RQs 2 and 3 are discussed in Chapter 5. The combined output of RQs would provide a focus towards the three contributions of OASoSIS for addressing the research gaps discussed in Chapter 6, blending a component-driven and system-driven SoS assessment for information security risks and related human factors concerns, and a SoS goal-driven modelling approach with tool-support from CAIRIS. This was applied, tested, and validated as presented in Chapters 7 and 8.

Chapter 4

A System of Systems Characterisation Process

Chapter 4 introduces a means for characterising a candidate set of independent systems as a type of SoS, to provide its specific SoS context and to identify where ownership, authority, and control of systems are in place for the SoS. Furthermore, from the context of the SoS scenario discussed, its SoS challenges and associated factors applicable towards a SoS information security risk assessment framework are considered. The application and findings based on the context of the scenario are presented to discuss each step applied towards addressing the research problem.

4.1 Motivation

Literature has shown that SoSs may be regarded as being complex, adaptive, large-scale, with different degrees of ownership and control, and have a potential for geographical constraints. However, it is not always clear in which context a system or systems become complex, or indeed whether it is attributed to the scale, or the number of system inter-connections used within the SoS. Moreover, as a result of the term being used inconsistently across audiences and creating ambiguity towards how a SoS may be represented, this emphasises a need for clarity when defining and characterising a SoS to align its context from a design, engineering, or security viewpoint.

Where it is now becoming common for socio-technical system evolution to combine systems in different ways, and which at times creates dynamic cross-system collaborations, a more diverse approach is required when designing, developing, and maintaining these systems or SoSs. Research suggests taking a traditional single system approach towards these collaborative system combinations may overlook certain aspects. This could include the inability to capture all stakeholder needs, goals, ownership and accountability, and requirements for security, interoperability, or vital inputs and outputs providing situational awareness supporting resilience across the whole. As a result, this may lead to increased levels of unaccounted for risk.

While there is some diversity in the approaches proposed for engineering SoSs, a gap is evident towards a formal process for defining, characterising, and modelling a SoS, where only commonly used descriptions are posited, with few illustrative examples demonstrating their initial classification and resulting SoS structure. It would, therefore, be useful to apply a candidate SoS, and illustrate how the example might be framed as a SoS given its characteristics. This clarity of context would specifically aim to support the first steps of a SoS security risk assessment process, given that any risk assessment process must be driven by its related context. These findings would then inform the application of suitable design techniques and SoS components appropriate to a SoS's type and complexity, considering where issues may exist and which may be assessed and modelled in the context of the SoS.

4.2 Grounding the System of Systems Context for Security Risk Assessment

Through research and stakeholder interactions, it has become evident that use of a common less-technical language of engineering, security, and risk can assist multilevel stakeholder understanding. Moreover, it is useful for operational stakeholders to first align with the concept of SoSs before its complexity can be identified and appreciated. Therefore, based on findings from the review of literature and SoSs examples considered, to assist the communication bridge between operations and SoSRE, a clearer SoS distinction and description is applied within the SoS characterisation process. An example using simple models is demonstrated in Figure 4.1 to introduce the SoS concept.

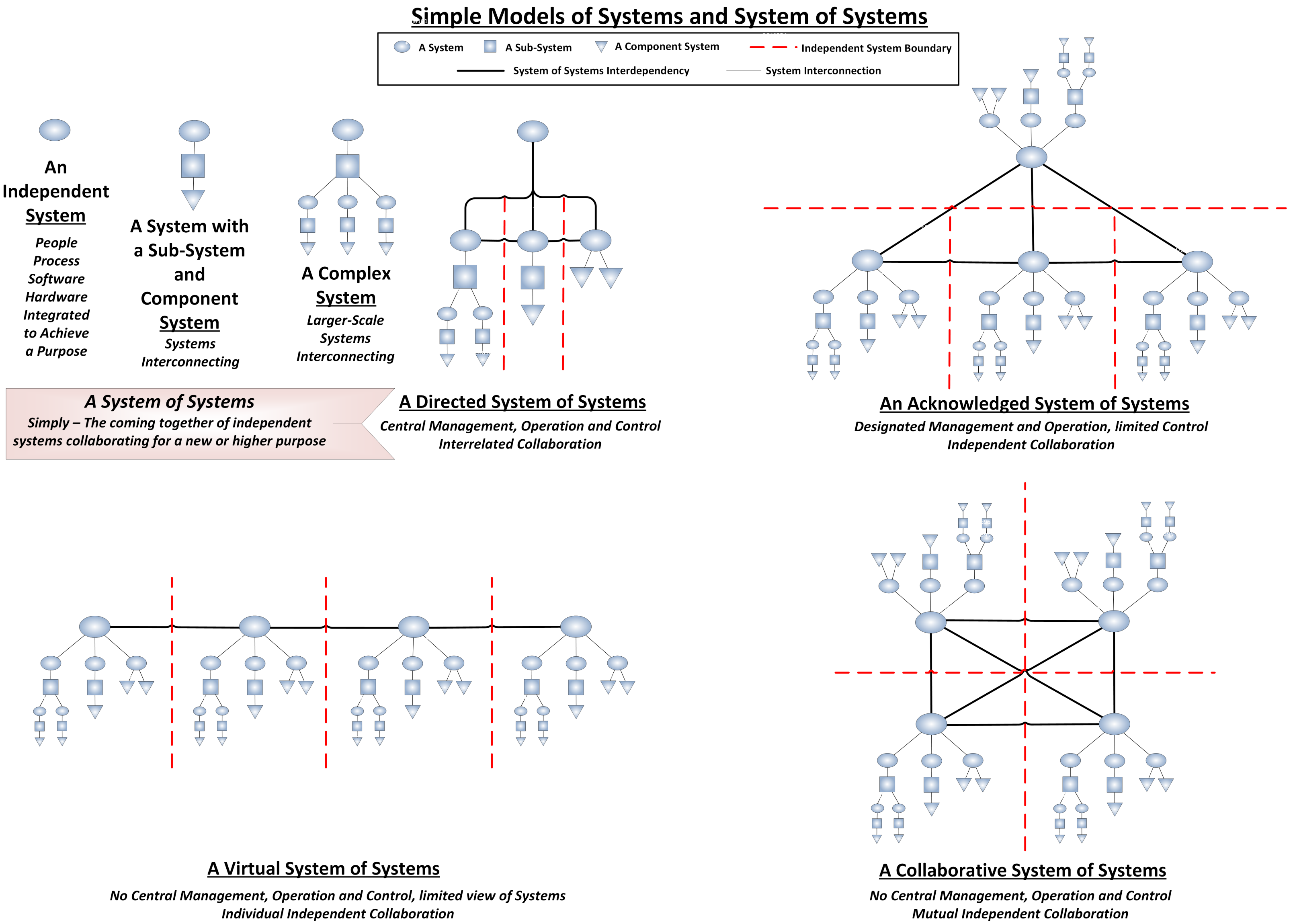

Simple Models of Systems and System of Systems
A System
A Sub-System
A Component System
Independent System Boundary
System of Systems Interdependency
System Interconnection
An Independent System
People Process Software Hardware Integrated to Achieve a Purpose
A System with a Sub-System and Component System
Systems Interconnecting
A Complex System
Larger-Scale Systems Interconnecting
A System of Systems
Simply – The coming together of independent systems collaborating for a new or higher purpose
A Directed System of Systems
Central Management, Operation and Control
Interrelated Collaboration
An Acknowledged System of Systems
Designated Management and Operation, limited Control
Independent Collaboration
A Virtual System of Systems
No Central Management, Operation and Control, limited view of Systems
Individual Independent Collaboration
A Collaborative System of Systems
No Central Management, Operation and Control
Mutual Independent Collaboration

Fig. 4.1 Simple Models for Systems and System of Systems

This was provided to ground the SoS concept and definition to support a characterisation process with stakeholders unfamiliar with the concept and types of SoSs, and which could contribute to a SoS security risk assessment process.

Pre-Context

As indicated in Figure 4.1, an improved description was applied to the process to simply define a *System of Systems* as being *'the coming together of independent systems collaborating for a new or higher purpose'*. Independent collaboration must be in place by one means or another for the SoS to exist, where systems are used and combined in different ways to that of their original purpose, otherwise they would simply be independent systems.

A Directed SoS seemingly has the most in common with the genetic make-up of a single independent system, usually with a top-down input, but still requires bottom-up input to function. Although, where centralised ownership and control is reduced in other types of SoS, the inputs may reduce and conflicts increase. Evolutionary and geographical challenges are important factors, but are also drivers for present day systems and innovation, as well as SoS collaborations. Emergence is, however, more likely within SoSs because of systems coming together in new ways.

The level of centralised control within a functional and operational SoS appears to be the overarching feature significant towards accounting for the SoS risks and ownership, combined with the level of collaboration from independent systems, their sub-systems, and trust boundaries. Therefore, to challenge and redefine current SoS descriptions further towards security aspects, situating control, ownership and accountability stemming from the levels of control within the SoS, within the process it was considered that:

- A Directed SoS has interrelated collaboration, with central management, operation and control over the SoS as a whole;
- An Acknowledged SoS has designated management, but has limited control over the independent collaboration of the SoS as a whole;
- A Collaborative SoS has no central management, so operation and control must be formed and agreed as a mutual independent collaboration;
- A Virtual SoS has individual independent collaboration with no central management, operation or control of the SoS as a whole.

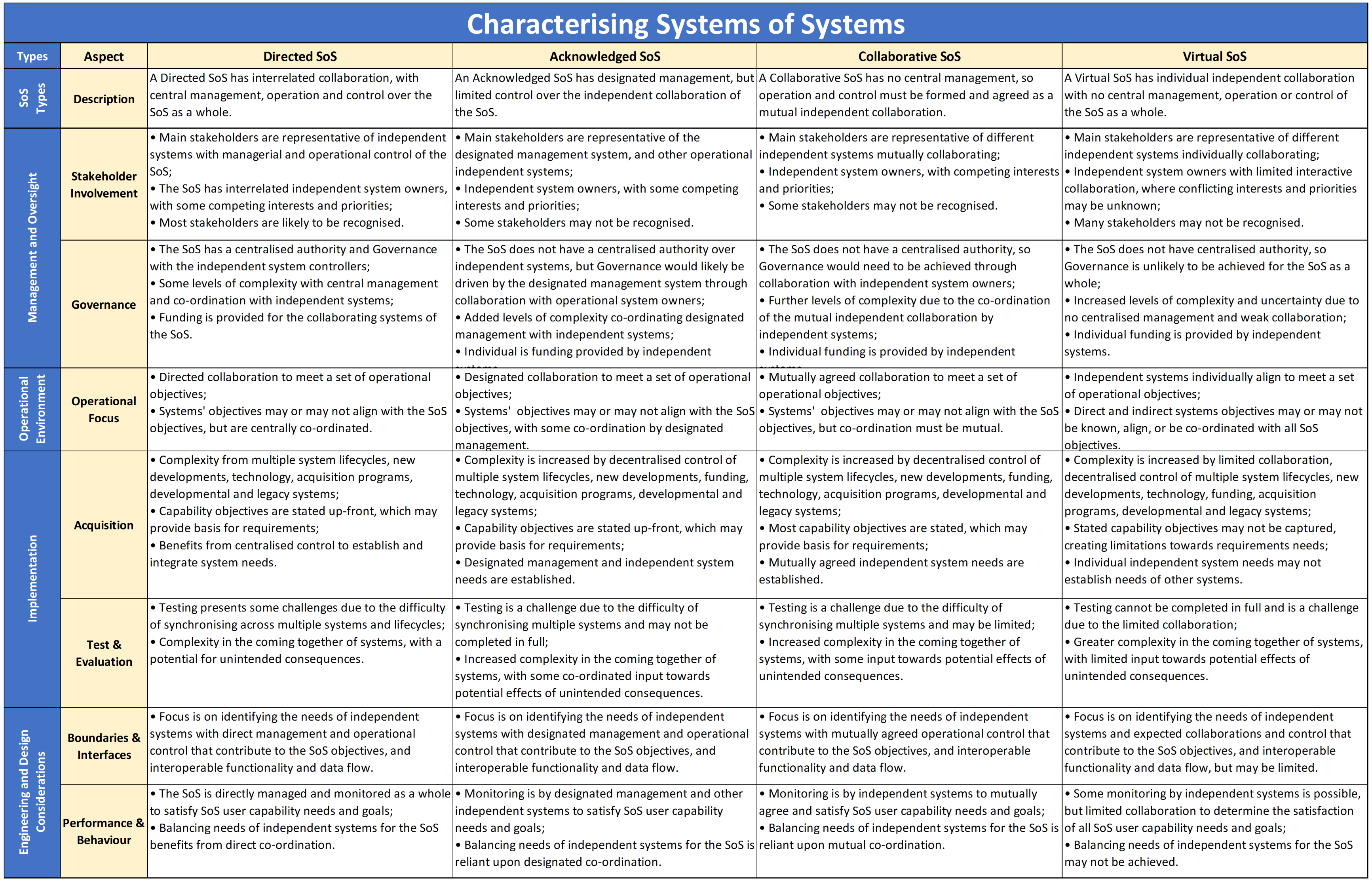
These redefined descriptions continue to align with other research of SoSs, e.g. Maier (1996), Dahmann and Baldwin (2008), Boxer and Garcia (2009), Sommerville (2015), and were used within the SoS characterisation process as illustrated in Figure 4.2, intended for alignment with a SoS security risk assessment framework.

Context and Characterisation

In addition to previously reviewed SoSs literature, a thematic review of publicly available literature was undertaken to introduce the Afghan Mission Network (AMN) as a SoS, related to the time period of the North Atlantic Treaty Organisation's (NATO) implementation of the AMN. Using the AMN scenario, a prototype of the characterisation process was applied.

The main element of the process integrates an approach based on work described by Dahmann and Baldwin (2008) drawing comparisons between a system and Acknowledged SoS, framed towards SoS engineering terminology. As articulated in Figure 4.2, this work was modified and expanded upon to consider the subtle differences between other types of SoSs as a means to classify a given example in a likely SoS environment, whilst considering concepts from Maier's parameters (Maier 2005). Supporting arguments towards the claims presented for each type of SoS in Figure 4.2 are illustrated in Appendix A, in Figures A.1 to A.4.

Using Figure 4.2 helps to frame considerations towards the SoS's management and oversight, its operational environment, implementation, and other design and engineering considerations, by indicating the degrees of input and complexity found across different types of SoSs. Whilst subtle differences between the indicated types of SoSs can help to determine the type of SoS under consideration, these differences could be quite significant in some scenarios. There is also a potential for other SoS types to exist at different levels within a SoS, thus progressing through the process begins to highlight the scope and complexity, and potential challenges for the SoS under consideration.



Characterising Systems of Systems

Types	Aspect	Directed SoS	Acknowledged SoS	Collaborative SoS	Virtual SoS
SoS Types	Description	A Directed SoS has interrelated collaboration, with central management, operation and control over the SoS as a whole.	An Acknowledged SoS has designated management, but limited control over the independent collaboration of the SoS.	A Collaborative SoS has no central management, so operation and control must be formed and agreed as a mutual independent collaboration.	A Virtual SoS has individual independent collaboration with no central management, operation or control of the SoS as a whole.
Management and Oversight	Stakeholder Involvement	• Main stakeholders are representative of independent systems with managerial and operational control of the SoS; • The SoS has interrelated independent system owners, with some competing interests and priorities; • Most stakeholders are likely to be recognised.	• Main stakeholders are representative of the designated management system, and other operational independent systems; • Independent system owners, with some competing interests and priorities; • Some stakeholders may not be recognised.	• Main stakeholders are representative of different independent systems mutually collaborating; • Independent system owners, with competing interests and priorities; • Some stakeholders may not be recognised.	• Main stakeholders are representative of different independent systems individually collaborating; • Independent system owners with limited interactive collaboration, where conflicting interests and priorities may be unknown; • Many stakeholders may not be recognised.
	Governance	• The SoS has a centralised authority and Governance with the independent system controllers; • Some levels of complexity with central management and co-ordination with independent systems; • Funding is provided for the collaborating systems of the SoS.	• The SoS does not have a centralised authority over independent systems, but Governance would likely be driven by the designated management system through collaboration with operational system owners; • Added levels of complexity co-ordinating designated management with independent systems; • Individual is funding provided by independent systems.	• The SoS does not have a centralised authority, so Governance would need to be achieved through collaboration with independent system owners; • Further levels of complexity due to the co-ordination of the mutual independent collaboration by independent systems; • Individual funding is provided by independent systems.	• The SoS does not have centralised authority, so Governance is unlikely to be achieved for the SoS as a whole; • Increased levels of complexity and uncertainty due to no centralised management and weak collaboration; • Individual funding is provided by independent systems.
Operational Environment	Operational Focus	• Directed collaboration to meet a set of operational objectives; • Systems' objectives may or may not align with the SoS objectives, but are centrally co-ordinated.	• Designated collaboration to meet a set of operational objectives; • Systems' objectives may or may not align with the SoS objectives, with some co-ordination by designated management.	• Mutually agreed collaboration to meet a set of operational objectives; • Systems' objectives may or may not align with the SoS objectives, but co-ordination must be mutual.	• Independent systems individually align to meet a set of operational objectives; • Direct and indirect systems objectives may or may not be known, align, or be co-ordinated with all SoS objectives.
Implementation	Acquisition	• Complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems; • Capability objectives are stated up-front, which may provide basis for requirements; • Benefits from centralised control to establish and integrate system needs.	• Complexity is increased by decentralised control of multiple system lifecycles, new developments, funding, technology, acquisition programs, developmental and legacy systems; • Capability objectives are stated up-front, which may provide basis for requirements; • Designated management and independent system needs are established.	• Complexity is increased by decentralised control of multiple system lifecycles, new developments, funding, technology, acquisition programs, developmental and legacy systems; • Most capability objectives are stated, which may provide basis for requirements; • Mutually agreed independent system needs are established.	• Complexity is increased by limited collaboration, decentralised control of multiple system lifecycles, new developments, technology, funding, acquisition programs, developmental and legacy systems; • Stated capability objectives may not be captured, creating limitations towards requirements needs; • Individual independent system needs may not establish needs of other systems.
	Test & Evaluation	• Testing presents some challenges due to the difficulty of synchronising across multiple systems and lifecycles; • Complexity in the coming together of systems, with a potential for unintended consequences.	• Testing is a challenge due to the difficulty of synchronising multiple systems and may not be completed in full; • Increased complexity in the coming together of systems, with some co-ordinated input towards potential effects of unintended consequences.	• Testing is a challenge due to the difficulty of synchronising multiple systems and may be limited; • Increased complexity in the coming together of systems, with some input towards potential effects of unintended consequences.	• Testing cannot be completed in full and is a challenge due to the limited collaboration; • Greater complexity in the coming together of systems, with limited input towards potential effects of unintended consequences.
Engineering and Design Considerations	Boundaries & Interfaces	• Focus is on identifying the needs of independent systems with direct management and operational control that contribute to the SoS objectives, and interoperable functionality and data flow.	• Focus is on identifying the needs of independent systems with designated management and operational control that contribute to the SoS objectives, and interoperable functionality and data flow.	• Focus is on identifying the needs of independent systems with mutually agreed operational control that contribute to the SoS objectives, and interoperable functionality and data flow.	• Focus is on identifying the needs of independent systems and expected collaborations and control that contribute to the SoS objectives, and interoperable functionality and data flow, but may be limited.
	Performance & Behaviour	• The SoS is directly managed and monitored as a whole to satisfy SoS user capability needs and goals; • Balancing needs of independent systems for the SoS benefits from direct co-ordination.	• Monitoring is by designated management and other independent systems to satisfy SoS user capability needs and goals; • Balancing needs of independent systems for the SoS is reliant upon designated co-ordination.	• Monitoring is by independent systems to mutually agree and satisfy SoS user capability needs and goals; • Balancing needs of independent systems for the SoS is reliant upon mutual co-ordination.	• Some monitoring by independent systems is possible, but limited collaboration to determine the satisfaction of all SoS user capability needs and goals; • Balancing needs of independent systems for the SoS may not be achieved.

Fig. 4.2 Differentiating SoS Characteristics - extended from work by Dahmann and Baldwin (Dahmann et al. 2008b)

The characterisation process is intended to drive initial questions and information gathering to support the identification of the points detailed in the different sections in Figure 4.2. This is intended to help identify the SoS's stakeholder involvement, it's Governance, focus on operations, and towards the design and engineering considering boundaries, interfaces, acquisition, testing, evaluation, performance and behaviours of the SoS.

In particular, this provides a high-level focus towards the stakeholders of the SoS, to ascertain the degrees of ownership, control, accountability and responsibilities required within the SoS to achieve and maintain its combined SoS goals. The characterisation process would then be aligned towards supporting a security risk assessment and modelling approach to guide the minimum amount of information to determine the context and scope of the independent system collaboration and its interdependencies, specifically where SoS managerial and operational control is in place towards mitigating SoS risks for independent systems and the SoS as a whole. This may, however, present challenges for some systems or types of SoS where there is a weak collaboration or trust relationships providing limited systems and risk-based information.

Initial questions to support the SoS context and characterisation should aim consider:

- Who are the high-level stakeholders - the main independent systems of the SoS?
- Who are the other relevant stakeholders important to the SoS achieving its mission?
- Who provides management oversight, governance, funding, and operational control of the SoS?
- Who is responsible for SoS design, development, testing and implementation?
- What system boundaries exist for the SoS - do restrictions apply?
- How is on-going SoS performance and behaviour monitored to provide a resilient SoS balancing independent system needs?

4.3 Applying the Process with the AMN SoS

4.3.1 Example System of Systems Scenario

Supported by literature describing the historical accounts of military coalitions, this scenario considers the AMN as a likely candidate SoS, assisting the discovery of its related complexities and challenges for consideration. The AMN acted as a wide-scale integration of the communication links and data feeds used by the NATO International Security Assistance Force (ISAF) during the Afghanistan campaign missions (Finn 2011). The evolution of the AMN was driven by a need to meet the requirements of many stakeholders, and the criticality of interoperable systems depended upon to assist communications and RBDM. For example, each Troop Contributing Nation (TCN) as independent systems of the SoS would communicate across systems using their own non-federated networks operating without a common core, thus making information sharing a challenge between TCNs (Buxbaum 2010).

Because of the criticality of these communications, a shift in the NATO cultural mind-set was required from a 'Need to Know' basis to a 'Share to Win' approach, specifically as ISAF recognised data restriction created greater risks (Nankervis 2011). This approach was further complicated by national concerns and restrictions on data sharing between other nations, regardless of their NATO status (Seffers 2011b). It was also found the technical problems of net-centric warfare were relatively minor compared to cultural issues and human factors, particularly as personnel interacting with intelligence information could no longer be considered as secondary actors (Finn 2011). Robust information management was therefore required to meet the needs of people, process and technology, and timely decision making within the AMN (Nankervis 2011).

By placing all information exchange on the common ISAF Secret network, during 2010, the AMN became the primary communications network for ISAF forces (Nankervis 2011). The AMN extended across Afghanistan to 48 TCNs servicing a total force of over 130,000 combined military and civilian personnel with human-to-human exchanges of basic services for text-based chat, audio-based Voice-over-Internet-Protocol (VoIP) telephone connectivity, video-based Secure Video Teleconferencing (SVTC), email, web access, and office productivity tools (Serena et al. 2014). The AMN provided Command & Control (C2) to support growing mission and coalition partner's needs, and evolved to become central to Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance (C5ISR) (Serena et al. 2014). This supported rapid decision making within the AMN by using coalition data and Common Operational Pictures (COPs) (Serena et al. 2014) to improve the SA within the security environments (Thiele 2013).

4.3.2 Characterising the AMN

Considering this scenario begins to highlight the managerial and operational independence, evolutionary nature, geographical separation, and a potential for emergent behaviours within the AMN. Because of the type or level of centralised control, this particular configuration presented a strong indication the AMN could be classed as an Acknowledged SoS, given NATO's centralised management and functional operation of the AMN, whilst TCNs provide there own functionality in which to interoperate with the AMN. NATO/ISAF and TCNs would also retain independence towards their own operations and related assets

To capture these aspects in a SoS context in further detail, the prototype characterisation process using the sub-categories described by Dahmann et al. (2008b) were implemented to frame the AMN, considering whether the scenario and context would indeed align with the characteristics of an Acknowledged SoS.

AMN Management and Oversight

Stakeholder Involvement

In Acknowledged SoSs, stakeholders are at both System level and SoS levels, and includes the system owners, with competing interests and priorities. In some cases, the system stakeholder has no vested interest in the SoS and all stakeholders may not be recognized (Dahmann and Baldwin 2008).

For the success of the AMN, considering stakeholder needs was an important challenge to ensure a continuous operation of local, military and civilian interaction priorities were met. Primary stakeholders included NATO/ISAF, TCNs and partners. The list of direct and in-direct stakeholders was extensive across all SoS and independent system levels, although stakeholders at system level would have a vested interest in the SoS given the nature of their participation. Other important in-direct stakeholders reliant upon the information flow of the AMN included NATO's civilian representation, the Afghanistan government, the UN Assistance Mission in Afghanistan, Non-Governmental Organisations (NGO's), other international organisations supporting humanitarian or aid efforts (Brooke-Holland and Mills 2012), and the Afghan population working to implement mutual goals for their nation.

Governance

In Acknowledged SoSs, there are added levels of complexity due to management and funding for both the SoS and individual systems, meaning the SoS does not have central authority over all the systems (Dahmann and Baldwin 2008).

Governance within the AMN was achieved at a number of levels, e.g. NATO/ISAF AMN Operations, testing and validation collectives, and other national level input. Therefore, added levels of complexity arise across all levels of the SoS Governance. Funding was focused at the SoS level, whereas individual systems connecting to and forming the AMN were funded, managed and operated by relevant participating nations, thus retaining a level of autonomy.

AMN Operational Environment

Operational Focus

In Acknowledged SoSs, they are called upon to meet a set of operational objectives using systems whose objectives may or may not align with the SoS objectives (Dahmann and Baldwin 2008).

The NATO Communication and Information Systems Services Agency (NCSA) and its Mission Detachment to ISAF (NMD-I) were responsible for the operation of in-theatre Communication and Information Systems (CIS) services. Meeting the needs of operational objectives and mission threads were, therefore, aligned with the SoS objectives. However, TCNs and other agencies were likely to have national objectives separate or in addition to SoS objectives.

Within the AMN, the Joint Mission Threads (JMTs) shown in Figure 4.3, such as Battlespace Awareness, Medical Evacuation, and Freedom of Movement, together with applicable services critical to their functioning were the primary means of

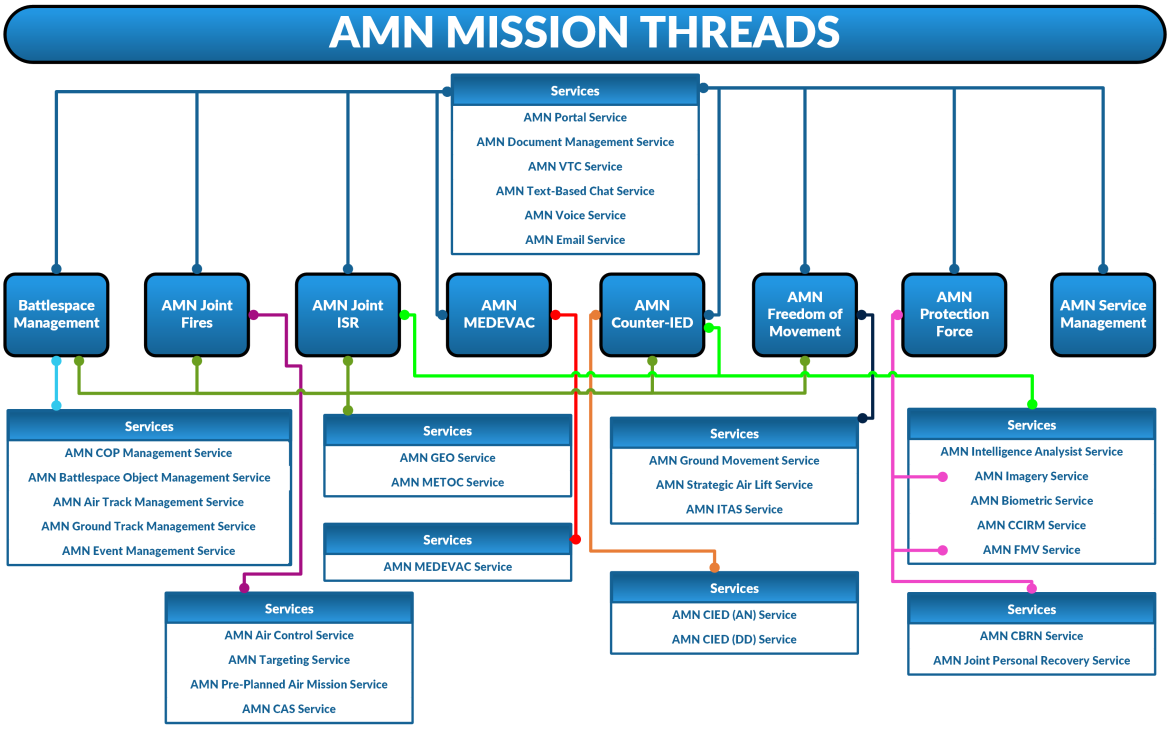


Fig. 4.3 AMN Mission Threads

aligning the goals and activities of the SoS to achieve its mission (Serena et al. 2014), thus being integral systems within the SoS.

AMN Implementation

Acquisition

In Acknowledged SoSs, added complexity exists due to multiple system life-cycles across acquisition programs, involving legacy systems, developmental systems, new developments, and technology insertion, which typically have stated capability objectives up front that may need to be translated into formal requirements (Dahmann and Baldwin 2008).

The NATO Consultation, Command and Control Agency (NC3A) primary role was to develop, acquire and implement capabilities using their expertise of C2 through to C5ISR, providing vital communications and data services supporting NATO forces across Afghanistan (Kenyon 2010). To meet the operational needs of the NMD-I, Thales were tasked by the AMN Architecture Working Group (AMN AWG) with the provision, operation and maintenance of a complete network, end-to-end logistics and integration of systems, including transfer of all equipment throughout the theatre of operations in Afghanistan (Thales 2008). However, participants at a system level were responsible for ensuring their legacy systems could interface with the AMN. Complexity existed across the multiple system life-cycles, but were reduced using tried and tested solutions, supported by testing and validation programmes providing feedback for improvements to core technology, systems and configurations within the SoS.

Test & Evaluation

In Acknowledged SoSs, testing is more challenging due to the difficulty of synchronizing across multiple systems' life-cycles, given the complexity of all the moving parts and potential for unintended consequences (Dahmann and Baldwin 2008).

The Coalition Interoperability Assurance and Validation (CIAV) programme provided in-theatre mission-based assurance testing and validation, and verified the status of interoperability among current, future, and experimental systems that would be deployed within the AMN (Serena et al. 2014). The CIAV Working Group (CIAV WG) were responsible for interoperability improvements within AMN governance structure, and integrated with accreditation groups providing security of coalition information and networks established under the Combined Federated Battle Laboratories Network (CFBLNet) (CFBLNet 2015).

The CFBLNet facilitated development of coalition interoperability, doctrine, procedures, and protocols that could be transitioned to operational networks in future coalition operations. This was carried out through 17 dedicated integrated labs based in ten nations (NATO Communications and Information Agency 2013), and bi-annual testing with the Coalition Test and Evaluation Environment (CTE2) and Coalition Warrior Interoperability Exercise (CWIX) (Anon. 2010) for new systems and architecture of specified CIAV assessments (Rose 2011).

AMN Engineering and Design Considerations

Boundaries and Interfaces

In Acknowledged SoSs, the focus is on identifying the systems that contribute to the SoS objectives and enabling the flow of data, control, and functionality across the SoS while balancing needs of the systems (Dahmann and Baldwin 2008).

The AMN AWG developed the architecture and modelling of the AMN mission threads to support multi-national C5ISR planning at the enterprise level (Rissinger 2011). SoS boundaries and interfacing requirements were identified through the NC3A, Thales, AMN AWG, and implemented by the NMD-I over a single core network at the classification level of ISAF Secret.

The AMN boundary generally ends with the connections to each of the TCNs, although some data distributed through the AMN may be disseminated through national level command structures, under national policy and control. Boundaries are also considered in different contexts, covering networks, people, process, and technology, across land, sea, air, space and cyber domains, where different parameters, characteristics and interfacing requirements exist.

Performance & Behaviour

In Acknowledged SoSs, performance is across the SoS that satisfies SoS user capability needs while balancing needs of the systems (Dahmann and Baldwin 2008).

NMD-I and Thales managed and monitored on-going performance of objectives to meet the SoS objectives of secure C5ISR data flow, with further performance and interoperability feedback provided by TCNs and the CIAV programme. Direction, oversight and monitoring of security behaviour for Cyber Defence was conducted by the NATO Cyber Defence Management Authority (NCDMA), whilst the NATO Computer Incident Response Capability (NCIRC) provided capabilities for maintaining the end-to-end network security. Security risks faced by the AMN often emanated from targeted network attacks using malicious software and Denial-of-Service (DoS) attacks, spam, malware, web defacements, or poor maintenance related vulnerabilities, system privilege abuse, authorised user indiscretions, and classified information leakage (Herrmann 2010).

4.3.3 Reviewing the AMN

A review of the literature supporting the AMN example identified the main dominant systems and stakeholders shown in Figure 4.4, directly an indirectly critical to the SoS and its interoperation, indicating where certain dependencies exist. Designated management and oversight was provided by NATO/ISAF in operational collaboration with TCNs.

Using the characterisation process highlighted where the central dependency for the SoS was the reliance upon the core of the AMN collaboration between NATO/ISAF and TCNs indicated in a main boundary in Figure 4.4. Although geographically, some stakeholder systems and their interactions were dispersed over many continents. All systems would also have their own overlapping boundaries with differing priorities and dependencies. Other representative stakeholder systems include those responsible for the acquisition, implementation and operations, testing and validation, in-theatre users, and other external entities that were identified.

Interviews with stakeholders representative of some of these military and defence based systems were conducted. Interview sessions were hosted by Dstl, and included a Security and Risk person experienced in NATO activities, and network-based representatives experienced in projects such as CFBLNet. Interviews considered some of the challenges for these entities when collaborating with such an example of a NATO SoS and federated networks.

Security and risk aspects, in particular, for inter-network connectivity, were reliant on TCN agreements for operating requirements, and relied upon the input provided by RMADs to support RBDM. The typical challenges associated with the integration and interoperation of this type of SoS and was also to some degree placed into context by discussions with other service personnel, and French engineers at a NATO conference that architect and integrate systems into NATO SoS environments. Together, their feedback assisted towards validating the identified context and challenges as being prevalent in this type of SoS.

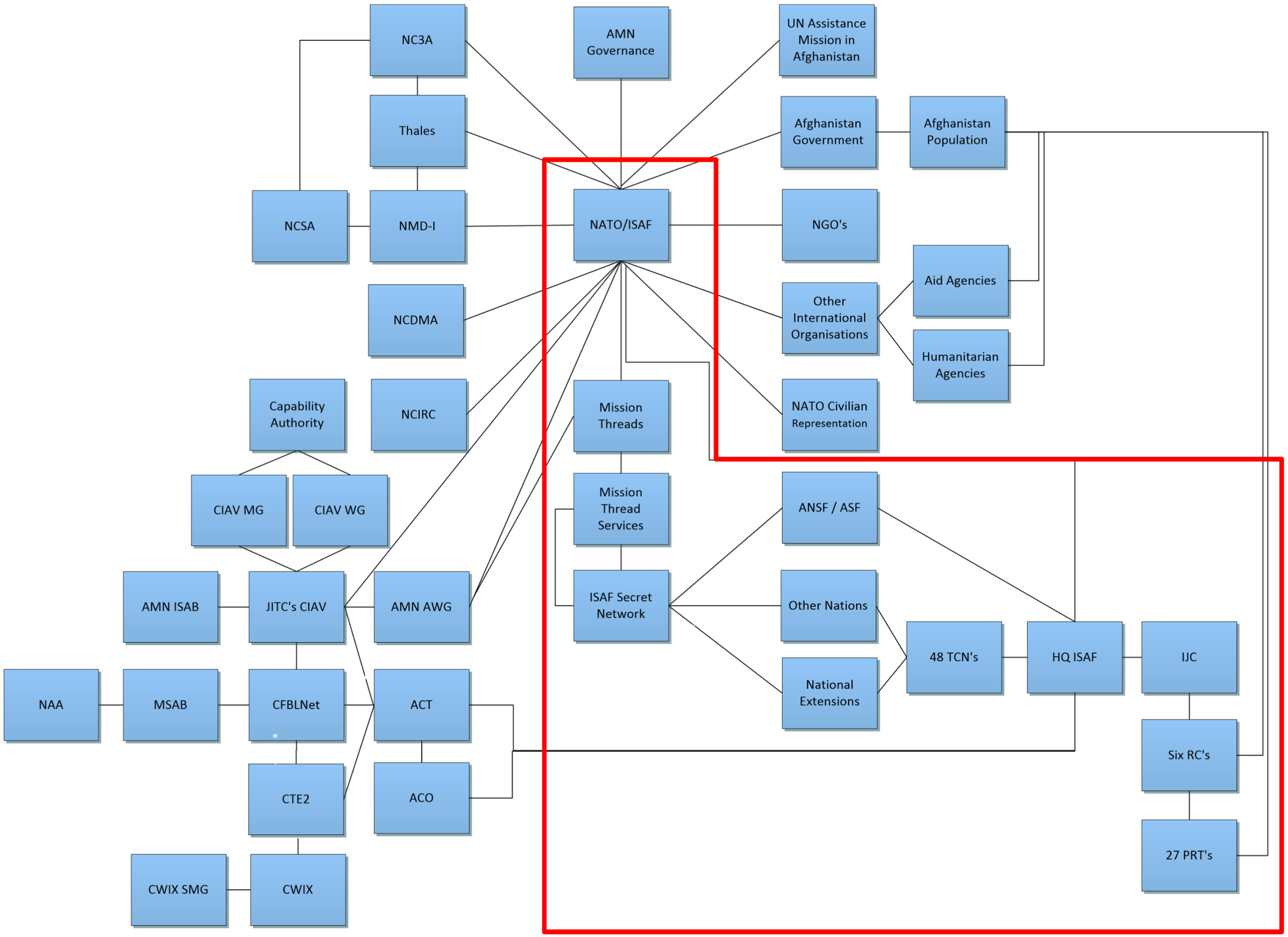


Fig. 4.4 AMN SoS Stakeholder Systems Model

4.4 Application Findings

When reviewing the AMN example of a SoS towards the research problem, a number of challenges were identified relating to the SoS context, scale, and dependencies towards meeting the SoS goals. The stakeholder systems shown in Figure 4.4 provided an indication as to the complexity of stakeholder interactions to develop and maintain the AMN. Many of the systems in the left portion of the model related in some way to NATO sub-system operations, although coalition testing and validation was also important to the wider operational picture. To help validate this scenario, certain stakeholders from this area of military and defence provided feedback for the characterisation and SoS context, and closing analysis.

Stakeholders in the upper right portion interacted in other ways with the AMN, and may be consulted or informed based on the data inputs and outputs of the AMN. Some may also be considered as benefactors of the AMN, rather than providing any form of managerial or operational control, but still nevertheless have important roles.

Having framed the AMN in the context of a mission-driven Acknowledged SoS, this provided a level of clarity considering the vested interest of stakeholders towards the AMN achieving its SoS mission objective, each with differing needs and interactions either at a SoS, system, or component level. Stakeholders should, therefore, be viewed as multi-dimensional and their interaction at differing levels should be understood. This focus should include an understanding of stakeholder objectives towards the SoS and the role they play at each stage of achieving the SoS mission, including the bi-directional dependencies on people, processes, technology, and trust during the implementation and operation of participating systems within the SoS.

To support set-up of operations in future SoS environments similar to the AMN, where applicable stakeholders provide differing inputs and outputs at varying stages of the systems and development life-cycles, joining options should be more straightforward with proven solutions for integration. Common service management and cost-effective cross provisioning of services incorporating data labelling for easier information sharing should be considered (Friedrich 2014), which can have a positive effect towards interoperability.

The AMN as a SoS supported the agile ‘Come as you are’ approach where future mission networks must interoperate with differing mission types and partners, with the need to communicate information at specified security classification levels (Whitehead 2014). There should, however, be a duty for the system entities within the SoS to identify a unified approach that answers the question ‘How should we come?’ This reinforces the need for global standardisation of data types, system and network configurations to improve interoperability. This need will become more prevalent in Acknowledged, Collaborative and Virtual SoS as central management or control is reduced.

Commonly defined and understood mission threads should be used to guide the development of future coalition data-sharing enterprises, and be supported with assurance and validation through programmes such as CIAV and the CFBLnet (Serena et al. 2014), both of which could also be considered as being SoSs. Testing becomes an iterative process that should focus on the end-state and mission thread success requirements, considering that components are put into systems, systems are put into platforms, platforms must interoperate with other families of platforms, and these family of platforms must interoperate via networks (Rissinger 2011). This demonstrates that in a SoS, at times there is a need for components and systems to scale-up to interoperate with higher groupings of systems to achieve its purpose as a SoS, which potentially becomes an area to observe for emergent behaviours.

The AMN also highlighted not only the dependency placed upon interoperability, but the different interoperability needs of people, information, and system interactions. To achieve a standardised, consistent and interoperable approach in a single, common mission-centric federated network such as the AMN, requirements may include the use of Commercial Off-The-Shelf (COTS) hardware and software, as opposed to developing expensive in-house alternatives, whilst maximising the use of other current applications, interfaces, web services (Herrmann 2010), reducing costs and resources, but may broaden aspects of ownership and control. Further consideration should also be given towards dependencies from the use of COTS products and risks created within the supply chain relating to product availability, or ensuring security and reliability of products before use and implementation in a SoS.

Human factor interoperability considerations were a particular challenge faced by the AMN, particularly when considering end-users in-theatre were dependent upon systems that were easy to administer and operate, and possessed the ability to provide reliable and timely CIS and SA in emergency scenarios (Veit 2011).

This finding correlates with other work in emergency services that found a key characteristic of a SoS is its inherent socio-technical nature, where social factors can become even more complex than technical interoperability (Dogan et al. 2011).

Using the characterisation process helped to provide a usable and repeatable format in which to frame the example SoS. This helped towards identifying the high-level goals, roles, interoperability needs and accountabilities providing sustenance to the context of the SoS, and would therefore provide useful input for a security risk assessment in the SoS context. This was considered important to related stakeholders, both from interviews and a separate presentation with military and defence stakeholders. The presentation was hosted by Dstl with the networks representatives in attendance along with other other Information Assurance personnel with experience of NATO activities.

After the presentation of the process and it's application, a discussion was held to determine further feedback in relation to the approach taken and it's findings. Feedback suggested for those configuring systems and networks within a NATO coalition, they are aware of the requirements towards information assurance, yet providing that assurance relies on trust, in the form of operating agreements, and accountability to provide the assurance. Capturing those roles is an important aspect, in particular where there may be conflicting requirements. The main challenge for stakeholders interviewed or presented to was the notion of SoSs, which was an unfamiliar term, albeit they generally understood the concept. For example, network engineers were familiar with the concept for network-of-networks, but not SoSs. Explanations using the simple models demonstrated in Figure 4.1 helped to reduce this problem by providing a clearer understanding of SoSs.

The characterisation process was found to indicate some of the design and engineering challenges and needs for consideration within a SoS context that may not have been considered in that way previously. As a result of the positive application of the process, this provided a means to characterise the SoS, whilst determining the subtle differences exhibited by different types of SoSs. More critically, this provided a means to identify where, what, and who has ownership, accountability, and control within the SoS context to achieve its goals.

4.5 Chapter Summary

This chapter presented an approach that provides the context and characterisation of a given SoS, enabling a platform for applying suitable design techniques to SoS components appropriate to SoS type and complexity. The prototyping of a characterisation process proved a useful means to frame the AMN as a SoS, and has benefited from taking a wider approach to clearly differentiate between other types of SoSs and their characteristics, whilst providing the context of the SoS. By considering the structure, management, and participation of systems and stakeholders within the SoS, this helped identify where dependencies and constraints may exist towards the SoS achieving its SoS mission objectives, and provided the context for which the SoS is situated in, thus useful for informing a related security risk assessment and modelling approach.

Findings suggest considerations for SoSs and future mission networks should include a specific focus towards identifying all relevant SoS stakeholders and individual mission-driven needs, including relevant human factor implementation and operational considerations. Cultural, environmental, and geographical considerations were of key importance in the AMN, with a high reliance and use of the cyber domain. Together, these created a greater dependency on interoperability for availability of systems and networks. It was also found that information and data sharing needs should be agreed and utilise common data labelling and classification formats using appropriate information management, security, and risk approaches.These considerations therefore demonstrated valuable insights gained from using the process that could support a security risk assessment of a SoS.

This research aimed to answer questions primarily in response to RQ1. However, findings from early modelling of the SoS and then identifying SoS characteristics and challenges gave further considerations towards aligning security risk approaches for SoSs, thus addressing RQ2. This provided some inference towards RQ3 by highlighting the notion of capturing independent system views encapsulating the direct interactions of each system, because capturing multiple views, or a view of the SoS as a whole may not be possible in all scenarios where there is decentralised management and control. In support of additional validation, peer review was gained through the presentation and publication of elements of this work in Ki-Aries et al. (2017b).

Chapter 5

Assessing and Modelling SoS Security Risks and Human Factors

Chapter 5 introduces a second SoS using an existing example of a Directed SoS, primarily to consider implications towards how security, risk, and human factors may be assessed and modelled in the SoS context. In particular, this considers how human factors, and impacts related to interoperability and emergence may be accounted for. This work considers lessons learned from the AMN example, and continues to identify challenges, concepts, and factors applicable for consideration towards assessing SoSs security risk, whilst accounting for related human factors. The context, application, and findings are presented to discuss each step applied to address the related research problem.

5.1 Motivation

There are many examples of different SoSs, each with different types of systems collaborating to achieve a new purpose and goal. Some may be organisational and enterprise based, or some may be regarded as Internet of Things (IoT) applications. These may consist of multiple software components, sensors, and communications modules, integrated with networks, core systems, processes, and people interaction with the technology (Bartolomeo 2014). For example, smart city sensors monitoring air quality or traffic. However, interoperability and emergence are such intrinsic properties of IoT applications that the classic notion of a *system* is inadequate for dealing with system complexity, and tackling security problems.

In recent years, there has been some interest in framing types of IoT systems as SoSs (Maia et al. 2014), which can help make sense of complexity associated with interoperability and emergence. However, while the notion of designing for a SoS can help manage some design complexity, there is little work providing guidance for what designing for SoS security entails, certainly given the various types of SoS examples. More specifically, although some literature exists considering SoS challenges to risk management, there has been little work focusing on information security risk assessment in SoSs, and the modelling and visualisation of such interactions using tool-support to integrate different models, concepts, and techniques.

Risk is a key concept in security, thus mitigating controls and requirements need to reflect a system's expected behaviour in the presence of risk. These requirements need to be verified and validated to ensure specified behaviour meets stakeholder expectations and operational needs. Assessing the security risk of SoSs is, however, likely to be a challenge due to the operational and managerial independence, with differing degrees of centralised control and decision making. For example, research in Chapter 4 identified constraints on geographical, environmental, evolutionary and emergent behaviour, human interaction and culture adding to SoS complexities, creating obstacles and opportunities towards interoperability.

Although SoSs are collaborative in different ways, in order to understand the SoS as a whole, an important aspect for SoSRE is to identify related characteristics at a system-element level (Simpson and Dagli 2008) that extend through relationships and concurrent behaviour between systems. This is easier to identify in Directed SoSs, but the challenge becomes greater as central management, access and control of constituent systems is reduced in Acknowledged, Collaborative, and Virtual SoSs. Consequently, classic approaches for security, risk assessment, human factors, requirements and systems engineering need to evolve to cope with challenges posed by different SoS characteristics (Dogan et al. 2011, Ncube et al. 2013).

Supporting research would therefore need to consider these types of challenges and key concepts that may need to be addressed when accounting for human and system interactions where there is a potential for risk in security. Identifying how these systems interact becomes a critical aspect towards accounting for potential areas of concern emanating from the different operational interactions, data flows, and dependencies. Related risk may then be assessed to analyse and evaluate which systems are not only at risk, but may create issues for other systems resulting from the of loss of availability and interoperability.

5.2 Integrating SoS Components for Security Risk Assessment

To consider these challenges and concepts, this would implement a previously published example of a pervasive SoS detailed by Whittington and Dogan (2015), to allow a focus towards exploring how we may assess and model the SoS security risks and related human factors. Although examples of their previous work primarily had a focus towards accessibility and assistive technology (Whittington et al. 2015), there was an appetite by its researchers to begin to consider where risk may be present in the SoS. For example, the notion towards capturing information about Human System Interactions, detailing where the human actions are performed with systems of the SoS, and where potential interoperability concerns may apply.

Stakeholder feedback and validation was gained iteratively in-person and through follow-up communications, providing useful insights for the stakeholder and their SoS operations. Working with Dr Paul Whittington as the main stakeholder for his pervasive SmartPowerchair SoS, research would identify and observe the interplay between the socio-technical aspects of the SoS towards performing a risk assessment.

This was achieved first through a scoping session with the stakeholder to explore the purpose and goals of the SoS, and how each of its systems were integrated to achieve the common goal. This included a walk-through of the interactions and dependencies important to interoperation of the SoS and its user. Follow-up communications were then conducted to clarify certain aspects towards those dependencies in relation to the SoS operation and security considerations, before applying early prototyping of selected components within a security risk assessment.

When accounting for interoperability and related dependencies across different SoS types, or their constituent and component systems, modelling can be introduced to highlight the impact upon aspects of the SoI influencing risk analysis within the SoS. Given the unpredictable nature of emergence, it is, however, a difficult challenge to capture risks centred on emergent behaviour of SoSs, but would nonetheless be useful to identify potential issues where possible. By gaining an understanding of these aspects related to the SmartPowerchair SoS, this would continue to inform the suitability of concepts for inclusion within a SoS security risk assessment framework.

5.2.1 Assessing Security Risk

In the first instance, a basic risk assessment approach would be adopted based on considerations of ISO 27005 (British Standards Institution 2011) to capture the potential for impacts on systems from threats and vulnerabilities. Three components would then be introduced to assist the SoS risk assessment, which could overlay with existing security and risk approaches. To account for human-related aspects, this considers the broader categories of HSI early in the process, then identifies and analyses potential impacts towards interoperability and emergent behaviour related to the pervasive SmartPowerchair SoS. The assessment data could then be carried over to begin to explore modelling options using tool-support from CAIRIS.

5.2.2 Human Systems Integration Analysis

The first component entails identifying and analysing human characteristics of those involved within the SoS. HSI as described by National Research Council and others (2007) is used to focus on roles, responsibilities and relationships of manpower and personnel, ownership, stakeholder interaction, training, safety and other factors. HSI could align with other user-centred approaches, and would be integrated to provide context towards socio-technical aspects applicable to security risk identification and analysis, whilst informing decision makers towards suitable requirements and controls within the context of the SoS and its users.

5.2.3 Interoperability Analysis

The second component considers the interoperability impact resulting from a security concern within the SoS using a qualitative assessment. In particular, this would support the ideation of capturing cross-domain interoperability, e.g. towards capturing the interoperability needs as described in the NCOIC Interoperability framework (NCOIC 2019a). Interoperability should be considered during the identification stage of an assessment, then within analysis to determine system impacts on the SoS. Although not all risks will necessarily have an impact on SoS level interoperability, the overall impact on SoS goals should be assessed against each risk identified. All details should be taken into consideration with results appropriately documented.

5.2.4 Emergent Behaviour Analysis

Some systems may be used in different contexts due to evolutionary changes, or the emergent behaviour of the users and systems; this may affect the utility of the SoS as a whole. Based on analysis, evaluation should consider the potential for emergent behaviour, and possible mitigating controls or requirements that risk-based decision makers may wish to consider.

5.2.5 Exploring Model Generation with Tool-Support

Once security risk has been assessed in the context of the SoS, data output from the assessment can be used to explore how the resulting risk data can inform a modelling and elicitation process using tool-support. In this instance, CAIRIS is introduced to model the socio-technical interactions of the SoS, and explore its model generation capabilities. During this stage, abstraction stacks are introduced (Simpson and Dagli 2008) to assist the security risk assessment as a means towards decomposing the SoS, and which supports the modelling of systems and components, thus defining its structure of interoperation.

5.3 Assessing and Modelling the SmartPowerchair SoS

5.3.1 Example System of Systems Scenario

The *SmartPowerchair* is a standard powered wheelchair (Powerchair) integrated with existing pervasive technologies. This is comprised of different systems, components, interactions and functions, with the aim of enabling independent living, improving quality of life for people with reduced physical abilities (Whittington and Dogan 2015, Whittington et al. 2015).

The SmartPowerchair is supported by SmartATRS using a Smartphone system to control an Automated Transport and Retrieval System (ATRS). ATRS is a technically advanced system using robotics technology with Light Detection and Ranging (LiDAR) to autonomously dock a Powerchair onto a platform lift. The lift is fitted into the rear of a standard Multi-Purpose Vehicle (MPV) system, and is operated and docked whilst a disabled driver is seated in the driver's automated Freedom seat.

Various system components are integrated with the Powerchair to meet overall requirements for the SoS as illustrated in an updated diagram shown in Figure 5.1. For example, the GoVue application is installed on the Smartphone to facilitate use of a rear view camera attached to assist with manoeuvring. SmartATRS is a key system in this SoS supporting interaction between the MPV and the Powerchair systems. SmartATRS improves usability of ATRS keyfobs and hand-held pendants by providing a Smartphone application to control the interaction between the MPV and Powerchair systems.

Integrated into the MPV system is a web server and relay board interfacing between SmartATRS and ATRS components (seat, lift and tailgate). The web server relay connects through Ethernet to a Wi-Fi router that transmits over secure Wi-Fi Protected Access II (WPA2) network. Smartphones or other Wi-Fi enabled devices interact with a GUI by entering the URL or bookmark into a browser. SmartATRS sends commands wirelessly to the relay board, executed by JavaScript.

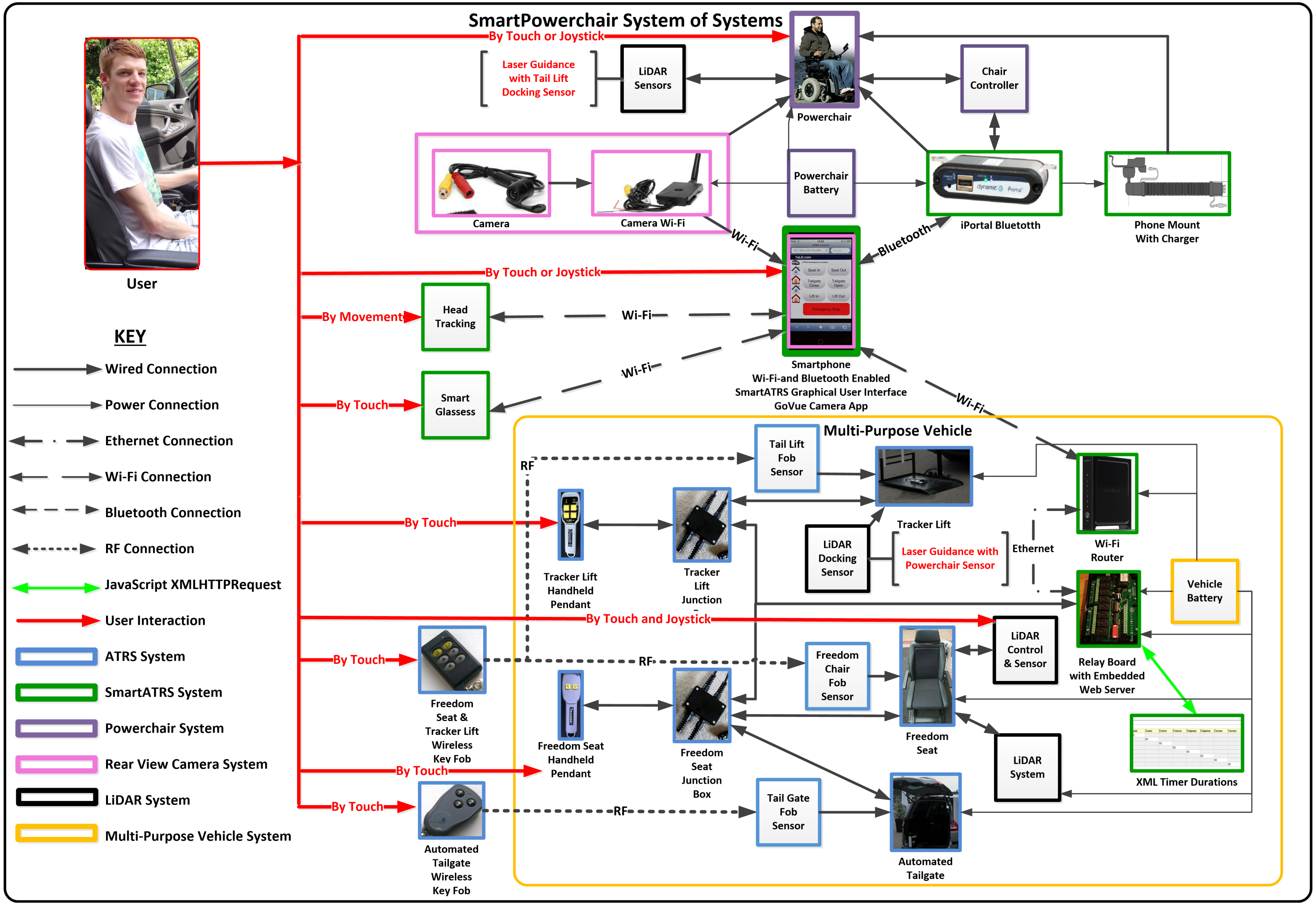


Fig. 5.1 SmartPowerchair System of Systems Architecture

The server stores the HTML and JavaScript GUIs as web pages and JavaScript XMLHTTPRequests are transmitted to access an eXtensible Markup Language (XML) file. The file contains the timer durations for each ATRS function as integers that represent the number of milliseconds that each function is switched on for. An XML editor can also be used to view and change the timer durations, whilst ensuring the process is not visible to end users.

The iPortal system operates via Bluetooth, providing an alternative to the touch-screen interface, using the Powerchair joystick interaction with the Smartphone and SmartATRS GUI, using left or right for screen navigation and forwards for selection. The Smartphone is the primary enabling system for control and communication with the user through the interface, Powerchair and joystick controller to receive commands.

Other technologies integrated with SmartATRS can provide alternative interaction mediums, such as Head Tracking and Smartglasses. Interoperability and emergent behaviour of such systems integrated into a SoS bring significant challenges to risk assessment. The complexity and number of interactions illustrated in the SmartPowerchair diagram in Figure 5.1 re-emphasises the importance of identifying SoS risks centred on human and system integration, interoperability and emergent behaviour.

5.3.2 Applying Human Systems Integration

Previous work from the SmartATRS project (Whittington and Dogan 2015, Whittington et al. 2015) carried out extensive work towards improving usability and interaction of the SmartPowerchair SoS. To build on this previous work taking a new perspective, HSI was implemented to account for the human factors associated with the management and operation of the SmartPowerchair SoS. HSI was applied by gaining input, demonstration, clarification, and validation from the Powerchair user regarding the typical functions, activities and potential dependencies of system interactions, thus providing a level of context for the security risk assessment.

5.3.3 Assessing the SmartPowerchair SoS Security Risks

Using the data and context captured thus far of the SoS, this provided considerations towards system assets and the user's interaction with systems. Availability was considered the primary security goal for this SoS, with integrity of data processed, stored or transmitted also of value. Although confidentiality of some assets were valued, some trade-offs were considered necessary.

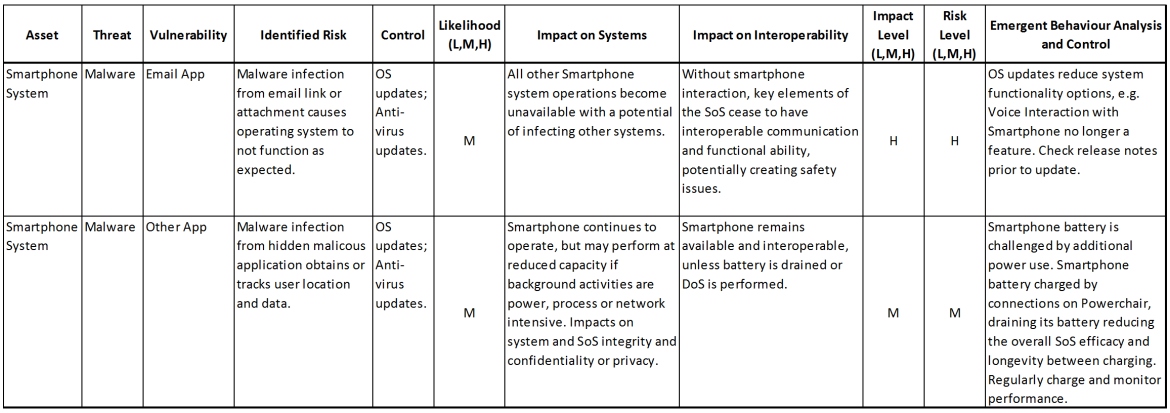
Further detail was incorporated into specific operations of the SoS, mission goals and context, or where dependencies and security trade-offs exist. An example of a system-level trade-off included the potential for using authentication to control access to the Smartphone, but this function was disabled due to accessibility constraints. Additionally, only one Smartphone Wi-Fi connection can be used at a time, meaning the iPortal web application controlling SmartATRS functionality with the Powerchair joystick and Smartphone cannot be used at the same time as the Camera system. This results in interoperability and availability trade-offs for both systems within the SoS.

To consider the system interactions, a threat model was used to guide the risk assessment to account for potential threats and vulnerabilities. The threat model was based on the “internet threat model” described in RFC 3552 (Rescorla and Korver 2003). This helped to consider potential threats and vulnerabilities carried out by a possible attacker and the potential impact placed upon security goals. Other threat model types could, however, be used to provide a consistent means in which to identify and analyse the potential for security concerns.

5.3.4 Capturing Impacts on Interoperability and Emergent Behaviour

Once the assessment was at the stage of analysing and evaluating related impacts, the effects towards interoperability and emergence considered their impacts towards a specified risk. An example from the risk assessment that demonstrates interoperability and emergence impacts is shown in Figure 5.2.

For interoperability, this specifically demonstrated where the system asset was at risk of interconnection issues with a majority of the SoS, thus losing the ability to control it. It is not uncommon for Smartphones to be integrated as a key system in



Asset	Threat	Vulnerability	Identified Risk	Control	Likelihood (L,M,H)	Impact on Systems	Impact on Interoperability	Impact Level (L,M,H)	Risk Level (L,M,H)	Emergent Behaviour Analysis and Control
Smartphone System	Malware	Email App	Malware infection from email link or attachment causes operating system to not function as expected.	OS updates; Anti-virus updates.	M	All other Smartphone system operations become unavailable with a potential of infecting other systems.	Without smartphone interaction, key elements of the SoS cease to have interoperable communication and functional ability, potentially creating safety issues.	H	H	OS updates reduce system functionality options, e.g. Voice Interaction with Smartphone no longer a feature. Check release notes prior to update.
Smartphone System	Malware	Other App	Malware infection from hidden malicous application obtains or tracks user location and data.	OS updates; Anti-virus updates.	M	Smartphone continues to operate, but may perform at reduced capacity if background activities are power, process or network intensive. Impacts on system and SoS integrity and confidentiality or privacy.	Smartphone remains available and interoperable, unless battery is drained or DoS is performed.	M	M	Smartphone battery is challenged by additional power use. Smartphone battery charged by connections on Powerchair, draining its battery reducing the overall SoS efficacy and longevity between charging. Regularly charge and monitor performance.

Fig. 5.2 Risk Overview with Interoperability and Emergence Analysis

IoT and SoS scenarios, despite the known impact this might have to IoT security (Khan and Shah 2016). This may contribute to the loss of SoS availability and interoperability if the device or operating system is compromised. Privacy could also be compromised if data theft or location tracking malware is inadvertently installed (Mylonas et al. 2011).

The emergent behaviour analysis attempted to uncover unanticipated emergent behaviour that may be associated with the related system interaction, the consequences of which could increase risk if the SoS mission and security goals are not met. HSI considerations would also help inform towards decision making when considering applicable controls and measures to reduce the likelihood of issues arising from emergent behaviour. Emergent behaviour was, however, harder to anticipate due to its unknown and uncertain nature. Stakeholder feedback included in the evaluation considered a previous operating system update offering enhancements to its security and functionality, but this no longer supported voice interaction functions previously used and tested with the SoS. Other updates by the operating system or application providers outside the SoS boundary were therefore considered, as these may have unexpected consequences.

5.3.5 Modelling the SmartPowerchair SoS with CAIRIS

Providing further visual assistance to frame the SoS context, models can help to reason with interactions of a system, and could assist when considering security aspects. To explore the use of tool-support with CAIRIS, whilst identifying how the risk assessment data can be used to support the modelling and visualisation of the SoS, using an asset model was the chosen method to capture the system assets and associations. These could be captured and modelled early in the assessment if required to help with visualisation.

Each system element was entered into CAIRIS as an individual asset, where assets can be of type: information, people, software, hardware, or systems. Security goals for confidentiality, integrity, availability, and accountability are also included within each asset description that can also be environment specific. Although CAIRIS has the ability to situate models in multiple environments as views, a single view was used in this scenario given the single user, owner, stakeholder view of the related systems coming together as a Directed SoS.

Using information from the SoS review, stakeholder discussions, and risk assessment data, initial modelling began by decomposing the SmartPowerchair SoS within its environment using the abstraction stack approach introduced by Simpson and Dagli (2008) to analyse the system parts that make up the whole. For example, starting from its highest level, an abstraction stack of a House is composed of rooms that consists of floors and walls, which in turn is made up from bricks and mortar. For SoSE, this approach can be used to determine then model and represent individual assets and system elements, understanding their position and relevance in the SoS.

However, by following this approach, it was identified that certain systems within the SoS were actually interconnected in a different way compared to the original stakeholder architecture diagram. To support the risk assessment, the user interactions with the SoS were therefore re-modelled to reflect the correct interactions, as was illustrated in Figure 5.1.

Example assets visualised using CAIRIS asset models are illustrated by Figure 5.3 showing a filtered model centred around the Smartphone system and its associations. These models, which are based on UML class diagrams, introduce the notion of associations, aggregations, and composition between an instance of individual components, systems, and the Directed SoS as a whole.

Goal models can also be introduced to associate system goals that need to be satisfied in order for the SoS goals to be achieved. Tasks can also be associated with goals. Tasks represent activities performed, and can relate to the system interactions

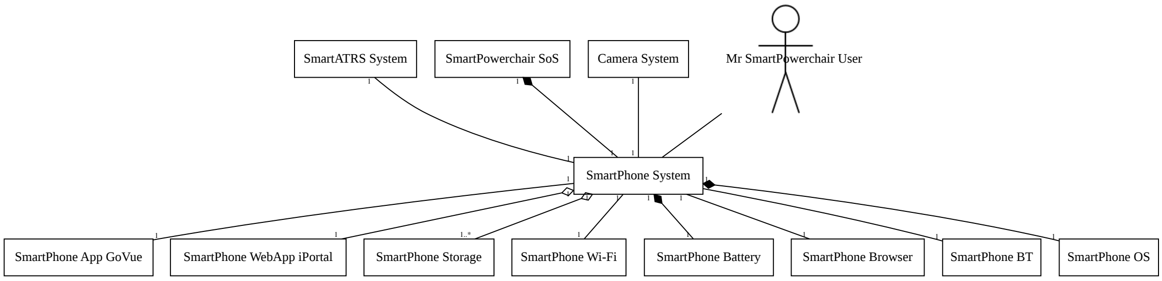


Fig. 5.3 CAIRIS Asset Model - Smartphone System and relations

identified in the risk assessment. Other risk data about assets used in tasks could then be added to the risk model to link the risk to assets in models.

5.4 Application Findings

To assist with the SoS security risk assessment of the *SmartPowerchair*, this approach introduced relevant SoS components addressing HSI, interoperability and emergent behaviour with a view to inform SoSRE. HSI was important towards understanding security concerns of human interaction, and interoperability analysis was found to be significant when determining the overall risk impact level. Risk assessment must, however, be based upon informed knowledge of the SoS context, constituent systems and components to ensure key stakeholders, user and system interactions are considered throughout the process. To help validate this scenario, stakeholder input was provided during both the assessment and closing analysis, specifically where security could be improved and controls may be specified.

5.4.1 HSI and Assessing Security Risk of the SmartPowerchair SoS

Having good stakeholder interaction throughout the process enabled a good understanding towards HSI needs and system assets, and which should be accounted for towards interactions considered within the security risk assessment. Direct interaction with the stakeholder and user of the system made it relatively straight-forward to capture the context and interactions of systems interoperating as part of the SmartPowerchair SoS.

However, when considering the scale and greater stakeholder needs, control, and interactions as was demonstrated with the AMN in Chapter 4, it would be more difficult to interact with all users, meaning other human factors approaches may be required to identify roles and activities critical to the SoS operation, whilst also factoring the different degrees of control. There was also some overlap when applying the risk assessment, as this was accounting for the activities of a single user, whereas an assessment with the AMN or other SoS contexts may need to account for different users interacting with different systems, and their services and information exchange.

In this scenario, the risk assessment focused on systems considered critical to the SoS, and where they may be at risk from something or someone. This was guided by the selected threat models towards questions and considerations for possible threats that may exploit a vulnerability causing a risk that has potential consequences and impacts. This could, however, be supported with other methods in which to identify and characterise potential attackers.

The likelihood and impact levels were assigned to each providing an overall risk score. Given these impacts in the first instance relate to the user and interoperation with related systems, it would have been useful to align the impacts with the HSI categories considered in the early information gathering, whilst making the impact to security goals more explicit. Then as a result of the impacts, how the system is affected, with the resulting effect upon the SoS. To some degree, this would be captured by analysis on interoperability.

Initial findings towards prioritising critical risks suggested the Camera system could be a potential attack vector, although this seemed remote when comparing the threat model for this system; with the remote likelihood of the passive or active attacks described. For example, a man-in-the-middle attack leading to inaccurate or delayed video was deemed unlikely as the attacker would have to shadow the user on-the-move in close proximity, potentially for a long period of time. Moreover, these security issues were unlikely to affect interoperability for the SoS as a whole.

Other threats and vulnerabilities identified the potential of compromising the GoVue application in some way, or accessing, transmitting, modifying and deleting GoVue image files stored on the Smartphone. Although this feature was not currently used, needs might arise where sensitive images could be stored, or information about journey routes and locations could be disclosed. This risk is likely to be minimal, but the authentication restrictions did increase the risk of an in-person attack, or unintentional mistake by the user or their assistant. Furthermore, a version of the GoVue application could potentially be downloaded from one of many unofficial sources listed on a search engine.

All of these example findings were shared with the stakeholder for their feedback, both in the context as an operational user, and as a stakeholder interested in improving the security of the SoS. After discussing the initial findings, it was found the user does not currently consider the risks to security and interoperability related to download sources. This consideration also highlighted that a critical system, which in this scenario was a smartphone, could be used in many ways as a personal device, but when used for a different purpose, this may require compromises or changes in the way it is used in order to increase security and reduce the potential for risks, specifically for the SoS. This was an aspect the stakeholder hadn't considered, as the smartphone was also central to other daily activities. It was, however, accepted that the smartphone was also critical to the SoS achieving its goals, thus helping the stakeholder to now make more informed risk-based decisions towards its dependencies and risk reduction in both contexts.

5.4.2 Analysis of Capturing Impacts on Interoperability and Emergent Behaviour

Interoperability impact at SoS level was considered against each potential risk, as demonstrated in Figure 5.2, providing further consideration towards dependencies and required control measures. For example, if the camera system was no longer interoperable, the SoS would continue to function. Despite the Camera system not appearing to demonstrate significant risks or impact on interoperability, it did highlight a specific attack vector due to consistent interactions and dependencies on most systems of the SmartPowerchair SoS.

If, for example, the Smartphone was compromised in some way, this would have a significant impact on security risks, availability and interoperability at a SoS level. If the Smartphone system cannot communicate with other constituent systems, the entire SoS ceases to function. Therefore, as agreed by the stakeholder, understanding the impact on interoperability at human, information, and system levels could be critical to achieving its SoS goals.

Moreover, in most cases it seems there is a common link between availability being achieved to maintain interoperability. When considering interoperability centres around the ability to interact and communicate, information and data integrity is also a factor, although if the integrity was affected in some way, this would potentially result in issues with its availability, thus indicating a link between security goals and interoperability. The impact of a risk upon interoperability could also align with categories of HSI, meaning that if impacts focused upon HSI categories, these would provide focus towards the range of dependencies placed upon the need for interoperability and the effect of different impacts.

Identifying or predicting emergent behaviour was challenged by the unknown effect of coupling systems into a SoS for a new purpose. However, it was evident this should be an ongoing exercise benefiting from performance monitoring and feedback of current and previous behaviour, which in this scenario, helped identify possible emergence and control measures.

In the example described in Figure 5.2, reviewing future operating system or application updates may be considered. However, updates from third-parties beyond SoS control may be required to ultimately improve system performance and security. This means trade-offs may exist to maintain safety and security in the SoS. Interoperability and emergent behaviour is, however, relatively complex, and requires further analysis and application to understand challenges posed by different SoS types.

In some scenarios, applicable controls may include data loss prevention and remote wiping tools, certainly where physical theft of the device is a potential risk. Policy, process, and security awareness towards permitted usage are other tools that may be incorporated. However, in this scenario, the SoS is managed and controlled by a single IoT user, which highlights a need to consider security for the user at design stage. This also raises the challenge of introducing basic steps and security awareness for IoT users, particularly when the interoperability of the Smartphone system becomes a critical element towards the success or failure of the SoS. Suitable control measures and mitigations also need to consider possible outcomes of steps taken for SoS resilience given the emergent behaviour associated with identified risks.

5.4.3 Modelling with CAIRIS

Using data captured from the risk assessment, this was integrated into CAIRIS to begin exploring the potential for model generation and integration to visualise elements of the SoS. Each of the systems and components were modelled in CAIRIS as assets associated with other relevant system assets composing the SoS.

Modelling the SoS first applied the notion of abstraction stacks to decompose the elements of the SoS. This helped to develop a visual representation of the system structure with an asset model, aligned with the model shown in Figure 5.1 to capture and visualise the interconnections and user interaction within the SoS. The asset model illustrated in Figure 5.3 was useful for reviewing and visualising assets, points of interoperability, and their relations with stakeholders. This indicated how they could be subsequently linked to threats, and modelling the related risks specific to the human and system activities.

The application of models and their outputs were useful when validating the decomposed elements and potential risks with the stakeholder, as the models helped to identify missing systems, components or interrelations, and areas of concern towards the SoS security. Tasks were useful to represent the SoS user interactions, and were helpful towards identifying how they contribute to a goal or goals being achieved or affected by potential security risks to the systems and activities. The risk model was also used and populated by data relating to a threat, vulnerability, an attacker, and a misuse case describing the misuse of the assets assessed used in tasks contributing to goal satisfaction. Furthermore, a benefit of the risk calculation was that in addition to accounting for the likelihood and severity of the risk to an asset, the impact upon the security goals is captured too.

CAIRIS offered useful tool-support for modelling and visualising a Directed SoS with parent-child relationships. It was, however, unclear how this clarity might be achieved with other types of SoS given their differences including levels of centralised management, access, and control, although independent system views could be captured in a separate environment to visualise its interactions and direct interactions with other systems. The use of goal modelling appears to play a central role towards how risk in its different forms may affect the SoS achieving its goals at different levels, where tasks, people, and processes also contribute to the SoS goals being achieved. Further analysis and application to case studies in other domains would, therefore, be useful for validating the effectiveness of CAIRIS as tool-support for eliciting and modelling security risks and their related human factors within a SoS context.

5.5 Chapter Summary

This chapter presented three components of consideration towards their integration within a SoS security risk assessment. This incorporated HSI, interoperability impact analysis, and emergent behaviour evaluation with control measures within a security risk assessment applied. Lessons learned from findings suggest the use of HSI and HF techniques to align with tasks performed in the SoS where resulting risk and impacts are to be captured, could be improved upon within the risk assessment process and tool-supported models. Capturing impacts towards interoperability was a useful exercise, and was found to be a critical aspect on many levels, not only at the more technical machine level, but also between people and their ability to interoperate within the context of the SoS. Detailing emergent behaviour was useful in principle, but in practice was difficult to determine. Although, the process did benefit from stakeholder input based on a previous issue, suggesting that ongoing risk monitoring would likely capture emergent behaviours, and should then feedback into any ongoing risk assessment activities as part of threat intelligence.

The abstraction stack decomposition of systems was applied to the modelling process using CAIRIS to explore risk modelling of security and socio-technical aspects of the SoS. Evaluating the components provided a holistic view of the SoS from which threat-sources and vulnerabilities to security and the SoS could be identified, modelled, and then validated with the stakeholder, thus supporting the SoS risk-based decision making towards mitigating requirements. Validating the process and its components with the stakeholder indicated its potential towards improving the security and safety of people with reduced physical abilities interacting with assistive technologies.

This work made a contribution towards current research challenges to SoSs, and how security risk may be modelled and assessed in a SoS context. This helped to direct further research considering other case study examples aligning SoS factors and tool-support. The research detailed within this chapter aimed to address considerations for RQ2 and RQ3, and helped support RQ1. In support of additional validation of the work within this chapter, peer review was gained through the publication of elements of this work in Ki-Aries et al. (2017a).

Chapter 6

An End-to-End Information Security Risk Assessment and Modelling process to assist RBDM in SoSRE

Chapter 6 introduces *OASoSIS* representing an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE. The OASoSIS framework combines three contributions, the need for which were derived from related literature and SoSs reviews applicable to the research gaps being addressed by the RQs posed. Using steps based on the original format of OA Caralli et al. (2007), this chapter details the steps to be taken throughout the process, providing direction and considerations for each step.

6.1 Introducing OASoSIS

Research and findings described in Chapter 2 suggests there is a gap towards SoS focused security risk approaches, and which integrate tool-support to model and visualise SoS security risk and human factors, helping to bridge the communication gap between operational needs and SoSRE. There are a range of tools or approaches designed for a single system context, but no clear guidance or limited tool-support integrating different techniques and modelling elements to visualise and assess the SoS security consequences in greater detail. Identifying and integrating different elements to suitably visualise these security risks and related human factors in a SoS context is required to account for the independent and interdependent system interactions of a SoS.

6.1.1 Aligning Security Risk Assessment for System of Systems

As identified, the term *System of Systems* can be applied to a number of scenarios with differing scale or complexity of interconnected systems, or geographical boundaries. This was also demonstrated when considering the SoSs in Chapters 4 and 5 where each were quite different, specifically in terms of scale and users.

Moreover, where there is a greater usage and reliance placed upon internet connected technology, geographical separation is becoming common through continued evolution, both in the systems and SoS contexts, and so are no longer entirely unique characteristics towards SoSs. Examples of systems converging to form a SoS may be less or more complex, or have differing levels of management, oversight, and control. Because these considerations are typically greater than that of a single system, the interactions and interdependencies can increase risks at different levels for independent systems, and the SoS as a whole.

However, because there has been little research or guidance towards integrating suitable concepts, models, and techniques that can be aligned towards an end-to-end SoS security risk assessment approach, when combined with associated issues, these make the already difficult problem of Security-RE (Cheng and Atlee 2009) even harder. When accounting for security risk in a SoS, each entity may only know or have access to a certain amount of information about each system in which to assess security risk as a whole. Having detailed information of the SoS interactions as a whole may therefore not be available or achievable in some SoS scenarios, yet we need to understand the given SoS context if we are to identify security risks and mitigating requirements.

Furthermore, without the assurance and warranting trust equations, this makes risk assessment more difficult to accurately determine potential impacts, and mitigations would need to be treated on a higher risk basis, e.g. least privilege, need-to-know. Nevertheless, security and risk should still aim to be assessed for the SoS as a whole, but may need to be performed at an independent system level if there is a weak collaboration with limited, or no useful information to support security risk assessment.

In a typical information security risk assessment within an organisational environment, the assessment view takes a top-down approach looking at the protection of assets under the management and control of the organisation for its own business purposes – its day-job – and outwards towards the third-parties providing services for the organisation and its operations. However, when assessing the security risk related to the SoS interaction, the view is reversed, because in addition to the organisation and technological systems' day-job or originally designed purpose, the assessment now needs to alter its direction of focus to consider the bottom-up interaction into the SoS where the organisation – now an independent system of the SoS – collaborates with other independent systems to achieve a new or higher purpose.

This interaction is in addition to the day-job or the original purpose it was designed for, relating to the physical, technological, and people elements of each independent system and the interoperations between each. What is considered the SoS as a whole, may therefore be constructed with differing degrees of these elements, working together integrating legacy systems with new technology, manual and automated processes.

To address this problem, the characteristics and context of a SoS must, therefore, be captured prior to any risk assessment to establish relevant high-level systems, assets, stakeholders, and users central to the SoS design and operation. A SoS characterisation process can be used to address this problem as a first step of an assessment, with a continued focus towards critical asset interactions as the assessment progresses.

If combinations of threats and vulnerabilities towards the critical information assets were to be realised, the impact assessed would first need to consider the impacts upon the assets and their security goals, along with how and where they are stored, transported, or processed. It should then consider the impact upon the organisation and systems towards the continued ability to interact with the SoS, and how resulting impacts affect the SoS goals being achieved.

Where issues may be identified that could potentially affect the day-job, this should feedback into the organisation's regular risk management and assessment. For example, this may include data storage and network capacity, personnel and manpower. It is, however, critical to identify issues and maintain stakeholder communication where the conflicts towards the day-job goals threaten the overall dependency towards the independent system's continued interaction with the SoS.

6.1.2 Informing Risk-based Decision Making for the System of Systems

Where applicable, the identified SoS risks should be shared and communicated with other independent system stakeholders and risk-based decision makers to determine risk mitigating outcomes, either internally to the organisation or transferred to another independent system. It is from these combined assessment inputs, modelling and visualisation, where the security risk to the SoS as a whole can be determined. However, at minimum, an independent SoI should have an understanding and means to elicit, assess, and mitigate their own SoS risk.

Although many areas of the SoS may be under different levels of management and control, the common link between independent systems to achieve its goals securely is accountability, both internally and externally focused. Accountability begins with each independent system, and should relate to each area of the physical, technical and people interoperations for SoS. Where each organisation may be divided into divisions, areas or departments, who use business processes, manual processes, or software and hardware combinations for technological processes, each of these will have accountability.

From the organisational body itself, down to the user within these system divisions, using physical processes or technological systems, an accountable person would, or at least should be in a role of responsibility throughout this chain. Within the information security risk assessment, information relating to an asset's ownership, responsibility and accountability should be captured. This will aim to identify where dependencies exist and accountability is in place for risk owners to ensure preventative controls are operational, and responsibilities are clear towards implementing reactive countermeasures to ensure a risk (threat & vulnerability) is addressed.

Given the differences in some types of SoSs where participation or complete managerial and operational control of the SoS by an independent system can range from total to none, it may be difficult to determine all information in which to assess the SoS interaction with other independent systems, or where accountability is in place for system interactions, or controls. Therefore, each independent system would need to provide their own assessment related to the SoS interaction. Depending on the strength of the SoS type and collaboration, this should be shared to agree a collaborative approach towards mitigating the risk related to the SoS, some of which may uncover further risks for independent systems that were previously unknown, such as the knock-on effect of risks affecting other SoS goals from being satisfied.

However, independent assessments may produce differing results depending upon the risk assessment processes used. Using a consistent approach across the SoS may not always be possible. For example, some organisations may need to follow ISO27001-5 or NIST approaches, whereas for some smaller organisations, basic standards may instead be followed. In most cases, providing a simple repeatable approach to assess security risk in a SoS context helping to inform RBDM would therefore be an advantage.

6.2 OASoSIS

To address this SoSs research need, OASoSIS has been formulated to represent an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE. This framework incorporates three main contributions to assist the end-to-end process.

This includes a process to provide the SoS characterisation and context, extended from work described by Dahmann and Baldwin (2008) discussed in Chapter 4. This process leads into the second contribution introducing an information security risk assessment process using a modified version of OA for SoSs. This contribution extends and modifies the work originally presented by authors of OA, Caralli et al. (2007).

The risk assessment process and its output is integrated within tool-support from CAIRIS (Faily 2018a) as the third contribution, extending the process for SoS information security risk and human factors modelling, visualisation and analysis.

The main order of Steps within OASoSIS are:

0 - Identify SoS context, structure, stakeholders, roles, goals, and dependencies;

1 - Establish risk measurement criteria;

2 - Develop information asset profile;

3 - Identify information asset containers;

4-5 - Identify areas of concern with threat scenarios, and identify vulnerabilities;

6 - Identify risks;

7 - Analyse risks;

8 - Prioritise critical risks, Model and visualise SoS risks, and Select mitigation approach to risks.

6.2.1 OCTAVE Allegro for Systems of Systems with CAIRIS

The characterisation process described in Chapter 4 forms *Step 0* of OASoSIS to support information gathering required to provide the SoS context under assessment with the modified OA. Continuing with *Step 1* of OA, the standard or suggested Risk Criteria impact area is extended to improve the focus towards socio-technical impacts in a SoS with HFSI – the combination of HFI and HSI elements (National Research Council and others 2007, BAESystems 2010), to acknowledge human factors, human and systems interoperability, and other related impacts of the SoS.

The critical information assets relevant to the SoS, including where they are stored, transported, and processed within the SoS and by whom, can then be captured to identify areas of concern for the potential of threats and vulnerabilities creating security risks to the assets. This would continue to be documented using versions of OA's paper-based worksheets and spreadsheet templates.

Information captured throughout the process can also be used to extend the mitigating requirements analysis and evaluation within OA, providing data for a developmental process, or a process that uses modelling to visualise and analyse risk towards information security and human factors in the SoS design. Once analysed, the effects can be evaluated and assist risk-based decision makers to make informed decisions towards the application of suitable mitigating actions, requirements, and controls.

Risk data may be refined, then modelled with tool-support from CAIRIS as the third contribution, capitalising upon the current CAIRIS concepts and components, whilst aligning their use towards a SoS context within the OASoSIS process. This integrates a goal-driven modelling process with various concepts and techniques to help decision makers towards making informed decisions to reduce security risks and related human factors concerns in the SoS.

For example, this could begin at an early stage when capturing information about SoS stakeholders, independent systems, goals, context and asset use, tasks and processes. Moreover, models can account for where critical information assets are stored, transported, and processed, along with areas of concern towards potential threats and vulnerabilities leading to risk. From analysing the roles, responsibilities, activities, and human interaction with the physical, technical, and people elements, related mitigating controls and requirements can be elicited within the context of the SoS.

When integrating tool-support such as CAIRIS for modelling the SoS, once a new project is created, separate environments can be added to represent the view of an independent SoI and its known and direct SoS interactions. If considering the views and interactions of more than one independent system, it is useful to be clear which assets, goals, and interactions should be situated within each environment prior to adding new elements to each environment.

Each environment or view can then be constructed based upon all known direct interactions with internal and external systems as assets. Roles and personas can be created representing the people element. Tasks are used to document the activities carried out by a persona, for which use cases can be used to represent the process steps of the task, and data flows can be mapped with the Data Flow Diagram.

Goals and Obstacles towards enabling the completion or obstruction of processes and tasks for the SoS mission goals can also be created, whilst providing the ability for operationalising tasks. Combining obstacles and goals can provide an element of addressing threats and vulnerabilities, although these are specifically considered using the Risk model, with attacker roles included with a supporting misuse case.

These and other models within CAIRIS can be shared and discussed with stakeholders refining the system interactions, leading to countermeasures, controls and requirements as an output from the elicitation, visualisation and assessment of the risk towards security and human factors within the SoS interaction. These may feed directly back into the completion of the OASoSIS process, whilst providing a platform for on-going assessment of the SoS security risks that will change overtime as the SoS evolves or dissolves. Models can, however, be quickly updated to consider changes to the SoS and resulting security risks.

6.3 OASoSIS Process Steps

The steps presented in this section were based upon the original format by authors of OA (Caralli et al. 2007), and demonstrates the modified SoS approach to the context of use, whilst indicating how models, concepts, and techniques can align with tool-support such as CAIRIS. Each of the steps indicates high-level decisions, considerations for completing tasks within each step of OASoSIS, and how the data captured within the OA worksheets discussed in Appendix B can support the assessment and modelling of the information security risk and human factors within the SoS using a tool such as CAIRIS. A Step Completion Criteria is provided for the assessor to validate each step has been performed as expected.

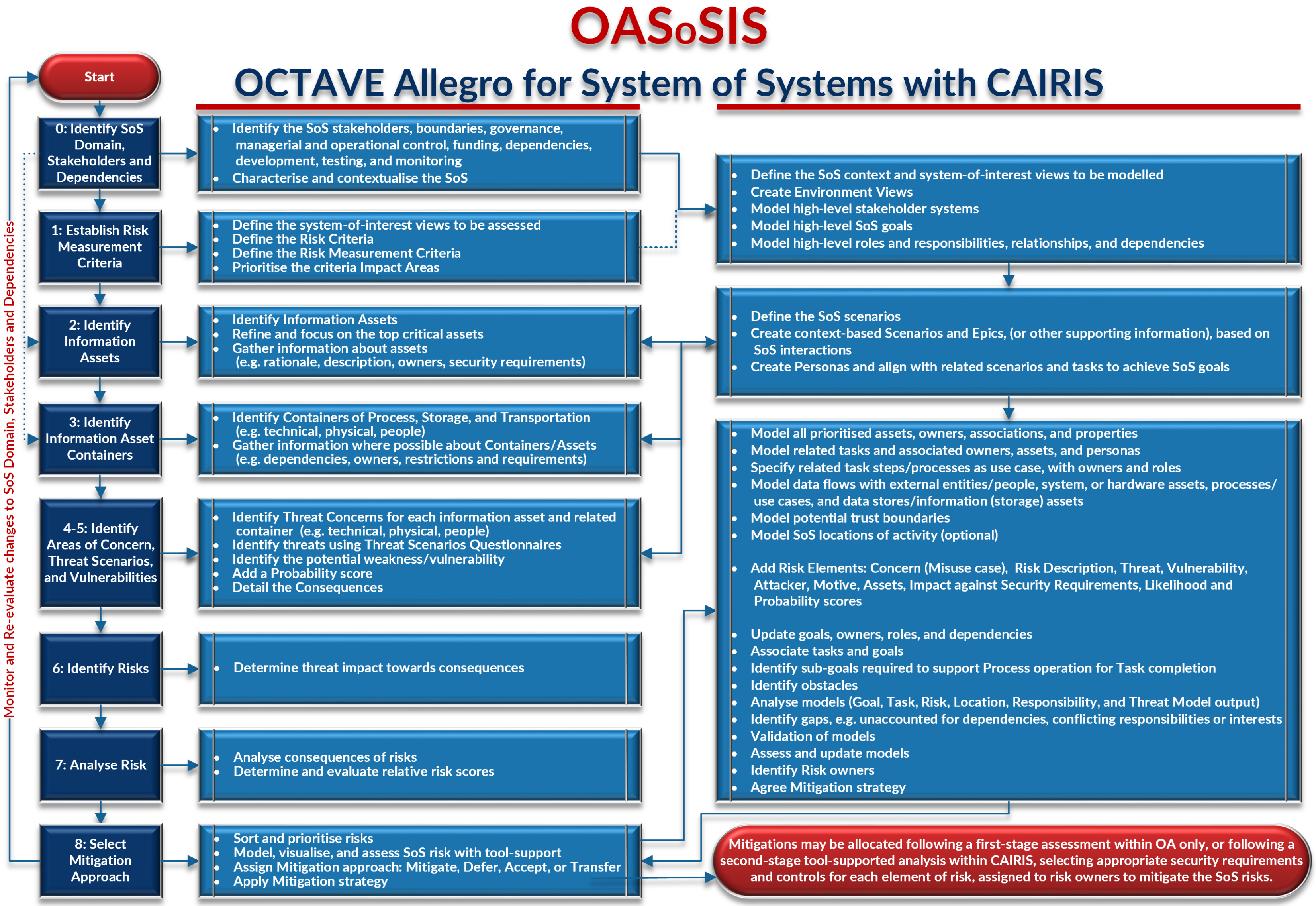
The OASoSIS process can be used in part or in full, and be used by different stakeholders. For example, in the first instance, the characterisation process and the modified OA element of the process can be used in an organisational context as a repeatable means for carrying out a high-level SoS information security risk assessment. This could therefore be performed by stakeholders of the SoS SoI with the relevant authority and expertise such as the Compliance and Risk Management team, the Information Security team, or as historically been the case, the IT team. Relevant roles are therefore defined as being *The Assessor*, under the authority of the organisational independent SoI to perform the SoS information security risk assessment.

Once achieving *Step 8* and mitigating controls have been agreed between stakeholders, the process may end, then be repeated and updated when required. Furthermore, this output may be passed to design and engineering stakeholders as input for SoS engineering purposes, continuing the OASoSIS process of modelling and visualising risk towards information security and human factors in the SoS, supporting the elicitation and specification of mitigating requirements and controls.

The OASoSIS process is, however, formulated with a focus towards SoSRE and RBDM, to be used by design and engineering teams for end-to-end information security risk assessment with modelling and visualisations centred around the SoS assets, and associated tasks, processes, goals, and risks. Users of OASoSIS would therefore individually or combined have an appropriate level of expertise towards the application of different models, and the assessment of security risk. Relevant roles in this context are also defined as being *The Assessor*, under the authority of the organisational independent SoI to perform the end-to-end SoS information security risk assessment for SoSRE supporting RBDM.

The end-to-end process would use the characterisation process and OA element of risk assessment for data collection and prioritisation of identified areas of concern and potential risks in the SoS. Then, extending *Step 8*, a more focused second-stage analysis through modelling and visualisation with tool-support such as CAIRIS provides a means for risk-based decision makers to identify and agree suitable risk mitigations for the SoS's context. In addition to the flexibility of the process application, different combinations of models may be used dependent upon the context or needs of assessors to determine mitigating requirements for the SoS interaction. The tracebailtiy afforded through using CAIRIS, along with its in-built validation checks provides further validation towards the output of the OASoSIS assessment.

Given the possibilities of use for OASoSIS, the following steps detail the required stages for completion of the OA element of the SoS information security risk assessment. This includes an indication towards the risk-based decision makers and other supporting stakeholders for each step, and how the information gathered within each step can contribute to modelling with tool-support. A high-level overview of the main steps is illustrated in Figure 6.1. How tool-support from CAIRIS can be used to model and visualise the SoS information security risk and human factors is then detailed in Section 6.4.



OASoSIS

OCTAVE Allegro for System of Systems with CAIRIS

Start

0: Identify SoS Domain, Stakeholders and Dependencies

- Identify the SoS stakeholders, boundaries, governance, managerial and operational control, funding, dependencies, development, testing, and monitoring
- Characterise and contextualise the SoS

1: Establish Risk Measurement Criteria

- Define the system-of-interest views to be assessed
- Define the Risk Criteria
- Define the Risk Measurement Criteria
- Prioritise the criteria Impact Areas

2: Identify Information Assets

- Identify Information Assets
- Refine and focus on the top critical assets
- Gather information about assets (e.g. rationale, description, owners, security requirements)

3: Identify Information Asset Containers

- Identify Containers of Process, Storage, and Transportation (e.g. technical, physical, people)
- Gather information where possible about Containers/Assets (e.g. dependencies, owners, restrictions and requirements)

4-5: Identify Areas of Concern, Threat Scenarios, and Vulnerabilities

- Identify Threat Concerns for each information asset and related container (e.g. technical, physical, people)
- Identify threats using Threat Scenarios Questionnaires
- Identify the potential weakness/vulnerability
- Add a Probability score
- Detail the Consequences

6: Identify Risks

- Determine threat impact towards consequences

7: Analyse Risk

- Analyse consequences of risks
- Determine and evaluate relative risk scores

8: Select Mitigation Approach

- Sort and prioritise risks
- Model, visualise, and assess SoS risk with tool-support
- Assign Mitigation approach: Mitigate, Defer, Accept, or Transfer
- Apply Mitigation strategy

- Define the SoS context and system-of-interest views to be modelled
- Create Environment Views
- Model high-level stakeholder systems
- Model high-level SoS goals
- Model high-level roles and responsibilities, relationships, and dependencies

- Define the SoS scenarios
- Create context-based Scenarios and Epics, (or other supporting information), based on SoS interactions
- Create Personas and align with related scenarios and tasks to achieve SoS goals

- Model all prioritised assets, owners, associations, and properties
- Model related tasks and associated owners, assets, and personas
- Specify related task steps/processes as use case, with owners and roles
- Model data flows with external entities/people, system, or hardware assets, processes/ use cases, and data stores/information (storage) assets
- Model potential trust boundaries
- Model SoS locations of activity (optional)

- Add Risk Elements: Concern (Misuse case), Risk Description, Threat, Vulnerability, Attacker, Motive, Assets, Impact against Security Requirements, Likelihood and Probability scores

- Update goals, owners, roles, and dependencies
- Associate tasks and goals
- Identify sub-goals required to support Process operation for Task completion
- Identify obstacles
- Analyse models (Goal, Task, Risk, Location, Responsibility, and Threat Model output)
- Identify gaps, e.g. unaccounted for dependencies, conflicting responsibilities or interests
- Validation of models
- Assess and update models
- Identify Risk owners
- Agree Mitigation strategy

Mitigations may be allocated following a first-stage assessment within OA only, or following a second-stage tool-supported analysis within CAIRIS, selecting appropriate security requirements and controls for each element of risk, assigned to risk owners to mitigate the SoS risks.

Monitor and Re-evaluate changes to SoS Domain, Stakeholders and Dependencies

Fig. 6.1 OASoSIS

6.3.1 Step 0

Decisions: Agree Area of Focus and Views within the SoS.
By: The Organisation/System, SoS Stakeholders, The Assessor.

Step 0-Task 1

To provide the SoS context and classification, the newly added Step 0 considers initial questions to frame the SoS, its mission and goals. When asking these questions, information may begin to be captured using Master sheets 1-3, identifying SoS roles, relationships and dependencies, organisational systems and containers, likely information assets, business owners of goals, processes, tasks, information assets and their related information custodians and other system owners, and any other related restrictions. Systems' day-job goals and potential conflicts should be noted. Also consider relevant naming conventions for all assets documented through the risk assessment, as assets will relate to multiple stakeholders.

Initial questions should consider:

- Who are the high-level stakeholders - the main independent systems of the SoS?
- Who are the other relevant stakeholders important to the SoS achieving its mission?
- Who provides management oversight and control?
- Who provides operational control of the SoS?
- Who provides governance?
- Who provides funding within the SoS?
- What system boundaries exist for the SoS - do restrictions apply?
- Who is responsible for SoS design, development, testing and implementation?
- What system dependencies or specific requirements exist for the SoS?
- What Trust mechanisms are in place or required?
- How is on-going SoS performance and behaviour monitored to provide a resilient SoS balancing independent system needs?
- Consider the classification type of this SoS.
- Do other SoSs exist within this SoS?
- Do any other challenges or conflicts exist for the SoS interaction?

Step 0-Task 2

Using information collected in Task 1, identify the main independent systems where managerial and operational control is provided. By aligning the SoS characterisation with the examples shown in Figure 4.2, this may be used to determine the type of SoS under consideration, framing important aspects that are useful for SoSRE and risk-based decision makers where there is a focus towards ownership, accountability, and responsibilities within the SoS to achieve its goals. This is considered later in the process.

Step 0-Task 3

Tasks 1 and 2 provided the SoS context in which the area of focus for the SoS views should be agreed. Confirm the SoS mission and goal, and identify the related goals of independent systems and stakeholders in which the SoS collaboration depends upon. Agree the scope of the SoI and continue to Step 1.

Step Completion Criteria

Confirm the following points:

- ☐ It is clear who and where the roles of managerial and operational control are provided for the SoS.
- ☐ It is clear who and where ownership, accountability, and responsibilities are designated within the SoS to achieve its goals.
- ☐ The SoS goals and supporting goal requirements have been indicated.
- ☐ All other initial questions have been answered.
- ☐ All related details are captured in the data templates.
- ☐ Conflicts and dependencies are clearly detailed.
- ☐ The scope for the assessment area of focus and SoI views within the SoS have been agreed.

The scope of organisation/system and its SoS interaction will be the focus for the risk assessment. The assessing authority must ensure the required expertise is provided to perform the assessment. However, this process may also be used by other levels of the organisation/system to provide further detail. For example, by department, division, or any other sub-level related to the organisation, system or SoS. This may also be adopted by other independent systems of the SoS to provide further consistency.

The Risk Criteria should therefore relate to the level assessed. Once this is agreed, the Risk Criteria in Step 1 may be defined and agreed, then Information Asset identification can commence for Step 2. Both of these steps can be completed separately, but both must be complete before Step 3.

Inputs for Modelling and Tool-Support, e.g. CAIRIS:
Master Sheets 2 & 3 provide Assets, with further Organisations in Master Sheet 1. Master Sheet 1 provides information on Roles, Relationships, and Dependencies. Step 0 may also provide certain Goals and Tasks.

6.3.2 Step 1

Decisions: Agree System or SoS risk measurement levels. Agree System or SoS levels of priority for the Impact Areas.
By: The Organisation/System, SoS Stakeholders, The Assessor.

Step 1-Task 1

Once the SoS context and systems-of-interest views to be assessed have been agreed, document the Risk Measurement Criteria in Master Sheet 4. The criteria categories includes a range of SoS and Human Factors System Integration impacts to be considered as shown in Table 6.1. Elements of the criteria may be modified or added to if required. Based on the criteria impact areas, define a qualitative set of measures for the Risk Measurement Criteria. This will be used to evaluate the impact of the risk on the organisation helping to determine the impact on meeting the needs of the SoS mission objectives.

Table 6.1 Risk Criteria with HFSI Elements based on (National Research Council and others 2007, BAESystems 2010)

Criteria	Example
Financial Costs and Losses	As a result of the impacts specified in the risk criteria, this is the likely cumulative amount of costs and losses, e.g. from loss of revenue, extra manpower, replacement or re-development of assets, systems, or other physical and technical processes, policy and procedure. If it is possible to quantify the financial impact of reputational losses, this should be included. In some cases, this may not be clear. Note: The Costs and Losses figure could exclude any Fines and Penalties, as this is accounted for separately.
Fines and Legal Penalties	As a result of a data breach, regulatory fines, for example, under the General Data Protection Regulations may be issued, with a possibility of other legal liabilities.
Reputation and Customer Confidence	Trust and reputation of the organisation, systems, and SoS as a whole can be negatively impacted by an incident resulting in the loss of confidence by customers, users, or other dependent systems.
Manpower and Personnel (Productivity)	Manpower and personnel requirements could reflect the number of military, government, civilian, or contractor personnel required, including the cognitive and physical capabilities required to train, operate, maintain, and sustain systems within the SoS.
Social and Organisational	The consideration of the characteristics of systems focused on satisfying the reliance on social aspects that interact with process and technology.
Human Factors Engineering	HFE considers the integration of human characteristics into system definition, design, development and evaluation to optimise human machine performance under operational conditions.
Training	The instruction or education and on-the-job or unit training required to provide personnel and units with their essential job skills, knowledge, behaviours, and attitudes.
Safety, Health and Environment	Environment, Safety and Occupational Health (ESOH) Hazards – The minimisation of human or machine errors or failures that cause injurious accidents.
Habitability	The consideration of the characteristics of systems focused on satisfying personnel needs that are dependent upon physical environment, such as berthing and hygiene.
Survivability	The characteristics of a system that can reduce fratricide, detectability and probability of being attacked, and can minimise system damage and human injury.

If the organisation has already developed a Risk Measurement Criteria, it can be used in the risk assessment, but should still maintain human factor considerations towards impact. Although this criteria is likely to represent the impact on the organisation/system-of-interest related to the SoS interaction, how that affects its own needs against the continued ability of interaction with the SoS should be the overall focus. The output may therefore feed directly back into its own internal risk assessment process for the organisation or system's day-job, whilst accounting its SoS risks.

Step 1-Task 2

Prioritise all of the impact areas from the Risk Criteria in order of importance to the organisation and its SoS interaction by using the Impact Area Ranking in Master Sheet 4.

For example, if you have ten impact areas, rank the most important area as number 10, and the least priority set to 1.

Conflicts may need to be agreed (e.g. Safety vs Manpower ranking).

Step Completion Criteria
Confirm the following points:

- □ Risk criteria impact areas have been agreed.
- □ Qualitative measures for levels of impact for each of the criteria impact areas have been defined.
- □ Priority levels for each of the criteria impact areas have been defined.

Inputs for Modelling and Tool-Support, e.g. CAIRIS:
This OA step is completed outside of CAIRIS, as Severity is calculated in a different manner. The level or range of Impact can however be aligned.
For example, Negligible 0 - Marginal 1 - Critical 2 - Catastrophic 3.

6.3.3 Step 2

Decisions: Agree Critical Information Assets for the SoS. Confirm Critical Asset SoS relations. Confirm Accountable Owners.
By: The Organisation/System, SoS Stakeholders, The Assessor.

Step 2-Task 1

The purpose of this step is to identify all related information assets dependable to the SoS interaction. Some of these may already have begun to be captured in Step 0 using Master Sheet 3. The focus will then be to determine which of the information assets are most important to the system / SoS interaction. User-centred techniques such as task analysis, scenarios, and personas may also be adopted to consider related human factors towards important user and asset interactions.

Ideally with a range of SoS stakeholders, perform activities such as brain storming or other techniques to identify the related information assets that are important to the organisation and its SoS interaction. For example, this could be within a focus group setting. You can begin to add this information to Master Sheet 3.

Consider the following questions:

- What information assets are used in supporting processes and operations for the SoS?
- What information classifications are there (e.g. TOP SECRET)?
- What information assets would significantly disrupt the organisation and the SoS interaction if accessed, modified, shared, lost or destroyed?
- What other assets are closely related to or dependent upon these assets?

Information assets directly related to or under control of the assessing organisation or system may already be documented under its current ’day job’ role. For example, an asset register, or details of a Data Protection Impact Assessment (DPIA). These or other supporting information can be used to assist this element of the process. However, they should be considered towards their additional interaction with SoS needs, identifying where conflicts may arise. Externally received information assets used for SoS purposes may also be documented if there is accountability towards its process, storage and transport under the control of the assessing system.

Step 2-Task 2

When identifying related information assets towards the SoS interaction, it is possible quite a number may be identified, some in greater detail, and some of which may have a greater element of risk of an adverse impact to the asset or the SoS. As a means of prioritisation, focus the risk assessment on assets deemed critical to the SoS interaction, whilst considering related restrictions and dependencies.

To determine which information assets are considered critical to the SoS interaction, consider which of the identified information assets in Master Sheet 3 would have an adverse impact on the organisation and its SoS interaction if assets were subjected to:

- Unauthorised access, use, modification, or disclosure;
- Loss or destruction;
- Disruption or loss of availability.

Where assets critical to the organisation and its SoS interaction are potentially affected by these scenarios, these critical assets become central to the risk assessment. Update Master Sheet 3 highlighting the asset's criticality.

Step 2-Task 3&4

In subsequent tasks of Step 2, further information gathering is required about the information asset. Continue entering this information directly into Master Sheet 3, or use Information Sheet(s) 1 if preferred for a paper-based activity.

Some information may already have been captured in Master Sheet 3. If required, use Information Sheet(s) 1, or continue updating Master Sheet 3 to record the asset information in more detail. For example, begin with the name of the critical information asset, and consider its classification (e.g. TOP SECRET), description, rationale, owners, restrictions and dependencies. Consider information that will assist with demonstrating its value and criticality to the SoS.

Initial questions to consider are:

- Why is this asset critical to the organisation, systems, or SoS?
- What dependencies exist for the SoS interaction, and to what degree?
- Is this critical information asset subject to regulatory or cross-border requirements? - If so, what are these?

Step 2-Task 5

When describing the critical information asset, be clear on its scope and importance to the SoS interaction.

The following points should be considered when describing the critical asset:

- Is this information used inside or outside of your control?
- How is it used and for what purpose?
- Is this critical information asset a person, physical or electronic?
- Indicate where specific regulations and requirements exist.
- Indicate the internal and external dependencies towards cross-boundary organisational processes or services used by or supporting this critical information asset for the SoS interaction.

Step 2-Task 6

Identify and document the owners of the critical information asset. This includes business owners, specific roles, and people responsible and accountable for the asset.

Consider the following questions when you are documenting the critical information asset owners:

- Which organisation is specifically responsible and accountable for this critical information asset, and at what stages?
- Is there cross-boundary/organisation shared accountability for this critical information asset?
- Who in the organisation is specifically responsible and accountable for this critical information asset?
- Which organisation, role and person are responsible for determining the value of this critical information asset?
- Who determines the security requirements?
- Which organisations, roles and people are responsible and accountable for each business processes where this critical information asset is used?
- What dependencies exist in relation to the critical information asset for both the organisation and SoS interactions?

- How would the impact of a comprise to the critical information asset affect the organisation and its continued ability to interact with the SoS?

Where possible, all related stakeholders of the critical information asset (owners, custodians, controllers, processors) should be involved within the decision making towards defining the asset. For example, related stakeholders should provide input towards the critical assets' security goals, needs and requirements. Later steps will help provide further focus towards related stakeholders.

Step 2-Task 7

Detail the Security Requirements of Confidentiality, Integrity, Availability, and Accountability for each critical information asset. If there is cross-boundary/organisation shared accountability for a critical information asset, these security requirements should be captured. Some conflicts may arise.

Detail the security requirements for each critical information asset. If applicable, detail other related requirements. Identify the most important security requirement for each critical information asset by noting the rationale. This will be considered later where risks may impact upon these areas, and additional requirements and controls must hold.

Security requirements for critical information assets are usually derived from legal & regulatory requirements, business policy, related procedures, or other contractual terms of engagement.

Step 2-Task 8

Ensure that information collected using Information Sheet 1 is entered into Master Sheet 3.

Step Completion Criteria

Confirm the following points:

- □ Information assets deemed critical to the SoS interaction have been identified and detailed with a rationale.
- □ Ownership, accountability, and responsibilities for each of the critical information assets deemed critical to the SoS interaction have been identified and detailed.
- □ Dependencies, restrictions, and other related requirements for each of the critical information assets deemed critical to the SoS interaction have been identified and detailed.
- □ Security goals and requirements have been detailed and prioritised for each of the critical information assets with a rationale.

Inputs for Modelling and Tool-Support, e.g. CAIRIS:
Master Sheet 3 (or Information Sheet(s) 1) provide further Information Assets.
This includes Owners and areas of Accountability, and Security Requirements.
Step 2 may also provide data for certain Goals, Tasks, and Personas.

6.3.4 Step 3

Decisions: Agree Known Critical Asset Containers across the SoS. Confirm Container Security Restrictions. Confirm Accountable Owners.
By: The Organisation/System, SoS Stakeholders, The Assessor.

Step 3-Task 1

Information Asset Container – *An information asset container is where information assets are stored, transported, or processed. It is a place where an information asset 'lives'. Containers generally include hardware, software, application systems, servers, and networks (technology assets), but they can also include items such as file folders (where information is stored in written form) or people (who may carry around important information such as intellectual property). They can also be both internal and external to an organisation* (Caralli et al. 2007).

Use the information assets listed in Master Sheet 3 (and/or Information Sheet(s) 1) with the Information Sheet 2 Guide to identify all containers where critical information assets are stored, transported, or processed.

Consider internal containers directly under the control of the organisation/system, and external containers controlled by other organisations/systems of the SoS. Identify any other external areas relating to the critical information asset, e.g. off-site physical or electronic data storage, or areas of the supply chain. Group these by owner and parent system, then by sub-system.

- Identify the internal and external *Technical* containers where each critical information asset is stored (usually electronically), transported (transmitted), or processed (usually electronically).
- Identify the internal and external *Physical* containers where each critical information asset is stored, transported, or processed (usually manually).
- Identify the internal and external *People* containers where each critical information asset is stored (e.g. in memory), transported (e.g. communicated), or processed (e.g. cognitively).

Based on the critical information assets listed in Master Sheet 3, add or update details of their containers to Master Sheet 2. For paper-based activity, use Information Sheets 2a, 2b, and 2c. Document the container information in as much detail as possible. Some of this information will also be used in Master Sheet 5 detailing the critical information asset and container combinations with areas of concern.

Ensure that information collected using Information Sheets 2a, 2b, and 2c is entered into Master Sheet 2. Document the owner(s) responsible and accountable for the containers applicable to the critical information assets, and where possible, capture the organisational roles of internal and external owners.

Communicate with relevant stakeholders where possible to determine details of the internal and external containers. This relationship will be important towards applying related security controls and requirements across the SoS when required. Consider how mitigation dependencies on other organisations and systems of the SoS will be managed.

Step Completion Criteria

Confirm the following points:

- □ All internal and external containers where critical information assets are stored, transported, or processed have been identified and detailed with a rationale.
- □ Owners responsible and accountable for the containers related to the critical information assets have been identified and detailed.
- □ Organisational roles of internal and external container owners, users and tasks have been identified and detailed where possible.
- □ Security restrictions and requirements for containers have been identified and detailed where possible.

Inputs for Modelling and Tool-Support, e.g. CAIRIS:

Master Sheet 2 (or Information Sheet(s) 2a,b,c) provide further System Assets.

This includes Owners and areas of Accountability.

Step 3 provides Information and System Asset Associations.

Step 3 may also provide certain data for Use Cases, Data Flows, Goals, and Tasks.

6.3.5 Steps 4&5

Decisions: Agree Asset Container Threat combinations. Agree the Probability score.

By: The Organisation/System, SoS Stakeholders, The Assessor.

Steps 4&5-Task 1

Once the containers of critical information assets have been identified, consider any related security risk-based areas of concern towards each container associated with the critical information asset. Use details from Master Sheets 2 & 3 (or with Information Sheets 1, and 2, 2a, 2b, or 2c) to record any areas of concern directly into Master Sheet 5 (or for paper-based activity use Information Sheet 3). Use Information Sheets 3a, 3b, and 3c to guide possible threat scenarios and questions to consider.

Using Master Sheet 2 (or Information Sheets 2a, 2b, and 2c), review each of the containers listed to drive discussion and decision making towards potential areas of concern.

Document each area of concern that you identify on Information Sheet(s) 3, and/or directly into Master Sheet 5. Identify the name of the critical information asset and container from Master Sheets 2 & 3 (or with Information Sheets 1, and 2, 2a, 2b, or 2c) and document the area of concern and related information in as much detail as possible. Use a separate entry for each potential area of concern, and each individual threat and vulnerability combination identified.

Using Information Sheet(s) 3, and/or Master Sheet 5, each entry will uniquely capture a single risk, thus equating to several entries or information sheets completed throughout the risk assessment. It is therefore important to ensure paper-based activities are collated correctly.

Steps 4&5-Task 2

Use the threat scenarios in Information Sheets 3a, 3b, and 3c to guide the areas of concern.

For each area of concern that you have recorded, the threat scenario questions in Information Sheets 3a, 3b, and 3c used earlier in the process will help to identify the actor, means, motive, and outcome. Complete as much details as possible. If you find that you have answered ‘yes’ to a question, but cannot apply it to a realistic scenario, it is potentially not a risk (or at great risk), so move to the next concern.

Using Master Sheet 5 (or Information Sheet 3), detail how the threat would affect the security requirements of the critical information asset. Continue to perform this activity for each threat and vulnerability combination of the area of concern. The remaining risk information will be gathered in a later step.

Threat categories within the OA threat model illustrated in Figure 6.2 demonstrates the decomposition of an actor’s threat motive, type, and consequences impacting upon security properties of a critical information asset.

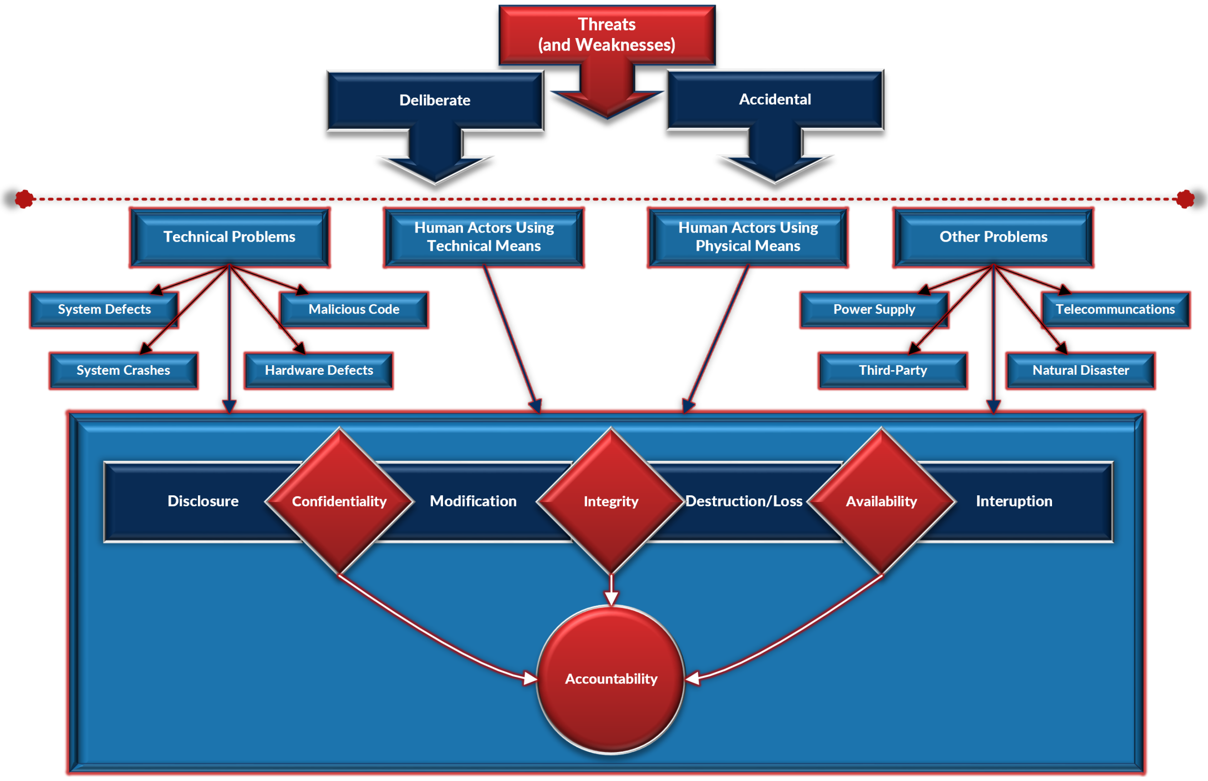


Fig. 6.2 OA Threat Model

Steps 4&5-Task 3

A single container may result in the identification of one or more areas of concern, each of which may have one or more threat and vulnerability combinations. If a specific vulnerability cannot be described, attempt to identify the general weakness that may have enabled the threat success.

Continue to work through each of the critical information asset and container combinations identified. Detail as many areas of concern as possible with their threat and vulnerability combinations.

If using Information Sheet 3, ensure all information is added to Master Sheet 5.

Steps 4&5-Task 4

Considering the Probability of a concern occurring helps to determine which of the scenarios are more likely given the operating contexts. However, as SoSs are often unique collaborations, this may be a challenge to fully determine at times. This information will, however, assist with the prioritisation of risk mitigation activities. Probability is considered by a higher or lower score, for where there is a high and low likelihood of the event occurring. The scale used is as follows:
Incredible 0 - Improbable 1 - Remote 2 - Occasional 3 - Probable 4 - Frequent 5

Assign a probability to each of the threat combinations identified.

Step Completion Criteria
Confirm the following points:

- □ Potential areas of concern towards internal and external containers where critical information assets are stored, transported, or processed have been identified and agreed.
- □ Threat scenarios have been applied and reviewed for each area of concern, identifying the actors, means, motives, and outcomes of individual threat and vulnerability combinations identified.
- □ The effect of each threat and vulnerability combination upon the security requirements of the critical information assets have been identified for each area of concern.
- □ Each threat and vulnerability combination has applied a probability estimation towards the likelihood of it occurring, supporting the prioritisation of each area of concern.

Inputs for Modelling and Tool-Support, e.g. CAIRIS:
Master Sheet 5 (or Information Sheet(s) 3, 3a,b,c) provide Risk Elements.
These are: Concern (Misuse Case Narrative), Risk Description, Threat, Vulnerability, Attacker, Motive, Impact against Security Requirements, Probability of Impact.
Steps 4 & 5 provide certain data for Roles, Tasks, Use Cases, Data Flows, Obstacles, Misuse Cases.

6.3.6 Step 6

Decisions: Agree Impacts on Information Assets.
By: The Organisation/System, SoS Stakeholders, The Assessor.

Step 6-Task 1

Consider, if the event occurred, what would be the consequential impact directly attributed to the organisation and its SoS interaction? How will this affect the SoS? Align impacts with the areas detailed in the Risk Criteria. This should account for the impact on the critical information asset and the container combination that is being assessed, and how that impacts upon the organisation and its continued ability to interact with the SoS, which helps identify the impact to the SoS achieving its goals.

Using Master Sheet 5 (or Information Sheet 3):

- Determine how the organisation and its SoS interaction would be impacted if this threat scenario was realised.
- Describe each consequence for the threat and vulnerability combination of the area of concern. This may help decompose the area of concern providing a refined risk title or description.

Step Completion Criteria
Confirm the following points:

□ Consequences from the impact of the threat and vulnerability combination have been identified, detailed, and aligned with the Risk Criteria categories for each area of concern.

□ This captured the impacts on the critical information asset, the container combination, the independent SoI, its continued ability to interact with the SoS, and subsequent impacts to the SoS.

Inputs for Modelling and Tool-Support, e.g. CAIRIS:
Step 6 is specific to Impacts on the OA Risk Criteria, but provides further consequence information.

6.3.7 Step 7

Decisions: Agree Impact on System or SoS Assessed. Agree Impact on SoS Interaction. Agree the potential Risk conflicts and priorities.
By: The Organisation/System, SoS Stakeholders, The Assessor.

Step 7-Task 1

From each consequence described, this should enable the level of severity of the impact to be measured against the Risk Measurement Criteria in Master Sheet 4. Severity levels are: *Negligible 0 - Marginal 1 - Critical 2 - Catastrophic 3 (Multiplied by the Criteria Priority)*

Confirm the level of severity for all impacts to the criteria categories detailed in Master Sheet 4. Select the related impact levels for all impact areas in Master Sheet 5 (or Information Sheet 3) to help determine a relative risk score.

Step 7-Task 2

When each of the levels of severity have been agreed, each level multiplied by its priority level will produce a score providing an indication as to its overall effect. The total impact scores are then multiplied by the Probability score to provide an overall relative risk score that can be compared and prioritised for further mitigating action.

- Calculate the score for each category impacted as detailed in the Risk Criteria of Master Sheet 4. Use the impact value of each threat and vulnerability combination, then multiply this by the category priority level number to return a score.
- Repeat this for each category, adding each score to create a total.
- Multiply the first total score by the Probability score to give an overall likelihood and severity risk score of the impact on the asset.
- Begin to identify those risks with a higher impact score, then contrast this with the overall score with probability to gain an indication which risks may need more immediate attention.

It should be noted the scores are only used to indicate a scale of potential risk for prioritisation purposes. Scores may differ where elements of the Risk Criteria in Master Sheet 4 are added or removed. For example, with ten areas ranked from 1-10, this equates from 0 to a maximum severity impact of 165, or 825 with probability, and can therefore be grouped into bands of priority of concern. If the criteria only had five areas, these maximum scores would be lower, but could still be grouped by relative bands. This may, for example, first group by probability scores, then sub-prioritise based on the impact only score.

The levels of concern may also differ, for example, one risk with a high probability with a lower impact, compared to a low probability with a higher impact, which may also indicate other patterns and anomalies. Furthermore, an impact or outcome may affect the organisation or system differently by comparison to the SoS as a whole. These type of considerations should also be taken into account when determining how the SoS will be affected. How risks are prioritised may therefore be context specific.

Based on the information gathered and assessed, the entire context should be taken into account before moving to Step 8, as this may highlight particular risks of interest to consider in Step 8.

Step Completion Criteria

Confirm the following points:

- ☐ For each area of concern, aligning with the previously prioritised risk criteria categories, the estimated level of severity for the identified impacts have been applied to each category.
- ☐ Each applied level of severity has been multiplied by its category priority level to produce a category score relative to the risk criteria.
- ☐ The total impact scores for each area of concern have been multiplied by the probability score to provide an overall relative risk score.
- ☐ In addition to the indicated areas of higher concern, high impacts with lower likelihoods, and low impacts with higher likelihoods, and other risk-related conflicts have been highlighted for review.

Inputs for Modelling and Tool-Support, e.g. CAIRIS:
Step 7 can provide an indication which of these Critical Information Assets and their Containers/System Assets need further attention. When modelling Information Assets in CAIRIS, all may be modelled, or this step can indicate which elements to give specific focus to model in further detail.

6.3.8 Step 8

Decisions: Agree Mitigation Strategy, and Security Requirements, External Conditions, Potential Controls, and Residual Risk.
By: The Organisation/System, SoS Stakeholder, The Assessor.

Step 8-Task 1

The purpose of this step is to prioritise the identified risks for further action. Ideally all risks should be reviewed to at least consider which are within or outside of direct control of the SoI within the SoS. Many risks may, however, be identified requiring a means in which to make risk-based decision towards the risks, where further modelling and investigation may be required before mitigating requirements and controls can be determined.

There are a number of ways risk scores can be divided from highest to lowest. For example, OA suggests a method of separating the risks into four pools with equal number of risks. The risks with the highest score go in Pool 1, and so on. Or, as suggested, first prioritise by overall score, then sub-prioritise by scores of impact only.

In this instance, (with ten impact areas, impact levels 0-3, and probability levels of 0-5) scores can also be considered using an impact band of 0 - 55 - 110 - 165, and/or the band with probability equates to 0 - 165 - 330 - 495 - 660 - 825.

Organise and prioritise the risks for further action using the chosen relative bands.

Step 8-Task 2

Decide how the chosen risk bands should be aligned towards a mitigation strategy. For example, using the example of Pools, the mitigation approach may consider mitigating everything in Pool 1, then mitigating, deferring, or accepting other level risks. It should, however, be noted that a SoS is dynamic, therefore risks may evolve and change. This means some risks that go unattended may create further risks either for the organisation/system, or the SoS interactions with other independent systems where some risk mitigations may need to be transferred.

- Select mitigation options for all risks/bands.
- Consider how mitigation dependencies on other organisations and systems of the SoS will be managed.
- Where possible, relevant stakeholders should consider these mitigation approaches. This may need to be co-ordinated with decisions documented.

Step 8-Task 3

All mitigation details must be captured regardless of whether a risk is being accepted, deferred, transferred, or mitigated against. If mitigated against, this should consider with what approach - detect, prevent, deter, or react. Consider any residual risk after the mitigation approach.

When considering a strategy to reduce and mitigate each risk, review all threat and vulnerability details to consider how the following examples should be addressed by the requirements and controls (Caralli et al. 2007):

- *How could the actor be prevented from exploiting a weakness?*
- *How could the means that the actor would use be prevented?*
- *How could the motive be prevented?*
- *How could the resulting outcome be prevented?*
- *Could the probability of the threat be reduced?*
- *If no proactive activity can be performed, can the impact of the threat be reduced?*
- *Can the organisation minimise the effect or impact of a realised risk?*
- *How will the security requirements for this critical information asset be satisfied by the mitigation strategy, and by whom?*

If using tool-support for modelling and visualisation of risks to security and human factors in the SoS design, it is at this stage where, as detailed in Section 6.4, Step 8 - Task 3 is extended for further analysis towards SoSRE. This aims to support risk-based decisions, contributing to the completion of these final tasks of Step 8 to apply mitigating requirements and controls, and which would lead into other stages of risk management.

Identify where there are external dependencies with other independent systems of the SoS for mitigating requirements and controls.

Where requirements and controls have been determined, note details of the containers in which the controls will need to be implemented. Detail all expected controls to be implemented, e.g. administrative, physical, technical requirements and controls.

Step 8-Task 4

Risk owners should ensure requirements and controls are in place. This may be achieved through a planned approach, and should be tracked and monitored to ensure this is completed and as expected. The level of each residual risk should not be relied upon until each completion.

Continue on-going monitoring and feedback until such time the risk assessment process is repeated. However, as SoSs are dynamic, the rate in which risk is assessed may also need to be dynamic.

Step Completion Criteria

Confirm the following points:

- □ All risk scores for each area of concern have been prioritised.
- □ High impacts with lower likelihoods, and low impacts with higher likelihoods have also been reviewed together with other anomalies, potential issues and risk conflicts.
- □ Appropriate mitigation approaches have been agreed and applied for all levels of prioritised risks.
- □ The mitigation strategy for each area of concern has been detailed, addressing how each combination of threat, vulnerability, and potential impacts could be reduced or prevented at different levels with applicable controls and requirements.
- □ Owners responsible and accountable for mitigating the risks related to the critical information assets have been identified and co-ordinated with where applicable.
- □ All other external dependencies with other independent systems also responsible and accountable for the mitigating risks have been identified and co-ordinated with where applicable.
- □ Risks have been managed, tracked and monitored to ensure the mitigation strategy in each instance has been completed as expected.

Inputs for Modelling and Tool-Support, e.g. CAIRIS:

For completion of Step 8, specified mitigations may be carried out within OA, and/or within CAIRIS, selecting the appropriate mitigating Security Requirements and Controls for each element of Risk.

6.4 Extending Step 8-Task 3 with Tool-Support

6.4.1 Using CAIRIS

Many of the steps within OA provide a wealth of information that can be utilised by tool-support to model and visualise information security risk and human factors in a SoS context, as illustrated in Figure 6.1. However, how CAIRIS is used may depend upon the context and the SoS to be modelled. Moreover, some development areas may focus less on approaches such as data flow modelling, and be more concerned with goals, tasks, and processes, whereas other areas may wish to consider the whole combination available. Different needs and modelling requirements may apply.

Furthermore, the SoS being modelled may be based upon an existing 'as is' SoS, or could be a development of a new SoS 'to be'. An existing SoS may already have mechanisms in place, whereas a new SoS may need to build relationships and mechanisms. An existing SoS may also provide accurate and quantitative information in which to base a security risk assessment upon including existing controls, but a new SoS may require research and assumptions based on what is 'to be', and therefore controls and mitigations need to be specified. It is for this reason the OA element does not consider existing controls when assessing risk, as these can instead be documented or identified and specified at this stage.

Supporting approaches towards design analysis, such as through using user-centred approaches may also be applied in different ways and at different stages. For example, an existing SoS may have systems, goals, tasks, and people for which a security risk assessment of critical information assets can be based upon. Personas could be created to represent archetypical users and behaviours based on these people, perhaps through interviews and observations, or other secondary data means with an augmentation model.

However, if the SoS is 'to be', then research may need to be undertaken to create the context related scenario in which representative personas would perform specified tasks where critical information assets are stored, processed, and transported. These may also be derived to some degree from the use of epics, user stories, and scenarios, which may also suggest where dependencies exist for stakeholders and data flows.

Much of the information that supports this early stage of the design process is captured within *Step 0* of OA, although further context may be required from domain stakeholders and experts, or further research in a given area. In some instances, certain elements such as user stories and personas may have already been created by a separate design team and be incorporated into the information security risk assessment along with subsequent modelling and visualisation. This process therefore allows the flexibility towards the context of use and integration with other security, risk, and design teams in the engineering and operational domains.

Information captured in OA *Steps 0-3*, along with any other supporting information not only provides the context for SoS to be assessed, but also directs the required input to begin modelling the SoS. This should begin by identifying the system views of interest, and creating a new environment for each required view. This would capture an independent system's all known direct interactions with internal and external systems as assets, linked to a view from another independent system.

Modelling Assets

Assets may be of type: Information, People, Software, Hardware, Combined Systems, General Organisational, Groups, or Social Systems, and a SoS. A SoS asset should, for example, be associated with the independent systems of the SoS as general system assets, who in turn have associations with other asset types as demonstrated in Figure 6.3. However, the viewing or visibility of associations would be environment specific, e.g. determined by who can see or has knowledge of what. Figure 6.3 is from the view of independent system 2 (S2) that has some direct interaction with S1, but not with S3.

Step 0 will provide important high-level system assets that can be captured in the first instance, whereas other assets, their associations, and security needs are likely to be derived from *Steps 2 and 3*. Moreover, once *Steps 4 to 7* are complete, this will help focus on which specific asset associations, goals, processes, and tasks need to be included within further modelling; this suggests an iterative process is required for efficiency.

Modelling Roles of Responsibility and Personas

Where Tags are present throughout CAIRIS, these should be used to represent the main body and if applicable directly related bodies (e.g. parent body) in relation to the object for its Ownership, Authority, Control, Accountability, and Trust Entity. Where there is an association, relation, or direct interaction between objects with tags, this can be considered as a relationship and dependency, with a chain of responsibility and accountability.

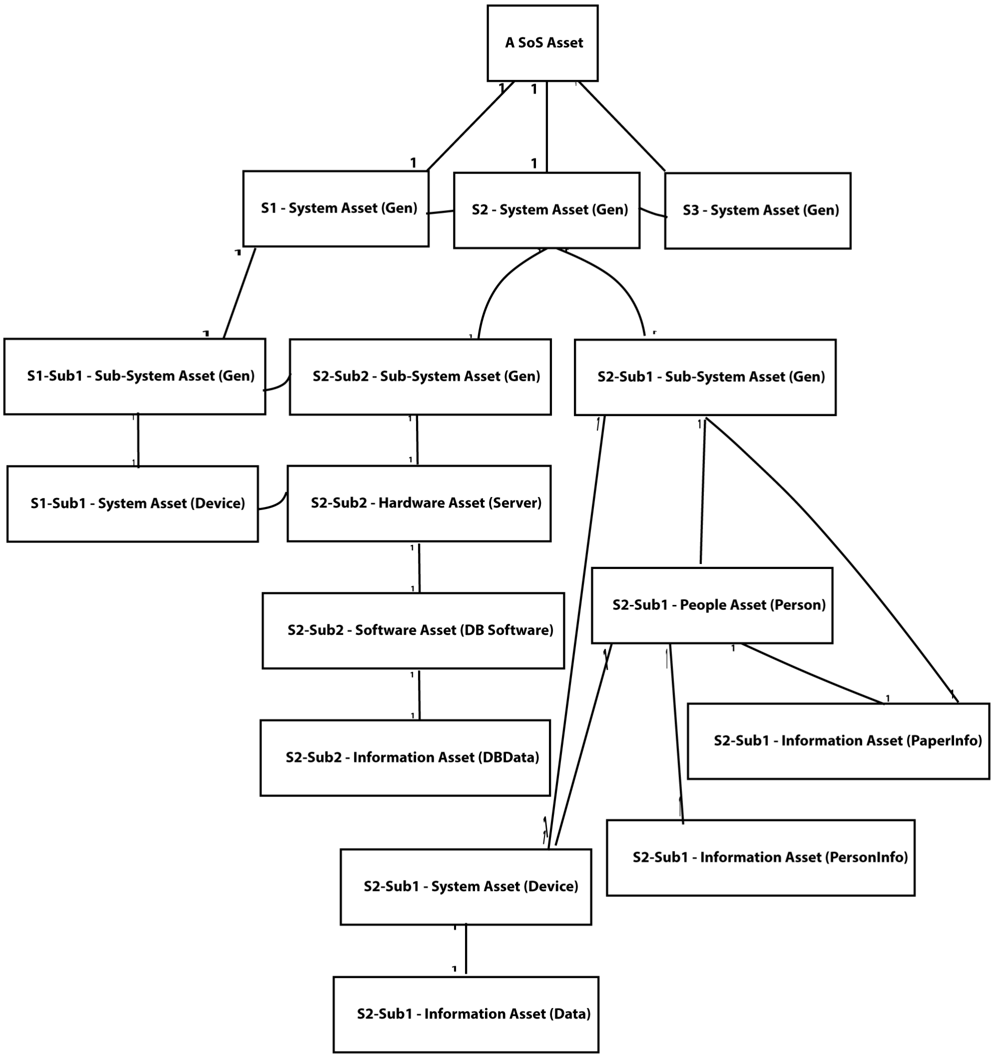

A SoS Asset
S1 - System Asset (Gen)
S2 - System Asset (Gen)
S3 - System Asset (Gen)
S1-Sub1 - Sub-System Asset (Gen)
S2-Sub2 - Sub-System Asset (Gen)
S2-Sub1 - Sub-System Asset (Gen)
S1-Sub1 - System Asset (Device)
S2-Sub2 - Hardware Asset (Server)
S2-Sub2 - Software Asset (DB Software)
S2-Sub1 - People Asset (Person)
S2-Sub2 - Information Asset (DBData)
S2-Sub1 - Information Asset (PaperInfo)
S2-Sub1 - Information Asset (PersonInfo)
S2-Sub1 - System Asset (Device)
S2-Sub1 - Information Asset (Data)

Fig. 6.3 Modelling the SoS Assets in CAIRIS

Step 0 will indicate high-level independent system roles to achieve the shared SoS mission needs and goals. *Steps 2 and 3* will provide specific responsibility roles, and personas can be created to represent the people element of interactions, although persona creation may be a separate activity outside of CAIRIS, or be incorporated within. Roles may relate to certain stakeholders with responsibility towards the SoS interactions, or be data controllers, processors, and subjects, or attackers. Roles may relate to personas carrying out tasks in the SoS.

Modelling Personas and Tasks with Use Cases

Tasks are used to document the different activities performed by personas. These may apply to general tasks towards goal completion, or specific tasks identified from the threat scenarios in *Steps 4 and 5*. Tasks have steps that can be considered as a process or processes, for which a role is likely related to a persona who performs each step of the task as illustrated in Figure 6.4. Each process can be represented as a Use Case contributing to the task, which itself has pre and post-conditions and steps for completion.

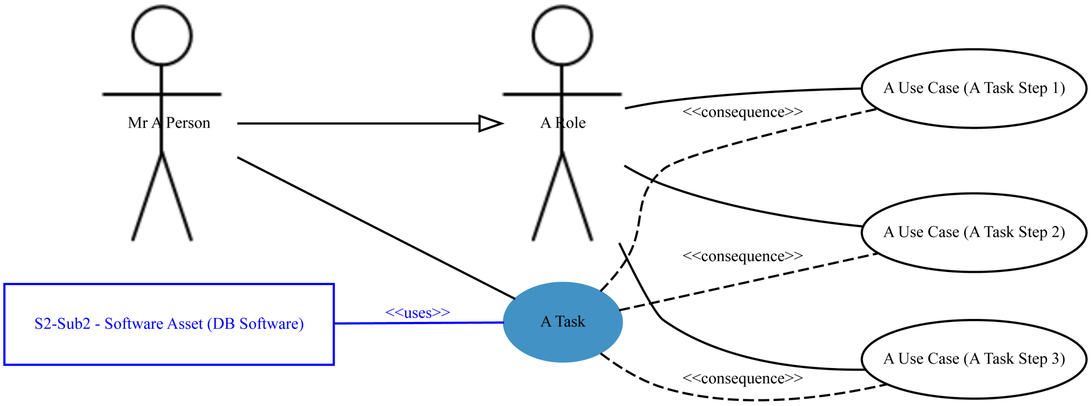

Mr A Person
A Role
A Use Case (A Task Step 1)
<<consequence>>
A Use Case (A Task Step 2)
<<consequence>>
S2-Sub2 - Software Asset (DB Software)
<<uses>>
A Task
A Use Case (A Task Step 3)
<<consequence>>

Fig. 6.4 Modelling the SoS Tasks and Use Case Processes in CAIRIS

Modelling Data Flows and Boundaries

Data output from *Step 3* details where critical information assets are stored, processed, and transported. This also indicates the potential data flows between use case processes, asset entities and data stores, and where trust boundaries may need to apply. Using this information can help with the population and generation of a Data Flow Diagram (DFD). A simple example is shown in Figure 6.5. Industry standard threat modelling with approaches such as STRIDE may compliment the use of DFDs if required. *Steps 4 and 5* do, however, provide an approach for threat model categories within the data capture.

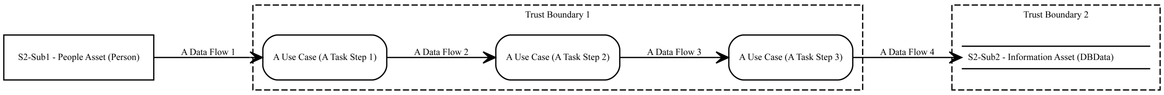
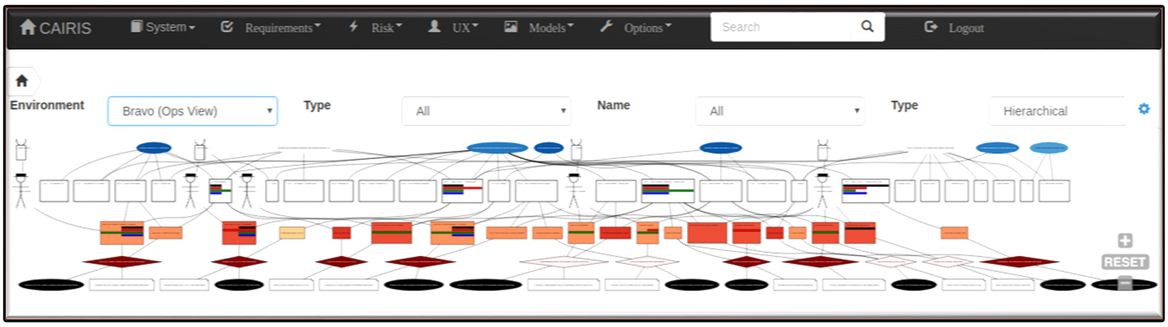

Trust Boundary 1
Trust Boundary 2
S2-Sub1 - People Asset (Person)
A Data Flow 1
A Use Case (A Task Step 1)
A Data Flow 2
A Use Case (A Task Step 2)
A Data Flow 3
A Use Case (A Task Step 3)
A Data Flow 4
S2-Sub2 - Information Asset (DBData)

Fig. 6.5 Modelling the SoS Data Flows in CAIRIS

Modelling Risk

Data output from *Steps 4 and 5* provides related elements of the potential risks identified. These specifically capture the Area of Concern that can be used as a narrative towards a Misuse Case, along with a name or description for the risk. These are derived from the information relating to the Threat, Vulnerability, Attacker, Motive, and impacted Security Requirements of the critical information asset. The Probability of Impact and related consequences are captured in *Steps 6 and 7*.



Environment: Bravo (Ops View)
Type: All
Name: All
Type: Hierarchical

Fig. 6.6 Modelling the SoS Risk in CAIRIS

CAIRIS does, however, relate the probability to the threat occurring, and the severity towards the vulnerability, and calculate the score to include the level of impact upon the security properties, which is different to the impact severity score used by OA in *Step 7*. From this information, a Risk model can be populated as seen in Figure 6.6. A separate threat model summary is provided, for example, where elements of data flows may be at threat, or highlights potential issues towards tasks where assets may be exploited.

Modelling Goals and Obstacles

When using goal modelling, a task can support a main goal, whereas a sub-goal may contribute towards enabling a process contributing to the task. This concept interplay that drives the goal-based approach is demonstrated in Figure 6.7.

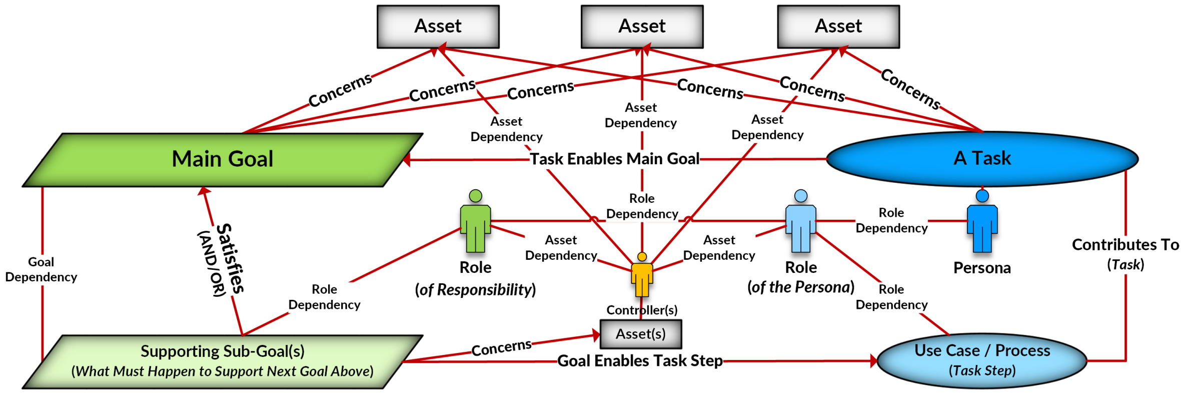


Fig. 6.7 Goal, Task, and Use Case interplay with Assets

Figure 6.7 demonstrates where a goal can have a sub-goal. The sub-goal contributes to a use case process completion that contributes the completion of an associated task, where the task and related assets contributes to an associated main goal to be achieved. Goals may be decomposed in a similar way to assets, with the overall SoS goal decomposed with any sub-goals that are associated with each high-level independent system goal as illustrated in Figure 6.8, until each goal can no longer be refined.

Sub-goal descriptions should be written as a requirement to state what the system element *shall* do to achieve the sub-goal, thus enabling the associated task step to be performed. Obstacles obstructing the completion of tasks for the SoS mission goals can be created, whilst providing the ability of addressing certain threats and vulnerabilities, although these are specifically considered using the Risk model, with attacker roles and personas included with a supporting misuse case.

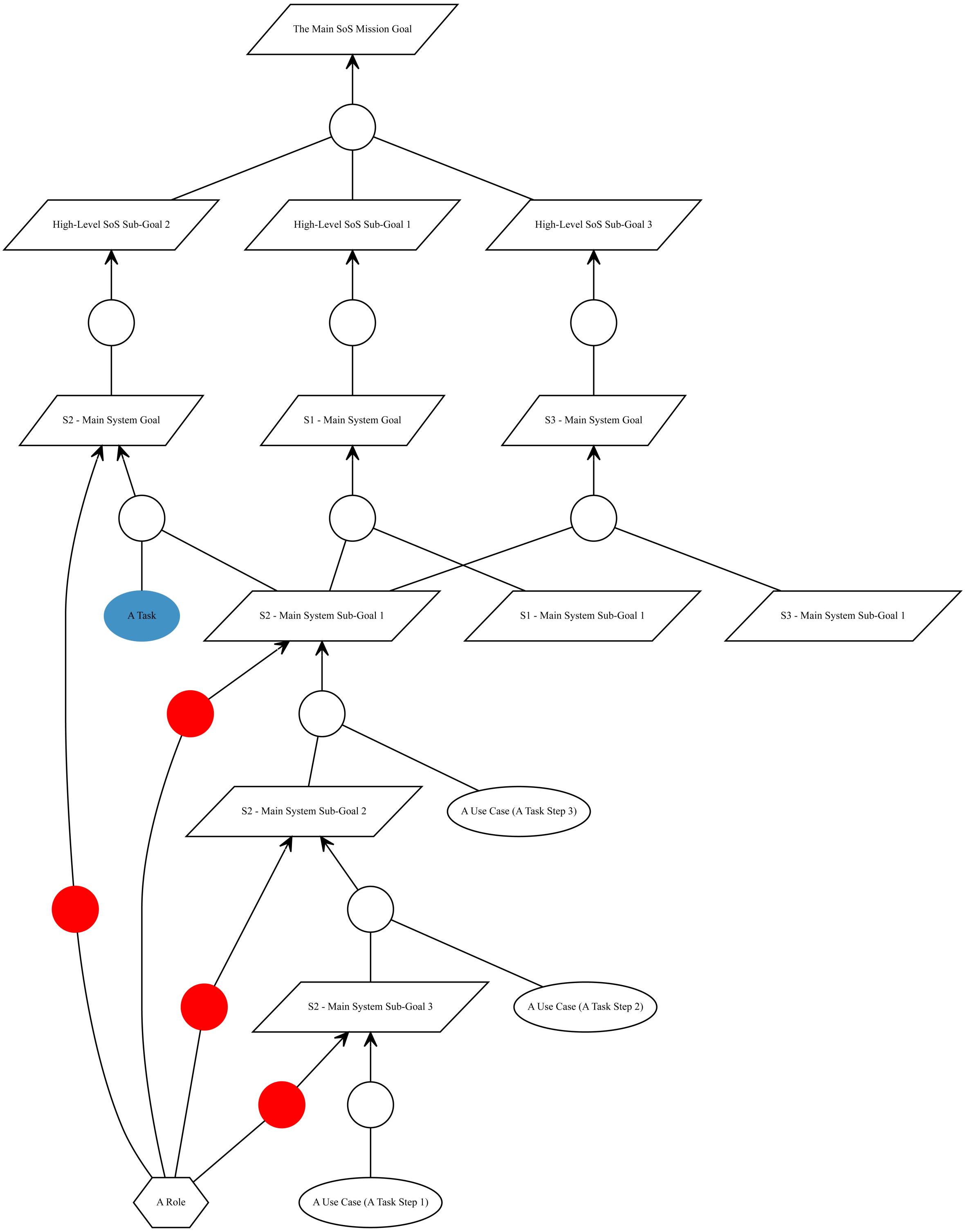

The Main SoS Mission Goal
High-Level SoS Sub-Goal 2
High-Level SoS Sub-Goal 1
High-Level SoS Sub-Goal 3
S2 - Main System Goal
S1 - Main System Goal
S3 - Main System Goal
A Task
S2 - Main System Sub-Goal 1
S1 - Main System Sub-Goal 1
S3 - Main System Sub-Goal 1
S2 - Main System Sub-Goal 2
A Use Case (A Task Step 3)
S2 - Main System Sub-Goal 3
A Use Case (A Task Step 2)
A Role
A Use Case (A Task Step 1)

Fig. 6.8 Modelling the SoS Goals in CAIRIS

Step Completion Criteria

Confirm the following points:

- □ Details of all selected prioritised critical information assets, and other software, hardware, people, systems, and organisational system assets are captured, associated, and asset modelled.
- □ Details of all related roles and personas performing tasks and processes where critical information assets are depended upon are captured, associated, and task modelled.
- □ Details of processes, and assets as external entities, data stores, and data-in-flow, have been associated and modelled as data flows.
- □ Details of all related goals, responsible roles, contributing tasks and processes depended upon are captured, associated, and goal modelled.
- □ Details of all selected threat, vulnerability, and attacker role combinations to critical information assets and other related assets are captured, associated, and risk modelled.
- □ Details of all selected threat, vulnerability, and attacker role combinations also represented as obstacles are captured, associated, and modelled with goals.
- □ From potential goal and task obstructions, further risks to other SoS goals being satisfied have been identified.
- □ Owners responsible and accountable for assets, tasks, processes, goals, and risks have been noted throughout.
- □ Model validation checks have been performed.
- □ Threat model data has been reviewed.
- □ The mitigation strategy for each area of concern has been detailed, addressing how each combination of threat, vulnerability, and potential impacts could be reduced or prevented at different levels with applicable controls and requirements. (Continue with Step 8 - Task 3 and Task 4)

6.4.2 Chapter Summary

Within the first step of OASoSIS, the information gathered should aim to identify all related stakeholders, specifically clarifying the independent system owners, their related SoS goals, and where operational and managerial control is in place. This would aim to support the identification of dependencies between systems for potential processes and people, contributing to related tasks and goal achievement. When identifying assets, this should include their owners and related restrictions or requirements, and security goals. Dependencies between asset owners and delegated roles using critical information assets with other system related assets for the storage, process, and transportation of information should be identified, along with their related processes, and tasks, relating to goals. Sub-goals along with their owners and roles of responsibility can be elicited to support or enable processes for tasks completion, whilst supporting the satisfaction of a parent goal.

When using OA as a standalone process, *Step 8* prioritises risks from high to low, and selects a response to the risk, e.g. to mitigate, accept, transfer, or defer. Controls and requirements may be specified at this stage. Alternatively, this step is used to identify which of these risks should receive further assessment, considering where risks may cause obstructions towards the success of specific goals, tasks, and processes, with their roles and representative personas. *Step 8* is extended to further model, visualise, and assess the security risk and related human factors with tool-support, providing traceability towards eliciting and specifying related requirements for the SoS.

Where potential areas of concern identify threats and vulnerabilities towards assets from threat agents, this supports risk-based decision makers by informing which owners and roles are relative to the associated SoS risks. A risk owner can be assigned, for example, to the assessing system or information owner. Where elements of the risk extend to interoperability between people, processes and tasks, and potential obstructions towards goal achievement, this specifically informs where elements of the risk may be delegated out or transferred to other owners and roles to implement related risk mitigating actions for the SoS.

Chapter 7

Case Study 1: Applying OASoSIS with a Military Medical Evacuation (MEDEVAC) SoS

Chapter 7 presents *Case Study 1* that builds upon the NATO focused research undertaken for the AMN in Chapter 4 and frames a NATO Military Medical Evacuation (MEDEVAC) scenario of that time period as a SoS. The *MEDEVAC Mission Network* (MMN) case study is used to introduce and validate the three contributions forming OASoSIS. As detailed in Chapter 6, when combined, OASoSIS would represent an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE.

7.1 Applying OASoSIS to the MMN SoS

The first contribution of OASoSIS of which forms the first step within the information security risk assessment process, includes a SoS characterisation process that was applied to identify the relevant context of the MMN SoS. This was aligned with the second contribution modifying the approach taken using the OA risk assessment process, and applied in a SoS context to assess information security risks identified within the MMN scenario. Feeding into the third contribution, the output of this first-stage risk assessment from using the modified OA process would then be modelled in tool-support for further analysis, using a goal-driven approach towards visualising information security risks and their related human factors. Findings towards the application of each contribution are discussed, along with process refinements for OASoSIS, supporting further testing and validation as an end-to-end process as detailed in Chapter 8.

7.1.1 Case Study Scenario

Armed forces around the world rely on a symbiotic relationship between people, processes, and technologies, and their systems have been designed with emergence in mind. Many goals that armed forces are called upon to achieve, depend upon interactions with *coalition* forces. However, each TCN to this coalition relies upon its own people, processes, and technologies, and while each contribute to achieving an overall SoS mission goal, each nation may have other goals that conflict with the goals of other nations.

In previous work described in in Chapter 4 with the AMN SoS, a range of services and mission threads vital to NATO operations were identified as shown in Figure 4.3, including support for MEDEVAC operations. These type of operations could be considered a SoS given the joint-force collaboration to provide a MEDEVAC service. Therefore, inspired by operations of that nature, supported by available literature and doctrine documents that summarise relevant SoS goals, a reduced-scale example of the typical interconnections of a Military MEDEVAC SoS was implemented.

There is much publicly available data in support of research activities towards examples of military SoSs, e.g. doctrine documents that summarise SoS goals, assisting with the identification of related requirements for the scenario. In addition to the research undertaken about NATO forces and the AMN in Chapter 4, the MMN scenario was based on documentation published by NATO and UK Ministry of Defence (MoD) (NATO 2013), although much of the technological software and hardware examples were only published through US and Department of Defence (DoD) sources, e.g. (Pahon 2012, MC4 2018, Seffers 2011a c, Meier 2011).

However, some technology that was actually used by the US in NATO operations has, in this example scenario, been moved under NATOs control, for example, patient data uploaded into a central data repository. Some variations may therefore exist in comparison to unpublished and classified activities. Nevertheless, the MMN SoS case study was used to apply and test the three contributions of OASoSIS, and gained feedback and validation through focus group interaction with UK military medical expert stakeholders, as discussed in Section 7.2.4.

In this scenario, the MMN considers a typical patient data-flow and interconnections of three collaborating independent systems – *Alpha*, *Bravo*, and *Charlie*. These are representative of a relationship such as a NATO operation with two TCNs, coming together as independent systems collaborating to achieve a new or higher purpose; to perform a continuum of care through medical evacuation. *Alpha* provides designated management with Command and Control, whereas *Bravo*, representative of a UK force triggers the MEDEVAC process, and *Charlie*, representative of a US force provides the systems for forward transportation and medical facilities. Each system is also reliant upon other sub-system interactions to fulfil the continuum of care.

Tracking casualty movement from Point of Injury (PoI) through to repatriation is required to regulate the treatment and flow of casualties, providing effective correctly documented treatment, meeting patient, organisational and regulatory needs (Hartenstein 2008b). As patient data is at the centre of the continuum of care, this provided a focus for testing OASoSIS, considering examples of critical information assets within the MMN SoS information security risk assessment.

The full MEDEVAC continuum of care provides additional patient evacuation co-ordination to other stage hospitals outside the area of operation, often leading to repatriation to other countries. Other stages would utilise a Patient Movement Request (PMR) for Tactical Air MEDEVAC patient transfer from the FST to a next stage HQ hospital. Strategic Air MEDEVAC would used to transfer patients outside of the area of operations; this along with further care and repatriation to the home nation is usually the responsibility of the independent system. At each stage of this SoS interaction, each system has their own role in achieving the continuum of care (Hartenstein 2008a b).

However, in this scenario, the primary focus is towards the initial MEDEVAC mission goal – for *Bravo* to initiate the process in-field with *Alpha*, then for *Charlie* Forward Air MEDEVAC to transport a patient from the PoI to a *Charlie* Forward Surgical Team (FST) within one hour – *The Golden Hour*.

To illustrate the MMN scenario with its combined interactions, dependencies, and data flows, this begins with a call raised for a MEDEVAC, initiated in-field by Bravo using a *9-Line request*; this is a template for the basic information needed for a medical evacuation. Once received by a Joint Operations Centre (JOC) Officer, this is communicated to and processed with the Patient Evacuation Co-ordination Cell (PECC) who together initiate the MEDEVAC. Their mission goal is to transport a patient to a FST within one hour from PoI, whilst depending upon multiple systems, processes, and people to achieve its SoS goals, and keep patient information secure.

A first-stage Forward Air MEDEVAC is called to evacuate in-field casualties, where the patient and details of care are provided by *Bravo* to *Charlie*. The Air MEDEVAC team are then responsible for the care and transfer of the patient to a suitable Forward Operating Base (FOB) FST, where details of care are provided, and captured electronically by sub-divisions and different systems of *Charlie*. Further context towards the interactions within this scenario is detailed throughout Section 7.1.2.

7.1.2 Applying OASoSIS

Prior to the risk assessment, the scope of the independent system collaboration and its interdependencies must be determined. The main focus would be on identifying where the SoS managerial and operational control was in place. During *Step 0*, when characterising a SoS with Figure 4.2, this helps us consider initial questions detailed in Section 4.2. It should, however, be noted that in order to answer these questions, intelligence gathering should first be conducted to capture this type of information. These questions may, therefore, guide the minimum amount of information for this process.

Step 0 - Characterising the MMN

In this scenario, the MEDEVAC operation depends upon three main independent system examples to perform a continuum of care through medical evacuation. These are described as Alpha, Bravo, and Charlie, coming together as independent systems collaborating to achieve a new or higher purpose. This scenario includes certain stakeholders within the chain of care responsible for retaining and communicating patient information at each stage. Details of this and other information are captured within the characterisation process to ascertain the wider context of the SoS and its stakeholders.

MEDEVAC Management and Oversight

Stakeholder Involvement

The primary stakeholders include Alpha, Bravo, and Charlie. Alpha provides managerial command and control to assist operations, although Alpha has other interconnecting systems to achieve this function. Alpha also provides medical oversight from the main HQ outside of the operational area, and Medical Director functions at each level of command. External stakeholders may exist, for example, with the integration of other Air Traffic Management Systems, or development of some systems. Bravo and Charlie each provide independent sub-systems of interaction for the SoS. For example, Charlie Force 1 provides Air MEDEVAC, and Force 2 provides FST medical treatment facilities. Moreover, both Bravo and Charlie may rely on individual external air and medical facilities outside the area of operations. A number of stakeholders therefore exist at different levels, although some local stakeholders may not be recognised by all systems.

Governance

Governance is provided by Alpha, with support from Bravo and Charlie, setting out formal procedures and doctrine broadly describing the collaboration requirements. Along with NATO type joining instructions and other third-party type agreements, these provide a foundation in which trust relationships are formed. Other requirements and regulations exist at independent system level. Managerial oversight, a secure network, services, data repositories, and some software is provided by Alpha. Whereas, funding for technical use and implementation sits with Bravo and Charlie (Hartenstein 2008a b).

MEDEVAC Operational Environment

Operational Focus

In this scenario, Bravo is the initiator of the process. A Bravo Field Unit's Medic provides in-field medical care, requesting the MEDEVAC and documents the care given to the casualty, creating a chain of patient related information. Trust mechanisms are likely to be in place, supported by technical measures to ensure this data-flow is maintained. Charlie has a greater role and depends upon more than one system to achieve its mission, each individually operated to fulfil the process, further managing patient care and documentation stored in Alpha's shared data repository. Bravo and Charlie, therefore, each retain a level of autonomy with some competing interests. However, operations are driven by Alpha command levels and the MEDEVAC operation, specifically through the PECC. Mission needs are guided by the coalition COP of tactical and medical SA to achieve its mission safely and securely (Hartenstein 2008a b, Meier 2011).

MEDEVAC Implementation

Acquisition

Some system and security requirements would be mandated by Alpha for participation, however, Bravo and Charlie would be responsible for capturing those needs within their differing requirements to ensure interoperability. Alpha provides an 'as is' configuration for command and control, using systems, services, and networks developed and tested outside of the operational area. Various systems are also integrated with different ownerships, e.g. the MC4 brand of in-field and theater medical systems, or the Joint Medical Workstation (JMeWS). However, Bravo and Charlie are responsible for acquiring and implementing their own systems. For Charlie, this includes the common MC4 medical data system using software from AHLTA provided by Alpha for accessing their central repository, the Theatre Medical Data Store (TDMS) system. Charlie also use Laptops with AHLTA-Theater software to add patient data. Other technical elements such as purpose-fitted Black Hawk MEDEVAC helicopters and FST facilities are also the responsibility of Charlie, but from separate sub-systems (Meier 2011).

Test & Evaluation

It is likely that many of the lower level systems may not be fully tested at SoS level before implementation. Trust boundaries may be an obstacle, as a negative could have adverse impact on external systems. MC4 systems would, however, have been tested by Alpha prior to its use and dependency. Charlie may achieve a degree of testing given its inter-relations, but it is more difficult to align with Bravo, and Alpha. MEDEVAC testing exercises outside of the operational environment may exist.

MEDEVAC Engineering and Design Considerations

Boundaries and Interfaces

Boundaries cover a range of contexts of people, process, and technology, across land, sea, air, space and cyber domains. However, given the flow of data, cyber, air, and geographical boundaries are of high importance, with multi-national data regulations applying. The most immediate trust boundaries are between the three independent systems and their sub-systems, interfacing with other systems and assets.

Performance & Behaviour

Alpha continue to provide command and control with SA provided to all throughout the continuum of care. This allows for on-going feedback to improve their own capabilities, whilst providing input for independent systems to align and balance SoS needs against system demands. Performance would also be monitored at casualty level, with reduction of issues and rates of survival from critical golden hour care and transportation (Hartenstein 2008a).

7.1.3 Steps 1-7 - Assessing Security Risk with OCTAVE Allegro

To perform a risk assessment, an amount of information gathering is required to identify data assets and associated system asset interactions where data may be processed, stored, and transported or transmitted. The new *Step 0* provided a process to support an assessment by framing the SoS and its context, and identifying the type of SoS by its characteristics from the given scenario. For example, understanding where various management and control was in place for systems and the SoS, indicating where accountability or conflicts may exist.

Using this process provided the foundations and scope of the SoS to determine the systems-of-interest and related elements to be assessed. The second contributing part implements OA *Steps 1-7* as detailed by Caralli et al. (2007). These are applied within the modified version of OA to perform the first-stage identification, analysis, and evaluation of SoS information security risk and human factors concerns.

Steps 1-7 were used to produce an example security risk assessment using the MMN, first from the view of one independent system, *Bravo* and their interaction with the SoS, then later repeating the process for other system assessment views. Having characterised the MMN scenario as an Acknowledged SoS, this process identified relevant stakeholders, boundaries, and where managerial and operational independence, and control were in place for MMN, pointing to areas of dependency, complexity, and potential risk.

In *Step 1*, system stakeholders would normally be relied upon to collaboratively agree the criteria in which risk may impact upon a system and its interaction with the SoS, and within which parameters. For example, if the impact of a risk would create financial penalties, the criteria category for financial penalties aligns with a scale to define a Low to High financial impact contributing to the risk equation. These were applied accordingly to the context of the scenario. In OASoSIS, the parameters are within the bounds of impacts being *Negligible 0 - Marginal 1 - Critical 2 - Catastrophic 3*, therefore the criteria would be divided into four horizontal sections accounting for impacts within these different degrees.

Much of the standard vertical categories in the OA criteria gives focus towards typical business impacts, but accounts less for the impact on human factors. Given the socio-technical nature of SoSs, aligning the concept of HFSI in *Step 1* aimed to address this gap, whilst accounting for impacts towards interoperability within the socio-organisational impacts. As the criteria categories are prioritised, e.g. 10 to 1, with 10 holding the highest importance, balancing business and human needs or impacts would require stakeholder discussions to agree each level of importance for each category, particularly in SoSs where safety is paramount.

Steps 2 and 3 considered the likely information assets used in the MMN scenario, specifically considering the critical assets and where they were stored, processed, transported or transmitted. For example, this included data captured by using a Field Medical Card (FMC), the 9-Line Request using radio communications, verbally communicated information between entities, and subsequent data stored electronically.

To identify and analyse potential areas of concern, *Steps 4 and 5* considered initial concerns towards how information assets are used, then introduces threat scenarios in order to establish likely threats and weaknesses towards assets with a potential for risk. *Steps 6 and 7* were applied to analyse the areas of concern towards information assets and their related systems, considering the probability of the threat and vulnerability combination occurring. Then, an impact score was applied relating to each of the risk criteria categories, and multiplied by its risk criteria level amount. This was multiplied again against the probability to account for the likelihood of the impact and severity, thus providing an overall risk score.

By the nature of OA, documenting threats and concerns of critical patient information assets could be spread out over many sheets of paper for a single asset. For flexibility, this was instead entered into spreadsheets, but later converted to a single line all-in-one spreadsheet, considering areas of concern for the process, storage and transmission of data, by people, physical, and technical means, then assessed the impact and probability of the occurrence.

Leading into *Step 8*, each of the risks were reviewed to identify groups of higher and lower risk, at which point a decision can be made whether to avoid, accept, transfer, or mitigate a risk. Suitable controls can be agreed and applied towards each risk relating to the system interactions within the SoS. Information assets with areas of concern that indicated higher probability and severity risk scores were, however, then selected for further modelling using CAIRIS, although the challenge was to identify how and where this information could be suitably extracted from OA and visualised with CAIRIS.

7.1.4 Step 8 - Modelling with Tool-support

The third contributing part of OASoSIS introduces certain concepts, models, and techniques, integrated with the use of tool-support to extend the assessment in *Step 8*. It is this contribution in particular that supports the SoSRE domain towards the modelling and visualisation of SoS risks and related dependencies to achieve the SoS goals securely. Moreover, it is by introducing this combined output that facilitates decision makers' understanding towards the criticality of activities performed with related assets. This includes the owners, roles and responsibilities for ensuring these are completed securely to achieve the SoS goals, and who would be responsible and accountable for mitigating identified risks.

To begin modelling a SoS in CAIRIS, a separate environment was created to represent the view of each independent system, and an additional overview environment to capture all interactions. In the initial *Bravo* view, an asset model was first populated, where an asset is used to represent the SoS as a single entity. This SoS could then be decomposed using a top-down approach associating each of the main independent systems and sub-systems assets with people and information assets.

In *Bravo's* view, this would include the known interactions between the constituent systems where *Bravo* has direct interaction with other systems. Associations may also be an aggregation or composition to its parent asset. This was later repeated for the other systems in other views, providing a bigger picture towards the different interactions interconnecting for the purpose of the MMN.

Systems are represented at higher level as an organisational level system asset who may in turn have lower level organisational systems, each of which have technological systems where human actors interact with software and hardware combinations. Information or data assets may also be physical and paper-based, or a person and the knowledge they hold that may also be communicated verbally, and which may then be entered into a software interface and database, creating an electronic version of the data.

Modelling Roles and Personas

All main assets from within the MMN scenario were modelled and associated with roles of key stakeholders and actors performing the continuum of care, reflecting areas of responsibility for systems and interoperability. This included certain activities and tasks performed by specific roles undertaken by a person. Specific risks carried over from the OA risk assessment also helped to highlight these activities where a data asset may be at risk by a human, accidentally or maliciously, or trust may be diminished in some way.

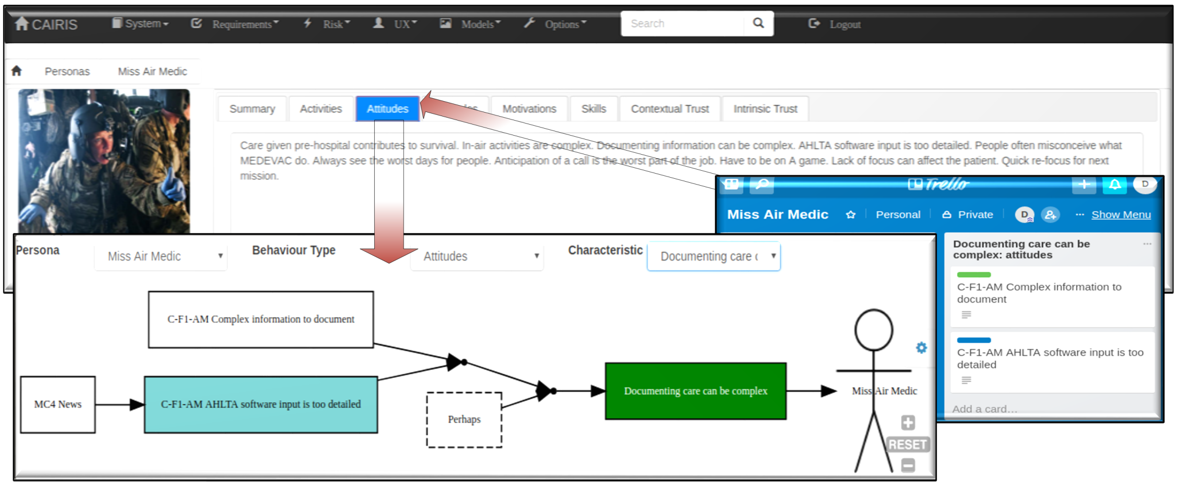
Roles were then associated with personas, representative of archetypical descriptions embodying the goals of users offering insights into threats and vulnerabilities. Attackers were modelled and assessed in a similar way, reasoning about the intent, skill, or means of an attack by an actor internal or external to the SoS. Personas were implemented to further reason with human factor considerations and the consequence of actions when assessing security risk and related requirements.

To do this, CAIRIS supports the alignments of Toulmin argumentation models to justify persona characteristics (Faily and Fléchais 2010). The Persona Helper Chrome plugin (Faily 2018c) was used to capture factoids from online and offline data, such as a webpage and clips of text within it. These factoids were stored within CAIRIS, and exported to a Trello board (Trello 2018) that itself can be used as part of the affinity diagramming process. A further example of using Trello for affinity diagramming is discussed by Faily and Iacob (2017). Elements relating the output of this process capturing an Air Medic persona's characteristics are shown in Figure 7.1. Once the factoids were grouped into characteristics, these were marked as a grounds, warrant or rebuttal supporting the argumentation of the characteristic, and imported directly back into CAIRIS to create a persona and related model derived by using grounded theory.

This resulted in the creation of six personas supporting the goals, tasks and scenarios. These were:

- A Field Medic;
- An Air Medic;
- A FST Technician;
- A JOC Officer;
- A PECC Co-ordinator; and
- A Casualty.

In CAIRIS, roles can also be attributed to being a 'data controller', similar to that of a 'data processor' in relation to a 'data subject'. Although these specifically relate to privacy requirements, they were added to the MMN model, but not tested. That said, the privacy validation did not return any errors, suggesting at a basic level,



Care given pre-hospital contributes to survival. In-air activities are complex. Documenting information can be complex. AHLTA software input is too detailed. People often misconceive what MEDEVAC do. Always see the worst days for people. Anticipation of a call is the worst part of the job. Have to be on A game. Lack of focus can affect the patient. Quick re-focus for next mission.

Persona: Miss Air Medic
Behaviour Type: Attitudes
Characteristic: Documenting care (

Documenting care can be complex: attitudes
- C-F1-AM Complex information to document
- C-F1-AM AHLTA software input is too detailed

Fig. 7.1 CAIRIS Persona Characteristics and Model with Trello

privacy elements were considered, but creates a future opportunity for incorporating privacy by design using this SoS model and scenario.

Modelling Personas and Tasks with Use Cases

Personas were associated with tasks, and use cases were created to represent steps of the task. The use case and its sub-steps represented the process for completing a task step carried out by an actor. A use case would, however, be associated with a role that would likely be associated with the persona, although other roles may apply. Once the tasks were created, the use cases representative of each of the task were linked to its related tasks through traceability links.

In this scenario, task steps would include an instance where no software and hardware interaction may occur with physical patient data, but would lead to steps where this does occur by users from other systems. For example, where information originating from the FMC based on patient injuries and care given, is verbally communicated and travels along the patient journey across organisational systems forming part of other medical information. Some of this information is also copied into electronic formats by two personas.

Modelling Data Flows and Boundaries

In parallel, data flows and trust boundaries were then mapped, further highlighting needs for interoperability. To create data flows, assets were used to represent external entities as people, systems or hardware, information assets were used as data stores, and use cases represented the processes between data flows. As some data flowed from assets of one environment to another, these interactions can be represented from one trust boundary to another, viewed in a Data Flow model.

Boundaries were further represented using the Location model, where a location can represent sub-locations in which an instance of an asset occurs, e.g. a house has rooms. We can also link these sub-locations, e.g. if we have a hall, these can be linked to the rooms. In this scenario, the different areas of operation were accounted for. All related assets for that location were populated along with personas carrying out a task in that environment. Locations included a FOB, in-the-field, and HQ. When risks were created, risks to assets were also seen in the Location model.

Modelling Risk

There were a number of options for modelling and visualising elements of risk in CAIRIS. The primary risk-focused option entailed modelling where threats and vulnerabilities were associated, which equate to a risk for systems and the SoS. Once assets, tasks, roles and attackers were created, threats and vulnerabilities could be added with an associated misuse case equating to a risk, viewed in the CAIRIS Risk Analysis and Task models. The models indicated where some risks may occur in one environment which may affect a system in another environment, or some risks may occur across all environments, or be specific to a sub-system in one environment.

However, this representation originally created a strange effect in CAIRIS, where a risk could be situated in one environment, but is applicable and visible to another where no misuse case is present. To remedy this, in addition to other built-in validation, CAIRIS developers added a means to identify and alert to where an instance of this risk scenario occurs; thus indicating a useful early finding towards improvements to CAIRIS, specific to the SoS context.

Once risk elements have been added and combined in CAIRIS, a threat model listing is self-generated, demonstrating where certain aspects, entities, and data flows are at threat. It is therefore from these combined visualisations of risks that we can begin to consider where requirements and controls need to be specified to mitigate the risks to assets, tasks, and goals, related to roles and persona interactions within the SoS.

Modelling Goals and Obstacles

Goal and Obstacle models in CAIRIS provided the option to model system-specific requirements, using a top-down or bottom-up approach, where goals and sub-goals were operationalised by tasks, and refined into requirements. However, in the MMN scenario, the required tasks and high-level system goals had been captured, but needed to further identify areas in which to elicit the system sub-goals. Each of the sub-goals were therefore selected to enable or support the process steps of a task carried out by a persona.

The representation of Responsibility models also added value by demonstrating where a role was responsible towards an asset, related to a task, goal, requirement, and elements of risk. Where a role is responsible for a goal, this can be added within the sub-goal association of the goal. The Responsibility model is another example of a self-populating model, generated as part of the KAOS Goal model as other elements are added and interlinked within CAIRIS. This model indicated a sense of where control was in place, and is generated primarily from goal model elements.

Obstacles were then used to represent a threat or vulnerability towards an information asset identified in the Risk model potentially obstructing the completion of other tasks and satisfaction of goals. For example, threats of unauthorised access, use, disclosure, disruption, modification, or destruction of data or systems affecting the continuum of care. To address the goal obstacles, these were refined into requirements to satisfy the system interaction with SoS goals. This became more difficult when there were conflicting requirements or where there was no direct relationship between some systems, meaning trade-offs needed to occur between systems and requirements to maintain interoperability and trust.

For example, the communication of the FMC information may require its *Integrity* and accuracy of patient data to be upheld. Whereas, for information that later becomes stored electronically by another system, *Availability* may be a higher desire, because without the information, treating the patient accurately is difficult. However, in both cases, once in electronic format, *Confidentiality* may be of higher importance, but in all cases *Accountability* should be present.

7.2 Discussion

The OASoSIS approach was introduced with the MMN scenario to align SoS factors and concepts suitable for eliciting, analysing, and modelling security risks and human factors using tool-support within the SoS context. The application of a reduced-scale example of a Military MEDEVAC SoS case-study was purposely limited to a simplified abstraction of a SoS. However, as is often the case, with any simplicity, there is always complexity, perhaps more so in a SoS scenario. By applying each of the contributions that form OASoSIS, this helped to provide an understanding towards those ensuing complexities of the SoS.

7.2.1 Applying Step 0

When using the characterisation process in *Step 0* with the MMN scenario, given that NATO joint-force operations may be considered as a grouping acting as one force, early assumptions could indicate some alignment with this type of SoS as being a Directed SoS. Although Alpha would mandate standard operating agreements (STANAGS) and doctrine, each independent system of the SoS operates with its own autonomy and operating procedures. This can be demonstrated where Alpha has no direct link to Charlie Air Corp, who have operational and managerial control of Air MEDEVAC, who Alpha does interact with.

Despite this type of example, Alpha, Bravo, and Charlie are reliant upon the collaboration to fulfil the SoS mission needs, suggesting qualities of a Collaborative SoS. The conclusion of the review determined the MMN to be an Acknowledged SoS based on its high-level distinction of designated management by Alpha, but with limited control over the independent collaboration of Bravo and Charlie who retain a high-degree of operational control in the SoS.

Other SoSs also exist within this configuration. For example, the Electronic Health Record (EHR) data flow to support the continuum of care consists of various systems providing input and output, some of which interface with home nations (Meier 2011). Also, the MC4 systems providing tools to digitally record and transfer medical data using joint medical software, with commercial and government-off-the-shelf products, acting as a deployed EHR repository for battlefield surveillance (MC4

2018). Additional considerations such as these may only become apparent once systems information has been gathered and assessed.

The characterisation process was important for identifying the main stakeholders and dependencies between independent systems, and identifying where other SoSs also exist within this configuration of the MMN. For example, the infrastructure supporting the MMN data flows, and the MC4 systems used by Charlie to digitally record and transfer medical data. However, as Bravo does not have processes in place and access to these systems, interoperability and communications is reduced towards patient data flow, suggesting an area of improvement for future joint-force operations. This point in particular was highlighted when validating the scenario and approach with military medical experts, who provided further clarity towards a typical joint-force MEDEVAC operation, and potential data flows at risk, helping to fine-tune the scenario and its assessment. Stakeholder feedback is discussed in Section 7.2.4.

7.2.2 Applying Steps 1-7

Where the OA element has been to be modified to provide a simple repeatable and reusable process for identifying information security risk in a SoS, early findings suggest the alignment of its data collection and output has the potential to align with selected concepts, models, and techniques in a tool such as CAIRIS. It was found that OA was generally asking the right questions, and could be useful as a means through CAIRIS to convey operational needs to SoSRE, but requires further refinement. For example, *Step 0* already begins to capture details of stakeholders, organisations, and other persons of accountability and their related SoS assets. However, as this feeds into *Steps 3 and 4*, there is an opportunity to document more of this information earlier as part of OA within the spreadsheets.

Steps 1-3 may also run in parallel, thus changing the original flow of OA. The introduction of HFSI to the risk criteria was useful towards capturing the human related impacts to the wider SoS, whilst indicating interoperability and other engineering impact related concerns. Being mindful of this from these early steps helped maintain that focus whilst progressing through other steps.

Changing the order of OA *Steps 4 and 5* to consider threat scenarios earlier to capture potential areas of concern would seem a more effective approach to provide focus to areas of exploitation. For example, the original steps first required the assessor to consider scenarios where there may be a concern, then provided threat scenario questionnaires to identify if they would actually be a potential risk. However, in OASoSIS, this should provide the threat scenarios earlier to indicate example areas of focus towards threats and vulnerabilities in order to establish likely concerns and potential for risk. This would not only improve the efficiency of the process steps, but would help less experienced stakeholders or assessors to arrive at the *how* and *why* aspects a little quicker guided by the scenario-based questionnaires.

Furthermore, where OA considers concerns, threats and threat scenarios, it does not explicitly document the potential weakness or vulnerability, where it perhaps should. This was, however considered to provide a more clear and complete risk equation, and further enables better data capture into CAIRIS towards addressing the weakness.

At the point of applying *Steps 6 and 7*, the spreadsheet capturing the risk data became quite large to manage, but more manageable than many pieces of paper. Nevertheless, these steps provided a means in which to analyse and evaluate the probability and severity of impacts that could the be prioritised for further attention leading into *Step 8*. This was not only an important consideration towards managing and prioritising quantities of risk, but also to be mindful of the quantity of assets that would be modelled, because even when using tool-support, models may become complex.

The focus did, however, remain towards identifying information security risks and their related human factors concerning information assets and their dependencies towards the MMN achieving its SoS goals. In comparison to the standard OA approach, the modified version was driven by this focus assisted by the broadening of socio-technical impacts towards independent systems and their ability to interoperate at different levels with the SoS to achieve its goals.

7.2.3 Applying Step 8

Data output from OA into CAIRIS provided most of the information required to generate selected models and requirements, with some additional details from initial data collection for rational. Unlike other versions of OCTAVE, the benefit of OA to operational areas is that it gives a specific focus towards the information asset and its related security properties, e.g. Confidentiality, Integrity, Availability, and Accountability. When translating this into CAIRIS, we find that we can identify what security properties must hold for each information asset, but have little indication of security needs for other types of system assets.

This appears to be a weakness or limitation of OA, but could be turned into a strength when considering how information assets from one owner or independent system should be treated by other people and systems within the SoS context towards its process, storage and transmission, some of which are outside of their control. Specific security and human factor needs and potential requirements conflicts may then be identified and addressed to meet SoS needs.

Combining models first provided a view for *Bravo* and their SoS interactions, with additional views added for *Alpha*, *Charlie*, and a combined view of all interactions. Each environment highlighted where dependent relations and security risk exists towards fulfilling the continuum of care, whilst supplying reasoning towards SoSRE. The use of environments representing views of independent systems helped to provide an element of clarity towards framing different aspects and concerns for each of the system views. When modelling multiple systems across different environments, naming convention and terms across environments did become a challenge to indicate in the models which element related to each independent system.

Understanding in what order to build SoS models is also a process efficiency consideration. In CAIRIS, this began with assets, roles and personas, then goals, tasks, and use cases. Others may be applied in different orders. However, models may also be used for various purposes across different engineering or design teams, therefore, understanding how these models inter-link plays a further role in understanding the viewpoints and varying needs of SoSRE and related stakeholders.

The integration of goal modelling is, however, central to the modelling element of OASoSIS, underpinning the process guided by the SoS goals identified during *Step 0*, and illustrated in *Step 8* as goal-driven requirements aligned with the supporting tasks, processes, people and roles related to the SoS context and the identified risks and concerns. From the analysis, the impact towards the SoS achieving its goals can be determined, helping to guide decisions towards mitigating risks and satisfying these goals, whilst reducing the wider risk criteria impact areas identified in OA. Moreover, by extending OA and applying the modelling process, this specifically helped to identify further impacts to the satisfaction of SoS goals that were not apparent from the first-stage assessment.

The responsibility model was useful for demonstrating the roles of responsibility that may be associated with elements of the risk equation, however, it is was evident there was still a gap for RBDM towards capturing the important link between the owners with authority for the different objects. For example, owners of assets, tasks, goals, processes, and risks, details of which were largely captured during *Steps 0 to 5*, but became redundant or unaccounted for when transferring data to the tool-support.

It is from these owners and authorities where authority is delegated to roles with specific responsibilities that could be made more explicit. Moreover, it would be useful to visually indicate those owners with accountability alongside the roles of responsibility within the modelling process. This would provide continuation and consistency of important data already captured, and provide critical information to help inform RBDM regarding the entities likely to be the risk owners responsible and ultimately accountable for mitigating the elements of risk attributed to the SoS.

7.2.4 Stakeholder Review

In addition to previous data and interviews to help ground the NATO-based scenario, expert military medical stakeholders representative of Bravo decision makers provided feedback and clarifications to help validate this scenario, whilst adding context towards how Bravo may interact in this scenario with Alpha and Charlie. This was extremely useful for OASoSIS towards shaping its application, fine-tuning the modelling and assessment, and validating the soundness of the SoS structure being generally representative for the scenario presented.

A focus group was arranged and chaired by Dstl, and hosted at a UK military facility. Five military and defence representatives were in attendance at the focus group, two of whom had extensive backgrounds towards UK and NATO communications, networks, and operations. Three other senior personnel with extensive experience in UK and NATO medical operations provided specific feedback towards co-ordinating the medical evacuation and patient data-flows from PoI to a medical treatment facility.

Stakeholder feedback suggested that by following the SoS characterisation process of *Step 0*, this approach provided a useful process for a SoS level stakeholder to first align with the SoS concept, and to identify specific characteristics of an interconnected systems environment. Then, potentially classify it as a SoS based on this output, clarifying where managerial and operational independence and control are in place for the SoS. This in-turn could direct future assessment of areas of dependency, responsibility, and complexity, or specific areas of concern and risk.

During the focus group, stakeholders also created a diagrammatic whiteboard board example of the operations relevant to the scenario. This was used as a point of reference throughout the discussions to review and compare various interactions and dependencies at different stages of the medical evacuation. The whiteboard diagram was also useful for validating how the structure was very similar to that which had been modelled within CAIRIS, and which was also very similar to a joint-force operational structure indicated in an unclassified but unpublished NATO document. Stakeholders were, however, keen to point out conflicts in terminology. For example, where much of the supporting information for the case study was based on the interactions of American forces with NATO, and supported by other NATO publications also, a Tactical Operations Centre would instead be referred to by British forces as a Joint Operations Centre. A simple, but nevertheless important observation for the stakeholders.

Stakeholders also clarified where Bravo would not have interoperable systems and processes in place to interact with some TCN systems. For example, Bravo reduces some of their security risks simply by continuing to use certain manual processes, whereas Charlie are much more dependent on electronic system interactions for patient data-flow, thus increasing their cyber element of security risks.

The risks identified when using OASoSIS, were otherwise considered representative for the MMN scenario, although it was acknowledged that co-ordinating changes to processes and controls with TCNs can be a challenge given the different levels of ownership and control across the systems. Nevertheless, it was considered that providing the means and traceability to support the need for change and risk reduction towards security goals is an important aspect for stakeholder communication in NATO operations, especially where there is an implication that lives and patient care may depend upon it.

7.3 Chapter Summary

In this chapter, based on work towards RQ1, and considerations to inform and learn from RQ2 and RQ3, OASoSIS was introduced and applied as an approach that combined three contributions to align SoS factors and concepts suitable for eliciting, analysing, and modelling SoS security risks using tool-support. The application of OASoSIS began with a simple repeatable characterisation process implemented with the MMN SoS example, helping to characterise and define the SoS collaboration, its context and environment. Risks to critical assets were identified and analysed, providing risk data output that could then be aligned with concepts, models, and techniques integrated with tool-support to provide further visualisation and analysis of SoS risks and goals to be accounted for within RBDM and SoSRE.

The application of OASoSIS demonstrated its value, with early findings suggesting the alignment with a tool such as CAIRIS can provide many benefits for translating operational needs into goal-driven requirements. Findings also highlighted where the modelling process could be extended within the tool-support to enhance the completeness of aligning ownership and accountability with responsibilities captured within OASoSIS, thus supporting RBDM.

In support of additional validation, peer review was gained through the publication of elements of this work, first with characterisation process in Ki-Aries et al. (2018b), and modelling with tool-support in Ki-Aries et al. (2018a). As a continuation of this research, the OASoSIS process would be further refined based on findings from the MMN case study. OASoSIS would then be re-applied as an end-to-end process with *Case Study 2* in Chapter 8 to identify and assess areas of information security risk and related human factors, thus providing further validation of OASoSIS as an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE.

Chapter 8

Case Study 2: Applying OASoSIS end-to-end with a Canadian Emergency Response SoS

Chapter 8 presents *Case Study 2* that considers a Canadian Emergency Response System as a SoS, applying OASoSIS to a real-world problem and intervention in support of possible future operations for Mutual Aid Alberta (MAA). This research fuses all RQs building upon previous findings to apply the refined process of OASoSIS to the case study scenario. This combines the three contributions tested and validated in *Case Study 1* representing an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE. The context, application, and findings of the case study are presented to discuss each step applied.

8.1 Applying OASoSIS to an Emergency Response SoS

There is an increasing reliance placed upon the technical and social system integrations to deal with consumer and economic demands, whilst coping with and responding to unexpected changes within the world. This is exemplified by how we adapt to natural disasters and the socio-technical interdependencies associated with dealing with such events to protect public interests, communities and the environment. However, communicative interoperability between all dependent entities becomes a challenge. Software systems that are integrated to help attend to such disasters, are not always designed towards the wider context, or therefore account for the wider socio-technical system perspectives.

For example, in some parts of the world, wildfires are more prone to start earlier in the season and are often lasting longer. Consequently, the effect of these events can have a long-term impact upon both the environment and the economy. As a result of a narrowed scope, this affects the ability to reason with the needs for strategic, operational, and tactical requirements and controls, which need to be better integrated to reduce the wider impact of such disasters.

An emergency management scenario is a classic example of a typical SoS where independent systems such as police, fire, ambulance, and local authorities, each with their own *day-job*, come together to meet the joint emergency response mission goals. Achieving and maintaining SoS-wide interoperability is particularly challenging for systems in these scenarios, e.g. through different processes or technology. Moreover, information assets related to the socio-technical interdependencies need to be secured, but available on-demand when required in emergency situations to facilitate communications and SA.

An example of this research challenge was posed by MAA: a Canadian non-profit organisation supporting Alberta's emergency response capability. MAA were considering design options for an instant messaging system that could potentially be used by emergency responders engaged within incident response, e.g. a wildfire. This software engineering design challenge was presented to the *RE Cares* track of the 26th IEEE Requirements Engineering conference in Banff during August 2018, where stakeholders from the RE community converged to help identify potential users of such an application, and the typical functionality required to fulfil its purpose (Dekhtyar et al. 2019).

However, given the wider context of the operational environment in which the application would be situated, and the multi-level stakeholders within the environment, it was considered that at a higher level, the MAA intervention would also benefit from applying a different perspective towards a SoS approach. Taking a SoS approach would instead aim to account for the wider technical and social system goals, perspectives, and potential risk-based impacts towards the SoS achieving its goals.

In the MAA example, early indications from collaboration with *RE Cares* suggested there were many related human factors and information security needs across multiple systems under different ownership, authority, and control, some of which may have no clear boundaries, conflicting requirements, and a web of complexity. This example further demonstrated the need for developing new approaches, and to evolve existing RE capabilities to cope with the complexity of SoSs. This need has been motivated by SoSRE communities, calling for a greater focus towards engineering for SoSs, including multi-level modelling techniques and security requirements frameworks for SoSs (Ncube 2011, Ncube et al. 2013, Ncube and Lim 2018) to capture the needs of SoSs against the potential for risk affecting goals of the SoS being achieved.

Nevertheless, it is acknowledged that when engineering for SoSs, bridging the communication gap to convey the operational needs of independent systems to SoSRE is difficult. Security requirements and system needs can become lost in translation. This is exacerbated in SoSs where multiple stakeholders exist, but not all are known. This means only limited information may be available to support RBDM. The trust placed upon the resilient interoperation of communications between systems, processes, and people is critical to the success of the SoS (Fan and Mostafavi 2018). Such trust is warranted only when potential SoS security risks are identified and managed.

8.1.1 Case Study Scenario

Within the original collaborative *RE Cares* and MAA project, the primary focus of the intervention was to support the software engineering process for application design. However, this case study implementation instead takes a different approach to the problem domain. To test and illustrate OASoSIS with further analysis of the modelling process supporting SoSRE, this took a snap-shot of a possible scenario related to the original *RE Cares* output of the MAA example (RECares 2018). The scenario was considered from a broader perspective, defining the MAA Emergency Response System instead as a SoS (ERSoS). Some variations exist in comparison to unpublished or classified business and emergency operations.

In this scenario, the infrastructure for the ERSoS would be provided by MAA to support the use of an emergency response application, specifically to facilitate command and control functionality assisting an emergency incident. This would be co-ordinated by local and provincial Incident Command Systems (ICS), whilst integrating supporting data from the MAA emergency resource portal maintained as part of their day-job.

MAA would come together with the ICS, which is made up of different systems and emergency responders using the emergency response application, e.g. Emergency Medical Technicians (EMT), Firefighters, and volunteers. Roles would be assigned within the proposed MAA software application relevant to the location of the emergency and related expertise. Also included is the Community as an entity, but individually become evacuees who would then be dependent upon the communication flow of the messaging system. This dependency becomes much greater if functionality is built-in for evacuees, either relying upon the software application for public information alerts, or individual requests and responses from evacuees.

In a larger-scale emergency, individual responses may require considerable resource and manpower to manage this function. Although there was a potential towards including functionality for evacuee notifications and alerts for members of the community, it was unclear to what capacity this may be facilitated, including the human and technical resource required to manage and monitor such alerts to the extent this could require.

Further domain-specific research also highlighted how the MAA ERSoS was actually part of a much greater set of SoSs. For example, where an instance of an ICS was itself a SoS feeding into the Municipal, Provincial, and Federal levels of the Canadian Emergency Management SoSs (EMSoS), supporting public safety throughout Canada. Although other SoSs form part of the bigger picture, the main focus and supporting data of this case study considers the view from MAA as an instrumental independent system to the ERSoS, where other immediate independent systems include the ICS and Communities, thus providing a focus towards the typical stakeholders, roles, activities, interactions, and communications for consideration and assessment within the scenario. Further context towards the interactions within this scenario is detailed throughout Section 8.1.2.

8.1.2 Applying OASoSIS

In addition to some participation working with stakeholders from MAA and *RE Cares* during the *RE Cares* workshop sessions, several publicly available datasets and user experience (UX) artefacts related to the MAA scenario and SoI were made available by *RE Cares* (RECares 2018). These would also be shared between stakeholders in a project setting to support design purposes, and could be used for further analysis.

Making use of the interactions with *RE Cares* and MAA and the subsequent published datasets would be complete enough to support the ideation around the design problem, extending from a software focus, instead to a wider SoS context of analysis. However, additional validity of the personas and scenarios derived by the *RE Cares* development stakeholders was required, as the assurance of data feeding into a risk assessment was important to identify where further information may be required, or assumptions may not be warranted. This assurance was be obtained through further requirements notes derived during the event that were overseen by the stakeholders, validating their relevance to the context of the MAA scenario.

OASoSIS would be applied to the MAA case study scenario utilising the *RE Cares* data, further validating the three contributions that represents an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE. The preliminary evaluation of OASoSIS demonstrated its suitability as a tool-supported information security risk assessment process within the organisational SoS context for independent systems. Based on the lessons learned from the evaluation in Chapter 7, OASoSIS was refined to provide a clearer indication towards the significance of tool-support. By decomposing the problem domain into different models from the view of an independent system, different perspectives of the system interactions throughout the SoS can be obtained. This includes the resulting dependencies between people, processes, assets, tasks, and goals, that may be impacted by identified information security risks.

With this as the focus, to capture the information security and human factor concerns in the MAA scenario, OASoSIS begins in *Step 0* with a process for characterising the SoS, identifying its goals, system stakeholders, levels of operational and managerial control, and roles and responsibilities for main system interactions of the SoS. The application of this step would be important towards identifying the MAA context and scope of the independent system collaboration and its interdependencies towards the ERSoS, and where managerial and operational control is in place with accountability.

The process in *Step 1* for establishing a risk criteria for the SoS interaction has been extended from the standard OA impact areas, combining considerations towards HFSI to acknowledge human related impacts of the SoS. *Steps 2 to 7* continue to identify critical information assets and the systems in which they are stored, processed, and transported, and by whom or what. Threat scenarios help to identify where there may be areas of concern towards the security of the assets, and subsequent outcomes if the threat to a weakness was realised.

Step 8 prioritises risks, and enables a second-stage deeper assessment integrating IRIS concepts with tool-supported modelling of the SoS using CAIRIS, fusing the goal-driven approach to support RBDM. Once *Step 8-Tasks 1 and 2* are complete, the resulting critical risk data enables further detail and context to model elements of the SoS. Roles, personas, high-level goals and independent systems as assets may, however, begin to be modelled with data captured from *Steps 0, 2 and 3*.

These elements of risk align with details of tasks and likely processes where information flow between systems and entities may be at risk, and where task and goal obstructions may occur. Tasks provide narratives describing how people carry out work in the system being specified. IRIS characterises people using personas, where responsibilities can be allocated to roles associated to personas. OASoSIS leverages the IRIS conceptual relationships between roles and responsibilities, as illustrated in Figure 8.1.

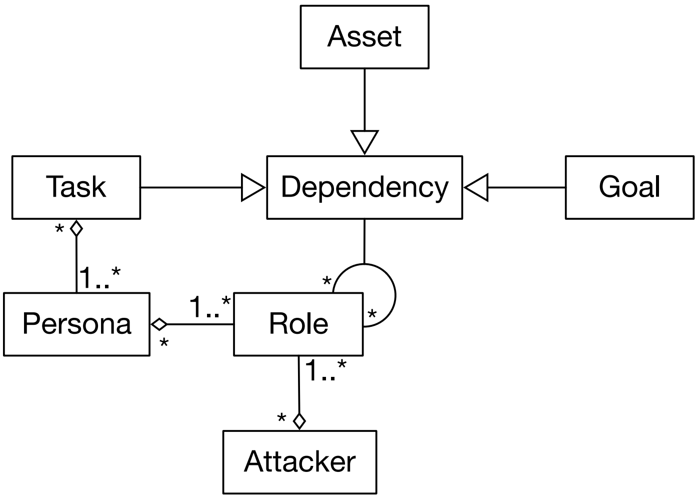


Fig. 8.1 IRIS Role and Responsibility relationships used by OASoSIS

This complements other IRIS concepts, for example, with IRIS risk and KAOS-based goal concepts (Van Lamsweerde 2009), and task concepts as shown in Figure 8.2. The integration of these concepts would also be helpful towards identifying where personas may become overloaded with responsibilities, or may be overly dependent on other people; this may lead to potential vulnerabilities (Faily 2018b).

Although not shown in Figure 8.2, some of the IRIS concepts present are aligned with DFD concepts. Use cases are synonymous with processes, and certain types of assets are synonymous with entities and data stores. With the additional concept of data-flow, this makes it possible to model DFDs in order to capture how information would potentially flow across the ERSoS. How IRIS is conceptually aligned with DFDs is described in more detail in Coles et al. (2018).

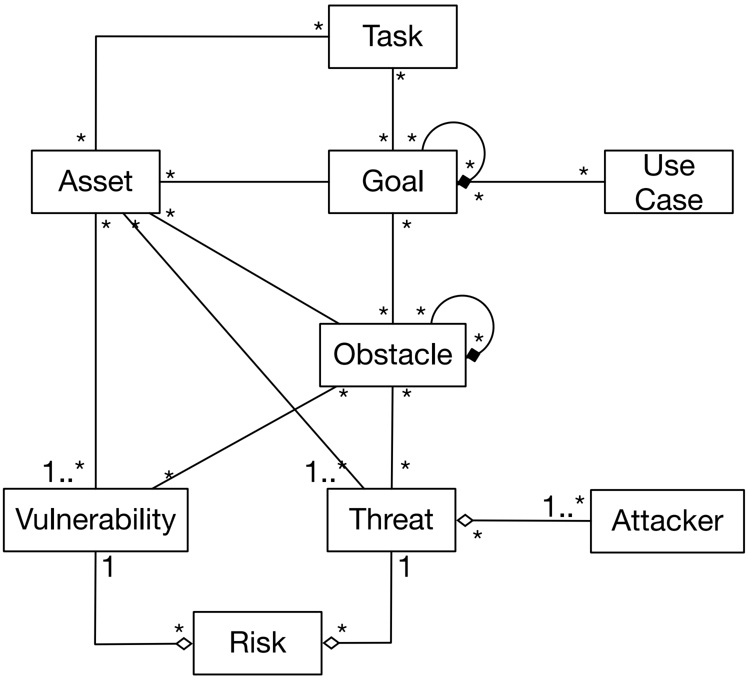


Fig. 8.2 IRIS Risk, Task, and Goal relationships used by OASoSIS

These combined elements would help to provide the foundation for deeper analysis into security and human factor concerns within the SoS, and reasoning towards system requirements to support or enable SoS processes and tasks, to achieve ERSoS goals.

Furthermore, previous findings in Chapter 7 also highlighted the evident gap towards the application of modelling, illustrating who is accountable for what, where, and whom, e.g. assets, tasks, processes, goals, risks, and their associated roles of responsibility within the SoS. When accounting for security and human factor risks and concerns during SoSRE, it is important to capture in as accurate detail as possible all known critical operations and system interactions of the SoS, and their nodes of ownership, authority, and accountability where independent systems and the SoS as a whole are dependent upon its operability and interoperability. In particular, where information flows are critical to the operation, it is crucial to clearly understand who controls what, and who is responsible and accountable (Boy and Grote 2011) where assets are used in tasks to achieve goals, which may be obstructed by risks and their potential consequences.

This may be captured, modelled, and analysed from different perspectives. For example, from an organisational and systems perspective, this identifies the general top-down structure, and bottom-up SoS interaction with specific goals, roles, and tasks important to the problem domain. Whereas, from an information security risk assessment perspective, this begins with who owns the information assets, the intended use, context, and security needs, then in which internal and external systems the information assets are to be stored, processed, and transported between, whilst capturing related owners and roles of responsibility.

The concept would, therefore, be aligned with other IRIS concepts. A meta-model representing the owner concept towards assets, goals, tasks, processes, and risk elements that aligns with IRIS concepts is shown in Figure 8.3. This would specifically align with meta-data already captured within each Tag field of the meta-model components integrated into CAIRIS that have been used to specify and capture the organisation, person, or role regarded as the owner with accountability. To implement this concept, the output of certain models were modified within the CAIRIS source-code to visualise these dependencies of ownership and accountability, leaving existing role associations to represent interactions of responsibility afforded to the role, or where a role should be consulted or informed about a particular aspect towards the activities or RBDM. How the owner concept in Figure 8.3 is applied is discussed in Section 8.1.5.

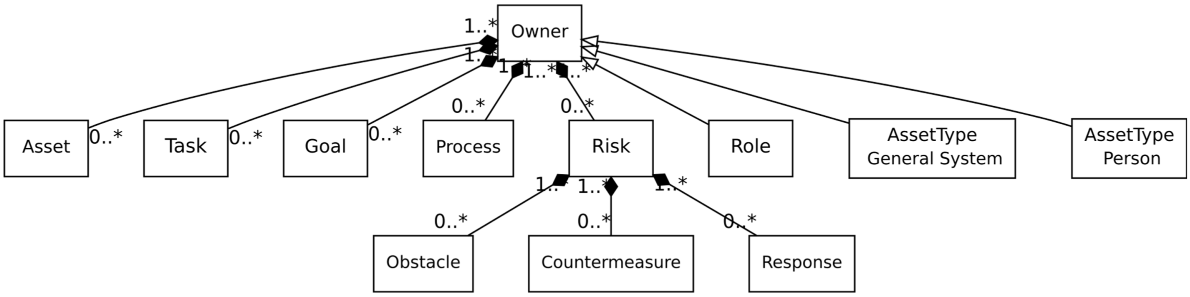


Fig. 8.3 Extension to IRIS concepts with an Owner meta-model used by OASoSIS

Applying Step 0 - Characterising the MAA Emergency Response System as a SoS

Stakeholder supplied information and EMSoS research provided the basis for the characterisation of the ERSoS in the first step of the process. This indicated the type of systems and information that would be used and communicated within the SoS. MAA, whose day-job it is to maintain community and industry relationships, and the emergency response portal, would use related portal information to support the emergency operations. MAA would, in this scenario, be integral to delivering the emergency response application and emergency situation infrastructure for messaging throughout Alberta, Canada.

MAA Emergency Response Management and Oversight

Stakeholder Involvement

In this scenario, the primary stakeholders include MAA, ICS, and Communities. MAA provides its own input into the SoS, in addition to the managerial command and control infrastructure to assist emergency operations, and its related stakeholders to provide this. Whereas, the ICS rely upon the emergency response application to support their own emergency response command and control activities. The ICS will contain a range of stakeholders related to emergency response activities at municipal and provincial levels. At one level, this includes responders such as firefighters, or at other levels, entities such as the Calgary and Alberta Emergency Management Agencies (CEMA/AEMA).

These systems are specifically dependent upon communication and information flow between interoperable systems when tending to an emergency scenario. Communities as evacuees also depend upon the public information flow to know what to do in an emergency. To what degree evacuees would be dependent, would relate to the level of use or reliance placed upon the emergency response application for evacuees. In this scenario, very limited interaction for evacuees has been applied, whereas the ICS users would have a quite different interaction with role dependent access to information.

Governance

The SoS governance is provided by MAA working with emergency response and industry partners. For example, fire departments, communities, and emergency management agencies. The supporting portal and emergency response application funding would be provided by MAA and partners. All users of the software application, e.g. the ICS, their responders, and community users would be required to own or operate a smart device to interact with the application. Governance specifically for the ICS would also be provided by CEMA or AEMA.

MAA Emergency Response Operational Environment

Operational Focus

MAA and its data input from the portal would provide important information to support ICS operations. The infrastructure provided by MAA would offer command and control capabilities to the ICS, where the ICS is managed and operated by the Incident Command and its Incident Commander. The ICS would be operationally responsible for its users interacting with the emergency response application for necessary data flow. The ICS would also be responsible for responding to evacuee notifications and related public information updates. Members of the community would be responsible for their use of the emergency response application.

MAA Emergency Response Implementation

Acquisition

The supporting infrastructure would be the responsibility of MAA to provide the required data centre and network access for services provided by the emergency response application. Where users are to be responsible for providing the smart device systems to interact with the application, constraints may apply regrading compatibility, software updates, and correct usage of the emergency response application. In some cases, the smart device may be owned by an entity within the ICS, such as a fire department, although in most cases the assumption is that personal devices would be used that are outside of the direct control of MAA and the ICS.

Test & Evaluation

In this scenario, the sole accountability for design and testing of the emergency response application and related infrastructure would reside with MAA and its engineering partners. However, what is outside of the control of MAA is the availability of local cell networks in real-time, compared to that of design-time. Mobile cell networks may be accounted for by municipal or provincial EMSoSs.

MAA Emergency Response Engineering and Design Considerations

Boundaries and Interfaces

In many EMSoS scenarios, the ICS maybe instantiated across multiple towns or provinces, thus creating a bigger set of SoSs with differing controls and regulations. In the first instance, the area of Calgary and throughout Alberta would be the main operational and geographical boundaries, which may be required to extend with other municipalities or provinces. Other boundaries and interconnections may include sea, air, and space domains, but would primarily be cyber and land based. The most immediate trust boundaries are between MAA and the ICS responders as system users, and between the ICS and the evacuees.

Performance & Behaviour

Each EMSoS and ICS provides a unique set of systems and scenario in which the emergency response application is operated. Ongoing usage can be monitored by MAA. Whereas, the effectiveness of the application, its interface, or functionality would be monitored by the ICS. Users of the emergency response application would likely monitor and report issues from their devices.

8.1.3 Identifying related Assets and Concerns

Applying Steps 1 to 5

The risk criteria in *Step 1* was aligned accordingly to the environment where safety and human factors are prevalent impact areas within this SoS domain. *Step 0* already provided a good indication towards the main stakeholders and users within the ERSoS. *Steps 2 and 3* centred around the information assets considered critical to MAA and their interaction with the SoS and its users, and in which systems they were to be stored, processed, and transported between.

Once the main stakeholders and systems were identified, along with high-level goals and dependencies, these were considered against tasks derived from the personas and scenarios. Six personas were used representing:

- An Incident Commander, who was also a Firefighter;
- An Emergency Medical Technician;
- An On-Site Supervisor;
- A Public Information Officer;
- An Emergency Manager of MAA; and
- An Evacuee.

Using the supplied personas and user stories provided an indication towards the possible scenarios in which related activities may occur. This would include data stored in the portal and transferred into the application by the MAA persona to support ICS operations, as well as data coming from ICS operations, processed by personas of responders and other personnel using the application that interfaces with the MAA servers and databases. Notifications related to the persona of the evacuee were also considered.

Steps 4 and 5 considered possible areas of concern guided by threat scenarios where unauthorised, disclosure, modification, destruction, and interruption may be attributed to potential threats or weaknesses to the SoS. When applying the OA threat scenarios, these were related to the activities performed by each persona, and where possible attackers may have a potential to exploit a weakness. Many of these concerns centred around the use of smart devices, where usability issues, human error, and malicious activity could occur. Other concerns also considered the potential for environmental concerns, such as smoke or forestry locations affecting cell and internet signals.

8.1.4 Analysing and Evaluating related Assets and Concerns

Applying Steps 6 to 8

Based on the severity of the consequences, and the likelihood of the occurrence, areas of concern and related risks were calculated and evaluated. Based on persona activities, 486 potential threat and vulnerability combinations were identified towards areas of concern, of which 57 risks were identified for secondary analysis. Risks of highest concern related to emergency responders and the reliance placed upon them to independently supply and control a smart device to operate the emergency response application. For example, as these were assumed to be personal devices used for a different purpose, e.g. to check emails or use other applications, a virus could not only disable the device, but affect the application and its data in some way.

Other risks considered personas having the correct role-based access to the application and data based upon their responder role, which may also change during operations. Usability, missed alerts, and therefore error became a growing theme for some activities or personas, e.g. the firefighter. Some risks that may appear lower based upon its likelihood, also required further acknowledgement. This included a loss of cell service in the area of operations due to the fire or smoke, or other network interruptions. It was identified that if this occurred, the initial impact would make the SoS redundant until service was resumed, which would potentially create other issues or consequences for the ICS. Identifying these concerns contributes to considerations for risk-based decision makers at different levels of the SoS to ensure the reliance and dependability placed upon the independent systems and sub-system interactions remains resilient.

8.1.5 Modelling the MAA ERSoS

Applying Step 8-Task3

Once the risk concern scores were calculated and prioritised, details of critical assets and their interactions captured within the data capture spreadsheets were entered into CAIRIS to begin populating the models. The models and their elements were each situated within an environment from the view of MAA. This main view was supported by additional views of the ICS, and with additional perspectives of the three levels of EMSoS for further context.

Roles and personas were one of the first set of elements to be captured in CAIRIS, along with high-level goals added to the KAOS goal model to represent SoS goals, where roles can then be assigned with responsibilities towards the goals. High-level SoS goals can be identified in a top-down approach, associating with supporting goals of independent systems to achieve the main SoS goal. Bottom-up system goals would also be captured later in the process. High-level systems assets were also added to the asset as illustrated in the filtered model example in Figure 8.4.

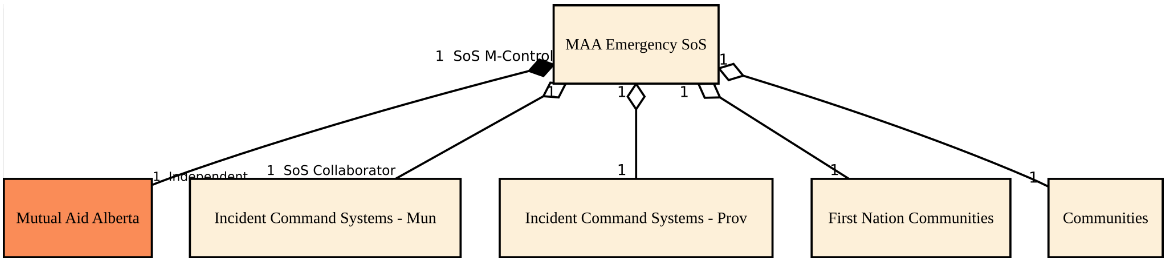


Fig. 8.4 Independent Systems of the SoS

Asset models were used to incrementally model the associations between systems, people, and information assets, showing how the SoS is decomposed in the context of the environment's perspective. Using asset models was a useful approach to visually identify in each view how the independent systems and sub-systems internal and external to the independent system of MAA have a direct interaction with other system elements. These associations were useful for highlighting the potential for different types of interoperability needs between the different assets.

Based on persona activities gained from user stories and scenarios, tasks identified in *Steps 2 to 5* were modelled then decomposed into task steps with use cases as processes to complete the task. From this data, 25 supporting use case processes were elicited with 11 related tasks, with two tasks each for the Incident Commander, Firefighter, and Emergency Manager, and one each for the remaining personas. Each task step represented by a use case could also have steps within its process, along with pre and post-conditions for use.

The conditions and process requirements also indicated where a sub-goal should be specified to support or enable the process, that when performed contributes to the task completion. The task would contribute to a main goal being achieved, which is associated to the derived sub-goal for the process. The role responsible for the process is captured, and will likely relate to a persona performing the associated task. As with goals, multiple roles may, however, be assigned to each, which begins to highlight where shared responsibilities and dependencies exist.

Data flows were modelled based on the tasks performed by a persona where the critical information assets were stored, processed, and transported between systems and external entities to fulfil system and SoS goals. The persona performing the task, also represented as a person asset, becomes the external entity modelled in the DFD. A threat model report indicates threats to each of the data flows at risk.

Because stakeholders might be concerned about tasks being completed rather than goals, many of the goals were elicited on a bottom-up rather than top-down basis. Where a task supported a goal being satisfied, the specified sub-goals would operationalise the task. These related to 73 leaf and root goals in support of the main SoS goal, providing both functional and security goals as requirements, many of which were elicited through the needs of process and task completion.

Tasks placed the goals into context and, in doing so, helped make sense of the wider scope of the SoS goal model. As a result, this assisted the elicitation of other goals making the tasks possible, and potential obstacles that might obstruct these goals, thereby obstructing the tasks and other higher level goals. For example, Figure 8.5 illustrates a slice of a generated goal model associated with the *Monitor Emergency Fire Response* task. The task operationalises the *Updates received* goal associated with the component Firefighter system. This goal is eventually refined into sub-goals that need to be satisfied by ICS system (*Responder to access data relate to role*) and EMT system (*Access to app on Smartphone provided* and *Up-to-date App Installed*). To explore the impact that an out-of-date app on an

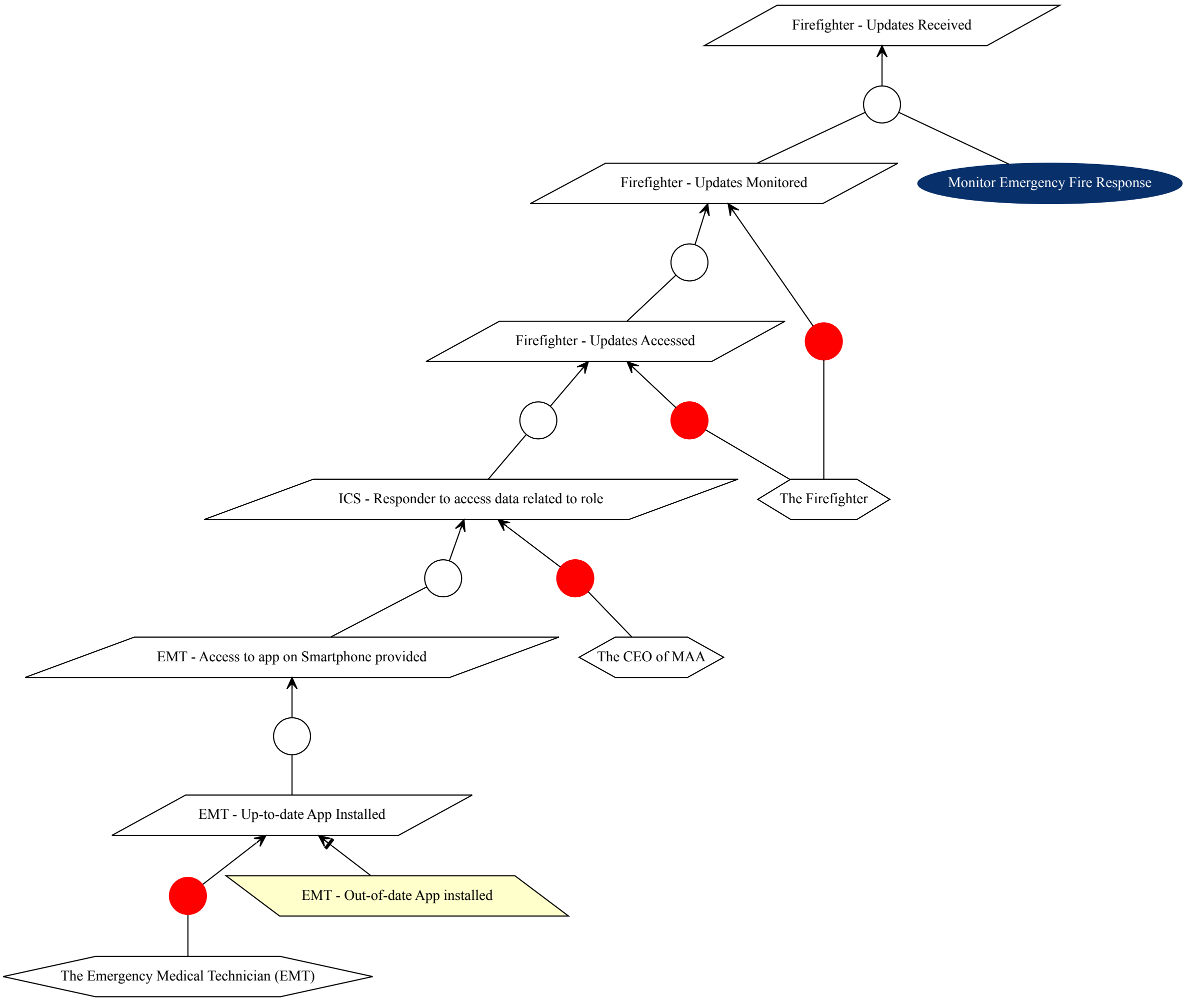

Firefighter - Updates Received
Firefighter - Updates Monitored
Monitor Emergency Fire Response
Firefighter - Updates Accessed
ICS - Responder to access data related to role
The Firefighter
EMT - Access to app on Smartphone provided
The CEO of MAA
EMT - Up-to-date App Installed
EMT - Out-of-date App installed
The Emergency Medical Technician (EMT)

Fig. 8.5 Goal and Task Obstruction

EMT's smartphone might have, an obstacle (*EMT - Out-of-date App installed*) was introduced to obstruct the *EMT Up-to-date App Installed* goal.

After demonstrating the usefulness and criticality towards understanding task and goal obstructions, this research finding helped inform CAIRIS developers towards integrating a related model validation check. When applying the validation tool within CAIRIS to validate the goal model, it was identified that not only was the *Monitor Emergency Fire Response* task obstructed, but 8 tasks in total across the SoS, thus affecting many of the SoS goals being achieved or maintained. This included responding to emergency calls from evacuees, sending approved alerts to evacuees, and initiating emergency response plans. This obstacle was then associated with the pre-existing vulnerability *Vulnerable app installed - Device*, thereby linking the SoS goals to potential security issues identified from the threat and weakness analysis in *Steps 4 and 5*.

More informed decisions may also be considered with regards to the humans performing tasks, or relying upon integrated systems for some purpose. This may indicate where processes and procedural effectiveness may need to be increased, or allocation of responsibilities reduced. Conflicts may also be identified in relation to SoS activities conflicting with the day-job activities. For example, a Firefighter is responsible for checking and sending fire related updates through the emergency response application. As part of the ICS, the firefighter's day-job is to tackle the wildfire. At times, it is difficult for a firefighter to do both, but both goals need to be satisfied. Moreover, if communication and cell coverage is lost, the availability of the emergency response application is affected. The ICS, therefore, needs fall-back methods of communication, indicating to the ICS that responders need to be trained for information flow continuity until availability is restored. This further demonstrates that, even when assessing from the view of MAA, risks and goals can be identified about the interactions of other systems across the SoS, highlighting where these systems too may need to adopt further controls to maintain a level of interoperability.

From this combined analysis, we can begin to identify SoS dependencies critical to its operation and information flow. These associations and dependencies can be modelled and visualised to identify further load-balancing concerns and areas of weakness from risk propagation across the SoS. For example, when using and combining certain modelling approaches, this enabled the identification in a corresponding element where a responsibility is or should be assigned to an object, and where another object, roles, and owner are dependent upon it for some purpose. This could include sub-goals that enable a system and its process action, performed by a role or specific persona to complete a task and achieve role-specific and system goals for the SoS.

This also begins to highlight where reliance and accountability exists between each of the independent systems, ultimately to achieve the SoS goals. To achieve each goal, this may therefore rely and depend upon a number of different owners and controlling authorities across each independent system and the SoS as a whole. To demonstrate this concept, a simple example of ERSoS interdependencies between owners, roles, goals, assets, a task and process is illustrated in Figure 8.6.

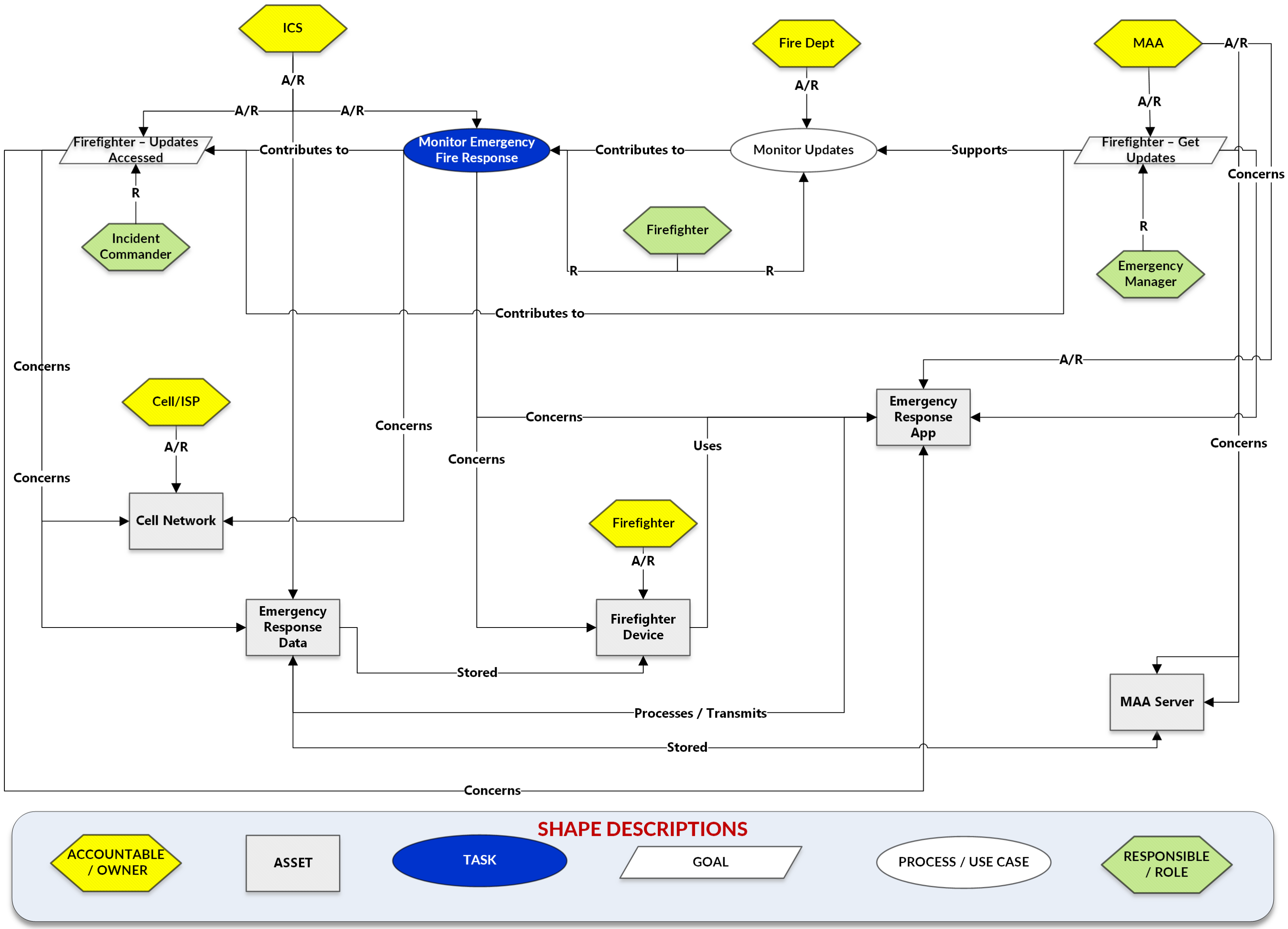


Fig. 8.6 An example chain of Responsibility and Accountability

This considers an example already modelled and accounted for through related ERSoS risks, but could by viewed from different perspectives. For example, this demonstrates a task performed by a *Firefighter* role using their smart device, where information assets may be stored, processed, or transported in different ways with other assets, roles, and people.

To achieve this task and the goal it contributes to, there are a number of dependencies between assets, goals, a process, and responsible roles. This model was then extended to show the highest level of responsibility by including a yellow hexagon shape to represent the accountable owner for an asset, goal, task, and process. Thus, when considering the example indicated in Figure 8.8 showing a filtered selection of tasks and goals that *The Firefighter* role is responsible for, this enhancement would also provide an upper layer to indicate the owners with accountability for those tasks and goals. An unfiltered model would, therefore, capture the SoS chain of accountability.

Within the first step of OASoSIS, the information gathered identified the SoS stakeholders, specifically clarifying the independent system owners and their related SoS goals. This supported the identification of dependencies between systems for potential processes and people, contributing to related tasks and goal achievement. When identifying assets, related information included their owners and specific restrictions or requirements, e.g. security goals. Dependencies between asset owners and delegated roles using information assets with other system assets for the storage, process, and transportation of information were identified. This indicated their related processes, and tasks, and associated goals. Sub-goals along with their owners and roles of responsibility were then elicited to support or enable processes for tasks completion, whilst supporting the satisfaction of a parent goal.

Having already populated the CAIRIS Tag field in many of these concepts with the corresponding accountable owner meta-data, using the integrated models towards tasks using assets and processes to achieve goals and where risk may be present, we can begin to infer and identify who may be accountable and responsible. By doing so, this indicates new dependencies between owners as well as those where authority has been delegated to another role of responsibility, e.g. to perform a process and task. However, since the aim is for using modelling and visualisation to inform decision makers, it was more useful and efficient for the model to indicate this chain of ownership and accountability, in addition to roles of responsibility, providing further clarity towards RBDM, as demonstrated in Figure 8.6 using the yellow hexagon shape. One example of this is shown in the filtered risk model shown in Figure 8.7 demonstrating two accountable owners of the task, which is a possibility in the SoS scenario given the collaborative nature. However, it was determined that in this example, the ICS would own the task, but the Fire Department would own the process, as was indicated in the example of Figure 8.6.

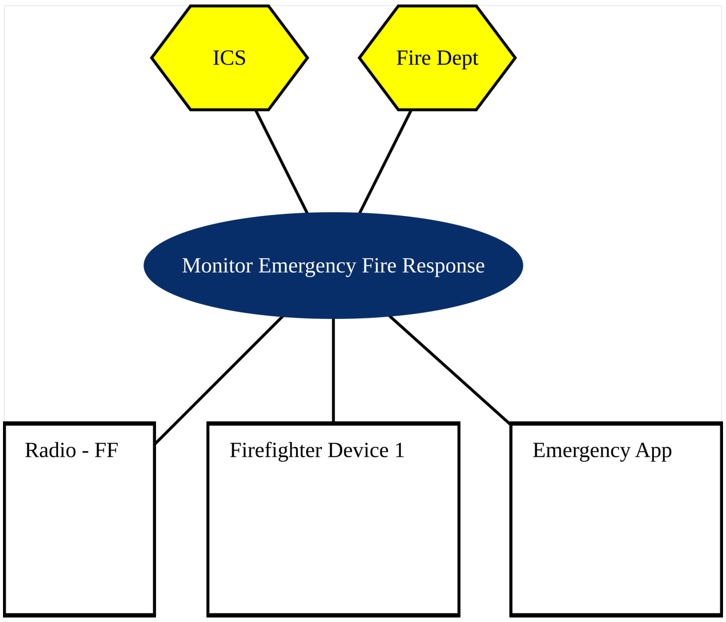


Fig. 8.7 Example of a filtered risk model enhanced to show the accountable owner(s) of the task

8.2 Discussion

Although focusing upon SoS assets, roles, and activities is central to OASoSIS, the over-arching concept that brings together the SoS context is through the integration of goals as a proxy for design rationale. This aligns directly with the concept of what a SoS aims to achieve through its collaboration. At the highest level, the goal represents the *Why* aspect of the existence of the SoS. This goal may be refined into leaf goals that support the main SoS goal being achieved and maintained. These would be refined and related to the root goal for each independent system's contributory goals, operationalised by their tasks and supporting processes to satisfy the systems' and SoS goals. To help validate this scenario and the application of the goal-driven approach, this considered input from the original MAA project stakeholders, and closing analysis provided by an expert in Disaster and Emergency management, as discussed in Section 8.2.3.

Following the early stage analysis, high-level goals were captured, aligning with identified user stories, scenarios, and tasks of personas. It was through these tasks and processes with their needs for completion that enabled further eliciting, specifying, and validating of supporting goals as requirements. Aligning the tasks performed by personas in a given scenario also helped to further integrate with security and human factors concepts, allowing for analysis towards user behaviours and associated security threats that could obstruct SoS goals from being satisfied.

From the outset, this analysis helped towards identifying the *Why* aspect of the SoS goals, and through discovery of the *What* and *How Well* tasks and processes should be enabled and performed to achieve the goals, this assists RBDM towards the prioritisation and evaluation of security risks, and possible mitigating controls and requirements.

8.2.1 ERSoS Integration Challenges and Opportunities

When considering human factors in the SoS from a wider perspective, although the evacuee's limited interaction with the application was modelled, in this scenario, it was found the MAA Emergency Manager would monitor incoming evacuee alerts, but the Incident Commander would be responsible for actioning the alerts or requests. The Public Information officer would be responsible for subsequent public announcements.

However, findings would suggest the requirement to include functionality for evacuees would need further work to consider whether the emergency response application should only act as a public information tool for evacuees, or to act as a public messaging system. In either case, these activities could require a considerable amount of resource and manpower to manage, which was not on place for this scenario. This could present a significant risk to the design and operation of the ERSoS as it was unclear who would be responsible for achieving this goal, and the magnitude of the responsibility would fall outside of the capability of the currently associated roles and personas. Moreover, it is possible this process should be integrated with the emergency management agencies, who may also implement additional crisis informatics capturing social media alerts from evacuees that can be effective for SA in an emergency scenario (Starbird et al. 2010, Dailey et al. 2018).

Other elements that were out of scope for the ERSoS scenario could be further explored towards the integration of other functionality. For example, this could include text-to-voice, and voice-to-text communications and data capture. To support RBDM, further investigation would need to consider how interoperability would be achieved if relying on different types of radio systems used by responders. Furthermore, how the responders would be made aware that audio data was being captured and stored, how and where this data would be used and stored securely ensuring its availability, and who would own this; who is in the chain of accountability. This functionality could reduce some manual interaction, but could also create other task, goal, and obstacle considerations.

During the *RE Cares* session, a requirement for capturing GPS data of responders was also proposed by the original stakeholders. Assuming informed consent would be provided, it was not clear what that purpose should be in relation to the communication flow depended upon by the SoS, or how and where else it could be used and stored securely. Incorporating map-based functionality within the application to show the real-time location of all responders using the application would be a useful opportunity. With appropriate access controls, this functionality would reduce the need for tasks relating to team communications and co-ordination relating to fire areas, responder, and evacuee locations.

In doing so, it would provide a COP to assist systems of the SoS to more efficiently co-ordinate emergency activities and achieve SoS goals. This would, however, create dependencies with map software and satellite communications for GPS signals. However, for users of the emergency response application, as part of the application installation and user agreement, each user would need to accept the requirement for location-based data capture, and enable their device location function. As highlighted in Section 8.1.5, fall-back measures may need to be considered if interoperability is affected towards providing real-time locations.

8.2.2 Integrating Concepts, Models, and Techniques

Environments and Assets

Using environments to capture different stakeholder views is useful where there are known interactions; this was the case in this ERSoS scenario for most systems. Environment views are also useful for considering the greater impact on the more abstract EMSoS goals. Environments also manage complexity by creating different views of what could otherwise be a complex single model. They provide focus towards the context of use for a SoI within the SoS, and its direct interactions relevant to the view being assessed and modelled. If a different perspective is required, another view can be created.

Each concept and model element served a relevant purpose towards their integration with OASoSIS. For example, using asset models to capture the structure of the SoS along with the related systems, information, and people assets critical to the SoS being assessed, and which each have interoperability needs. Each asset association is also representative of a need for interoperability between the asset types. Interoperability needs can also be analysed in the data flow model, considering the dependency placed on information flows between systems and people within the ERSoS.

However, as a consequence of the OA element of the OASoSIS approach that centres on information assets, their owners and required security attributes, the security needs for systems are not captured. The implications of this do, however, help decision makers to determine and specify how related security must be applied for the protection of the information assets when they are stored, processed, and transported to achieve ERSoS goals.

Personas and Scenarios with Tasks and Processes

Human and technical interoperability concerns are highlighted through the modelling of personas and scenarios. This has the effect of bringing the design to life from the ability to walk in the shoes of the personas to really understand challenges from their point-of-view, rather than considering stereotypes, or what the designer thinks.

Personas and their scenarios helped to characterise users and their behaviours. This is particularly useful when there are conflicting voices. For example, the *Mrs*

Firefighter persona is focused on tackling the fire, and may not be able to hear or see the emergency response application's alerts under her breathing apparatus. Because she wears fireproof gloves, she might accidentally delete important information too when using the application's user interface.

Mrs Incident Commander, who is acting for the Fire Department may not have these restrictions, but would need to control the operations using the emergency response application. In this role, she is more concerned about being provided the correct authority and information from MAA to permit all registered responders access to the application. This is in addition to monitoring information flow, and managing the Incident Command area of operations. Task overload could therefore become a factor. The personas may, therefore, interoperate with the application in similar ways, but have different needs and behaviours that need to be captured and accounted for.

Walking in the shoes of the persona helps analysts to reflect and provide context to the needs of the personas. This clarity highlights dependencies, and suitable requirements to address these needs whilst preventing obstructions to goal satisfaction. Understanding how each persona performs a task related to SoS dependencies helped to ensure the human factor remained central to usability considerations, where security was an important aspect. Personas and scenarios provided the colour and context to the tasks being performed to achieve the SoS goals.

Goals, Obstacles, Roles, and Responsibilities

To satisfy these goals, it was useful to consider how they could be achieved, and what related goals were required to enable supporting processes contributing to task completion. Or indeed, which tasks and goals may be obstructed, thus causing issues towards goals and tasks being achieved elsewhere in the SoS.

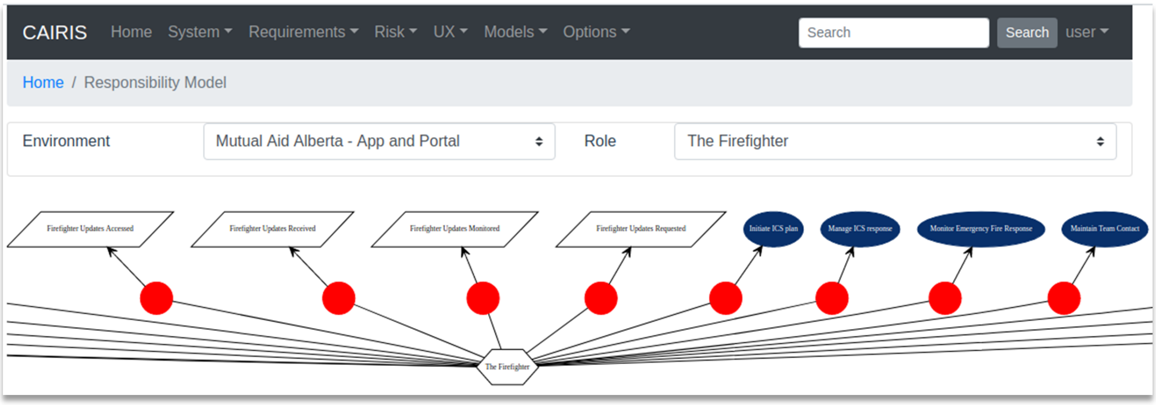
Linking use cases as processes was a logical bridge between the goal and task elements from both an interaction viewpoint, and given its use as a process within data flows. Related assets could also be associated with tasks and supporting goals. Identified dependencies of importance can then be added to CAIRIS and visualised in the responsibility model.

Goal modelling within OASoSIS captured the SoS goals required for the SoS interoperation, but as further detail was added, the SoS's size and complexity increased. Because of this, the SoS models benefit greatly from not only the ability to filter model elements, but also the ability to perform model validation checks, e.g. as described in Section 8.1.5. These checks can identify errors or omissions, or highlight design concerns where, for example, asset security properties may need to be specified.

This is similar in the asset or task model where there are many associations and interactions. However, the benefits of tool-support were relied upon to filter most models into manageable sections for focused analysis, as indicated in Figure 8.5. This reinforces the need for *Step 8-Tasks 1 and 2* to prioritise critical information assets and their interactions, otherwise models may become extremely complex, losing focus towards the most important aspects.

When integrating concepts and models, it is from these goal, task, and process elements that related trust needs and other dependencies can be identified towards roles that are dependent upon a combination of these elements to achieve SoS goals. These dependencies and specified roles of responsibility can be viewed in the responsibility model.

For example, Figure 8.8 shows a filtered selection of tasks and goals that *The Firefighter* role is responsible for. However, despite being an important factor at the beginning of the process to capture accountable owners, what was not clear from these models, was at a SoS level, who were the accountable owners that would be associated with the roles of responsibility with delegated authority, for which they are accountable for and dependent upon to achieve the SoS goals securely.


CAIRIS
Home
System
Requirements
Risk
UX
Models
Options
Search
Search
user
Home / Responsibility Model
Firefighter Updates Accessed
Firefighter Updates Received
Firefighter Updates Monitored
Firefighter Updates Requested
Initiate ICS plan
Manage ICS response
Monitor Emergency Fire Response
Maintain Team Contact
The Firefighter

Environment: Mutual Aid Alberta - App and Portal

Role: The Firefighter

Fig. 8.8 Filtered Responsibility model example

Accountability with Responsibility

In the first instance, when assessing security risk towards assets, it can be determined where there may be a weakness or potential threat that may, for example, do harm and affect the availability of the information and the system where it is used. This may be derived from activities performed by people in roles of responsibility, using related information assets, systems, and processes to achieve a SoS goal. Equally, it can be determined which related information, systems, tasks, processes, goals, roles, and their related dependencies may be affected from the propagation of the original risk scenario, and where accountability resides between owners to mitigate the potential risk with related requirements and controls.

Moreover, from this we should be able to determine if specific roles or personas performing tasks could have been overloaded from tasks or increased responsibility, which may have resulted in the risk scenario. Or, where they may potentially become overloaded from the resulting propagation of a different risk scenario that could subsequently impact another asset, process, task, or goal and their related dependencies. It would be useful to identify who would therefore be accountable in these scenarios in order for the risks to be addressed and mitigated by those deemed responsible for doing so.

Thus, when specifically focusing on information security and related human factors, the impacts and requirements go beyond that of a limited area of focus. Instead, in the SoS context, the security focus must consider the wider scope towards the people, processes, and the technology interoperability between organisations and other systems of the SoS interacting as a whole. This includes capturing those accountable, specifically regarding risk-based decisions towards mitigating SoS risks.

The risk, task, goal, and responsibility models were modified to introduce the additional symbols that are populated based on the accountable owner meta-data. As a result of the enhancement, this now indicated a more complete picture in which to capture those responsible and accountable for ensuring the secure interoperation within the SoS. Where potential areas of concern identified threats and vulnerabilities towards assets from threat agents, this enhancement supports RBDM by informing which owners and roles are relative to the risk equation. A risk owner can be assigned, e.g. the assessing system or information owner. Where elements of the risk extend to processes and tasks, and potential obstructions towards goal achievement, this informs where elements of the risk may be delegated out or transferred to other owners and roles for risk mitigating actions.

8.2.3 Stakeholder Review

Unfortunately, at the time of completion of the assessment, the original project stakeholders were no longer working on this project, perhaps due to some of the viability concerns highlighted. This also meant that where the stakeholders were now working on different projects and priorities, closing feedback and stakeholder validation was not available. Nevertheless, an expert stakeholder with extensive experience within Disaster and Emergency management instead provided feedback towards the ERSoS context, that would be used and depended upon within an EMSoS scenario.

Validation towards the context and application was first gained through an introductory meeting to provide an overview of the project and how the process of OASoSIS was applied. After the expert stakeholder had taken time to review the project material and models, a follow-up meeting was conducted. The purpose of the discussion was to provide more in-depth detail about the application of OASoSIS to the ERSoS scenario, and thus gain feedback about the risks, models, and findings, then with further concluding feedback provided towards the application of the end-end process, including the concepts concerning accountability and responsibility.

Initial comments from the expert stakeholder relating to identified risks also questioned the viability and scale of activities required to support evacuee communications that would potentially require a separate focus and platform with suitable manpower. The most prevalent concern regarded the dependency surrounding the smart device application requiring available cell service. From their experience, this concern was often a problem in those active incident environments, meaning missed alerts and a reduced ability to communicate from noise restrictions, tending to the incident, and lack of cell service could lead to further problems.

All risks and impacts were discussed, although the central concern revolved around the dependencies on users, their devices, and the time-critical need for real-time communications. Where users may experience usability issues that could affect the timely interaction and flow of information, the process was useful for indicating weaknesses towards the reliability of the SoS, and therefore enabling decision makers to address these concerns at design stage. However, if not addressed, it was suggested that reliance may instead continue towards radio communications, thus enabling a reduction in inter-system interoperability, rather than increasing it as intended by the SoS goals.

Capturing the concept of obstructions and their knock-on effect creating wider risks to the SoS was indicated as a useful contribution by the expert stakeholder, as the wider impact may otherwise have not been considered or be unknown based solely on a system level risk assessment. It was this type of information indicating the wider effects to the SoS that would add value to holistic RBDM in the ERSoS, and supporting EMSoS scenarios.

The complexity of some models was highlighted by the stakeholder, however, it was found that filtered models provided focus towards certain aspects of the SoS, that could for example, by examined in greater detail. The readability and understandability of models was found to be positive, although how some concepts within CAIRIS were aligned and interlinked required further explanation. It was found that having the ability to generate model elements in this way with tool-support, e.g. assets, personas and tasks, data flows, use case/processes, goals, and elements of risk, was considered very useful in comparison to manually aligning concepts within the process, as is often the case in other assessment processes.

Moreover, by building upon the concept of ownership and accountability, this was considered to provide a useful means of indicating other stakeholders important towards RBDM and the reduction of SoS risk. Having discussed this concept with the expert stakeholder, it was found in hindsight surprising this was an important aspect within risk assessments, but would be overlooked to some degree in current risk-focused modelling processes. However, by including this simple but effective enhancement, feedback suggested this resulted in the process becoming more complete towards identifying the relevant stakeholders and risk owners, supporting subsequent decision making processes. It was therefore considered a positive contribution to the process for RBDM and SoSRE.

8.3 Chapter Summary

In this chapter, *Case Study 2* was introduced to test and apply the three contributions combined as the end-to-end process of OASoSIS. The characterisation process and supporting *RE Cares* stakeholder information provided the foundation for the information security assessment process. This helped to guide the interactions of interest within the end-to-end information security risk assessment for the ERSoS with OASoSIS.

A main focus of the chapter was to also elaborate upon how using tool-support with a goal-driven approach helped to fuse concepts, models, and techniques when assessing and modelling the SoS information security risks and related human factors with OASoSIS. When combined, these were used to account for SoS goals, tasks, processes, obstacles, and security risks to assets. Moreover, the notion of obstructions towards tasks and goals, thus preventing other tasks and wider SoS goals from being achieved, was considered very useful for indicating the knock-on affect of risks within the SoS context.

This benefits decision makers with clarity and a point of reference for roles, responsibilities, and authority for making risk-based decisions in a SoS, in particular, where models were specifically enhanced to also show who was ultimately accountable, thus highlighting further related dependencies within the chain of accountability. Stakeholder feedback indicated this feature within the goal-driven use of tool-support was useful and important towards capturing accountability, whilst providing risk-based visualisation of the SoS being assessed, thus informing the SoS decision making processes for the security, human factors, and SoSRE communities. The combined application and alignment of these concepts, models, and techniques demonstrated the important supporting role of integrating tools for SoSRE towards capturing the broader SoS context for the information security risk assessment process and RBDM.

Chapter 9

Conclusion

In this chapter, a summary of findings and related challenges towards the problem domain are discussed. This chapter concludes by summarising how findings related to the RQs in Chapter 1 have been addressed, and how these informed the three main contributions that aimed to address the identified research gaps. An indication towards future work and research considerations is provided, either for continued validation or to expand upon other areas of interest within the problem domain.

9.1 Summary of Key Findings

Reviews of related literature demonstrated certain research gaps, in particular, where there appeared to be no SoS focused information security risk assessment approach or tool-support that aligns modelling and visualisation of related risks, people, process, and technology in a SoS context. Furthermore, there is a lack of clear guidance to inform how different concepts, models, and techniques may be integrated towards a SoS context. Another research gap also indicated a need to formulate a means in which to characterise the SoS to be assessed, thus helping to capture the context of the SoS required within an information security risk assessment.

This highlighted an industry-wide need for identifying the alignment of SoS factors and concepts suitable for eliciting, analysing, validating information security risks and their related human factors within the SoS context. To address this need, the aim of the research was focused towards identifying challenges for SoSs and how information security risks may be assessed, whilst capturing related human factor concerns. The process would be extended by aligning SoS factors and concepts suitable for eliciting, analysing, and validating these risks and concerns with the use of tool-support, to support RBDM and SoSRE activities.

9.1.1 Combining Needs

As described in Chapter 4, research gaps were first addressed by contributing a design artefact and process to support the early steps of the SoS information security risk assessment process, providing context and clarity towards systems and stakeholders of the SoS. This was found to be an important aspect of the process when interacting with different stakeholders, given that many were unfamiliar with the concept of SoSs, but could relate to the challenges towards dependencies between collaborations. The most important aspect was, however, identifying who owns, controls, and is therefore accountable for what, where, or whom in the SoS context.

Good stakeholder interaction is important, but may not always be possible in a SoS context. Moreover, user interaction may be on a small scale, or could be part of a much wider collaboration, meaning different demands upon interoperability, system needs, and application would need to be accounted for. Therefore, accounting for these needs captured in part by the characterisation process would then benefit from aligning with a socio-technical risk assessment process, but could also suit limited stakeholder interaction in which to perform it.

To address other research gaps, focus was then placed upon identifying and aligning suitable concepts, models, and techniques within the framework to help with modelling, visualising, and further assessing the interactions of a SoS using tool-support to assist risk-based decision makers towards mitigating risks to SoS goals. Considerations towards assessment and modelling were first applied in Chapter 5 to account for security risk, human factors, interoperability, and emergence.

It was found that incorporating analysis of emergent behaviour was useful, but difficult to predict and would require feedback mechanisms through ongoing monitoring to support analysis. Moreover, where interoperability perhaps had a more technical focus, it was found this should be more focused towards other social aspects, but particularly where there is a reliance upon the availability of information and communication between humans and systems. Modelling of these interactions provided a useful means in which to analyse the different interactions in more detail.

It was also determined that including the concepts of people, performing tasks and processes, interacting with assets to achieve goals, thus contributing to the satisfaction of SoS goals, would therefore support the notion of a goal-driven approach towards identifying and mitigating related risks within the SoS.

9.1.2 Implementing OASoSIS

Findings from the implementation and testing of approaches in Chapters 4 and 5 were integrated as part of OASoSIS in Chapter 6, providing useful research contributions to support an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE. This included the SoS characterisation process, then introduced OA modified towards the SoS context, and was aligned with tool-support using CAIRIS. OASoSIS was then applied in Chapters 7 and 8 to test and validate the process.

OASoSIS was first applied in Chapter 7 with a NATO-based Military MEDEVAC case study, using an example scenario related to MEDEVAC activities and its typical information flow between systems. The characterisation process was useful towards structuring information about the SoS and its stakeholders, whilst identifying its type and degrees of ownership and control within the SoS context. This context was useful towards framing the SoS and capturing related activities within the information security assessment to identify, analyse, and evaluate potential risks for the SoS, that could then be visualised in tool-support for further assessment, ultimately aligning towards how the SoS goals were being satisfied or affected by risk.

Discussing related findings with stakeholders proved a useful exercise in validating the scenario and typical structure of the SoS collaboration implemented with the asset model. However, it was indicated that where American forces integrate a greater level of technology to capture, process, store, and transmit patient data, interoperability is reduced within the SoS as other forces do not use this technology. Although, in the case of British forces, this reduces risk to some degree, where in current processes, the need to capture this degree of data is reduced by comparison, thus reducing their level of concern towards security risks. Trust assurance is also complicated by many factors, although it was determined that identifying and maintaining accountability at each level can go some way towards providing assurance.

Findings in Chapter 7 also demonstrated the useful link between people, processes, tasks, and goals, where assets are relied upon to achieve these goals. Therefore, capturing risks to these assets aligns towards how the SoS goals are being satisfied or affected by risk. Thus, when determining the needs and responsibilities of stakeholders in which to mitigate these risks, this process and its modelling and visualisation helps to inform decision makers, specifically towards risk and informs the security and human factor requirements to be captured within SoSRE. Each of these contributions are useful serving their own purpose, but combined they provide a structured approach towards assessing and modelling information security risk and human factors in SoSs.

To apply and validate OASoSIS further as an end-to-end process, Chapter 8 introduced a real-world problem and intervention based on stakeholder interaction towards the potential for an Emergency Response SoS. Related stakeholder data and artefacts provided input into the process, first gaining the characterisation and context of the SoS, then performing a first-stage assessment on the scenario with the OA steps now flowing more efficiently from the subtle changes to the process. The resulting data output provided a wealth of information in which to model using the structured approach. This incorporated personas related to tasks, who may also be associated to specified roles, and who may also be responsible for goals and processes. Assets could be modelled and associated with tasks and goals, and be captured as part of the Data Flow model. Risks and obstacles towards tasks and goals may then be realised, providing a view of the knock-on effect of risk to the success and satisfaction on other SoS goals.

In both cases, it was the modelling element of the analysis that brought the risk visualisation to life. For example, by combining different models and concepts provided different perspectives for each environment view, such as through the use of personas and tasks, or attackers with threats, vulnerabilities, and risks. Moreover, the asset models were useful for indicating the structure of the SoS related to each environment view, and the goal model for capturing the roles and goals with contributing tasks and use case processes associated with the systems assessed, aligning with the responsibility model.

However, as was evident by Chapter 8, the concept of ownership, which was an important aspect throughout the assessment, should therefore be captured and more clearly modelled with other responsibilities to provide a more complete picture towards identifying ownership and accountability, directing decision making towards mitigating SoS risks. After the models were enhanced and applied in this way, the visual result of this concept gained positive feedback from the disaster and emergency management expert stakeholder supporting its importance and logical inclusion into the process. In particular, it was determined this aspect could help communicative interoperability between those identified in a position of accountability and responsibility towards managing and mitigating the SoS risks for people and systems to remain interoperable, and SoS goals to be achieved.

9.2 Evaluation of Contributions

The aim of this research was to identify the alignment of SoS factors and concepts suitable for eliciting, analysing, validating risks within the SoS context, and to explore opportunities to integrate the use of a tool-supported approach for modelling and visualising risks in the SoS to assist RBDM. Research questions provided a means for identifying challenges associated with security risk assessment in SoSs, supported by the literature reviewed in Chapter 2. Continuing work aimed to address all research questions by considering approaches that frame SoSs, and their challenges, human factors, information security risk and modelling approaches. Based on research findings and application, this thesis claimed that *OASoSIS represents an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE*, and implemented two case studies to validate this claim and associated processes.

9.2.1 An end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE

This framework combined three main contributions to address research gaps driven by findings of the RQs posed, which together represent an end-to-end information security risk assessment and modelling process to assist RBDM in SoSRE. The framework aligns a process to provide the SoS characterisation and context, extended from work described by Dahmann and Baldwin (2008) discussed in Chapter

4, with the second contribution introducing an information security risk assessment process using a modified version of OA for SoSs. This contribution extends and modifies the work originally presented by authors of OA, Caralli et al. (2007), and was chosen as a foundation for enhancement based on findings in Chapter 5, and informed by findings from literature reviews and Chapter 4. Risk data output from the OA risk assessment is aligned with the third contribution, applying concepts, models, and techniques using tool-support from CAIRIS (Faily 2018a) to assist the process for modelling, visualisation and analysis of SoS information security risks and related human factor concerns, to help inform risk-based decision makers and SoSRE.

The first contribution gained peer review from presentation and publication of elements of this work in Ki-Aries et al. (2017b) and Ki-Aries et al. (2018b). Whereas the considerations towards the second and third contributions gained peer review from presentation and publication of elements of this work in Ki-Aries et al. (2017a) and Ki-Aries et al. (2018a). Moreover, each of the SoS examples used within research leading to the implementation and application of these contributions has gained stakeholder input and feedback at different levels.

Following the application and validation towards OASoSIS in Chapter 7, the process was however refined slightly. Some changes to the worksheets and spreadsheets were incorporated, for example, explicitly capturing the weakness or vulnerability, and improving the steps towards identifying potential threats to assets. The modelling process was also given more structure, but remains flexible to some degree towards the SoS to be modelled. Moreover, to address an evident gap identified in Chapter 7 where the concept of ownership and accountability could be made more explicit within the modelling, aligning with other associated roles of responsibility, the Tag field within CAIRIS concepts would be adopted to detail the owner, e.g. for an asset, process, task, goal, or risk. This would be visualised in certain models later in the process.

Applying OASoSIS to the Emergency Response SoS scenario in Chapter 8 was effective towards uncovering some significant risks, concerns, and challenges towards the ERSoS's usability, interoperability, and dependability that could be presented to stakeholders. Given that the original stakeholders who provided early input were now working on other projects, much of the application review to this scenario and its findings was therefore validated with a separate disaster and emergency management expert who agreed with the critical assessment findings of potential risks for the SoS described.

Of particular interest to the expert stakeholder was their observations towards the use and structuring used within asset and goal models. This was considered helpful for capturing the more horizontal and perhaps strategic aspects of the SoS, in addition to the more vertical aspects of tactical and operational levels for different systems. However, where models were large and complex, the ability to filter elements of these models proved useful for more focused discussion and analysis of the interactions and dependencies towards achieving and maintaining interoperability at different levels.

To address the need for clarity towards accountable and responsible entities, the models within CAIRIS were enhanced adding a symbol to represent the accountable owner of a related concept. Stakeholder feedback indicated it was this element of the contribution that was perhaps the most significant. In particular, with regards to RBDM and understanding the accountable owners at different horizontal and vertical levels who would be responsible for attending to information security risk and human factor concerns towards achieving the SoS goals.

What would, however, be of interest to the stakeholder in future work, was how this process could capture a similar scenario but in a developing country where the infrastructure towards emergency response and emergency management is less clear or structured by comparison to the ICS and EMSoS in Chapter 8, and may need to account for other environmental and cultural factors. Applying OASoSIS to the ERSoS scenario did provide a good level of assurance this application could be repeated with success, but could nonetheless consider opportunities if presented towards this extended scenario in future work, whilst providing further validation of OASoSIS.

9.3 Evaluation of Research Questions

9.3.1 RQ1 - What SoSs factors contribute to challenges of security risk assessment of SoSs?

A review of related literature had already begun to indicate differences in SoSs, either due to size, complexity, or geographical constraints. Findings discussed in previous chapters concluded that ownership and decentralised control present challenges for SoSs towards securely achieving and maintaining interoperability, and where conflicts may arise due to multiple stakeholders with different needs and dependencies both at system and SoS levels. Moreover, emergent behaviour is difficult to account for in a SoS security risk assessment, but should be captured as part of ongoing monitoring and SA.

Capturing the context of the SoS and its related systems and stakeholders would be an important step for a design process, and should identify the SoS-specific challenges to be captured by a security risk assessment related to its context. Understanding this context and the characteristics of a SoS would be critical towards supporting a security risk assessment of the SoS for identifying and interacting with related stakeholders important to the secure interoperation of the SoS. It was found the characterisation process should support the continuing identification of potential risks to security and human factors, whilst helping to identify related goals, tasks, people, and processes important to the SoS collaboration.

The process described in Chapter 4 aimed to address this need and was applied as part of OASoSIS with a further two case studies in Chapters 7 and 8. However, where in some SoSs there may be limited interaction between stakeholders, it is accepted that there may also be limited input towards accounting for, assessing, and modelling all aspects of the SoS interactions. This remains a challenge towards RBDM, but would nevertheless be based on available information towards the protection of independent systems of the SoS under consideration within the assessment.

9.3.2 RQ2 - What concepts are suitable to support a framework for security risk assessment with requirements elicitation in SoSs?

Research carried out in Chapter 4 towards answering RQ1 helped to inform RQ2 by considering the type of challenges presented to SoSs, elements of which should also be captured within a risks assessment framework. The importance placed upon interoperability is central to the secure interoperation of systems within the SoS, and therefore central towards achieving its goals. However, because interoperability can be depended upon at different levels, capturing the different needs towards SoS activities and people also need to be accounted for within the context of the SoS.

As was first demonstrated in in Chapter 5, this would begin during the risk assessment and would be further analysed in tool-support with combined models aligning interactions between assets. It was considered that suitable concepts to support a framework for information security risk assessment with requirements gathering should also align with RQ3. In particular, where interoperability is considered, people using assets with processes in tasks may be subject to risks from attackers, creating an impact to the systems and SoS goals, and interoperability issues between these elements at different levels.

Providing adequate information for each of these areas is required to capture the security risks and human factor concerns, that when prioritised may be aligned with tool-support for further modelling and analysis to support RBDM and SoSRE towards the wider impacts to SoS goals. Deductive research concluded OA could offer a suitable foundation that could also be enhanced and aligned towards conducting a SoS information security risk assessment, and that would support the alignment with research carried out towards RQ3.

9.3.3 RQ3 - How can the newly developed SoS security risk assessment framework be extended using modelling and visualisation software tools to assist the SoS security risk and requirements process?

RQ3 has been addressed through a review of literature, and testing the application of CAIRIS with three SoS examples to assist with modelling of information security risks and related human factors, to support RBDM and SoSRE. The results of early work in Chapter 5 were positive, indicating the potential concepts that would align between the first-stage risk assessment and a second-stage using tool-support, making use of the benefits from automatic model generation.

An alignment of OA with concepts, models, and techniques were introduced in Chapter 6 and applied as part of OASoSIS with two case studies in Chapters 7 and 8. Although a number of approaches were introduced, it was the goal-driven approach that underpinned the risk assessment by not only identifying how risk can impact upon goals being achieved, but also considering how the knock-on effect of risks can have a wider impact upon achieving other tasks and goals throughout the SoS. Capturing accountability in models extends the dependencies and illustrates the related owners and assigned roles of responsibility providing a more complete picture for RBDM by informing who would be accountable and responsible for managing and mitigating risks across the SoS.

The benefit of using tool-support within the process directly related to the ability to combine different models situated in environments, providing different perspectives of the SoS, supported by a database of correlated data towards the context of use. Models may be easily updated to account for alternate interactions and risk scenarios. Tool-support such as CAIRIS provides a level of traceability towards the requirements elicitation process, and provides a useful means in which to share models with stakeholders to analyse the SoS consequences in greater detail, and which may uncover SoS risks that may otherwise not have been accounted for. Details regarding CAIRIS model files used in case studies is discussed in Appendix C.

Moreover, a specific benefit of using CAIRIS was by maximising the use of the IRIS concepts used in CAIRIS, and establishing a process for aligning risk data types towards with these concepts in CAIRIS. These are integrated to further assess, model, and visualise in greater detail the SoS interactions, elements of risk, and risk impacts towards interoperability, people, tasks, processes, assets, and goals of the SoS. It was through combining these concepts, models, and techniques in a SoS context that assisted towards capturing the wider knock-on effect of risks throughout the SoS, whilst informing risk-based decision makers who would be responsible and accountable at different system levels towards managing and mitigating potential risks to the SoS. To support the notion of accountability, the enhancements made in some models to show an accountability symbol also demonstrated the potential for future development possibilities towards the open-source code that CAIRIS is built upon, helping to provide further context and clarity to SoS models.

9.3.4 Research Limitations

As indicated throughout, certain limitations have been a factor towards completing related research and validation. For example, where research in Chapters 4 and 7 were military-based centred around NATO activities. Although stakeholder input and feedback was good and extremely useful, detailed depth was not available for security reasons, given the need for outputs to be publishable in civilian environments. This was different by contrast to research in Chapter 5, where the focus was on a much smaller person-centred IoT SoS example, and stakeholder input and feedback was more fluid and not subject to restrictions.

Furthermore, where in Chapter 8 the original MAA stakeholders' input fed into the design data that the OASoSIS process consumed, there was no opportunity to validate the resulting models with the original stakeholders once the process was complete. However, because a single CAIRIS platform managed all the OASoSIS data, it was still possible to review the models with another expert in disaster and emergency management, who also provided a good level of assurance towards their expertise and related feedback towards the scenario assessed.

Limitations are also acknowledged towards the SoS examples used. For example, Chapter 5 considered a small-scale IoT example, and although not risk assessed, Chapter 4 considered a larger-scale NATO communications network. Extending the NATO theme, Chapter 7 considered NATO MEDEVAC operations, which had some similarities to Emergency Management and Response activities considered in Chapter 8. OASoSIS was therefore mainly tested with more organisational and operational examples of SoS, in particular towards their information assets and data flow. To strengthen the validity of OASoSIS, other SoS types and configurations could therefore be tested and validated in future work.

Moreover, where the body of research has been conducted by the researcher, future applications of OASoSIS would continue to benefit from good stakeholder interaction, and collaborative input with other researchers to ensure different perspectives and needs are captured as the process and SoS context it applies to evolves. Feedback from users adopting the use of OASoSIS would also be desirable to any future enhancements.

9.4 Future Work

9.4.1 Further Application of OASoSIS

Where SoSs can be classified as being Directed, Acknowledged, Collaborative, and Virtual, there can be many examples that may fall into these categories, and may have systems which themselves are SoSs. Some SoSs may be highly dependent upon technology, whereas for others there is a greater dependency upon people, both however rely on the ability to interoperate and communicate at different levels.

Given the vast amounts of different system types and configurations representing SoSs, to strengthen the validity of OASoSIS, it would benefit from the application to different SoS scenarios with other stakeholders for further feedback and validation. A continuing focus would be towards the people central to the secure operations within the SoS, to whom interoperability is depended upon at many levels. Capturing these human interactions, goals, dependencies, roles of responsibility and accountable owners would remain central to the research focus towards assessing information security risks of the SoS.

9.4.2 Explainability and Traceability within OASoSIS

Explainability and traceability are also important factors, therefore models and documentation need to provide a level of assurance towards the identification, analysis, and evaluation of security risks and human factor concerns, and how they inform mitigating controls and requirements. However, when modelling a SoS, there is a potential for model complexity that could reduce the readability and explainability towards the messages they attempt to convey, meaning further work would need to be undertaken to find a suitable balance, whilst maximising the model's ability communicate related concerns of SoS interactions to decision makers. To support this, there is a potential for tool-support such as CAIRIS to be modified further to provide specified model validation checks, or models could be enhanced to suit any further identified needs that would improve the process.

To further enhance and validate the OASoSIS framework, other SoS examples could be applied, covering the different degrees of socio-technical activity and goals, where each would tell a different story, but would nonetheless account for the information security risks and related human factor concerns within the SoS. Moreover, continuing with a focus on how the notion of capturing accountability together with responsibilities can be useful for decision makers, further enhancements could be made to add further clarity and context to models, e.g. explicitly notating their related dependencies in addition to other system dependencies, or aligning impacts to asset accountability needs to those in the chain of accountability.

9.4.3 Other Applications of Research

As contributions such as the characterisation process could be used in a standalone nature, for example, in other engineering projects, this application could produce useful insights, both towards its application, and capturing different types of stakeholders and interactions, which may inform other elements of research. Research could perhaps also shift the focus slightly to other engineering model types used at different stages of the development life-cyle that were out of scope in current research.

Understanding the needs of different stakeholders or teams within the life-cycle is also important, as in some scenarios there may be no dedicated security or risk personnel with expertise to perform these duties. This means that an information security risk assessment and modelling process should be easily repeatable in different scenarios by different stakeholders, whilst helping to inform towards their design needs for addressing information security risks, capturing human factors concerns. Moreover, this supports the ideation of building in security-by-design in systems and SoSs. Future research could also consider how this may be achieved through privacy-by-design in systems and SoSs. For example, related work in Coles et al. (2018) began to explore how IRIS concepts and CAIRIS could help to capture privacy needs within the modelling process, helping to inform towards potential risks. Although the example SoI in Coles et al. (2018) was modelled at a system level, the electronic prescription service it described would actually be integrated and operated within a SoS environment and context. Therefore, extending tool-support concepts to assess and model privacy risks or concerns in the SoS context using different scenarios would offer further value to the research body of knowledge.

References

Ackoff, R. L., 1971. Towards a system of systems concepts. *Management science*, 17 (11), 661–671.

Adams, J., 1999. Cars, cholera, and cows. *Policy Analysis*, 335, 1–49.

Aitken, J. M., Alexander, R. and Kelly, T., 2011. A risk modelling approach for a communicating system of systems. *Systems Conference (SysCon), 2011 IEEE International*, IEEE, 442–447.

Alberts, C. J. and Dorofee, A., 2002. *Managing information security risks: The OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc.

Albrechtsen, E., 2007. A qualitative study of users' view on information security. *Computers & security*, 26 (4), 276–289.

Alcalde, B., Dubois, E., Mauw, S., Mayer, N. and Radomirović, S., 2009. Towards a decision model based on trust and security risk management. *Proceedings of the Seventh Australasian Conference on Information Security-Volume 98*, Australian Computer Society, Inc., 61–70.

AlhajHassan, S., Odeh, M. and Green, S., 2016. Aligning systems of systems engineering with goal-oriented approaches using the i* framework. *Systems Engineering (ISSE), 2016 IEEE International Symposium on*, IEEE, 1–7.

Alkhabbas, F., Spalazzese, R. and Davidsson, P., 2016. IoT-based Systems of Systems. *Proceedings of the 2nd edition of Swedish Workshop on the Engineering of Systems of Systems (SWESOS 2016)*, Gothenburg University.

Allan, G., 2003. A critique of using grounded theory as a research method. *Electronic journal of business research methods*, 2 (1), 1–10.

Altuhhova, O., Matulevičius, R. and Ahmed, N., 2012. Towards definition of secure business processes. *International Conference on Advanced Information Systems Engineering*, Springer, 1–15.

Amyot, D., Horkoff, J., Gross, D. and Mussbacher, G., 2009. A lightweight GRL profile for i* modeling. *International Conference on Conceptual Modeling*, Springer, 254–264.

Anon., 2010. Coalition Warrior Interoperability Exercise (CWIX) [online]. NATO Command and Control Centre of Excellence (C2COE) C2pedia. Available From: http://www.c2coe.org/c2pedia/index.php?title=Coalition_Warrior_Interoperability_Exercise_(CWIX) [Accessed 25 November 2016].

Apvrille, L. and Roudier, Y., 2013. SysML-Sec: A SysML environment for the design and development of secure embedded systems. *APCOSEC, Asia-Pacific Council on Systems Engineering*, 8–11.

Ardi, S., Byers, D., Meland, P. H., Tondel, I. A. and Shahmehri, N., 2007. How can the developer benefit from security modeling? *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, IEEE, 1017–1025.

Arnowitz, J., Arent, M. and Berger, N., 2010. *Effective prototyping for software makers*. Elsevier.

Atzeni, A., Cameroni, C., Faily, S., Lyle, J. and Fléchais, I., 2011. Here's Johnny: A Methodology for Developing Attacker Personas. *Availability, Reliability and Security (ARES), 2011 Sixth International Conference*, IEEE, 722–727.

Baadshaug, E. T., Erdogan, G. and Meland, P. H., 2010. Security modeling and tool support advantages. *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, IEEE, 537–542.

BAESystems, 2010. *The People in Systems TLCM handbook*. Created by Aerosystems International Ltd on behalf of the Human Factors Integration Defense Technology Centre consortium.

Bailey, B. P., Gurak, L. J. and Konstan, J. A., 2003. Trust in cyberspace. *Human factors and Web development*, 311–21.

Baldwin, K., Dahmann, J. and Goodnight, J., 2011. Systems of Systems and Security: A Defense Perspective. *Insight*, 14 (2), 11–14.

Baldwin, W. C. and Sauser, B., 2009. Modeling the characteristics of System of Systems. *System of Systems Engineering, 2009. SoSE 2009. IEEE International Conference on*, IEEE, 1–6.

Bartolomeo, M., 2014. Internet of things: Science fiction or business fact. *A Harvard Business Review Analytic Services Report, Tech. Rep.*

Bass, T. and Robichaux, R., 2001. Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations. *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE*, IEEE, volume 1, 64–70.

Behnia, A., Rashid, R. A. and Chaudhry, J. A., 2012. A survey of information security risk analysis methods. *SmartCR*, 2 (1), 79–94.

Benbasat, I., Goldstein, D. K. and Mead, M., 1987. The case research strategy in studies of information systems. *MIS quarterly*, 369–386.

Bernstein, P. L., 1996. *Against the Gods: The remarkable story of risk*. Wiley New York.

Boardman, J. and Sauser, B., 2006. System of Systems-the meaning of of. *2006 IEEE/SMC International Conference on System of Systems Engineering*, IEEE, 6.

Bodeau, D. and Graubart, R., 2011. Cyber Resiliency Engineering framework. *MTR110237, MITRE Corporation, September*.

Bodeau, D. J., 1994. System-of-systems security engineering. *Computer Security Applications Conference, 1994. Proceedings., 10th Annual*, IEEE, 228–235.

Böröcz, I., 2016. Risk to the Right to the Protection of Personal Data. *European Data Protection Law Review*, 2 (4), 467–480.

Boxer, P. and Garcia, S., 2009. Limits to the use of the zachman framework in developing and evolving architectures for complex systems of systems. Technical report, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Boy, G. A., 2017. Human-Centered Design of complex systems: An experience-based approach. *Design Science*, 3.

Boy, G. A. and Grote, G., 2011. The authority issue in organizational automation. *The handbook of human-machine-interaction. Ashgate, London*, 131–151.

Boyson, S., 2014. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34 (7), 342–353.

Branagan, M., Dawson, R. and Longley, D., 2006. Security Risk Analysis for Complex Systems. *ISSA*, 1–12.

British Standards Institution, 2011. BS ISO/IEC 27005, Information technology - Security techniques - Information security risk management.

British Standards Institution, 2012. ISO/IEC 27032:2012. Information technology – security techniques – guidelines for cybersecurity.

British Standards Institution, 2013. BS ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements [Electronic version].

Brooke-Holland, L. and Mills, C., 2012. Afghanistan: The Timetable for Security Transition [online]. techreport Commons Briefing papers SN05851, House of Commons Library, International Affairs and Defence Section. Available From: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN05851 [Accessed 22 November 2016].

Bruseberg, A., 2008. Human views for MODAF as a bridge between human factors integration and systems engineering. *Journal of Cognitive Engineering and Decision Making*, 2 (3), 220–248.

Buxbaum, P., 2010. Network for a Mission. *Military Information Technology*, 14 (9).

Cappelli, D., Moore, A., Trzeciak, R. and Shimeall, T. J., 2009. Common sense guide to prevention and detection of insider threats 3rd edition–version 3.1. *Published by CERT, Software Engineering Institute, Carnegie Mellon University, http://www.cert.org*.

Caralli, R. A., Stevens, J. F., Young, L. R. and Wilson, W. R., 2007. Introducing OCTAVE Allegro: Improving the information security risk assessment process. Technical report, DTIC Document.

Carney, D., Anderson, W. and Place, P., 2005. Topics in Interoperability: Concepts of Ownership and Their Significance in Systems of Systems. Technical report, Carnegie-Mellon Universsity Pittsburgh PA Software Engineering Inst.

CESG, 2012. Good Practice Guide Information Risk Management. *Good Practice Guide No. 47*, 47 (1).

CFBLNet, 2015. CFBLNet Publication 1 – Annex A, CFBLNet Terms of Reference [online]. Technical Report v8, Combined Federated Battle Laboratories Network (CFBLNet). Available From: http://www.disa.mil/CFBLNet/Docsl [Accessed 18 January 2017].

Checkland, P., 1999. *Systems thinking, systems practice*. John Wiley & Sons.

Cheng, B. H. and Atlee, J. M., 2009. Current and future research directions in requirements engineering. *Design requirements engineering: A ten-year perspective*, Springer, 11–43.

Chiprianov, V., Gallon, L., Munier, M., Aniorte, P. and Lalanne, V., 2014. Challenges in Security Engineering of Systems-of-Systems. *Troisième Conférence en IngénieriE du Logiciel*, 143.

Chowdhury, M. J. M., 2014. Security risk modelling using SecureUML. *Computer and Information Technology (ICCIT), 2013 16th International Conference on*, IEEE, 420–425.

Christopher, M. and Peck, H., 2004. Building the resilient supply chain. *The international journal of logistics management*, 15 (2), 1–14.

Clark, J. O., 2009. System of Systems Engineering from a Standards V-Model and from a Standards, V-Model, and Dual V-Model Perspective. *Systems and Software Technology Conference*.

Cleland-Huang, J., 2013. Meet Elaine: a persona-driven approach to exploring architecturally significant requirements. *IEEE Software*, 30 (4), 18–21.

Cleland-Huang, J., 2014. How well do you know your personae non gratae? *IEEE software*, 31 (4), 28–31.

Cleland-Huang, J., 2016. Stakeholders on the prowl. *IEEE Software*, 33 (2), 29–31.

Coles, J., Faily, S. and Ki-Aries, D., 2018. Tool-supporting Data Protection Impact Assessments with CAIRIS. *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*, IEEE, 21–27.

Coole, M., Corkill, J. and Woodward, A., 2012. Defence in depth, protection in depth and security in depth: A comparative analysis towards a common usage language.

Cooper, A., 1999. *The inmates are running the asylum*. Macmillan Publishing Company Inc.

Cooper, A., Reimann, R., Cronin, D. and Noessel, C., 2014. *About Face: The essentials of interaction design*. John Wiley & Sons.

Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M. and Smith, R., 2013. Privacy Considerations for Internet Protocols. RFC 6973, RFC Editor.

Corbin, J. and Strauss, A., 2008. *Basics of qualitative research (3rd ed.): Techniques and procedures for developing grounded theory*. Thousand Oaks, California: SAGE Publications Ltd, 3rd edition.

Currall, S. C. and Judge, T. A., 1995. Measuring trust between organizational boundary role persons. *Organizational behavior and Human Decision processes*, 64 (2), 151–170.

Dahmann, J., Baldwin, K. J. and Rebovich, G., 2009. Systems of systems and net-centric enterprise systems. *7th Annual Conference on Systems Engineering Research*.

Dahmann, J., Lane, J., Rebovich, G. and Baldwin, K., 2008a. A model of systems engineering in a system of systems context. *Proceedings of the Conference on Systems Engineering Research, Los Angeles, CA, USA (April 2008)*.

Dahmann, J., Rebovich, G., McEvilley, M. and Turner, G., 2013. Security Engineering in a System of Systems environment. *Systems Conference (SysCon), 2013 IEEE International*, IEEE, 364–369.

Dahmann, J., Rebovich, G. and Turner, G., 2014. An actionable framework for system of systems and mission area security engineering. *Systems Conference (SysCon), 2014 8th Annual IEEE*, IEEE, 12–17.

Dahmann, J. S. and Baldwin, K. J., 2008. Understanding the current state of US defense systems of systems and the implications for systems engineering. *Systems Conference, 2008 2nd Annual IEEE*, IEEE, 1–7.

Dahmann, J. S., Rebovich Jr, G. and Lane, J. A., 2008b. Systems Engineering for Capabilities. Technical report, DTIC Document.

Dailey, D., Soden, R. and LaLone, N., 2018. Crisis informatics for everyday analysts: A design fiction approach to social media best practices. *Proceedings of the 2018 ACM Conference on Supporting Groupwork*, ACM, 230–243.

De Bruijn, H. and Herder, P. M., 2009. System and actor perspectives on sociotechnical systems. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 39 (5), 981–992.

Dekhtyar, A., Hayes, J. H., Hadar, I., Combs, E., Ferrari, A., Gregory, S., Horkoff, J., Levy, M., Nayebi, M., Paech, B. et al., 2019. Requirements engineering (re) for social good: Re cares [requirements]. *IEEE Software*, 36 (1), 86–94.

DeLaurentis, D., 2007. Role of Humans in complexity of a System-of-Systems. *International Conference on Digital Human Modeling*, Springer, 363–371.

Dezfuli, H., Stamatelatos, M., Maggio, G., Everett, C., Youngblood, R., Rutledge, P., Benjamin, A., Williams, R., Smith, C. and Guarro, S., 2010. NASA Risk-Informed Decision Making Handbook.

Diaper, D. and Stanton, N., 2004. *The handbook of task analysis for human-computer interaction*. Lawrence Erlbaum.

Dillard, K., Pfost, J. and Ryan, S., 2006. *The Security Risk Management Guide*. Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence.

Director of Systems Engineering, 2010. *Systems Engineering Guide for Systems of Systems: Summary*. Department of Defense, Office of the Director, Defense Research and Engineering, Washington, D.C.

Dogan, H., Pilfold, S. A. and Henshaw, M., 2011. The role of Human Factors in addressing Systems of Systems complexity. *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*, IEEE, 1244–1249.

Dyson, G. B., 2012. *Darwin among the machines: The evolution of global intelligence*. Basic Books.

Ellison, R., Alberts, C., Creel, R., Dorofee, A. and Woody, C., 2010. Software Supply Chain Risk Management: From Products to Systems of Systems [online]. Technical Report CMU/SEI-2010-TN-026, Carnegie Mellon University Pittsburgh PA Software Engineering Inst., Pittsburgh, PA. Available From: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9377 [Accessed 10 February 2017].

Everett, C., 2011. A risky business: ISO 31000 and 27005 unwrapped. *Computer Fraud & Security*, 2011 (2), 5–7.

Faily, S., 2018a. CAIRIS web site. https://cairis.org.

Faily, S., 2018b. *Designing Usable and Secure Software with IRIS and CAIRIS*. Springer, 1st edition.

Faily, S., 2018c. Personahelper. Chrome Web Store. Available From: https://chrome.google.com/webstore/detail/persona-helper/mhojpjjecjmdbbooonpglohcedhnjkho [Accessed 2 May 2018].

Faily, S. and Fléchais, I., 2010a. Barry is not the weakest link: Eliciting Secure System Requirements with Personas. *Proceedings of the 24th BCS Interaction Specialist Group Conference*, British Computer Society, 124–132.

Faily, S. and Fléchais, I., 2010b. A meta-model for usable secure requirements engineering. *Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems*, ACM, 29–35.

Faily, S. and Fléchais, I., 2010. The secret lives of assumptions: Developing and refining assumption personas for secure system design. *Proceedings of the 3rd Conference on Human-Centered Software Engineering*, Springer, volume LNCS 6409, 111–118.

Faily, S. and Fléchais, I., 2014. Eliciting and Visualising Trust Expectations using Persona Trust Characteristics and Goal Models. *Proceedings of the 6th International Workshop on Social Software Engineering*, ACM, SSE 2014, 17–24.

Faily, S. and Iacob, C., 2017. Design as code: Facilitating collaboration between usability and security engineers using cairis. *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)*.

Faily, S., Lyle, J., Namiluko, C., Atzeni, A. and Cameroni, C., 2012. Model-driven architectural risk analysis using architectural and contextualised attack patterns. *Proceedings of the Workshop on Model-Driven Security*, ACM, 3.

Fan, C. and Mostafavi, A., 2018. Establishing a framework for disaster management system-of-systems. *2018 Annual IEEE International Systems Conference (SysCon)*, IEEE, 1–7.

Finn, W., 2011. Afghan Mission Network: The Human Factor [online]. Available From: http://amrel.com/2011/02/02/afghan-mission-network-the-human-factor/ [Accessed 15 November 2016].

Firesmith, D. G., 2003. Analyzing and specifying reusable security requirements. Technical report, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Fléchais, I., Riegelsberger, J. and Sasse, M. A., 2005. Divide and Conquer: The role of trust and assurance in the design of secure socio-technical systems. *Proceedings of the 2005 workshop on New security paradigms*, ACM, 33–41.

Flemisch, F., Heesen, M., Hesse, T., Kelsch, J., Schieben, A. and Beller, J., 2012. Towards a dynamic balance between humans and automation: authority, ability, responsibility and control in shared and cooperative control situations. *Cognition, Technology & Work*, 14 (1), 3–18.

Frank, M., 2014. The Human Factor in Systems Engineering: Engineering Systems Thinking. *Advances in Human Factors, Software, and Systems Engineering*, 6, 163.

Friedenthal, S., Moore, A. and Steiner, R., 2014. *A practical guide to SysML: the systems modeling language*. Morgan Kaufmann.

Friedrich, G., 2014. From Afghanistan Mission Network to Federated Mission Networking [online]. *NATO C4ISR Industry Conference & TechNet International 2014: Session 2 – New Generation C2 Services*, AFCEA Europe, NCI Agency. Available from: https://www.eiseverywhere.com/file_uploads/2f6043f27e1576122f1b3e0319d5b1d8_FromAMNtoFMN-Friedrich.pdf [Accessed 24 November 2016].

Furnell, S., 2005. Why users cannot use security. *Computers & Security*, 24 (4), 274–279.

Ghanavati, S., Rifaut, A., Dubois, E. and Amyot, D., 2014. Goal-oriented compliance with multiple regulations. *Requirements Engineering Conference (RE), 2014 IEEE 22nd International*, IEEE, 73–82.

Giannopoulos, G., Filippini, R. and Schimmer, M., 2012. Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. *JRC Technical Notes*.

Gillham, B., 2000. *Case study research methods*. Bloomsbury Publishing.

Giorgini, P., Kolp, M., Mylopoulos, J. and Pistore, M., 2004. The tropos methodology. *Methodologies and software engineering for agent systems*, Springer, 89–106.

Given, L. M., 2008. *The Sage encyclopedia of qualitative research methods*. Sage publications.

Glaser, B. G., 1978. Advances in the methodology of grounded theory: Theoretical sensitivity.

Glaser, B. G., Strauss, A. L. and Strutzel, E., 1968. The discovery of grounded theory; strategies for qualitative research. *Nursing research*, 17 (4), 364.

Go, K. and Carroll, J. M., 2004. Scenario-Based Task Analysis. D. Diaper and N. A. Stanton, eds., *The Handbook of Task Analysis for Human-Computer Interaction*, Lawrence Erlbaum Associates.

Gonzalez, J. J. and Sawicka, A., 2002. A framework for human factors in information security. *Wseas international conference on information security, Rio de Janeiro*, 448–187.

Goulding, C., 2002. *Grounded theory: A practical guide for management, business and market researchers*. Sage.

Gov.UK, 2015. Cyber Essentials Scheme: Overview [online]. Department for Business, Energy & Industrial Strategy, Gov UK. Available From: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview [Accessed 22 April 2017].

Grandison, T. and Sloman, M., 2003. Specifying and analysing trust for internet applications. *Towards the Knowledge Society*, Springer, 145–157.

Griffee, D. T., 2005. Research tips: Interview data collection. *Journal of Developmental Education*, 28 (3), 36–37.

Haimes, Y. Y., 2017. Risk Modeling of Interdependent Complex Systems of Systems: Theory and Practice. *Risk Analysis*.

Haley, C. B., Laney, R. C., Moffett, J. D. and Nuseibeh, B., 2004. The effect of trust assumptions on the elaboration of security requirements. *12th IEEE International Conference on Requirements Engineering (RE 2004), 6-10 September 2004, Kyoto, Japan*, 102–111.

Harkins, M., 2012. *Managing Risk and Information Security: Protect to enable*. Apress.

Hartenstein, C. D. I., 2008a. Medical Evacuation in Afghanistan: Lessons Identified Lessons Learned [online]. Technical report. Available From: https://stopthemedevacmadness.files.wordpress.com/2012/02/nato-medical-evacuation-in-afghanistan-mp-hfm-157-05.pdf[Accessed 19 January 2018].

Hartenstein, C. D. I., 2008b. Medical Evacuation Policies in NATO: Allied Joint Doctrine for Medical Evacuation [online]. Technical report. Available From: https://stopthemedevacmadness.files.wordpress.com/2012/02/nato-medical-evacuation-policies-in-nato-mp-hfm-157-01.pdf [Accessed 19 January 2018].

Harvey, C. and Stanton, N. A., 2014. Safety in System-of-Systems: ten key challenges. *Safety science*, 70, 358–366.

Hennink, M., Hutter, I. and Bailey, A., 2010. *Qualitative research methods*. Sage.

Henshaw, M. J. d. C., 2016. Systems of Systems, Cyber-Physical Systems, the Internet-of-Things... Whatever Next? *Insight*, 19 (3), 51–54.

Henshel, D., Cains, M., Hoffman, B. and Kelley, T., 2015. Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, 3, 1117–1124.

Henson, S. A., Henshaw, M., Barot, V., Siemieniuch, C., Sinclair, M., Jamshidi, M., Dogan, H., Lim, S., Ncube, C. and DeLaurentis, D., 2013. Towards a systems of systems engineering eu strategic research agenda. *System of Systems Engineering (SoSE), 2013 8th International Conference on*, IEEE, 99–104.

Herrmann, A. and Paech, B., 2009. Practical challenges of requirements prioritization based on risk estimation. *Empirical Software Engineering*, 14 (6), 644–684.

Herrmann, K., 2010. Assured and Secure End-to-End CIS Services Provision in Network-Enabled Environment [online]. *TechNet International 2010: Session II*, AFCEA. Available From: http://www.afcea.org/europe/events/tni/10/documents/LtGenHerrmann.pdf [Accessed 22 November 2016].

Hignett, S., Tutton, W. M. and Tatlock, K., 2017. Human Factors Integration (HFI) in UK healthcare route map for 1 year, 5 years, 10 years and 20 years. *Proceedings of the Annual Conference of the Chartered Institute of Ergonomics & Human Factors, 25-27 April 2017*, Contemporary Ergonomics & Human Factors 2017:, Daventry, Northamptonshire, UK: © Chartered Institute of Ergonomics & Human Factors.

Homeland Security, 2016a. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies [online]. Available From: https://ics-cert.us-cert.gov/Recommended-Practice [Accessed 30 June 2017].

Homeland Security, 2016b. Strategic Principles for Securing the Internet of Things [online]. Available From: https://www.dhs.gov/securingtheIoT [Accessed 30 June 2017].

Homeland Security, 2017. The System of Systems Approach for Interoperable Communications [online]. Available From: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2458&file=SOSApproachforInteroperableCommunications_02.pdf [Accessed 4 October 2017].

Howard, M. and Lipner, S., 2006. *The Security Development Lifecycle*, volume 8. Microsoft Press Redmond.

Institute of Electrical and Electronics Engineers (IEEE), 1990. *Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. IEEE, New York, NY.

International Council of Systems Engineering, 2007. *Systems Engineering Handbook*. INCOSE, version 3.1 edition.

International Organization for Standardization, 2006. ISO/IEC 16085, Systems and Software Engineering — Lifecycle processes — Risk Management.

International Organization for Standardization, 2018. ISO31000: 2018 Risk management–Principles and guidelines. *International Organization for Standardization, Geneva, Switzerland*.

International Organization for Standardization, I., 2008. ISO/IEEE 12207:2008(E) Systems and Software Engineering - Software Life Cycle Processes. *International Organization for Standardization, Geneva, Switzerland*.

International Organization for Standardization, I., International Electrotechnical Commission (IEC), 2010. ISO/IEC/IEEE 24765:2010(E) Systems and Software Engineering - System and Software Engineering Vocabulary (SEVocab). *International Organization for Standardization, Geneva, Switzerland*.

Ivankova, N. V., 2014. *Mixed methods applications in action research*. Sage.

Jackson, M. C. and Keys, P., 1984. Towards a system of systems methodologies. *Journal of the operational research society*, 473–486.

Jamshidi, M., 2011. *System of systems engineering: innovations for the twenty-first century*, volume 58. John Wiley & Sons.

Jones, A., 2007. A framework for the management of information security risks. *BT technology journal*, 25 (1), 30–36.

Karabacak, B. and Sogukpinar, I., 2005. Isram: information security risk analysis method. *Computers & Security*, 24 (2), 147–159.

Keating, C. B., Padilla, J. J. and Adams, K., 2008. System of systems engineering requirements: challenges and guidelines. *Engineering Management Journal*, 20 (4), 24–31.

Keeves, J. P., 1997. Educational research, methodology, and measurement: An international handbook.

Kenyon, H. S., 2010. NATO Focuses on the Bottom Line to Support Warfighters [online]. *SIGNAL Magazine, AFCEA International*. Available From: http://www.afcea.org/content/?q=nato-focuses-bottom-line-support-warfighters [Accessed 29 November 2016].

Kesler, G., Kates, A. and Oberg, T., 2016. Design smart decision-making into the organization (and forget RACI). *People and Strategy*, 39 (3), 36.

Khan, M. H. and Shah, M. A., 2016. Survey on security threats of smartphones in Internet of Things. *Automation and Computing (ICAC), 2016 22nd International Conference*, IEEE, 560–566.

Ki-Aries, D., Dogan, H., Faily, S., Whittington, P. and Williams, C., 2017a. From Requirements to Operation: Components for Risk Assessment in a Pervasive System of Systems. *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)-Proceedings of 4th International Workshop on Evolving Security & Privacy Requirements Engineering*, IEEE, 83–89.

Ki-Aries, D. and Faily, S., 2017. Persona-Centred Information Security Awareness. *Computers & Security*, 70, 663–674.

Ki-Aries, D., Faily, S., Dogan, H. and Williams, C., 2017b. Re-framing “The AMN”: A Case Study Eliciting and Modelling a System of Systems using the Afghan Mission Network. *11th IEEE International Conference on Research Challenges in Information Science 10-12 May 2017 Brighton, UK*, IEEE.

Ki-Aries, D., Faily, S., Dogan, H. and Williams, C., 2018a. Assessing System of Systems Security Risk and Requirements with OASoSIS. *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)*, IEEE, 14–20.

Ki-Aries, D., Faily, S., Dogan, H. and Williams, C., 2018b. System of systems characterisation assisting security risk assessment. *IEEE 13th System of Systems Engineering Conference*, IEEE.

Kinder, A., Barot, V., Henshaw, M. and Siemieniuch, C., 2012. System of Systems: “Defining the System of Interest”. *System of Systems Engineering (SoSE), 2012 7th International Conference*, IEEE, 463–468.

Kissel, R., 2013. Glossary of key Information Security terms. *NIST Interagency Reports NIST IR*, 7298 (3).

Kivunja, C. and Kuyini, A. B., 2017. Understanding and Applying Research Paradigms in Educational Contexts. *International Journal of Higher Education*, 6 (5), 26–41.

Kovacic, S., Sousa-Poza, A. and Keating, C., 2008. Complex situations: an alternative approach for viewing a system of systems. *2008 IEEE International Conference on System of Systems Engineering*.

Kraemer, S. and Carayon, P., 2007. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, 38 (2), 143–154.

Kumar, R., 2019. *Research methodology: A step-by-step guide for beginners*. Sage Publications Limited.

Lane, J. A. and Bohn, T., 2013. Using SysML modeling to understand and evolve systems of systems. *Systems Engineering*, 16 (1), 87–98.

Lane, J. A. and Epstein, D., 2013. What is a System of Systems and why should I care? *University of Southern California*.

Lane, J. A. and Valerdi, R., 2007. Synthesizing SoS concepts for use in cost modeling. *Systems Engineering*, 10 (4), 297–308.

Lapouchnian, A., 2005. Goal-oriented requirements engineering: An overview of the current research. *University of Toronto*, 32.

Laracy, J. R. and Leveson, N. G., 2007. Apply STAMP to critical infrastructure protection. *Technologies for Homeland Security, 2007 IEEE Conference on*, IEEE, 215–220.

Lee, L., Egelman, S., Lee, J. H. and Wagner, D., 2015. Risk Perceptions for Wearable Devices. *arXiv preprint arXiv:1504.05694*.

Lee, M., 2012. Securing the human to protect the system: Human factors in cyber security.

Liginlal, D., Sim, I. and Khansa, L., 2009. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *computers & security*, 28 (3), 215–228.

Lock, R. and Sommerville, I., 2010. Modelling and analysis of socio-technical system of systems. *Engineering of Complex Computer Systems (ICECCS), 2010 15th IEEE International Conference on*, IEEE, 224–232.

Lock, R., Storer, T., Sommerville, I. and Baxter, G., 2010. Responsibility modelling for risk analysis.

London Assembly, 2006. Report of the 7 July Review Committee [online]. Available From: https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/archives/assembly-reports-7july-report.pdf [Accessed 18 March 2019].

Lund, M. S., Solhaug, B. and Stølen, K., 2010. *Model-driven risk analysis: The CORAS approach*. Springer Science & Business Media.

Maia, P., Cavalcante, E., Gomes, P., Batista, T., Delicato, F. C. and Pires, P. F., 2014. On the Development of Systems-of-Systems Based on the Internet of Things: A Systematic Mapping. *Proceedings of the 2014 European Conference on Software Architecture Workshops*, ACM, ECSAW '14, 23:1–23:8.

Maiden, N., Jones, S., Ncube, C. and Lockerbie, J., 2011. Using i* in Requirements Projects: Some Experiences and Lessons. E. Yu, ed., *Social Modeling for Requirements Engineering*, MIT Press.

Maier, M. W., 1996. Architecting principles for systems-of-systems. *INCOSE International Symposium*, Wiley Online Library, volume 6, 565–573.

Maier, M. W., 2005. Research challenges for Systems-of-Systems. *2005 IEEE International Conference on Systems, Man and Cybernetics*, IEEE, volume 4, 3149–3154.

Marsh, S. and Dibben, M. R., 2005. Trust, untrust, distrust and mistrust–an exploration of the dark (er) side. *International Conference on Trust Management*, Springer, 17–33.

Matulevičius, R. and Dumas, M., 2010. A comparison of secureUML and UMLsec for rolebased access control. *Proceedings of the 9th Conference on Databases and Information Systems*, 171–185.

Maxwell, J. A., 2012. *Qualitative research design: An interactive approach*, volume 41. Sage publications.

MC4, 2018. The MC4 System [online]. MC4 US Army. Available From: http://www.mc4.army.mil/Mc4System/Mc4Sys.aspx [Accessed 15 January 2018].

McElroy, K., 2016. *Prototyping for designers: developing the best digital and physical products*. O'Reilly Media, Inc.

McKnight, D. H. and Chervany, N. L., 1996. The meanings of trust.

Mead, N., Shull, F., Spears, J., Heibl, S., Weber, S. and Cleland-Huang, J., 2017. Crowd sourcing the creation of personae non gratae for requirements-phase threat modeling. *2017 IEEE 25th International Requirements Engineering Conference (RE)*, IEEE, 412–417.

Mead, N. R. and Stehney, T., 2005. *Security quality requirements engineering (SQUARE) methodology*, volume 30. ACM.

Meier, M. J., 2011. A provider's perspective: Utilizing deployed information technology to care for our wounded warriors. The Joint Staff, J4/HSSD, presented at the 2011 Military Health System Conference, January 24-27, National Harbor, Maryland: The Defense Technical Information Center. Available From: http://www.dtic.mil/dtic/tr/fulltext/u2/a556202.pdf [Accessed 19 January 2018].

Meland, P. H. and Jensen, J., 2008. Secure software design in practice. *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, IEEE, 1164–1171.

Microsoft, 2017. Visio [online]. Available From: https://products.office.com/en-gb/visio/flowchart-software?tab=tabs-1 [Accessed 20 November 2017].

Miller, K. W., Voas, J. and Laplante, P., 2010. In trust we trust. *Computer*, 43 (10), 85–87.

M'manga, A., Faily, S., McAlaney, J. and Williams, C., 2017a. Folk Risk Analysis: Factors Influencing Security Analysts' Interpretation of Risk.

M'manga, A., Faily, S., McAlaney, J. and Williams, C., 2017b. System Design Considerations for Risk Perception.

MODAF Partners, 2005. *MOD Architectural Framework Acquisition Community of Interest Deskbook*. The Ministry of Defence, 0.9 edition.

Moody, D. L., Heymans, P. and Matulevičius, R., 2010. Visual syntax does matter: improving the cognitive effectiveness of the i* visual notation. *Requirements Engineering*, 15 (2), 141–175.

Moore, A. P., Ellison, R. J. and Linger, R. C., 2001. Attack modeling for information security and survivability. Technical report, Carnegie Mellon University Pittsburgh PA Software Engineering Inst.

Morris, E., Levine, L., Meyers, C., Place, P. and Plakosh, D., 2004. System of systems interoperability (SOSI). Technical report, Carnegie Mellon University Pittsburgh PA Software Engineering Inst.

Morris, E., Place, P. and Smith, D., 2006. System-of-systems governance: New patterns of thought. Technical report, Carnegie Mellon University Pittsburgh PA Software Engineering Inst.

Mouratidis, H., 2011. Secure software systems engineering: the Secure Tropos approach. *JSW*, 6 (3), 331–339.

Myers, J. J., 2002. Risk-based Decision Making (RBDM) Guidelines - United States Coast Guard. 2.

Mylonas, A., Dritsas, S., Tsoumas, B. and Gritzalis, D., 2011. Smartphone security evaluation: The malware attack case. *Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference*, IEEE, 25–36.

Nankervis, J., 2011. Afghan Mission Network. *Command and Control In Network Enabled Capabilities Environment: Seminar Review Document*, NATO / National Defence University, 24–25.

National Research Council and others, 2007. *Human-system integration in the system development process: A new look*. National Academies Press.

NATO, 2013. NATO Standard AMedP-8.1 A1 [online]. NATO Standardization Agency. Available From: https://shape.nato.int/resources/site6362/medica-secure/publications/amedp-8.1%20eda%20v1%20e.pdf [Accessed 14 January 2018].

NATO Communications and Information Agency, 2013. CF-BLNet [online]. NCI Agency Website. Available From: https://www.ncia.nato.int/Documents/Agency%20publications/CFBLNet.pdf [Accessed 26 November 2016].

NCOIC, 2019a. NCOIC - Cross-Domain Interoperability [online]. https://www.ncoic.org/cross-domain-interoperability/ [Accessed 20 August 2019].

NCOIC, 2019b. NCOIC - What is Interoperability [online]. https://www.ncoic.org/what-is-interoperability/ [Accessed 20 December 2019].

NCSC, 2018. Introducing component-driven and system-driven risk assessments [online]. National Cyber Security Centre, Gov UK. Available From: https://www.ncsc.gov.uk/collection/risk-management-collection/component-system-driven-approaches/introducing-component-driven-and-system-driven-risk-assessments [Accessed 12 April 2018].

Ncube, C., 2011. On the Engineering of Systems of Systems: key challenges for the requirements engineering community. *2011 Workshop on Requirements Engineering for Systems, Services and Systems-of-Systems*, IEEE, 70–73.

Ncube, C. and Lim, S. L., 2018. On Systems of Systems Engineering: a Requirements Engineering Perspective and Research Agenda. *Requirements Engineering Conference (RE), 2018 IEEE 26th International*, IEEE.

Ncube, C., Lim, S. L. and Dogan, H., 2013. Identifying top challenges for international research on requirements engineering for systems of systems engineering. *Requirements Engineering Conference (RE), 2013 21st IEEE International*, IEEE, 342–344.

Neumann, W. P., 2007. Inventory of Human Factors Tools and Methods - A Work-System Design Perspective. Technical report, Ryerson University.

NHS, 2017. Information Governance (IG) Toolkit [online]. NHS - Department of Health. Available From: https://www.igt.hscic.gov.uk/ [Accessed 15 November 2017].

Nielsen, C. B., Larsen, P. G., Fitzgerald, J., Woodcock, J. and Peleska, J., 2015. Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions. *ACM Comput. Surv.*, 48 (2), 18:1–18:41.

NIST, 2017. NIST Special Publications [online]. NIST Computer Security Resource Centre. Available From: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 22 April 2017].

Noor, K. B. M., 2008. Case study: A strategic research methodology. *American journal of applied sciences*, 5 (11), 1602–1604.

North Atlantic Treaty Organization, 2012. *NATO Risk Management Guide for Acquisition Programmes - ARAMP-1*. NATO Standardization Agengy (NSA), 1 edition.

O'Brien, R., 2016. Privacy and security: The new European data protection regulation and it's data breach notification requirements. *Business Information Review*, 33 (2), 81–84.

Office of the Deputy Under Secretary of Defense, for Acquisition and Technology, Systems and Software Engineering, 2008. *Systems and Software Engineering. Systems Engineering Guide for Systems of Systems*. Washington, DC: ODUSD(A&T)SSE, 2008, 1 edition.

Öğütçü, G., Testik, Ö. M. and Chouseinoglou, O., 2016. Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83–93.

ben Othmane, L., Ranchal, R., Fernando, R., Bhargava, B. and Bodden, E., 2015. Incorporating attacker capabilities in risk estimation and mitigation. *Computers & Security*, 51, 41–61.

Ottens, M., Franssen, M., Kroes, P. and Poel, I., 2005. 8.1. 1 systems engineering of socio-technical systems. *Incose international symposium*, Wiley Online Library, volume 15, 1122–1130.

OWASP, 2017. Threat Risk Modeling [online]. Available From: https://www.owasp.org/index.php [Accessed 1 September 2017].

Pahon, E., 2012. Best Soldiers for the worst days: Medevac crews in Afghanistan save lives day, night [online]. US Army. Available From: https://www.army.mil/article/83749/best_soldiers_for_the_worst_days _medevac_crews_in_afghanistan_save_lives_day_night [Accessed 15 January 2018].

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L., 2010. Human Factors and Information Security: Individual, culture and security environment. Technical report.

Rasmussen, J., 1985. The role of hierarchical knowledge representation in decisionmaking and system management. *IEEE Transactions on systems, man, and cybernetics*, (2), 234–243.

Reason, J., 1990. *Human Error*. Cambridge university press.

Rebovich Jr., G. and Authors, M., 2014. *MITRE Systems Engineering Guide [online]*. MITRE Corporation. Available From: https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf [Accessed 10 October 2016].

RECares, 2018. RE Cares. https://wsrecares.wixsite.com/recares.

Rescorla, E. and Korver, B., 2003. Guidelines for writing RFC text on security considerations. Technical report, Internet Architecture Board (IAB).

Rhee, H.-S., Ryu, Y. U. and Kim, C.-T., 2012. Unrealistic optimism on information security management. *Computers & Security*, 31 (2), 221–232.

Richardson, C., 2012. *Bridging the air gap: an information assurance perspective*. Ph.D. thesis, University of Southampton.

Riegelsberger, J., Sasse, M. A. and McCarthy, J. D., 2005. The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies*, 62 (3), 381–422.

Rissinger, T., 2011. 13058 - “Coalition Interoperability Assurance & Validation (CIAV) and Coalition Test & Evaluation Environment (CTE2)-A Model for Coalition Interoperability in a Distributed Construct [online]. *Track 6 - Mission 3, Effective Test and Evaluation*, NDIA 14th Annual Systems Engineering Conference, San Diego, CA, USA: NDIA. Available from: www.dtic.mil/ndia/2011system/13058_RissingerWednesday.pptx [Accessed 28 November 2016].

Rose, J., 2011. Coalition Inoperability Assurance and Validation Charter [online]. Document Version 1.02, Coalition Interoperability Assurance & Validation (CIAV). Available From: https://wss.apan.org/2525/CIAV/CIAV%20Charter%20v1.02.pdf [Accessed 26 November 2016].

Ross, R., McEvilley, M. and Oren, J. C., 2016. Systems Security Engineering. *NIST Special Publication*, 800, 33.

Roudier, Y. and Apvrille, L., 2015. SysML-Sec: A model driven approach for designing safe and secure systems. *Model-Driven Engineering and Software Development (MODELSWARD), 2015 3rd International Conference on*, IEEE, 655–664.

Saltzer, J. H. and Schroeder, M. D., 1975. The protection of information in computer systems. *Proceedings of the IEEE*, 63 (9), 1278–1308.

Salvaneschi, P., 2016. Modeling of information systems as systems of systems through DSM. *Proceedings of the 4th International Workshop on Software Engineering for Systems-of-Systems*, ACM, 8–11.

SANS, 2015. Information Security Resources [online]. SANS Institute. Available From: https://www.sans.org/information-security/ [Accessed 20 May 2016].

Schneier, B., 2011. *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Scotland, J., 2012. Exploring the Philosophical Underpinnings of Research: Relating Ontology and Epistemology to the Methodology and Methods of the Scientific, Interpretive, and Critical Research Paradigms. *English language teaching*, 5 (9), 9–16.

SEBoK Authors, 2016. *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*, Hoboken, NJ: The Trustees of the Stevens Institute of Technology.: BKCASE, chapter Stakeholder Needs and Requirements. 1.7. edition.

SEBoK Authors, 2019. *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*, Hoboken, NJ: The Trustees of the Stevens Institute of Technology.: BKCASE, chapter Emergence. 2.1 edition.

Seffers, G. I., 2011a. A Lot of Blood in Kandahar [online]. SIGNAL Magazine, AFCEA International. Available From: https://www.afcea.org/content/lot-blood-kandahar [Accessed 16 January 2018].

Seffers, G. I., 2011b. Combat communicators bust paradigms [online]. *SIGNAL Magazine, AFCEA International*. Available From: http://www.afcea.org/content/?q=combat-communicators-bust-paradigms [Accessed 22 November 2016].

Seffers, G. I., 2011c. Military Treats Outbreak of Chat Rooms in Afghanistan [online]. SIGNAL Magazine, AFCEA International. Available From: https://www.afcea.org/content/military-treats-outbreak-chat-rooms-afghanistan [Accessed 16 January 2018].

Serena, C. C., Porche III, I. R., Predd, J. B., Osburg, J. and Lossing, B., 2014. Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network. Technical report, DTIC Document.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M., 2016. Taxonomy of information security risk assessment (ISRA). *Computers & Security*, 57, 14–30.

Shostack, A., 2014. *Threat modeling: Designing for security*. John Wiley & Sons.

Simon, H. A., 1979. *The American Economic Review*, 69 (4), 493–513.

Simpson, J. J. and Dagli, C. H., 2008. System of systems: Power and paradox. *System of Systems Engineering, 2008. SoSE'08. IEEE International Conference on*, IEEE, 1–5.

Sindre, G. and Opdahl, A. L., 2005. Eliciting security requirements with misuse cases. *Requirements engineering*, 10 (1), 34–44.

Software Engineering Institute, 2016. System-of-Systems Engineering [online]. Software Engineering Institute and Carnegie Mellon University. Available From: http://www.sei.cmu.edu/sos/research/sosengineering/index.cfm [Accessed 25 November 2016].

Sommerville, I., 2007a. Causal responsibility models. *Responsibility and Dependable Systems*, Springer, 187–207.

Sommerville, I., 2007b. Models for responsibility assignment. *Responsibility and dependable systems*, Springer, 165–186.

Sommerville, I., 2015. *Software Engineering*. Pearson, 10th edition.

Sommerville, I., Cliff, D., Calinescu, R., Keen, J., Kelly, T., Kwiatkowska, M., Mcdermid, J. and Paige, R., 2012. Large-scale complex IT systems. *Communications of the ACM*, 55 (7), 71–77.

Sommerville, I., Lock, R., Storer, T. and Dobson, J., 2009. Deriving information requirements from responsibility models. *International Conference on Advanced Information Systems Engineering*, Springer, 515–529.

Staker, R., 2001. Decision support for complex systems-of-systems. *Proceedings of the 16th National Conference of the Australian Society for Operations Research*, Citeseer.

Starbird, K., Palen, L., Hughes, A. L. and Vieweg, S., 2010. Chatter on the red: what hazards threat reveals about the social life of microblogged information. *Proceedings of the 2010 ACM conference on Computer supported cooperative work*, ACM, 241–250.

Stephenson, P., 2004. Risk and incident management–getting started. *Computer Fraud & Security*, 2004 (11), 17–19.

Stølen, K. and Solhaug, B., 2015. The CORAS Method [online]. Technical report, Sandia National Laboratories. Available From: http://coras.sourceforge.net/ [Accessed 18 November 2017].

Stoneburner, G., Goguen, A. Y. and Feringa, A., 2002. SP 800-30. Risk Management Guide for Information Technology Systems. Technical report, Gaithersburg, MD, United States.

Strawser, B. J. and Joy Jr, D. J., 2015. Cyber security and user responsibility: surprising normative differences. *Procedia Manufacturing*, 3, 1101–1108.

Stringer, E. T., 2013. *Action research*. Sage Publications.

Swanson, M. and Guttman, B., 1996. SP 800-14. Generally Accepted Principles and Practices for Securing Information Technology Systems.

Syalim, A., Hori, Y. and Sakurai, K., 2009. Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. *2009 International conference on availability, reliability and security*, IEEE, 726–731.

Szwed, P. and Skrzyński, P., 2014. A new lightweight method for security risk assessment based on fuzzy cognitive maps. *International Journal of Applied Mathematics and Computer Science*, 24 (1), 213–225.

Tadros, M. S., 2013. Integrating the human element into the systems engineering process and MBSE methodology. Technical report, Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States).

Taylor, S. J., Bogdan, R. and DeVault, M., 2015. *Introduction to qualitative research methods: A guidebook and resource*. John Wiley & Sons.

Thales, 2008. Thales and NATO strengthen partnership [online]. Available From: https://www.thalesgroup.com/en/content/thales-and-nato-strengthen-partnership [Accessed 16 December 2016].

The CERT Division, 2017. Octave [online]. Carnegie Mellon University. Available From: http://www.cert.org/resilience/products-services/octave/ [Accessed 30 May 2017].

Thiele, R. D., 2013. Enabling Cooperation via Common Situational Awareness – Pragmatic Considerations on NATO-China Cooperation. Technical Report 220, Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW.

Trello, 2018. Trello. Trello. Available From: https://trello.com/ [Accessed 2 May 2018].

Unuakhalu, M., 2014. Integrating Risk Management in System Development Life Cycle 1.

U.S. Customs and Border Protection, 2014. C-TPAT's Five Step Risk Assessment Process [online]. Available From: https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf [Accessed 1 May 2017].

Valerdi, R., Ross, A. M. and Rhodes, D. H., 2007. A framework for evolving system of systems engineering. *CrossTalk*.

Van Lamsweerde, A., 2009. *Requirements engineering: From system goals to UML models to software*, volume 10. Chichester, UK: John Wiley & Sons.

Van Lamsweerde, A., Brohez, S., De Landtsheer, R., Janssens, D. et al., 2003. From system goals to intruder anti-goals: attack generation and resolution for security requirements engineering. *Proc. of RHAS*, 3, 49–56.

Van Lamsweerde, A. and Letier, E., 2000. Handling obstacles in goal-oriented requirements engineering. *IEEE Transactions on software engineering*, 26 (10), 978–1005.

Veit, K. F., 2011. The Afghanistan Mission Network (AMN) – A model for network enabled capabilities [online]. *Berlin Security Conference: Panel VIII - C4ISR in NATO and EU - Command and Control in Operations*. Available from: http://www.european-defence.com/Review/2011/binarywriterservlet?imgUid=a3740d83-f8c1-b331-76b8-d77407b988f2&uBasVariant=11111111-1111-1111-1111-111111111111 [Accessed 25 November 2016].

Visual Paradigm, 2017. Solutions [online]. Available From: https://www.visual-paradigm.com/solution/ [Accessed 20 November 2017].

Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, 38, 97–102.

Warfel, T. Z., 2009. *Prototyping: a practitioner's guide*. Rosenfeld media.

Weilkiens, T., Lamm, J. G., Roth, S. and Walker, M., 2015. *Model-based system architecture*. John Wiley & Sons.

Wensveen, S. and Matthews, B., 2015. Prototypes and prototyping in design research. *The Routledge Companion to Design Research. Taylor & Francis*.

Werneck, V. M. B., Oliveira, A. d. P. A. and do Prado Leite, J. C. S., 2009. Comparing GORE Frameworks: i-star and KAOS. *WER*.

Whitehead, S., 2014. Achieving Joint Force 2020 Through Coalition Information Sharing [online]. Association for Enterprise Information (Website). Available from: http://www.afei.org/PE/4A05/Documents/Whitehead_4A05%20%20AFEI%20Draft %205%20Mar%2014%20(Smooth)1630.pdf [Accessed 24 November 2016].

Whitman, M. E. and Mattord, H. J., 2011. *Principles of information security*. Cengage Learning.

Whittington, P. and Dogan, H., 2015. SmartPowerchair: A pervasive system of systems. *System of Systems Engineering Conference (SoSE), 2015 10th*, IEEE, 244–249.

Whittington, P. and Dogan, H., 2016. SmartPowerchair: Characterization and Usability of a Pervasive System of Systems. *IEEE Transactions on Human-Machine Systems*.

Whittington, P., Dogan, H. and Phalp, K., 2015. SmartPowerchair: To boldly go where a powerchair has not gone before. *Proceedings of the International Conference on Ergonomics & Human Factors 2015*, 233–240.

Willis, J. W., Jost, M. and Nilakanta, R., 2007. *Foundations of qualitative research: Interpretive and critical approaches*. Sage.

Woodcock, J., Cavalcanti, A., Fitzgerald, J., Larsen, P., Miyazawa, A. and Perry, S., 2012. Features of CML: A formal modelling language for systems of systems. *2012 7th International conference on system of systems engineering (SoSE)*, IEEE, 1–6.

Workman, M., Phelps, D. C. and Gathegi, J. N., 2012. *Information Security for Managers*. Jones & Bartlett Publishers.

Yin, R. K., 2013. *Case study research: Design and methods*. Sage publications.

Yoon, H. S. and Occeña, L., 2014. Impacts of customers' perceptions on internet banking use with a smart phone. *Journal of Computer Information Systems*, 54 (3), 1–9.

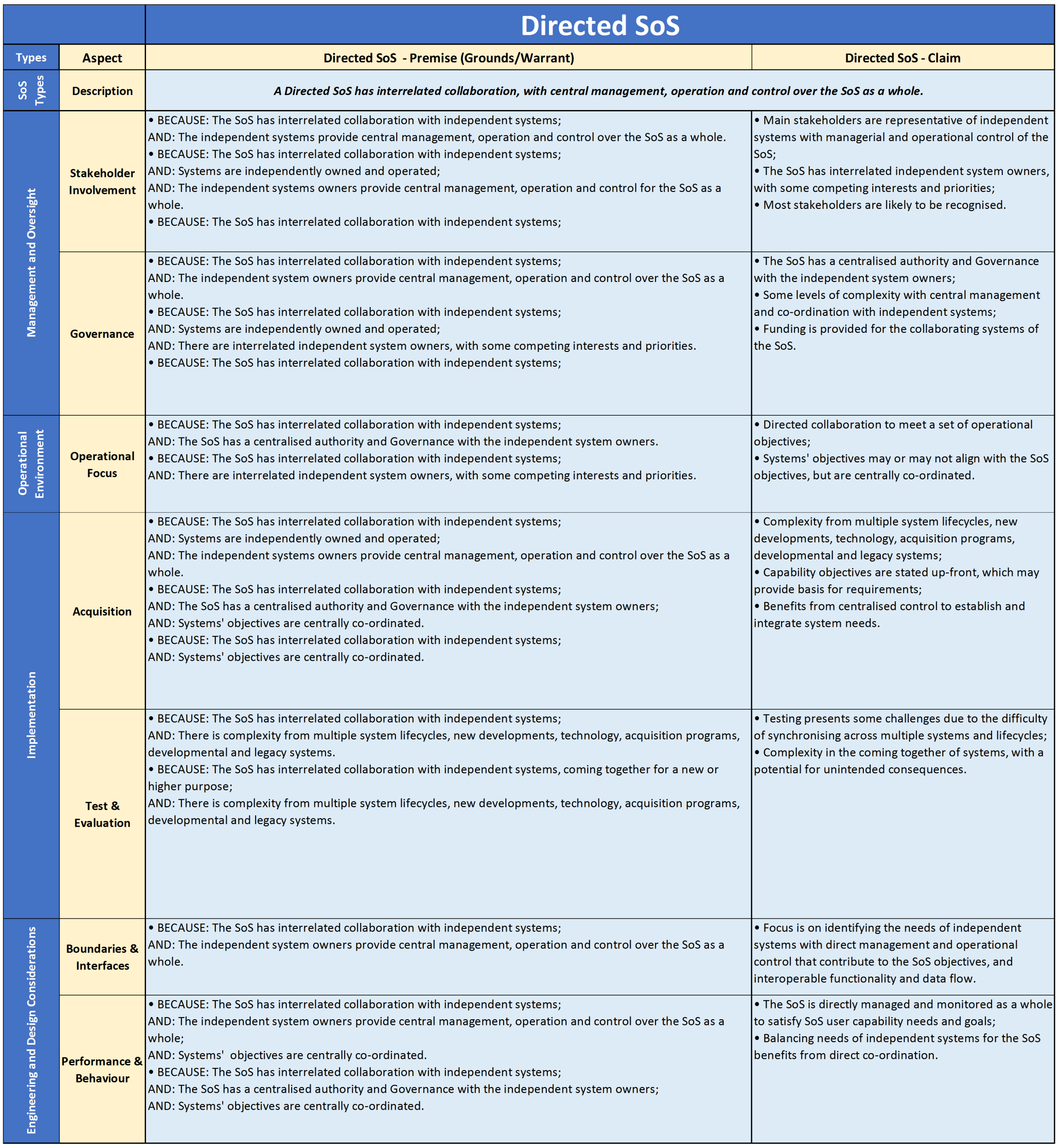
Zand, D. E., 1972. Trust and managerial problem solving. *Administrative science quarterly*, 229–239.

Zhou, B., Drew, O., Arabo, A., Llewellyn-Jones, D., Kifayat, K., Merabti, M., Shi, Q., Craddock, R., Waller, A. and Jones, G., 2010. System-of-systems boundary check in a public event scenario. *System of Systems Engineering (SoSE), 2010 5th International Conference on*, IEEE, 1–8.

Zumbado, J. R., 2015. *Human Systems Integration (HSI) Practitioner's Guide*. NASA Center for AeroSpace Information, Hanover, MD , USA, nasa/sp–2015-3709 edition.

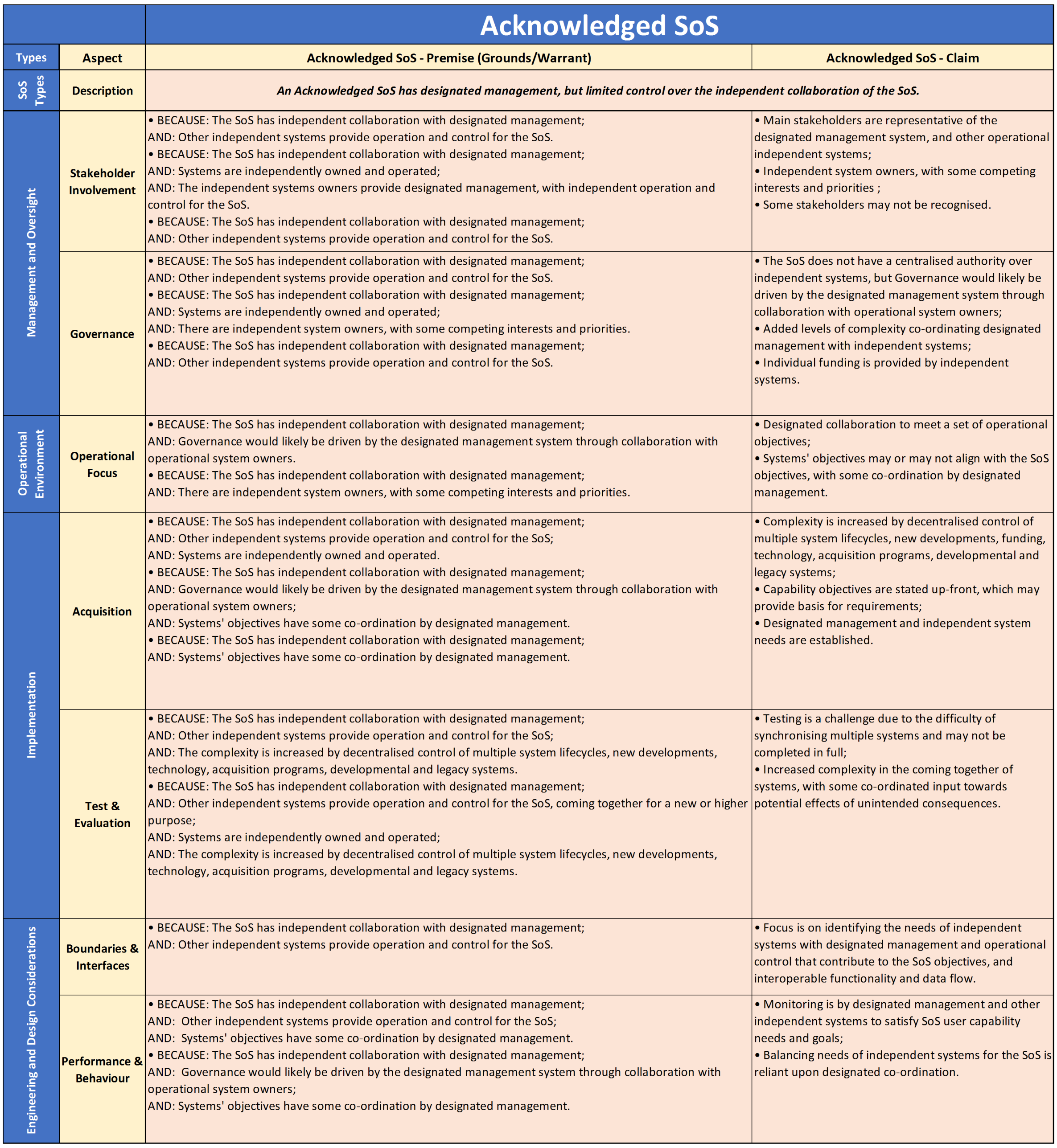
Appendix A

Arguments supporting SoS Types and their Characteristics



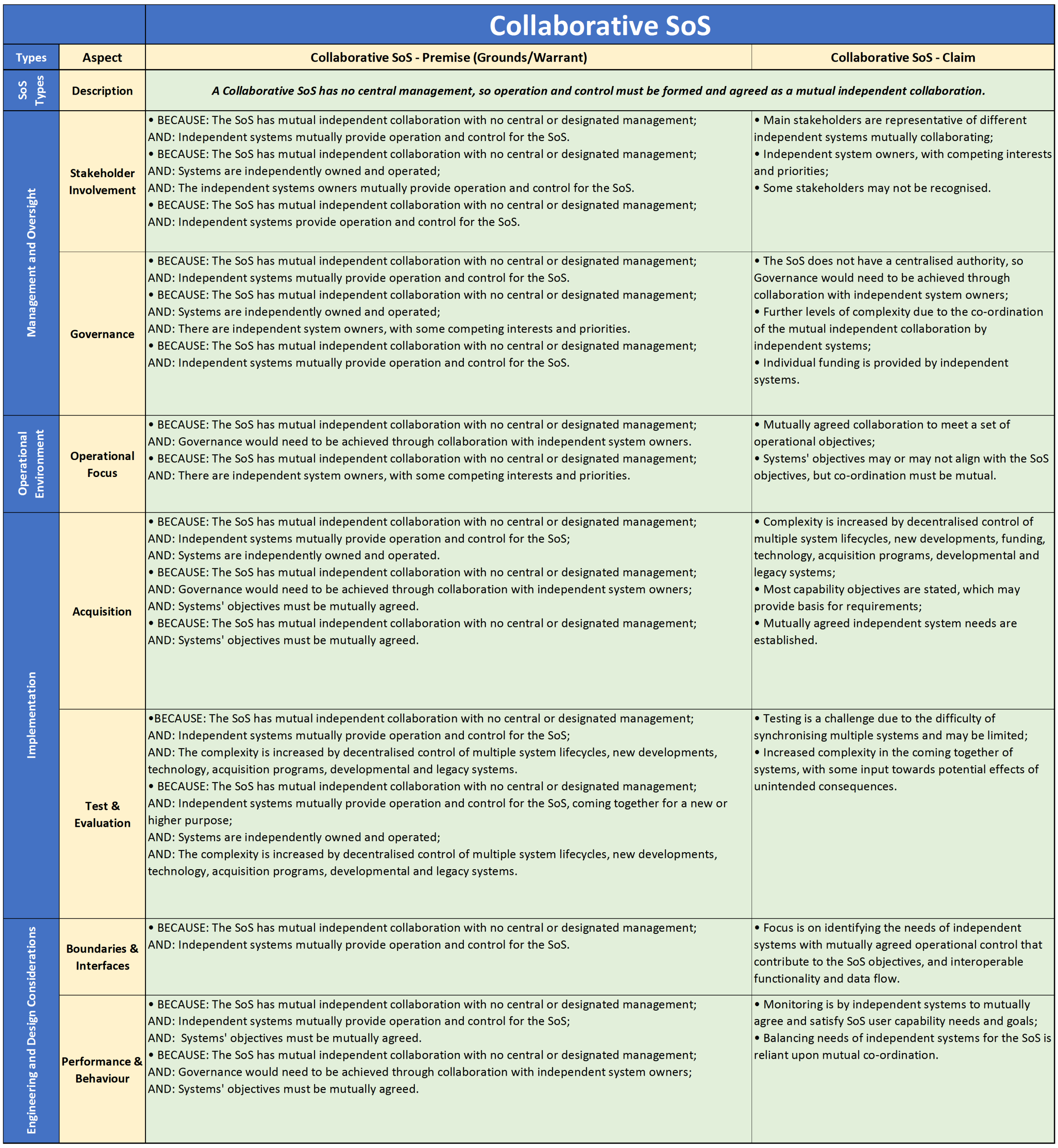
Types	Aspect	Directed SoS - Premise (Grounds/Warrant)	Directed SoS - Claim
		Directed SoS	
SoS Types	Description	*A Directed SoS has interrelated collaboration, with central management, operation and control over the SoS as a whole.*	
Management and Oversight	Stakeholder Involvement	• BECAUSE: The SoS has interrelated collaboration with independent systems; AND: The independent systems provide central management, operation and control over the SoS as a whole. • BECAUSE: The SoS has interrelated collaboration with independent systems; AND: Systems are independently owned and operated; AND: The independent systems owners provide central management, operation and control for the SoS as a whole. • BECAUSE: The SoS has interrelated collaboration with independent systems;	• Main stakeholders are representative of independent systems with managerial and operational control of the SoS; • The SoS has interrelated independent system owners, with some competing interests and priorities; • Most stakeholders are likely to be recognised.
	Governance	• BECAUSE: The SoS has interrelated collaboration with independent systems; AND: The independent system owners provide central management, operation and control over the SoS as a whole. • BECAUSE: The SoS has interrelated collaboration with independent systems; AND: Systems are independently owned and operated; AND: There are interrelated independent system owners, with some competing interests and priorities. • BECAUSE: The SoS has interrelated collaboration with independent systems;	• The SoS has a centralised authority and Governance with the independent system owners; • Some levels of complexity with central management and co-ordination with independent systems; • Funding is provided for the collaborating systems of the SoS.
Operational Environment	Operational Focus	• BECAUSE: The SoS has interrelated collaboration with independent systems; AND: The SoS has a centralised authority and Governance with the independent system owners. • BECAUSE: The SoS has interrelated collaboration with independent systems; AND: There are interrelated independent system owners, with some competing interests and priorities.	• Directed collaboration to meet a set of operational objectives; • Systems' objectives may or may not align with the SoS objectives, but are centrally co-ordinated.
Implementation	Acquisition	• BECAUSE: The SoS has interrelated collaboration with independent systems; AND: Systems are independently owned and operated; AND: The independent systems owners provide central management, operation and control over the SoS as a whole. • BECAUSE: The SoS has interrelated collaboration with independent systems; AND: The SoS has a centralised authority and Governance with the independent system owners; AND: Systems' objectives are centrally co-ordinated. • BECAUSE: The SoS has interrelated collaboration with independent systems; AND: Systems' objectives are centrally co-ordinated.	• Complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems; • Capability objectives are stated up-front, which may provide basis for requirements; • Benefits from centralised control to establish and integrate system needs.
	Test & Evaluation	• BECAUSE: The SoS has interrelated collaboration with independent systems; AND: There is complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems. • BECAUSE: The SoS has interrelated collaboration with independent systems, coming together for a new or higher purpose; AND: There is complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems.	• Testing presents some challenges due to the difficulty of synchronising across multiple systems and lifecycles; • Complexity in the coming together of systems, with a potential for unintended consequences.
Engineering and Design Considerations	Boundaries & Interfaces	• BECAUSE: The SoS has interrelated collaboration with independent systems; AND: The independent system owners provide central management, operation and control over the SoS as a whole.	• Focus is on identifying the needs of independent systems with direct management and operational control that contribute to the SoS objectives, and interoperable functionality and data flow.
	Performance & Behaviour	• BECAUSE: The SoS has interrelated collaboration with independent systems; AND: The independent system owners provide central management, operation and control over the SoS as a whole; AND: Systems' objectives are centrally co-ordinated. • BECAUSE: The SoS has interrelated collaboration with independent systems; AND: The SoS has a centralised authority and Governance with the independent system owners; AND: Systems' objectives are centrally co-ordinated.	• The SoS is directly managed and monitored as a whole to satisfy SoS user capability needs and goals; • Balancing needs of independent systems for the SoS benefits from direct co-ordination.

Fig. A.1 Argument for SoS Characteristics - Directed SoS



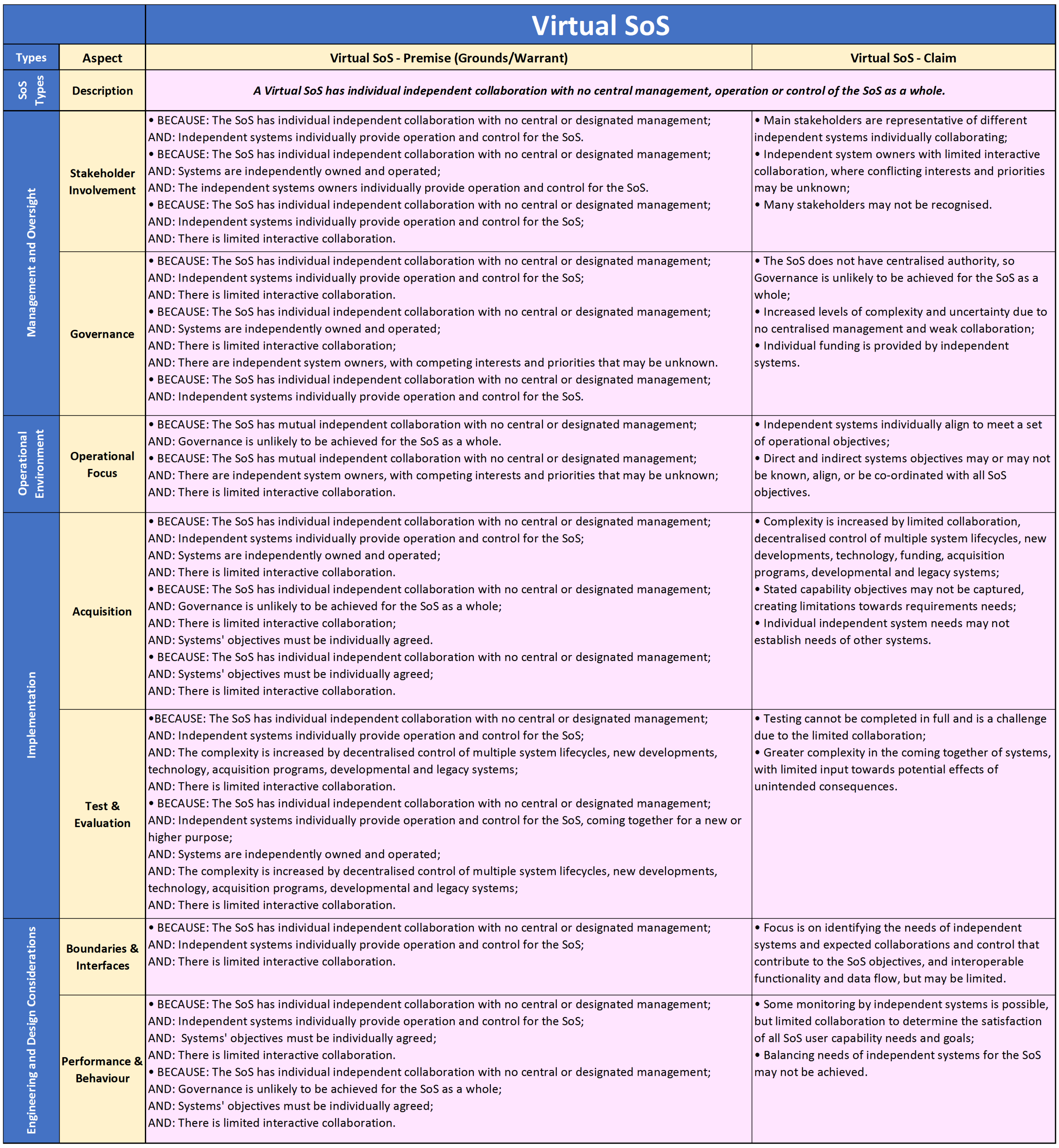
		Acknowledged SoS	
Types	Aspect	Acknowledged SoS - Premise (Grounds/Warrant)	Acknowledged SoS - Claim
SoS Types	Description	*An Acknowledged SoS has designated management, but limited control over the independent collaboration of the SoS.*	
Management and Oversight	Stakeholder Involvement	• BECAUSE: The SoS has independent collaboration with designated management; AND: Other independent systems provide operation and control for the SoS. • BECAUSE: The SoS has independent collaboration with designated management; AND: Systems are independently owned and operated; AND: The independent systems owners provide designated management, with independent operation and control for the SoS. • BECAUSE: The SoS has independent collaboration with designated management; AND: Other independent systems provide operation and control for the SoS.	• Main stakeholders are representative of the designated management system, and other operational independent systems; • Independent system owners, with some competing interests and priorities ; • Some stakeholders may not be recognised.
	Governance	• BECAUSE: The SoS has independent collaboration with designated management; AND: Other independent systems provide operation and control for the SoS. • BECAUSE: The SoS has independent collaboration with designated management; AND: Systems are independently owned and operated; AND: There are independent system owners, with some competing interests and priorities. • BECAUSE: The SoS has independent collaboration with designated management; AND: Other independent systems provide operation and control for the SoS.	• The SoS does not have a centralised authority over independent systems, but Governance would likely be driven by the designated management system through collaboration with operational system owners; • Added levels of complexity co-ordinating designated management with independent systems; • Individual funding is provided by independent systems.
Operational Environment	Operational Focus	• BECAUSE: The SoS has independent collaboration with designated management; AND: Governance would likely be driven by the designated management system through collaboration with operational system owners. • BECAUSE: The SoS has independent collaboration with designated management; AND: There are independent system owners, with some competing interests and priorities.	• Designated collaboration to meet a set of operational objectives; • Systems' objectives may or may not align with the SoS objectives, with some co-ordination by designated management.
Implementation	Acquisition	• BECAUSE: The SoS has independent collaboration with designated management; AND: Other independent systems provide operation and control for the SoS; AND: Systems are independently owned and operated. • BECAUSE: The SoS has independent collaboration with designated management; AND: Governance would likely be driven by the designated management system through collaboration with operational system owners; AND: Systems' objectives have some co-ordination by designated management. • BECAUSE: The SoS has independent collaboration with designated management; AND: Systems' objectives have some co-ordination by designated management.	• Complexity is increased by decentralised control of multiple system lifecycles, new developments, funding, technology, acquisition programs, developmental and legacy systems; • Capability objectives are stated up-front, which may provide basis for requirements; • Designated management and independent system needs are established.
	Test & Evaluation	• BECAUSE: The SoS has independent collaboration with designated management; AND: Other independent systems provide operation and control for the SoS; AND: The complexity is increased by decentralised control of multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems. • BECAUSE: The SoS has independent collaboration with designated management; AND: Other independent systems provide operation and control for the SoS, coming together for a new or higher purpose; AND: Systems are independently owned and operated; AND: The complexity is increased by decentralised control of multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems.	• Testing is a challenge due to the difficulty of synchronising multiple systems and may not be completed in full; • Increased complexity in the coming together of systems, with some co-ordinated input towards potential effects of unintended consequences.
Engineering and Design Considerations	Boundaries & Interfaces	• BECAUSE: The SoS has independent collaboration with designated management; AND: Other independent systems provide operation and control for the SoS.	• Focus is on identifying the needs of independent systems with designated management and operational control that contribute to the SoS objectives, and interoperable functionality and data flow.
	Performance & Behaviour	• BECAUSE: The SoS has independent collaboration with designated management; AND: Other independent systems provide operation and control for the SoS; AND: Systems' objectives have some co-ordination by designated management. • BECAUSE: The SoS has independent collaboration with designated management; AND: Governance would likely be driven by the designated management system through collaboration with operational system owners; AND: Systems' objectives have some co-ordination by designated management.	• Monitoring is by designated management and other independent systems to satisfy SoS user capability needs and goals; • Balancing needs of independent systems for the SoS is reliant upon designated co-ordination.

Fig. A.2 Argument for SoS Characteristics - Acknowledged SoS



		Collaborative SoS	
Types	Aspect	Collaborative SoS - Premise (Grounds/Warrant)	Collaborative SoS - Claim
SoS Types	Description	*A Collaborative SoS has no central management, so operation and control must be formed and agreed as a mutual independent collaboration.*	
Management and Oversight	Stakeholder Involvement	• BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Independent systems mutually provide operation and control for the SoS. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Systems are independently owned and operated; AND: The independent systems owners mutually provide operation and control for the SoS. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Independent systems provide operation and control for the SoS.	• Main stakeholders are representative of different independent systems mutually collaborating; • Independent system owners, with competing interests and priorities; • Some stakeholders may not be recognised.
	Governance	• BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Independent systems mutually provide operation and control for the SoS. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Systems are independently owned and operated; AND: There are independent system owners, with some competing interests and priorities. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Independent systems mutually provide operation and control for the SoS.	• The SoS does not have a centralised authority, so Governance would need to be achieved through collaboration with independent system owners; • Further levels of complexity due to the co-ordination of the mutual independent collaboration by independent systems; • Individual funding is provided by independent systems.
Operational Environment	Operational Focus	• BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Governance would need to be achieved through collaboration with independent system owners. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: There are independent system owners, with some competing interests and priorities.	• Mutually agreed collaboration to meet a set of operational objectives; • Systems' objectives may or may not align with the SoS objectives, but co-ordination must be mutual.
Implementation	Acquisition	• BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Independent systems mutually provide operation and control for the SoS; AND: Systems are independently owned and operated. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Governance would need to be achieved through collaboration with independent system owners; AND: Systems' objectives must be mutually agreed. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Systems' objectives must be mutually agreed.	• Complexity is increased by decentralised control of multiple system lifecycles, new developments, funding, technology, acquisition programs, developmental and legacy systems; • Most capability objectives are stated, which may provide basis for requirements; • Mutually agreed independent system needs are established.
	Test & Evaluation	•BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Independent systems mutually provide operation and control for the SoS; AND: The complexity is increased by decentralised control of multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Independent systems mutually provide operation and control for the SoS, coming together for a new or higher purpose; AND: Systems are independently owned and operated; AND: The complexity is increased by decentralised control of multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems.	• Testing is a challenge due to the difficulty of synchronising multiple systems and may be limited; • Increased complexity in the coming together of systems, with some input towards potential effects of unintended consequences.
Engineering and Design Considerations	Boundaries & Interfaces	• BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Independent systems mutually provide operation and control for the SoS.	• Focus is on identifying the needs of independent systems with mutually agreed operational control that contribute to the SoS objectives, and interoperable functionality and data flow.
	Performance & Behaviour	• BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Independent systems mutually provide operation and control for the SoS; AND: Systems' objectives must be mutually agreed. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Governance would need to be achieved through collaboration with independent system owners; AND: Systems' objectives must be mutually agreed.	• Monitoring is by independent systems to mutually agree and satisfy SoS user capability needs and goals; • Balancing needs of independent systems for the SoS is reliant upon mutual co-ordination.

Fig. A.3 Argument for SoS Characteristics - Collaborative SoS

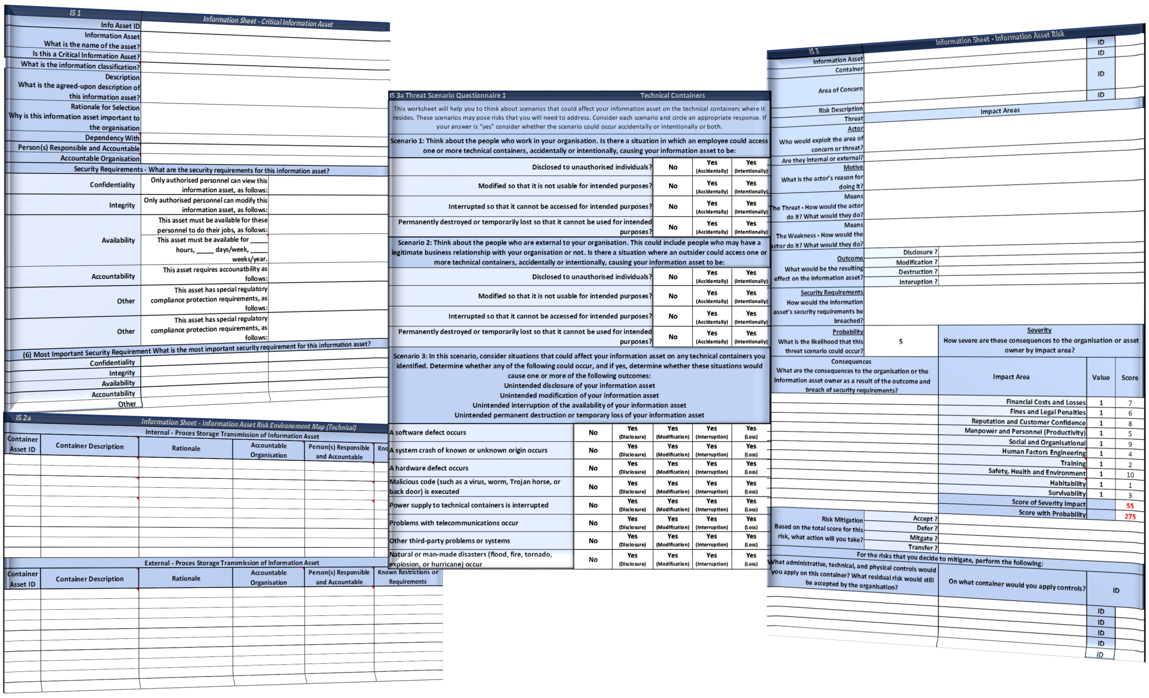


Types	Aspect	Virtual SoS - Premise (Grounds/Warrant)	Virtual SoS - Claim
		Virtual SoS	
SoS Types	Description	***A Virtual SoS has individual independent collaboration with no central management, operation or control of the SoS as a whole.***	
Management and Oversight	Stakeholder Involvement	• BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Independent systems individually provide operation and control for the SoS. • BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Systems are independently owned and operated; AND: The independent systems owners individually provide operation and control for the SoS. • BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Independent systems individually provide operation and control for the SoS; AND: There is limited interactive collaboration.	• Main stakeholders are representative of different independent systems individually collaborating; • Independent system owners with limited interactive collaboration, where conflicting interests and priorities may be unknown; • Many stakeholders may not be recognised.
	Governance	• BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Independent systems individually provide operation and control for the SoS; AND: There is limited interactive collaboration. • BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Systems are independently owned and operated; AND: There is limited interactive collaboration; AND: There are independent system owners, with competing interests and priorities that may be unknown. • BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Independent systems individually provide operation and control for the SoS.	• The SoS does not have centralised authority, so Governance is unlikely to be achieved for the SoS as a whole; • Increased levels of complexity and uncertainty due to no centralised management and weak collaboration; • Individual funding is provided by independent systems.
Operational Environment	Operational Focus	• BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: Governance is unlikely to be achieved for the SoS as a whole. • BECAUSE: The SoS has mutual independent collaboration with no central or designated management; AND: There are independent system owners, with competing interests and priorities that may be unknown; AND: There is limited interactive collaboration.	• Independent systems individually align to meet a set of operational objectives; • Direct and indirect systems objectives may or may not be known, align, or be co-ordinated with all SoS objectives.
Implementation	Acquisition	• BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Independent systems individually provide operation and control for the SoS; AND: Systems are independently owned and operated; AND: There is limited interactive collaboration. • BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Governance is unlikely to be achieved for the SoS as a whole; AND: There is limited interactive collaboration; AND: Systems' objectives must be individually agreed. • BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Systems' objectives must be individually agreed; AND: There is limited interactive collaboration.	• Complexity is increased by limited collaboration, decentralised control of multiple system lifecycles, new developments, technology, funding, acquisition programs, developmental and legacy systems; • Stated capability objectives may not be captured, creating limitations towards requirements needs; • Individual independent system needs may not establish needs of other systems.
	Test & Evaluation	•BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Independent systems individually provide operation and control for the SoS; AND: The complexity is increased by decentralised control of multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems; AND: There is limited interactive collaboration. • BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Independent systems individually provide operation and control for the SoS, coming together for a new or higher purpose; AND: Systems are independently owned and operated; AND: The complexity is increased by decentralised control of multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems; AND: There is limited interactive collaboration.	• Testing cannot be completed in full and is a challenge due to the limited collaboration; • Greater complexity in the coming together of systems, with limited input towards potential effects of unintended consequences.
Engineering and Design Considerations	Boundaries & Interfaces	• BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Independent systems individually provide operation and control for the SoS; AND: There is limited interactive collaboration.	• Focus is on identifying the needs of independent systems and expected collaborations and control that contribute to the SoS objectives, and interoperable functionality and data flow, but may be limited.
	Performance & Behaviour	• BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Independent systems individually provide operation and control for the SoS; AND: Systems' objectives must be individually agreed; AND: There is limited interactive collaboration. • BECAUSE: The SoS has individual independent collaboration with no central or designated management; AND: Governance is unlikely to be achieved for the SoS as a whole; AND: Systems' objectives must be individually agreed; AND: There is limited interactive collaboration.	• Some monitoring by independent systems is possible, but limited collaboration to determine the satisfaction of all SoS user capability needs and goals; • Balancing needs of independent systems for the SoS may not be achieved.

Fig. A.4 Argument for SoS Characteristics - Virtual SoS

Appendix B

Worksheets, Spreadsheets, and Information Guides



IS 1 Information Sheet - Critical Information Asset

Info Asset ID		
Information Asset What is the name of the asset?		
Is this a Critical Information Asset?		
What is the information classification?		
Description What is the agreed-upon description of this information asset?		
Rationale for Selection Why is this information asset important to the organisation		
Dependency With		
Person(s) Responsible and Accountable		
Accountable Organisation		
Security Requirements - What are the security requirements for this information asset?		
Confidentiality	Only authorised personnel can view this information asset, as follows:	
Integrity	Only authorised personnel can modify this information asset, as follows:	
Availability	This asset must be available for these personnel to do their jobs, as follows:	
	This asset must be available for _____ hours, _____ days/week, _____ weeks/year.	
Accountability	This asset requires accounatbility as follows:	
Other	This asset has special regulatory compliance protection requirements, as follows:	
Other	This asset has special regulatory compliance protection requirements, as follows:	
(6) Most Important Security Requirement What is the most important security requirement for this information asset?		
Confidentiality		
Integrity		
Availability		
Accountability		
Other		

IS 2a Information Sheet - Information Asset Risk Environement Map (Technical)

Internal - Proces Storage Transmission of Information Asset

Container Asset ID	Container Description	Rationale	Accountable Organisation	Person(s) Responsible and Accountable	Kno

External - Proces Storage Transmission of Information Asset

Container Asset ID	Container Description	Rationale	Accountable Organisation	Person(s) Responsible and Accountable	Known Restrictions or Requirements

IS 3a Threat Scenario Questionnaire 1 Technical Containers

This worksheet will help you to think about scenarios that could affect your information asset on the technical containers where it resides. These scenarios may pose risks that you will need to address. Consider each scenario and circle an appropriate response. If your answer is "yes" consider whether the scenario could occur accidentally or intentionally or both.

Scenario 1: Think about the people who work in your organisation. Is there a situation in which an employee could access one or more technical containers, accidentally or intentionally, causing your information asset to be:

Disclosed to unauthorised individuals?	No	Yes (Accidentally)	Yes (Intentionally)
Modified so that it is not usable for intended purposes?	No	Yes (Accidentally)	Yes (Intentionally)
Interrupted so that it cannot be accessed for intended purposes?	No	Yes (Accidentally)	Yes (Intentionally)
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	No	Yes (Accidentally)	Yes (Intentionally)

Scenario 2: Think about the people who are external to your organisation. This could include people who may have a legitimate business relationship with your organisation or not. Is there a situation where an outsider could access one or more technical containers, accidentally or intentionally, causing your information asset to be:

Disclosed to unauthorised individuals?	No	Yes (Accidentally)	Yes (Intentionally)
Modified so that it is not usable for intended purposes?	No	Yes (Accidentally)	Yes (Intentionally)
Interrupted so that it cannot be accessed for intended purposes?	No	Yes (Accidentally)	Yes (Intentionally)
Permanently destroyed or temporarily lost so that it cannot be used for intended purposes?	No	Yes (Accidentally)	Yes (Intentionally)

Scenario 3: In this scenario, consider situations that could affect your information asset on any technical containers you identified. Determine whether any of the following could occur, and if yes, determine whether these situations would cause one or more of the following outcomes:
Unintended disclosure of your information asset
Unintended modification of your information asset
Unintended interruption of the availability of your information asset
Unintended permanent destruction or temporary loss of your information asset

A software defect occurs	No	Yes (Disclosure)	Yes (Modification)	Yes (Interruption)	Yes (Loss)
A system crash of known or unknown origin occurs	No	Yes (Disclosure)	Yes (Modification)	Yes (Interruption)	Yes (Loss)
A hardware defect occurs	No	Yes (Disclosure)	Yes (Modification)	Yes (Interruption)	Yes (Loss)
Malicious code (such as a virus, worm, Trojan horse, or back door) is executed	No	Yes (Disclosure)	Yes (Modification)	Yes (Interruption)	Yes (Loss)
Power supply to technical containers is interrupted	No	Yes (Disclosure)	Yes (Modification)	Yes (Interruption)	Yes (Loss)
Problems with telecommunications occur	No	Yes (Disclosure)	Yes (Modification)	Yes (Interruption)	Yes (Loss)
Other third-party problems or systems	No	Yes (Disclosure)	Yes (Modification)	Yes (Interruption)	Yes (Loss)
Natural or man-made disasters (flood, fire, tornado, explosion, or hurricane) occur	No	Yes (Disclosure)	Yes (Modification)	Yes (Interruption)	Yes (Loss)

IS 3 Information Sheet - Information Asset Risk

Information Asset		ID	
Container		ID	
Area of Concern		ID	
		ID	
Risk Description	Impact Areas		
Threat			
Actor Who would exploit the area of concern or threat?			
Are they internal or external?			
Motive What is the actor's reason for doing it?			
Means The Threat - How would the actor do it? What would they do?			
Means The Weakness - How would the actor do it? What would they do?			
Outcome What would be the resulting effect on the information asset?	Disclosure ?		
	Modification ?		
	Destruction ?		
	Interuption ?		
Security Requirements How would the information asset's security requirements be breached?			
Probability What is the likelihood that this threat scenario could occur?	5	Severity How severe are these consequences to the organisation or asset owner by impact area?	

Consequences What are the consequences to the organisation or the information asset owner as a result of the outcome and breach of security requirements?	Impact Area	Value	Score
	Financial Costs and Losses	1	7
	Fines and Legal Penalties	1	6
	Reputation and Customer Confidence	1	8
	Manpower and Personnel (Productivity)	1	5
	Social and Organisational	1	9
	Human Factors Engineering	1	4
	Training	1	2
	Safety, Health and Environment	1	10
	Habitability	1	1
	Survivability	1	3
	Score of Severity Impact		55
	Score with Probability		275

Risk Mitigation Based on the total score for this risk, what action will you take?	Accept ?	
	Defer ?	
	Mitgate ?	
	Transfer ?	

For the risks that you decide to mitigate, perform the following:

What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organisation?	On what container would you apply controls?	ID	
		ID	
		ID	
		ID	
		ID	
		ID	

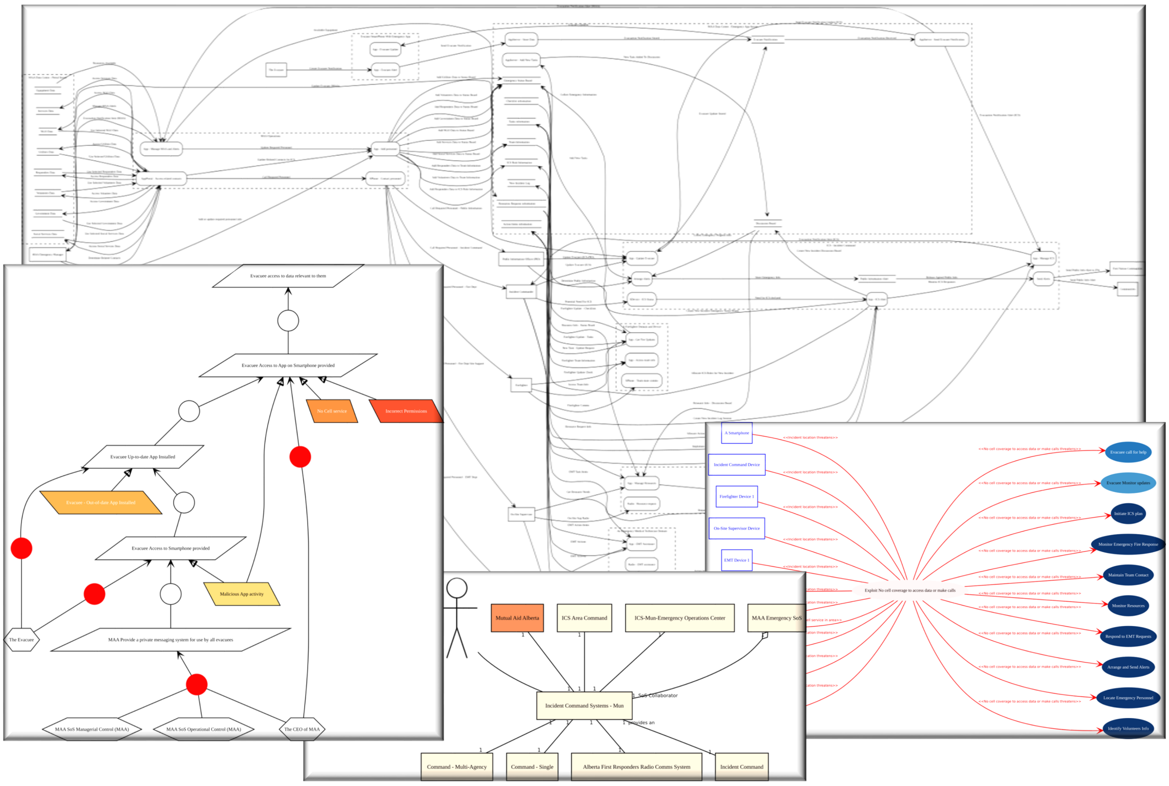
Fig. B.1 Example worksheets based on OA (Caralli et al. 2007)

When conducting the information security risk assessment process, worksheets and spreadsheets are used to capture supporting information. Which worksheets and master spreadsheets are to be used in each of the steps of the process were detailed in Chapter 6. As illustrated in Figure B.1, there are a number of these used within the process, and are also supported by additional guides and information towards risk criteria impact areas. For brevity, these have not been individually represented graphically in this Appendix. Instead, an electronic copy of the worksheet and spreadsheet templates used within OASoSIS can be found stored within the online folder at https://github.com/D-Dev/cairis. Or specifically in https://github.com/D-Dev/cairis/tree/master/oasosis. These include:

Information - OCTAVE Allegro Definitions;
Information - OASoSIS Initial Questions;
Information - OASoSIS Characterisation Chart.
Master Sheet 1 - Capturing stakeholder information;
Master Sheet 2 - Capturing all containers where information assets are stored, processed, or transported;
Master Sheet 3 - Capturing critical information assets;
Master Sheet 4 - Detailing the Risk Criteria;
Master Sheet 5 - Detailing all concerns and risks to assets from threats, vulnerabilities, and attackers;
Information Sheet 1 - Capturing critical information assets;
Information Sheet 2 - Container guide;
Information Sheet 2a - Capturing Technical containers;
Information Sheet 2b - Capturing Physical containers;
Information Sheet 2c - Capturing People containers;
Information Sheet 3 - Capturing threats and risk analysis towards assets;
Information Sheet 3a - Threat Scenario Questionnaire for Technical containers;
Information Sheet 3b - Threat Scenario Questionnaire for Physical containers;
Information Sheet 3c - Threat Scenario Questionnaire for People containers;
Information - Risk Criteria impact area - Manpower;
Information - Risk Criteria impact area - Personnel;
Information - Risk Criteria impact area - Social and Organisational;
Information - Risk Criteria impact area - Human Factors Engineering;
Information - Risk Criteria impact area - Training;
Information - Risk Criteria impact area - Environment, Safety, and Health;
Information - Risk Criteria impact area - Habitability;
Information - Risk Criteria impact area - Survivability;

Appendix C

CAIRIS Model Files



Evacuee access to data relevant to them
Evacuee Access to App on Smartphone provided
No Cell service
Incorrect Permissions
Evacuee Up-to-date App Installed
Evacuee - Out-of-date App Installed
Evacuee Access to Smartphone provided
Malicious App activity
The Evacuee
MAA Provide a private messaging system for use by all evacuees
MAA SoS Managerial Control (MAA)
MAA SoS Operational Control (MAA)
The CEO of MAA
Mutual Aid Alberta
ICS Area Command
ICS-Mun-Emergency Operations Center
MAA Emergency SoS
Incident Command Systems - Mun
SoS Collaborator
provides an
Command - Multi-Agency
Command - Single
Alberta First Responders Radio Comms System
Incident Command
A Smartphone
Incident Command Device
Firefighter Device 1
On-Site Supervisor Device
EMT Device 1
<<Incident location threatens>>
Exploit No cell coverage to access data or make calls
<<No cell coverage to access data or make calls threatens>>
Evacuee call for help
Evacuee Monitor updates
Initiate ICS plan
Monitor Emergency Fire Response
Maintain Team Contact
Monitor Resources
Respond to EMT Requests
Arrange and Send Alerts
Locate Emergency Personnel
Identify Volunteers Info

Fig. C.1 Models in CAIRIS

When conducting the information security risk assessment with tool-support from CAIRIS, a number of models are generated as representations of the data entered into its database. When exporting the model files, these are saved as xml files that can be imported into CAIRIS to generate the models again. As illustrated in Figure C.1, there are a number of these models used within the process, some of which become large and complex, and therefore do not scale-down well within the parameters of this document for readability.

Therefore, if required to visualise these further, the CAIRIS xml model files used as part of the application of OASoSIS in the case studies can be found stored within the online folder at https://github.com/D-Dev/cairis. Or specifically in https://github.com/D-Dev/cairis/tree/master/oasosis. These can be uploaded to the demo version of CAIRIS found online at https://demo.cairis.org, using *test* - *test* to login.

Furthermore, to view the enhanced models showing accountability, the project development version of CAIRIS will continue to be stored at https://github.com/D-Dev/cairis, and can be installed following the CAIRIS installation instructions found at https://cairis.readthedocs.io/en/latest/install.html, being sure to change the git clone address to https://github.com/D-Dev/cairis.