Computers & Security 117 (2022) 102690

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Assessing system of systems information security risk with OASoSIS

Duncan Ki-Aries[a],[*], Shamal Faily[b], Huseyin Dogan[a], Christopher Williams[c]

[a] *Department of Computing & Informatics, Bournemouth University, Fern Barrow, Poole, United Kingdom*
[b] *School of Computing, Robert Gordon University, Garthdee House, Garthdee Road, Aberdeen, United Kingdom*
[c] *Defence Science and Technology Laboratory, Porton Down, United Kingdom*

ARTICLE INFO

Article history:
Received 29 January 2021
Revised 23 December 2021
Accepted 9 March 2022
Available online 21 March 2022

Keywords:
System of systems
Information security
Risk
Human factors
Requirements engineering
CAIRIS

ABSTRACT

The term *System of Systems* (SoS) is used to describe the coming together of independent systems, collaborating to achieve a new or higher purpose. However, the SoS concept is often misunderstood within operational environments, providing challenges towards the secure design and operation of SoSs. Limitations in existing literature indicates a need for discovery towards identifying a combination of concepts, models, and techniques suitable for assessing SoS security risk and related human factor concerns for SoS Requirements Engineering. In this article, we present OASoSIS, representing an information security risk assessment and modelling process to assist risk-based decision making in SoS Requirements Engineering. A characterisation process is introduced to capture the SoS context, supporting a SoS security risk assessment process that extends OCTAVE Allegro towards a SoS context. Resulting risk data provides a focused means to assess and model the SoS information security risk and related human factors, integrating tool-support using CAIRIS. A medical evacuation SoS case study scenario was used to test, illustrate, and validate the alignment of concepts, models, and techniques for assessing SoS information security risks with OASoSIS, where findings provide a positive basis for future work.

1. Introduction

In modern day social and organisational environments, there is a growing demand for dynamic interactions and collaborations integrating people, process, and technology in new ways. In some scenarios, independent organisations, networks, software and hardware information systems may need to come together to achieve a new combined purpose and common goal that could only be achieved through the collaboration. This would be in addition to their normal day-job or originally designed purpose. This type of collaboration would, therefore, be described as a *System of Systems* (SoS) - providing a set of systems for a task that none can accomplish on their own. Each independent system would, however, retain their own management and operations of their day-job, whilst integrating with SoS activities to meet additional SoS goals (ODUSD, 2008).

There are many examples of systems converging to form a SoS where some may be less or more complex, and be managed and operated in different collaborative ways. SoS challenges and risks arise from the independent yet inter-dependant interactions of collaborating systems. For example, an emergency response unit as part of a SoS may need to interoperate with the fire and ambulance services, volunteers, communities, or other critical services. This need for interoperability is required across many levels, in most cases for communications and mission critical dependencies. Each of the emergency scenario stakeholders may be considered an independent system with its own purpose, people, processes and technology, but collaborates with the emergency response unit to meet emergency response SoS mission objectives (Ki-Aries et al., 2017a, 2017b).

Given there are many differences in SoSs, identifying, assessing, and mitigating security risk is challenged, in particular, by weak collaborations and decentralised control between stakeholders, re-

Abbreviations: CAIRIS, Computer Aided Integration of Requirements and Information Security; Dstl, Defence Science and Technology Laboratory; EHR, Electronic Health Record; EMT, Emergency Medical Technician; FMC, Field Medical Card; FOB, Forward Operating Base; FST, Forward Surgical Team; HFSI, Human Factors System Integration; JOC, Joint Operations Centre; JMeWS, Joint Medical Workstation; MEDEVAC, Medical Evacuation; MMN, MEDEVAC Mission Network; NATO, The North Atlantic Treaty Organisation; 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; PMR, Patient Movement Request; PoI, Point of Injury; RBDM, Risk-Based Decision Making; SoS, System of Systems; SoSs, Systems of Systems (Plural); SoSRE, SoS Requirements Engineering; TCN, Troop Contributing Nation; TDMS, Theatre Medical Data Store.

[*] Corresponding author.

E-mail addresses: dkiaries@bournemouth.ac.uk (D. Ki-Aries), s.faily@rgu.ac.uk (S. Faily), hdogan@bournemouth.ac.uk (H. Dogan), cwilliams@mail.dstl.gov.uk (C. Williams).

https://doi.org/10.1016/j.cose.2022.102690

sulting in limited information and assurance towards their interactions and controls. Despite this, there is a need for a consistent repeatable approach to capture and assess the security risks of the SoS. The SoS should ideally be assessed from the view of the SoS as a whole, although it may not be possible to capture all perspectives, or at the same time.

Furthermore, SoSs typically have differing system requirements and controls, owners, goals, trust boundaries, levels of assurance, and a potential for risks, some of which may be unknown or not exist until the coming together of the SoS. These differences and conflicts may increase security related concerns if unaccounted for, and can be further complicated by subsequent emerging behaviours from the SoS evolution.

Because the combined effect of these considerations are greater than that of single systems, the interactions and interdependencies increase risks not only for the independent systems, but the SoS as a whole. When framing a single SoS to assess its security risks, to address associated challenges there is a need to be clear about the context of the SoS, and from what or whose view within the SoS the risk is being assessed. Identifying the SoS context is, therefore, a vital prerequisite to a SoS-focused security risk assessment process if we are to capture the SoS mission and complexities from both top-down and bottom-up.

When accounting for operational needs and specifying requirements to mitigate SoSs risks, several methods supporting SoS Requirements Engineering (SoSRE) exist, e.g. ICSE (2007); ODUSD (2008); Ross et al. (2016). However, current informal and implicit models of people rarely focus on how people make security decisions (Shostack, 2014). Research suggests there has been limited progress towards identifying suitable combinations of methods for characterising, assessing and modelling SoSs security risks and their related human factors concerns integrated with tool-support. There are a number of modelling tools or approaches designed with a focus towards the standard single system context. Unfortunately, there appears to be limited tool-support, and no clear guidance towards how we may integrate different elements to model and assess the SoS security aspects and concerns in greater detail.

Consequently, to further assist the assessment of SoSs risks, there is a need for better models visualising how various people approach a security task, their mental models or security-related skills and knowledge. Therefore, to address these limitations, a focus is required towards identifying combinations of tool elements to suitably visualise information security risk and related human factors in a SoS context, helping to bridge the communication gap between operational needs and SoSRE. Meeting the criticality of the independent system requirements to accurately reflect interdependent users' needs is crucial to the success of the secure operation of the SoS (AlhajHassan et al., 2016; Ncube et al., 2013).

In this article, to address these identified gaps and needs for improvement, we first introduce a method for characterising and classifying a SoS to support a security risk assessment process. This is used to identify the relevant SoS context prior to assessment. The risk assessment approach adopted for alignment towards the SoS context as a second element uses the process of OCTAVE Allegro (OA) for Information Security risk assessment (Caralli et al., 2007).

Risk data outputs from OA are transferred into a third element integrating tool-support to align with different of concepts, models, and techniques suitable for eliciting, analysing, and validating SoS security risks. The tool-support implemented uses the open-source CAIRIS (Computer Aided Integration of Requirements and Information Security) platform (Faily, 2018a). By combining the use of OA for SoS with CAIRIS, we refer to this combination as OASoSIS that represents an information security risk assessment and modelling process to assist risk-based decision making (RBDM) in SoSRE.

In Section 2, we present the related works upon which the formulation of OASoSIS was based. Section 3 details the approach taken, first introducing a case study example based on a military medical evacuation scenario – the *MEDEVAC Mission Network* (MMN) SoS. This section details the steps taken towards implementing the MMN case study, along with its use towards using the characterisation process aligned with OA. The models, techniques, and steps used within the tool-supported element of the process are indicated, along with how those elements would be tested, then validated through expert military stakeholder feedback. The application and testing of those elements to assess and model the security risks of the MMN SoS are illustrated in Section 4. A summary of findings, lessons learned, and stakeholder feedback towards the application and testing of the elements are discussed in Section 5, with conclusions towards future work with OASoSIS in Section 6.

2. Background and related literature

2.1. Systems of systems

Systems can be described in many ways, but are commonly composed of parts or elements with relational interactions between other elements of the system designed for a specific purpose (Sommerville, 2015). For example, organisational, social and technological systems are decomposed of various sub-systems and component systems interconnecting to fulfil related system needs as a whole.

The term "System of Systems" is often applied in different scenarios and environments of varying scales and complexities of interconnected systems as observed in previous work (Ki-Aries et al., 2017a, 2017b). The SoS concept is, therefore, likely to mean different things to different people. For example, in an organisational context, a dependency is in place towards the interaction between different enterprises or internal systems of the SoS for sharing core business information across functional and geographical areas. A military and defence SoS may differ with configurable sets of constituent-systems within dynamic communication infrastructures (Lane and Epstein, 2013). However, research suggests that using the term *System of Systems* specifically in operational environments generally creates confusion. Moreover, outside of the engineering communities, and occasionally within, the SoS term is relatively unknown and may instead be considered in a similar context as being a *Network of Networks* or *Enterprise of Enterprises*.

To qualify as being defined as a SoS, it should include operational independence, managerial independence, geographic distribution, evolutionary development, and emergent behaviour (Maier, 1996). Given there is a great focus towards the level of managerial and operational control within a SoS, each SoS can be further categorised. However, within the limited range of engineering guides and supporting SoSs literature, many refer to the four main SoSs categories and descriptions provided by Maier (1996), Dahmann and Baldwin (2008). These are described as Directed, Acknowledged, Collaborative, and Virtual, where a Virtual SoS has no centralised control, whereas the transition through to a Directed SoS does provide centralised control.

Because SoSs are composed of systems that come together in ways they were not originally designed for, emergent behaviours and interoperability are two specific aspects for SoSs requiring focus. *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, 2022). This would include human-to-human activities as well as technology-to-technology interoperations, communications, and decision making processes. This presents an information sharing problem and complexities resulting from interoperability needs of the SoS (Dogan et al., 2011), in particular, towards the availability of systems and data.

Achieving interoperability will depend on the ability of two or more systems or elements that store, process, or transport information to interoperate, whilst attending to risk mitigations for other security related aspects along the communication channels between systems and the external world (IEEE, 1990; Zhou et al., 2010). Moreover, the Network Centric Operations Industry Consortium (NCOIC, 2019) indicates that interoperability within and across domains is better achieved when considering and addressing all dimensions. This includes technology, mission, business value, policies and regulations, culture and people. Policy, process, and procedural requirements should be determined and implemented to achieve the goals of the systems and SoS as a whole, whilst continuing to observe any subsequent emerging behaviours (AlhajHassan et al., 2016; Morris et al., 2006).

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). The term *Emergence* is often used when describing the formation of new behaviours emerging as consequence of the evolutionary SoS processes coming together (Chiprianov et al., 2014) in ways they were not originally designed for. As the SoS evolves, we must therefore learn how to allow desirable behaviours of emergence to flourish whilst maintaining interoperability and availability, and retaining agility to quickly detect and defend against unintended consequences (Boardman and Sauser, 2006).

As identified in Alkhabbas et al. (2016); Ki-Aries et al. (2017a,b); Whittington and Dogan (2016), there are many examples of systems built and used for one purpose, and interconnected within a SoS for another. These range from small-scale smart device operations where strategic principles are required for design and operation (Homeland Security, 2016), or distributed business systems and software dependent systems, communications systems, assistive technologies, larger-scale military operations, smart cities, and critical infrastructure. One example is where at a national level, the health infrastructure has a dependence upon hospitals, medical centres, transportation, communication systems and networks, power systems, and others in which to operate as a complex interconnected infrastructure (Branagan et al., 2006).

Given the socio-technical nature of SoSs, better emphasis needs to be given to account for the human interactions within SoSs, and the effect uncertainty might have towards people and risk. Trust and assurance are important factors towards SoS security and risk, and play a continuing role as SoSs evolve (Ncube and Lim, 2018). At a general level, trust is the willingness to be vulnerable, based on the positive expectations about the actions of others (Zand, 1972). There have been many documented types of trust (McKnight and Chervany, 1996) that equate to different levels of trust and context, usually where an individual has reliance on another party under conditions of dependency and risk (Currall and Judge, 1995).

2.2. SoS security and risk

Security risk assessment within a SoS context could be applied at different levels, for example, at the operational level, or within a development life-cycle. Moreover, as SoSs evolve and the attack surface grows, accounting for supply chain risk becomes another factor. These elements would need to be accounted for to provide further assurance of security and risk mitigations throughout acquisition and the development life-cycle (Boyson, 2014).

The risk assessment process should begin with identifying the context of use, mission goals, boundaries, relevant stakeholders, scope, and risk criteria. Stakeholder needs should be captured to ensure the system interconnections are interoperable across the boundaries of the SoS. Systems ownership and operation within a SoS by different independent stakeholders may lead to limitations on the exchange of information without direct interaction and communication (Nielsen et al., 2015). For example, where SoSs do not have centralised risk assessments and control as with a Directed SoS, the assessment of risk is carried out independently whilst only accounting for their own participation within the SoS, and other applicable collaborations.

Given the challenges, scale and complexity of SoSs with different levels of collaboration, it is likely that at minimum, the assessment will need to account for the interactions from an independent system-of-interest's perspective, and its impact towards achieving the SoS goals. However, where the collaboration and communication is stronger, different perspectives can be coupled, thus providing for more informed decision making.

The communication between independent system stakeholders and SoSRE is essential for achieving risk reduction in SoS security. Where stakeholders are not always recognised across the SoS, or stakeholders of individual systems have conflicting interest and priorities, risk to the SoS may increase (ODUSD, 2008). Moreover, this is an important consideration towards maintaining interoperability, given the focus goes beyond achieving point-to-point interoperability and goes further to encompass the management of information flows, systems, security, and related risks.

Independent systems of differing types may not have gone through the same risk or security processes as each other, presenting interoperability issues or new risks across the SoS (Chiprianov et al., 2014). Systems may have applied one of a number of methods for security risk management covering relevant security techniques and controls, e.g. British Standards Institution (2011); NIST (2017). However, security risk and requirements identification should begin with asset analysis based on their related environment and context (Firesmith, 2003). This should consider how and where information assets are stored, processed and transported along with human factors and interoperability critical for the SoS operation. To achieve this, a range of standard risk assessment approaches may be used that should lead to a clear and consistent risk statement to identify possible adverse effects (Böröcz, 2016). A risk assessment should incorporate modelling, and be repeatable, measurable, and auditable (Jones, 2007).

Considering many of these factors, the OCTAVE methodology of OA was identified as an approach that could potentially be used as a foundation for a SoSRE Information Security risk assessment process for small to large SoSs. The different OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) approaches introduce three levels of application. The original version provides a larger-scale comprehensive and technical assessment of security risk, whereas the second version was designed for small-medium enterprises. The third version using OA was designed by it's authors (Caralli et al., 2007) to provide a more robust streamlined process, and was specifically aligned towards information assets.

Therefore, OA has been considered as a candidate for use and modification towards the SoS context. In particular, because of OA's ability to apply an Information Security risk assessment without the need for extensive technical or risk assessment knowledge from all stakeholders, and where stakeholder interaction may be limited. Given that SoSs have differing levels of collaboration across stakeholders, where access or direct interaction is not always possible, OA is suited towards a high-level SoS assessment. The OA approach also reduces the need for participatory workshops and interaction from all organisational system levels, which may be a challenge for SoSs.

Moreover, using OA risk data output with tool-support could potentially assist with on-going assessments that will need to identify where independent system changes may alter risk equations that might otherwise have gone unidentified (Dahmann et al., 2013).

2.3. Models and tool-support

Several security requirements approaches account for threats and vulnerabilities, e.g. Elahi et al. (2010); Faily and Fléchais (2010a), but there has been little work considering how tools can be used to assess SoS security risks for requirements elicitation (Trivellato et al., 2013). Stakeholder collaboration benefits from the use of interoperable tools (Meland and Jensen, 2008), and awareness of security concerns can be raised by visualising how people associated to roles approach security tasks across the SoS to achieve its goals.

Models of SoSs should capture the role of each independent system stakeholder within the SoS, being clear to define SoS purpose, mission, goals, and any related requirements. Implications of interactions of different security decisions should also be accounted for. System modelling may use a combination of top-down and bottom-up processes, and model system goals in the context of the SoS (AlhajHassan et al., 2016). A range of modelling tools or approaches could potentially be used to assist a model-based SoS risk assessment. These include the CORAS method that uses a tool designed to support security risk analysis using its custom risk modelling notation (Den Braber et al., 2006), and the Secure Tropos approach to model stakeholders, system and social goals, and the impact of risk-related concepts upon these goals (Mouratidis, 2011).

The KAOS approach to modelling goals 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. These could operationalise processes, supporting the completion of tasks operationalised by the goal and their associated roles, related to activities performed by human users.

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).

Personas can be introduced to 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 (Atzeni et al., 2011; Cooper, 1999; Cooper et al., 2014; Faily and Fléchais, 2010a; 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). Moreover, research has shown how persona and role aligned usability models are helpful towards forming the basis of validation checks of initial design models Faily et al. (2020a,b).

As engineering and modelling approaches are often applied towards a single system context, further work is required to understand how we may integrate these combinations of tool elements and models to visualise a SoS in context. This may provide assurance that countermeasures address SoS risks relating to the behaviours of attackers, threats and vulnerabilities (Ardi et al., 2007) in individual systems. Models can help to reason about these concerns, but can become expensive and time-consuming to build and maintain as the SoS grows (Sommerville, 2015).

Although not explicitly designed to support SoSs, the open-source CAIRIS platform (Faily, 2018a) appears to support many of the security, system engineering, and human factors concepts necessary for assessing SoS risk as a result of the IRIS framework upon which it is based (Faily, 2018b).

CAIRIS supports the automatic generation of visual models as data is input, allowing users to validate and make sense of the security and usability of a design as it evolves. Several types of system models can be automatically generated based on data input of security and usability elements added to a CAIRIS model, e.g. goals, tasks, assets, and data flows linking to threat models and risk views. These models enable users to explore the impact of threats and vulnerabilities affecting different systems, thus promoting stakeholder discussion for RBDM. A view for each independent system of the SoS can be represented in model *environments* and be aligned with the contexts of use to frame the system specification.

3. Approach

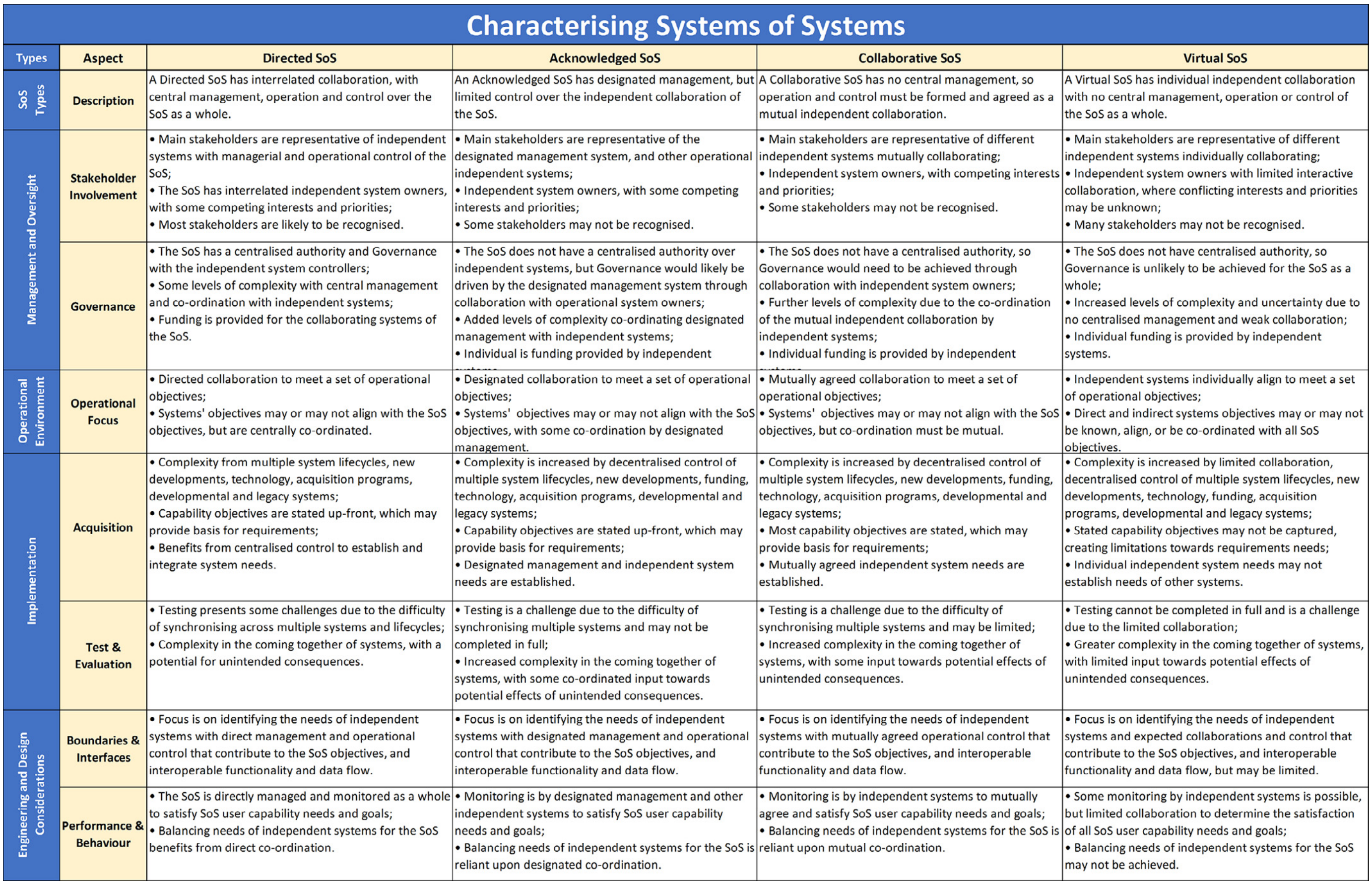
Building upon previous work to understand the characteristics of SoSs (Ki-Aries et al., 2017b) along with early indications towards how they may be assessed and modelled (Ki-Aries et al., 2017a), we identified that SoSs have many complexities, and in some cases, limited interaction with stakeholders. Assessing security risk is consequently a challenge in SoSs where active participation in risk assessments and risk-based information is reduced.

From our review in current work, it was evident certain security and risk approaches would not benefit the SoS context, as many do require greater active participation from a range of actors with technical skills to apply the risk assessments. In SoSs, this is not always possible. For example, this is evident in other versions of OCTAVE that specifies vulnerability testing of systems, or requires greater stakeholder input. We therefore aligned a tool-supported approach for assessing SoS information security risk based around OA because of the flexibility it offers with limited stakeholders and input. OA has a potential to be applied towards a number of scenarios where the security of information assets is of importance.

3.1. The case study scenario

In order to apply and test the elements of OASoSIS for assessing SoS information security risk, a case study example was introduced based on a military medical evacuation scenario – the MMN SoS. The case study scenario is discussed in Section 4.1.

In previous work (Ki-Aries et al., 2017b), a range of services and mission threads vital to NATO operations were identified including support for MEDEVAC operations. These type of operations could be considered a SoS given the joint-force collaboration to provide a MEDEVAC service. 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 in Ki-Aries et al. (2017b), 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 Depart-



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. 1. SoS Characteristics - extended from work by Dahmann et al. (2008).

ment of Defense (DOD) sources, e.g. MC4 (2018); Meier (2011); Pahon (2012); Seffers (2011a,b).

Therefore, 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 could be implemented. 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.

3.2. The SoS characterisation process

Using the MMN scenario, the three main elements within OASoSIS would be applied and tested. This begins with a process to provide SoS characterisation and context, extended from work described by Dahmann and Baldwin (2008). As illustrated in Fig. 1, we build upon the work of Dahmann et al. (2008) by expanding the focus to other SoS types, detailing their subtle differences to distinguish between other SoSs types. This can be used as a means to classify an example collaborative scenario in a likely SoS environment. This was designed to assist the initial steps of OASoSIS to give context, clarity, and useful data to support the SoS security risk assessment using a tool-supported framework, which is intended to act as a further bridge between operations and engineering environments.

The process of characterisation forms *Step 0* of OASoSIS. When characterising a SoS with Fig. 1, this helps us consider initial questions to guide the minimum amount of information to support the SoS security risk assessment process.

Initial questions in *Step 0* include:

- 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?

3.3. The SoS information security risk assessment process

The characterisation process leads into the second element, introducing an information security risk assessment process using a version of OA in a SoSs context, whilst initially following the steps of the process originally presented by authors of OA (Caralli et al., 2007). These steps become *Steps 1–7* of OASoSIS, however, *Step 1* was updated to introduce additional human factor considerations. The OA spreadsheet templates, along with an example version of the CAIRIS MMN model file used as part of the application of OASoSIS can be found stored within the online folder at https://github.com/D-Dev/cairis/tree/master/oasosis.

3.4. The SoS information security risk modelling and assessment process

Forming *Step 8* of OASoSIS, risk data may be refined, then modelled with tool-support from CAIRIS as the third element. This inte-

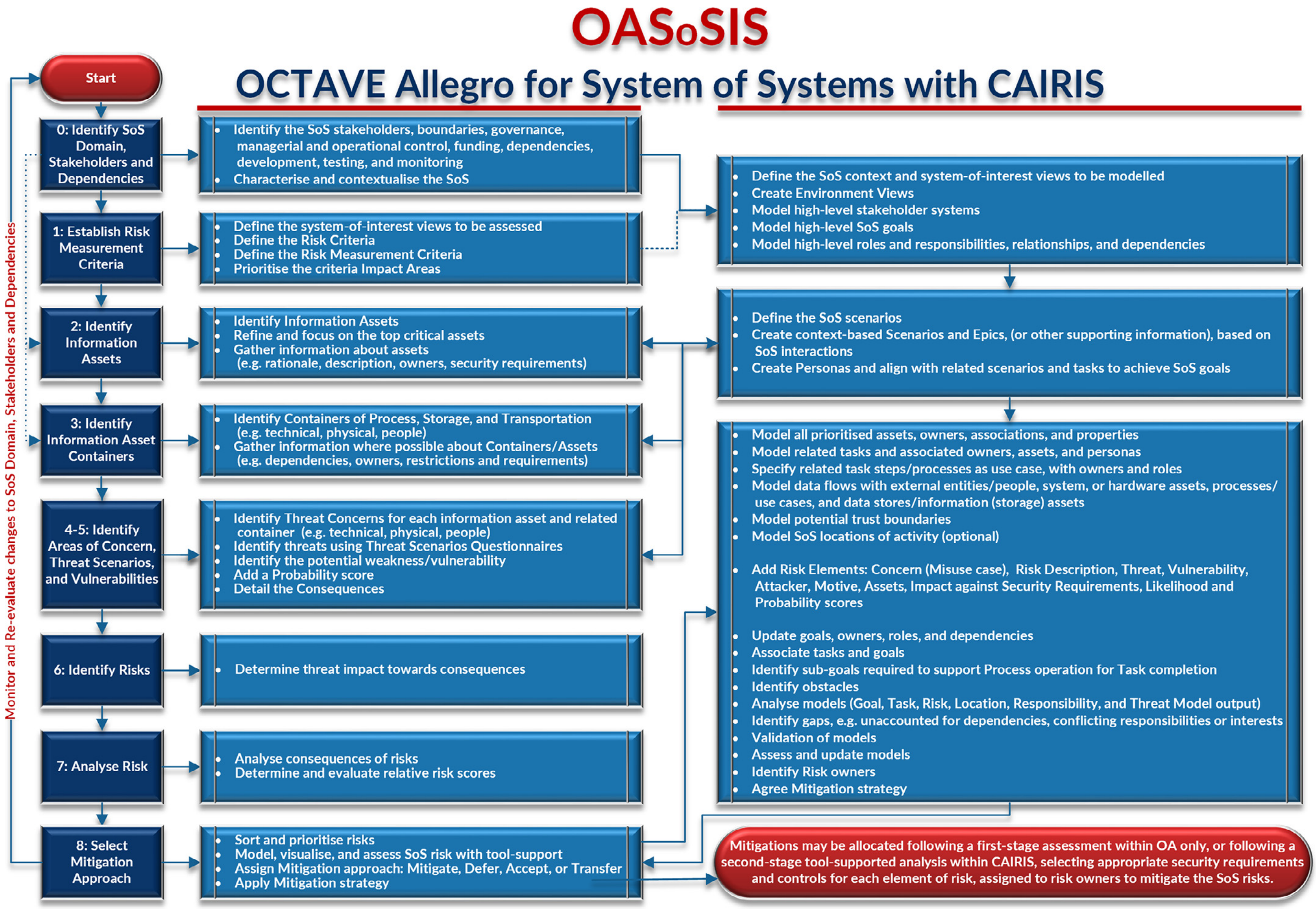

OASoSIS
OCTAVE Allegro for System of Systems with CAIRIS
Start
0: Identify SoS Domain, Stakeholders and Dependencies
Identify the SoS stakeholders, boundaries, governance, managerial and operational control, funding, dependencies, development, testing, and monitoring
Characterise and contextualise the 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
Monitor and Re-evaluate changes to SoS Domain, Stakeholders and Dependencies
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.

Fig. 2. OASoSIS.

grates a KAOS goal-driven modelling process with various concepts and techniques to help decision makers towards making informed decisions to reduce security risk and human factors concerns in the SoS. System goals, needs, dependencies, and expectations begin to be captured from early in the process.

An early part of the modelling process includes the creation and use of Personas. To do this, CAIRIS supports the alignments of Toulmin argumentation models to justify persona characteristics (Faily and Fléchais, 2010c). The Persona Helper Chrome plugin (Faily, 2018c) would be used to capture factoids from online and offline data, such as a webpage and clips of text within it. These factoids would be stored within CAIRIS, and exported to a Trello board (Trello, 2018) that was used as part of the affinity diagramming process. A further example of using Trello for affinity diagramming is discussed by Faily and Iacob (2017). Once the factoids are grouped into characteristics, these would be 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.

UML-based asset modelling is then introduced, which align with the task models, where tasks using assets are performed by a persona. Related roles that generally align with personas would be created. Use case descriptions related to those tasks would be created and aligned with roles. The use cases also act as the processes in a dataflow diagram, and assets represent the entities and datastores. Trust boundaries may be included.

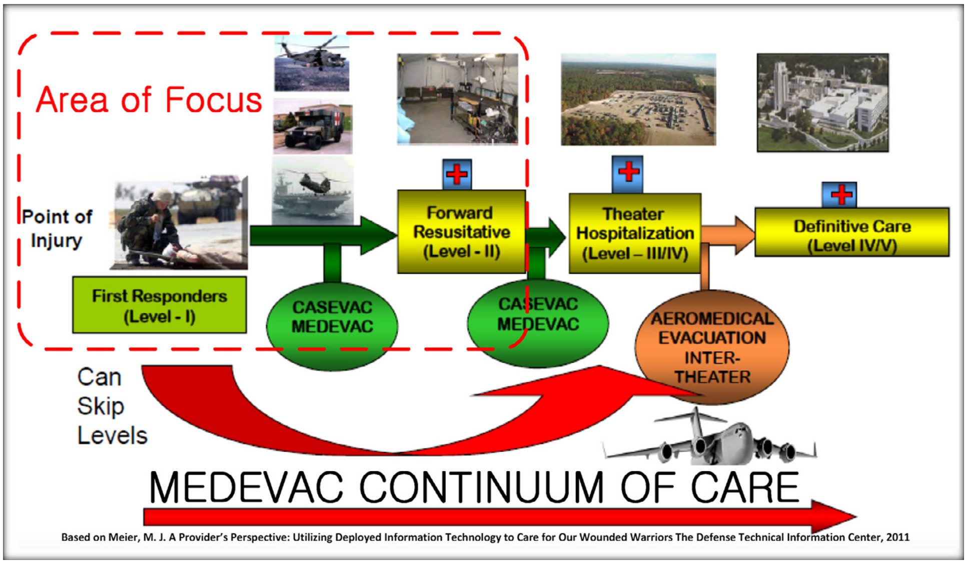
Risk elements previously captured in OA are populated and modelled. KAOS goals may have already begun to be captured, then expanded upon at this stage. Obstacle models may also be used to represent threats and vulnerabilities. Obstacles can be aligned to obstruct the system goals. Analysis and evaluation is then undertaken to identify any gaps, consider the risks, and identify risk owners required within the risk mitigation strategy.

3.5. Stakeholder feedback and validation

Following the completion of applying OASoSIS with the MMN SoS case study, a focus group interaction with UK military medical expert stakeholders would be used to gain feedback and validation towards the MMN scenario, the modelling and assessment of the scenario using OASoSIS. An overview of the OASoSIS process steps are illustrated in Fig. 2. Stakeholders feedback is discussed in Section 5.4.

4. Applying OASoSIS to the MMN SoS

The first step of OASoSIS includes a process to help characterise the SoS that was applied to identify the relevant context of the MMN. This was aligned with the OA information security risk assessment process, and applied in a SoS context to assess information security risks identified within the MMN scenario. 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 of the process.


Area of Focus
Point of Injury
First Responders (Level - I)
CASEVAC MEDEVAC
Forward Resusitative (Level - II)
CASEVAC MEDEVAC
Theater Hospitalization (Level – III/IV)
AEROMEDICAL EVACUATION INTER-THEATER
Definitive Care (Level IV/V)
Can Skip Levels
MEDEVAC CONTINUUM OF CARE

Based on Meier, M. J. A Provider's Perspective: Utilizing Deployed Information Technology to Care for Our Wounded Warriors The Defense Technical Information Center, 2011

Fig. 3. SoS Focus of MEDEVAC Continuum of Care, based on Meier (2011).

4.1. 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 Troop Contributing Nation (TCN) to this coalition relies upon its own people, processes, and technologies. 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 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. An example of the relations for each of the systems and sub-systems is illustrated in Section 4.4.

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 Forward Surgical Team (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, 2008b).

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* FST within one hour – *The Golden Hour*. An example demonstrating the area of focus for the MMN SoS scenario is shown in Fig. 3.

4.1.1. The scenario

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 4.2.

4.2. Applying OASoSIS: Step 0 - characterising the MMN

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 Fig. 1, this helps us consider initial questions detailed in Section 3. 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.

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.

4.2.1. 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, sub-systems of Charlie, include Force 1 who provides Air MEDEVAC, and Force 2 who 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; 2008b).

4.2.2. 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 system is 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 Common Operational Picture of tactical and medical Situational Awareness to achieve its mission safely and securely (Hartenstein, 2008a; 2008b; Meier, 2011).

4.2.3. 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, which could consequently have an 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 interrelations, but it is more difficult to align with Bravo, and Alpha. MEDEVAC testing exercises outside of the operational environment may exist.

4.2.4. 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 situational awareness 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).

4.3. 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 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.

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. 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 concepts of Human Factors Integration and Human

Systems Integration (HFSI) into *Step 1* of OA 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. This also considered 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.

4.4. 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. How models can be generated and interpreted when using CAIRIS is detailed within its online manual (Faily, 2018a).

Introducing this combined output helps to facilitate 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.

Fig. 4 provides a high-level overview of main systems and their sub-system assets with people and information assets considered in this scenario, for which the asset model was based upon. This includes *Alpha* (A) providing command and control, *Bravo* (B) as the initiating the call for MEDEVAC, and *Charlie* (C) providing systems for medical transportation and treatment.

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.

When modelling the scenario, systems were 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.

Within the asset model filtered to show *Bravo's* view, this would, for example, only include the known interactions where *Bravo* has direct interaction with other *Alpha* and *Charlie* systems, but not the unknown interactions only between *Alpha* and *Charlie*. As the asset model is UML-based, associations between assets may also be modelled as an aggregation or composition. Security properties for each of the assets are also added within the asset details, e.g. Confidentiality, Integrity, Availability, and Accountability. This was later repeated for the other system views, providing a bigger picture towards the different interactions interconnecting for the purpose of the MMN.

4.4.1. 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. Elements relating the output of this process capturing an Air Medic persona's characteristics are shown in Fig. 5.

Following this process 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, privacy elements were considered, but creates a future op-

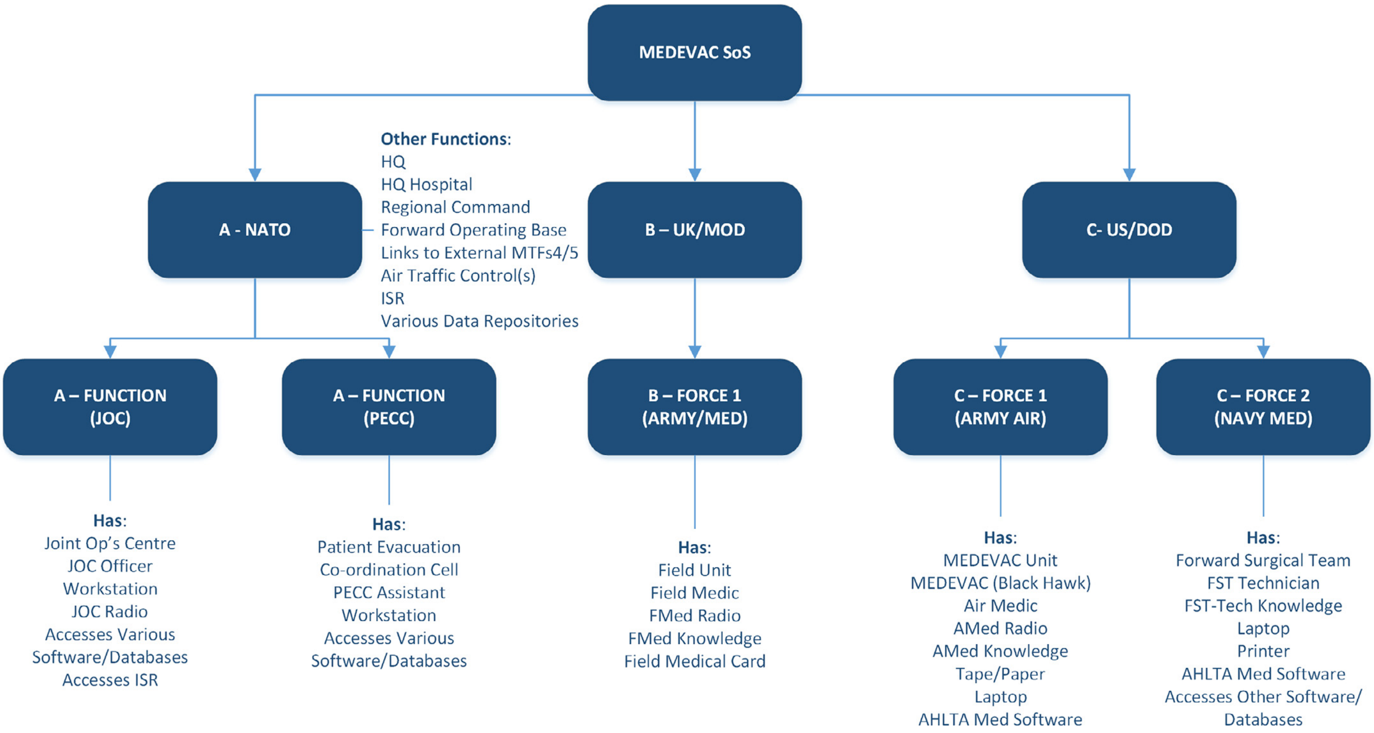
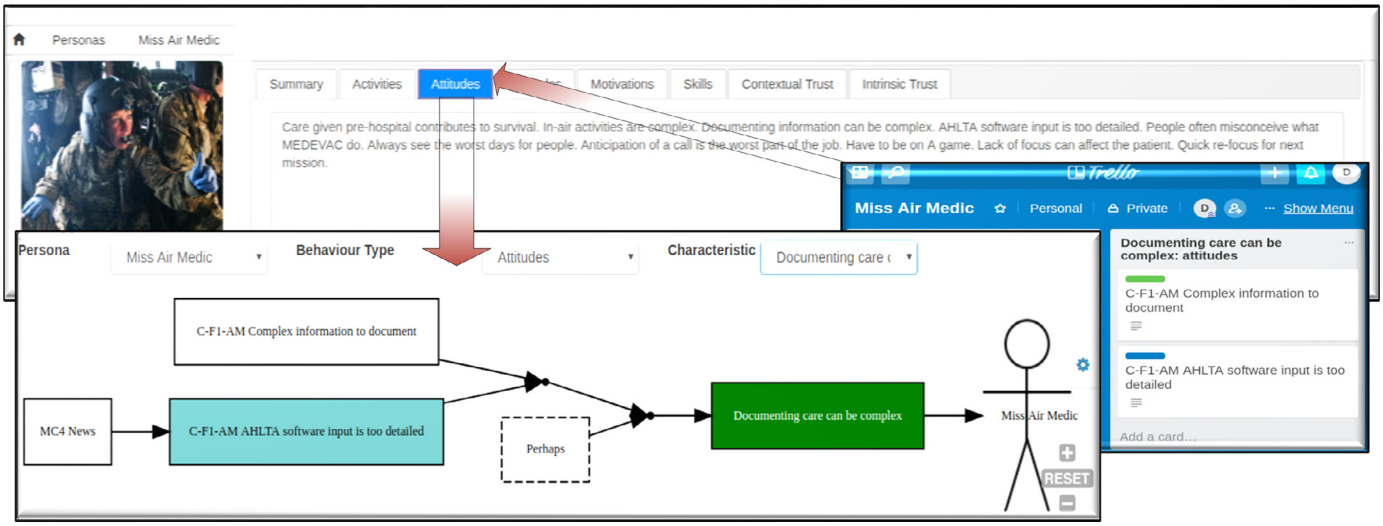


Fig. 4. High-level relations of the MMN SoS scenario.



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 (

C-F1-AM Complex information to document

C-F1-AM AHLTA software input is too detailed

Documenting care can be complex

Documenting care can be complex: attitudes

C-F1-AM Complex information to document

C-F1-AM AHLTA software input is too detailed

Fig. 5. CAIRIS Persona Characteristics and Model with Trello.

portunity for incorporating privacy by design using this SoS model and scenario.

4.4.2. 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 (systems) roles may apply. Once the tasks were created, the use cases relating to each task were linked to tasks through traceability links.

In this scenario, task steps could also include an instance where information is shared, but no software and hardware interaction may occur. 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 later copied into electronic formats by two other personas.

4.4.3. 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.

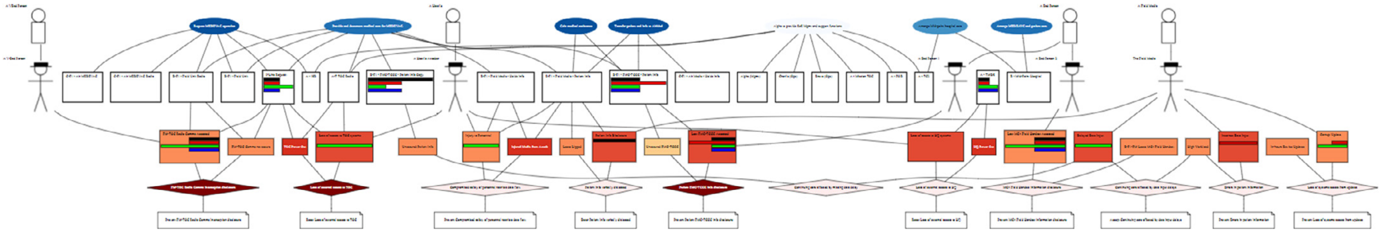


Fig. 6. CAIRIS Risk Model.

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.

4.4.4. 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 model demonstrated in Fig. 6 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.

4.4.5. 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 self-populating 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.

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.

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. A number of these graphically generated models were 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.

However, when viewing these models within CAIRIS, it is possible to focus-in upon a set of goals that may have a goal/task obstruction with elements of risk from a KAOS obstacle. Where a goal/task obstruction occurs further down in the goal tree, we can then focus-out within the model to visualise all other goals that may not be achieved as a knock-on effect form the impact of original risk element.

5. Discussion and lessons learned

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.

5.1. 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's HQ would mandate standard operating agreements and doctrine, Alpha would decide upon different policies within the doctrine regarding the SoS interaction, whereas each independent system of the SoS would operate 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. However, independent systems could potentially interpret and implement elements of the doctrine differently.

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 exhibited the characteristics of 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.

Although the characterisation process was useful towards classifying the type of SoS, the important benefit was the resulting clarification towards identifying the main stakeholders and dependencies between independent systems, and who has managerial and operational control within the SoS.

For example, the infrastructure supporting the MMN data flows, and the MC4 systems used by Charlie to digitally record and transfer medical data. However, we learned that as Bravo does not have processes in place and access to these systems, interoperability and communications are 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 5.4.

5.2. Applying Steps 1–7

The OA element was introduced and adapted to provide a simple repeatable and reusable process for identifying information security risk in a SoS. Early findings and lessons learned suggest the alignment of OA's 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. We learned 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.

Lessons learned indicated that 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 of the SoS to arrive at the *how* and *why* aspects a little quicker guided by the scenario-based questionnaires.

Furthermore, we learned that 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*, we found the spreadsheet capturing the risk data became quite large to manage, but more manageable than many pieces of paper. Nevertheless, we found 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, as more asset and context of use data is added, model complexity will increase.

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.

5.3. Applying Step 8

The refined data output of higher level risks captured in OA was transferred into CAIRIS, and 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, we found 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 we have learned this 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. We found the use of environments to represent views of independent systems helped to provide an element of clarity towards framing different aspects and concerns for each of the system views. We learned that 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.

We found that 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. 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.

We found the integration of goal modelling became central to the modelling element of OASoSIS. This helped to underpin the process guided by the SoS goals identified during *Step 0*, and then illustrated in *Step 8* as goal-driven requirements that aligned with the supporting tasks, processes, people and roles along with the identified risks and concerns. From the analysis, we found 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, we found 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, through lessons learned it 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, we found that details about owners of assets, tasks, goals, processes, and risks were largely captured during *Steps 0 to 5*, but became redundant or unaccounted for when transferring data into the tool-support.

We would argue clarity about those owners and authorities where authority is delegated to roles with specific responsibilities 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. We believe 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.

5.4. 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. Stakeholders also provided further context towards how Bravo may interact in this scenario with Alpha and Charlie. We found 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.

Based on stakeholder feedback, we learned 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 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. We found 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 (JOC). 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.

Based on stakeholder feedback, we found the risks identified when applying the elements of OASoSIS were otherwise considered representative for the MMN scenario. However, 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, an important lesson learned based on stakeholder feedback indicated 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.

6. Conclusion

In this article, OASoSIS was introduced, illustrating an approach for SoS information security risk assessment, which was applied and tested using a Military MEDEVAC SoS case study scenario. The approach implemented an adapted version of OA aligned with a SoS characterisation process for identifying the SoS context for the risk assessment using OA.

Previous research identified confusion around the use of the SoS term, predominately within operational environments, and when defining collaborating systems as a SoS. The characterisation process supported by simple definitions of SoSs was introduced to reduce this confusion and provided a focus towards where the SoS managerial and operational control was in place. Identifying control and governance is critical to the resilience of the SoS in achieving its SoS mission.

During the first-stage of the assessment using OA, risks to critical assets were identified and analysed. This output produced risk data that enabled the alignment with concepts, models, and techniques integrated with tool-support from CAIRIS to provide further visualisation and analysis of SoS risks and goals to be accounted for within RBDM and SoSRE.

When designing this approach, we considered the diversity of small and large-scale SoS examples, many of which are presented in a different context, with different configurations and challenges. Independent systems may also have different standards and policies in place to achieve its day job, whilst also integrating with SoS needs and requirements.

This simple repeatable process can be used to support a SoS information security risk assessment approach, and provides a means to identify the scale and complexity of interacting systems towards integration and operational challenges. This is important to ensure asset identification and requirements are accounted for in the OA assessment and within tool-support to ensure the needs are met towards stakeholders, situational awareness, security, interoperability, and mitigation of risks in these areas.

6.1. Limitations

Certain limitations have been a factor towards completing related research and validation. For example, where research conducted in this article and supporting work in Ki-Aries et al. (2017b) were military-based centred around NATO activities. Although the stakeholder input and feedback they provided was good and extremely useful, detailed depth was not available for security reasons, given the need for outputs to be publishable in civilian environments.

Limitations are also acknowledged towards the reduced-scale SoS example used, although it did provide suitability towards testing the components within OASoSIS before further application to a larger and more current SoS example. To strengthen the validity of OASoSIS, other SoS types and configurations could therefore be tested and validated in future work.

6.2. Applicability

Using the OA approach applied in a SoS context provides the means for organisations or the SoSRE community to carry out an information security risk assessment that suits limited interaction between all SoS stakeholders, and may be completed without the need for great technical expertise. It would, however, require risk assessors to have a good understanding of the related context, environment, and threats.

This provides a repeatable process that can be used for smaller organisations, or areas with larger more established risk management processes, e.g. NIST or ISO, whereby OA can fit comfortably within the risk assessment stages. This could also accommodate risk stages within development or engineering approaches. The level of required training or implementation costs associated with users and implementers of this process would depend of the type and nature of the SoS collaboration. However, the related process and open-source tool-support are currently freely available to use.

For the SoRE community and academia, this research follows-on from previous research in this area, and provided a further contribution in an area that lacks in a depth of research towards modelling and assessing SoS security risks, and associated RBDM. The characterisation process shown in Fig. 1 is also likely to provide value as a standalone item for other SoS engineering related projects. Based on the findings of this research, it provided the foundation to reapply the approach with few refinements to a new SoS scenario to gain further testing and validation of OASoSIS.

6.3. Future work

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. Lessons learned from using OASoSIS with the MMN have enabled us to update and streamline the process to some degree, whilst integrating new elements into the modelling process. For example, applying *Steps 1–3* in parallel, changing the order of *Steps 4 and 5* to consider threat scenarios earlier whilst continuing to capture vulnerabilities where possible. 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 and accountability towards mitigating risk.

Research therefore continues to identify how combining different model elements with the use of tool-support can assist the visualisation of information security risk and related human factors to support RBDM for the SoSRE communities. As a continuation of this research, OASoSIS would be reapplied to an Emergency Response SoS considered for use within a Canadian Emergency Management System (of Systems). OASoSIS would be used to identify and assess areas of information security risk and related human factors of the SoS, thus providing further testing and validation of OASoSIS as an information security risk assessment and modelling process to assist RBDM in SoSRE.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The research described in this paper was funded by Bournemouth University studentship DSTLX1000104780R_BOURNEMOUTH_PhD_RASOS. We are also grateful to Dstl for their sponsorship of this work.

References

AlhajHassan, S., Odeh, M., Green, S., 2016. Aligning systems of systems engineering with goal-oriented approaches using the *i** framework. In: IEEE International Symposium on Systems Engineering (ISSE), 2016. IEEE, pp. 1–7.

Alkhabbas, F., Spalazzese, R., Davidsson, P., 2016. IoT-based systems of systems. In: Proceedings of the 2nd Edition of Swedish Workshop on the Engineering of Systems of Systems (SWESOS 2016). Gothenburg University.

Ardi, S., Byers, D., Meland, P.H., Tondel, I.A., Shahmehri, N., 2007. How can the developer benefit from security modeling? In: Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on. IEEE, pp. 1017–1025.

Atzeni, A., Cameroni, C., Faily, S., Lyle, J., Fléchais, I., 2011. Here's Johnny: a methodology for developing attacker personas. In: Availability, Reliability and Security (ARES), 2011 Sixth International Conference. IEEE, pp. 722–727.

Boardman, J., Sauser, B., 2006. System of systems-the meaning of. In: 2006 IEEE/SMC International Conference on System of Systems Engineering. IEEE, p. 6.

Böröcz, I., 2016. Risk to the right to the protection of personal data. Eur. Data Protect. Law Rev. 2 (4), 467–480.

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., Longley, D., 2006. Security risk analysis for complex systems. In: ISSA, pp. 1–12.

British Standards Institution. BS ISO/IEC 27005, Information technology - Security techniques - Information security risk management 2011.

Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R., 2007. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Technical Report. DTIC Document.

Checkland, P., 1999. Systems Thinking, Systems Practice. John Wiley & Sons.

Chiprianov, V., Gallon, L., Munier, M., Aniorte, P., Lalanne, V., 2014. Challenges in security engineering of systems-of-systems. In: Troisième Conférence en IngénieriE du Logiciel, p. 143.

Cleland-Huang, J., 2013. Meet Elaine: a persona-driven approach to exploring architecturally significant requirements. IEEE Softw. 30 (4), 18–21.

Cooper, A., 1999. The Inmates are Running the Asylum. Macmillan Publishing Company Inc.

Cooper, A., Reimann, R., Cronin, D., Noessel, C., 2014. About Face: The Essentials of Interaction Design. John Wiley & Sons.

Currall, S.C., Judge, T.A., 1995. Measuring trust between organizational boundary role persons. Organ. Behav. Hum. Decis. Process. 64 (2), 151–170.

Dahmann, J., Rebovich, G., McEvilley, M., Turner, G., 2013. Security engineering in a system of systems environment. In: Systems Conference (SysCon), 2013 IEEE International. IEEE, pp. 364–369.

Dahmann, J.S., Baldwin, K.J., 2008. Understanding the current state of US defense systems of systems and the implications for systems engineering. In: Systems Conference, 2008 2nd Annual IEEE. IEEE, pp. 1–7.

Dahmann, J.S., Rebovich Jr, G., Lane, J.A., 2008. Systems Engineering for Capabilities. Technical Report. DTIC Document.

Den Braber, F., Brændeland, G., Dahl, H.E.I., Engan, I., Hogganvik, I., Lund, M.S., Solhaug, B., Stølen, K., Vraalsen, F., 2006. The CORAS Model-Based Method for Security Risk Analysis, vol. 12. SINTEF, Oslo, pp. 15–32.

Diaper, D., Stanton, N., 2004. The Handbook of Task Analysis for Human-Computer Interaction. Lawrence Erlbaum.

Dogan, H., Pilfold, S.A., Henshaw, M., 2011. The role of human factors in addressing systems of systems complexity. In: Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on. IEEE, pp. 1244–1249.

Elahi, G., Yu, E., Zannone, N., 2010. A vulnerability-centric requirements engineering framework: analyzing security attacks, countermeasures, and requirements based on vulnerabilities. Requir. Eng. 15 (1), 41–62.

Faily S., 2018a. CAIRIS [online]. Available from: https://cairis.org [Accessed 28 February 2018].

Faily, S., 2018b. Designing Usable and Secure Software with IRIS and CAIRIS, first ed. Springer.

Faily S., 2018c. Personahelper. Chrome Web Store; Available From: https://chrome.google.com/webstore/detail/persona-helper/mhojpjjecjmdbbooonpgloh cedhnjkho [Accessed 2 May 2018].

Faily, S., Fléchais, I., 2010a. Barry is not the weakest link: eliciting secure system requirements with personas. In: Proceedings of the 24th BCS Interaction Specialist Group Conference. British Computer Society, pp. 124–132.

Faily, S., Fléchais, I., 2010b. A meta-model for usable secure requirements engineering. In: Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems. ACM, pp. 29–35.

Faily, S., Fléchais, I., 2010c. The secret lives of assumptions: developing and refining assumption personas for secure system design. In: Proceedings of the 3rd Conference on Human-Centered Software Engineering, vol. LNCS 6409. Springer, pp. 111–118.

Faily, S., Iacob, C., 2017. Design as code: facilitating collaboration between usability and security engineers using CAIRIS. In: Proceedings of the 4th International Workshop on Evolving Security & Privacy Requirements Engineering, ESPRE 2017. IEEE. To Appear

Faily, S., Iacob, C., Ali, R., Ki-Aries, D., 2020a. Identifying implicit vulnerabilities through personas as goal models. In: Computer Security. Springer, pp. 185–202.

Faily, S., Scandariato, R., Shostack, A., Sion, L., Ki-Aries, D., 2020b. Contextualisation of data flow diagrams for security analysis. In: Graphical Models for Security: 7th International Workshop, GraMSec 2020, Boston, MA, USA, June 22, 2020 Revised Selected Papers. Springer, p. 186.

Firesmith, D.G., 2003. Analyzing and Specifying Reusable Security Requirements. Technical Report. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Hartenstein Col. Dr., I., 2008a. Medical Evacuation in Afghanistan: Lessons Identified Lessons Learned [online]. Technical Report. Available From: https://stoptheme devacmadness.files.wordpress.com/2012/02/nato-medical-evacuation-in-afghanistan-mp-hfm-157-05.pdf [Accessed 19 January 2018].

Hartenstein Col. Dr., 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].

Homeland Security. Strategic Principles for Securing the Internet of Things [online]. 2016. Available From: https://www.dhs.gov/securingtheIoT [Accessed 30 June 2017].

International Council of Systems Engineering. Systems Engineering Handbook. INCOSE; version 3.1 ed.; 2007.

Institute of Electrical and Electronics Engineers (IEEE), 1990. Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. IEEE, New York, NY.

I. International Organization for Standardization, International Electrotechnical Commission (IEC), ISO/IEC/IEEE 24765:2010(E) Systems and Software Engineering - System and Software Engineering Vocabulary (SEVocab), International Organization for Standardization, Geneva, Switzerland.

Jones, A., 2007. A framework for the management of information security risks. BT Technol. J. 25 (1), 30–36.

Ki-Aries, D., Dogan, H., Faily, S., Whittington, P., Williams, C., 2017a. From requirements to operation: components for risk assessment in a pervasive system of systems. In: 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)-Proceedings of 4th International Workshop on Evolving Security & Privacy Requirements Engineering. IEEE, pp. 83–89.

Ki-Aries, D., Faily, S., 2017. Persona-centred information security awareness. Comput. Secur. 70, 663–674.

Ki-Aries, D., Faily, S., Dogan, H., Williams, C., 2017b. Re-framing “the AMN”: a case study eliciting and modelling a system of systems using the Afghan mission network. In: 11th IEEE International Conference on Research Challenges in Information Science 10–12 May 2017 Brighton, UK. IEEE.

Lane, J.A., Epstein, D., 2013. What is a System of Systems and Why Should I Care?. University of Southern California.

Maier, M.W., 1996. Architecting principles for systems-of-systems. In: INCOSE International Symposium, vol. 6. Wiley Online Library, pp. 565–573.

MC4, 2018. The MC4 System [online]. MC4 US Army, Available From: http://www.mc4.army.mil/Mc4System/Mc4Sys.aspx [Accessed 15 January 2018].

McKnight D.H., Chervany N.L., 1996. The meanings of trust.

Meier, M.J., 2011. A provider’s perspective: utilizing deployed information technology to care for our wounded warriors. In: Presented at the 2011 Military Health System Conference, January 24–27, National Harbor, Maryland: The Joint Staff, J4/HSSD. The Defense Technical Information Center. Available From: http://www.dtic.mil/dtic/tr/fulltext/u2/a556202.pdf [Accessed 19 January 2018].

Meland, P.H., Jensen, J., 2008. Secure software design in practice. In: Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, pp. 1164–1171.

Morris, E., Place, P., 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.

NATO. NATO Standard AMedP-8.1 A1 [online]. 2013. 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].

NCOIC. NCOIC - What is Interoperability [online]. 2019. https://www.ncoic.org/what-is-interoperability/ [Accessed 20 December 2019].

Ncube, C., Lim, S.L., 2018. On systems of systems engineering: a requirements engineering perspective and research agenda. In: Requirements Engineering Conference (RE), 2018 IEEE 26th International. IEEE.

Ncube, C., Lim, S.L., Dogan, H., 2013. Identifying top challenges for international research on requirements engineering for systems of systems engineering. In: Requirements Engineering Conference (RE), 2013 21st IEEE International. IEEE, pp. 342–344.

Nielsen, C.B., Larsen, P.G., Fitzgerald, J., Woodcock, J., 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. NIST Special Publications [online]. 2017. NIST Computer Security Resource Centre, Available From: http://csrc.nist.gov/publications/PubsSPs.html [Accessed 22 April 2017].

Office of the Deputy Under Secretary of Defense, for Acquisition and Technology. Systems and Software Engineering, Systems and Software Engineering. Systems Engineering Guide for Systems of Systems, Washington, DC: ODUSD(A&T)SSE, 2008, 1st Edition. 2008.

Pahon E.. Best Soldiers for the worst days: Medevac crews in Afghanistan save lives day, night [online]. 2012. 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].

Ross, R., McEvilley, M., Oren, J.C., 2016. Systems security engineering. NIST Spec. Publ. 800, 33.

Seffers G.I.. A Lot of Blood in Kandahar [online]. 2011a. SIGNAL Magazine, AFCEA International, Available From: https://www.afcea.org/content/lot-blood-kandahar [Accessed 16 January 2018].

Seffers G.I.. Military Treats Outbreak of Chat Rooms in Afghanistan [online]. 2011b. SIGNAL Magazine, AFCEA International, Available From: https://www.afcea.org/content/military-treats-outbreak-chat-rooms-afghanistan [Accessed 16 January 2018].

Shostack, A., 2014. Threat Modeling: Designing for Security. John Wiley & Sons.

Sindre, G., Opdahl, A.L., 2005. Eliciting security requirements with misuse cases. Requir. Eng. 10 (1), 34–44.

Sommerville, I., 2015. Software Engineering, tenth ed. Pearson.

Trello. 2018. Trello. Trello, Available From: https://trello.com/ [Accessed 2 May 2018].

Trivellato, D., Zannone, N., Glaundrup, M., Skowronek, J., Etalle, S., 2013. A semantic security framework for systems of systems. Int. J. Coop. Inf. Syst. 22 (01), 1350004.

Van Lamsweerde, A., 2009. Requirements Engineering: From System Goals to UML Models to Software, vol. 10. John Wiley & Sons, Chichester, UK.

Whittington, P., Dogan, H., 2016. Smartpowerchair: characterization and usability of a pervasive system of systems. IEEE Trans. Hum. Mach. Syst. 47 (4), 500–510.

Zand, D.E., 1972. Trust and managerial problem solving. Adm. Sci. Q. 229–239.

Zhou, B., Drew, O., Arabo, A., Llewellyn-Jones, D., Kifayat, K., Merabti, M., Shi, Q., Craddock, R., Waller, A., Jones, G., 2010. System-of-systems boundary check in a public event scenario. In: System of Systems Engineering (SoSE), 2010 5th International Conference on. IEEE, pp. 1–8.

Dr Duncan Ki-Aries is a Lecturer in Computer Science and Cyber Security at Bournemouth University (BU), and a Programme Leader of the M.Sc. Cyber Security and Human Factors at BU. Duncan is also an active member of the Requirements Engineering (RE) community. Current and previous research has explored how techniques from Requirements Engineering can be used to align with the assessment of security, risk, and human factors, specifically in the context of Systems of Systems, whilst integrating the use of tool-support with CAIRIS, and which now explores inclusive and accessible security by design. Duncan's work has appeared in leading security and system engineering venues such as Computers & Security and the IEEE SoSE, in addition to the international workshop on Evolving Security & Privacy Requirements Engineering (ESPRE) 2017 and ESPRE 2018. Duncan has also served as a student volunteer at British HCI 2016, and RE conferences over recent years, and since 2019 has been part of the organising committee of ESPRE, co-located with RE.

Dr Shamal Faily is a Lecturer in Cyber Security at the School of Computing at Robert Gordon University (RGU), and Programme Leader of RGU's Cyber Security undergraduate degree. Shamal is also a RISCS Fellow in Secure Development Practices, and a SPRITE+ Expert Fellow. Shamal's research explores how security can be 'built in' at the earliest stages of a software product or service's design, and how software can be designed to ensure it remains secure and usable when used in different contexts. As such, Shamal's research interests are at the intersection of Cyber Security, Software Engineering, and Human-Computer Interaction (HCI). Shamal serves on the editorial board of the International Journal of Systems and Software Security and Protection (IJSSSP), was a general cochair of British HCI 2016, and one of the founding chairs of the Evolving Security and Privacy Requirements Engineering (ESPRE) annual workshop series.

Dr Huseyin Dogan is an Associate Professor and the Deputy Head of Department in Computing and Informatics at Bournemouth University. Huseyin's recent research was funded by the industry, Innovate UK, Engineering and Physical Sciences Research Council (EPSRC), European Commission (EC) and Higher Education Innovation Fund (HEIF). Huseyin was the General Co-Chair for the 30th International British Computer Society Human Computer Interaction Conference. He has over 100 publications and his research on Assistive Technologies (with Dr Paul Whittington) featured on the BBC South, BBC Radio Solent, The Ergonomist, Auto Express, Bournemouth Echo and The Sunday Times magazine. Huseyin was also the General Co-Chair for the 30th International British Computer Society Human Computer Interaction Conference (BCS HCI 2016).

Dr Chris Williams is a Senior Principal Engineer with Dstl. Chris graduated from the University of Oxford with a First in Engineering Science, and subsequently gained his Ph.D. from Bristol University on the topic of chaotic waveforms for communications. Alongside periods in industry (Research Manager for Fujitsu) and academia (Research Fellow at Bristol University) much of his career has been in Government defence research (Dstl and predecessors). Areas of expertise include novel waveforms, communications signal processing, dynamic spectrum access, risk based decision making, agile systems and requirements engineering.