System of Systems Characterisation assisting Security Risk Assessment

Duncan Ki-Aries, Shamal Faily, Huseyin Dogan
Bournemouth University
Fern Barrow, Poole, UK
{dkiaries,sfaily,hdogan}@bournemouth.ac.uk

Christopher Williams
Defence Science and Technology Laboratory
Porton Down, UK
cwilliams@mail.dstl.gov.uk

***Abstract*—*System of Systems* (SoS) is a term often used to describe the coming together of independent systems, collaborating to achieve a new or higher purpose. However, clarity is needed when using this term given that operational areas may be unfamiliar with the terminology. In this paper, we present an approach for refining System and SoS descriptions to aid multi-stakeholder communication and understanding; building on previous work, we illustrate an example of characterising a likely SoS. By identifying key stakeholders, systems, management and control, this approach supports the initial steps of a SoS security risk assessment approach using a tool-supported framework that supports operational needs towards requirements engineering.**

***Index Terms*—System of Systems, MEDEVAC, Security, Risk.**

I. Introduction

To meet evolutionary demands, independent organisations, networks or systems may need to come together to achieve a greater or combined purpose. This leads to challenges and risks arising from the independent yet inter-dependant interactions of collaborating systems. For example, an emergency response unit may need to interoperate with the police, fire, ambulance, coastguard, or other critical services. Each service 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 mission objectives.

This example of systems coming together for a greater interaction collaborating with the emergency response unit could, therefore, be described as being a *System of Systems* (SoS). Other examples of systems converging to form a SoS may be less or more complex, or have differing levels of management and oversight. SoSs are further challenged by geographical, organisational, safety, security, and human factors considerations affecting risk within the SoS as a whole. Because these considerations are typically greater than that of a single system, the interactions and interdependencies increase risks for independent systems, and the SoS as a whole.

Security risks are exacerbated by differing requirements, goals, trust boundaries, and levels of assurance, some of which may be unknown. Some risks may, therefore, not exist until the coming together of the SoS, with further emerging risks through the evolution of the SoS. Moreover, accounting for security risk may depend on the structure of the SoS, its management and control structure, and from what or whose view within the SoS risk is being assessed. For example, the emergency response unit provides management, but has limited control of independent systems. The SoS may be assessed from the emergency response unit point of view to form the SoS with independent systems. Alternatively, the police may assess SoS integration with other systems and the emergency response unit, independently or as a whole. In either case, a challenge for SoSs is where each entity may only know or have access to varying levels of information about each system in which to assess security risk as a whole. In other scenarios, a SoS may have limited or no central management, meaning that security and risk should still be assessed at a SoS level, but may need to be done at a system level if there is a weak collaboration with limited or no useful information to support security risk assessment. Identifying the SoS context is, therefore, vital to security risk assessment if we are to appreciate the SoS mission and complexities.

In this paper, we present a method of characterising and classifying a SoS to support a security risk assessment process identifying relevant SoS context prior to assessment. We present the related work upon which our approach is based in Section II, before presenting the approach in Section III. We illustrate this approach with a case-study example based on a military medical evacuation scenario in Section IV. We discuss the implications of this approach in Section V, before concluding with pointers to future work in Section VI.

II. Related Work

Systems are composed of parts or elements with relationships between other elements of the system [1]. A system may be defined as being a functionally, physically, and/or behaviourally related group of regularly interacting interdependent elements forming a unified whole [2]. However, how the parts and relationships are gathered together as a whole must be understood to appreciate how it forms as a system [3] [4].

System of Systems (SoS) is a term used to classify an arrangement of independent and interdependent systems collectively coming together for a task that none of the systems can accomplish independently. However, systems generally retain their own identities, management authorities, responsibilities, goals and resources to support current and evolving needs whilst adapting to meet SoS goals [5] [6]. The SoS concept may, however, mean different things to different people. In an

organisational context, the SoS is the enterprise-wide sharing of core business information across functional and geographical areas, often through third-party arrangements. Whereas, military and defence SoSs are usually configurable sets of constituent-systems in dynamic communication infrastructures [7]. However, anecdotal evidence suggests that, outside of engineering, the SoS term is relatively unknown, although *Network of Networks* is occasionally used in a similar context.

SoSs can be considered as large-scale concurrent and distributed systems, comprised of complex systems with autonomy [8] [9] [10]. However, a SoS is equally a system that contains two or more independently managed elements [1], regardless of scale. A SoS is said to exist when there is a majority presence of five characteristics: operational independence, managerial independence, geographic distribution, evolutionary development, and emergent behaviour [11] from combined system interactions in ways not intended by the original single system designers. This means actions cannot be predicted through analysis at any level other than the SoS as a whole [12]. Types of SoSs are generally classified as follows.

- *Directed SoS*: these are built and managed to fulfil specific purposes; they are centrally managed during long-term operation to continue to fulfil and evolve those purposes. Component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose [11].
- *Acknowledged SoS*: these have recognised objectives, a designated manager, and resources, but constituent systems retain their independent ownership, objectives, funding, as well as development and sustainment approaches. Changes to systems are based on collaboration between the SoS and systems [13].
- *Collaborative SoS*: these are distinct from Directed SoSs in that the central management organisation has no coercive power to run the system. The component systems voluntarily collaborate to fulfil the agreed upon central purposes [11].
- *Virtual SoS*: these lack both central management authority and centrally agreed upon purposes; they may exist deliberately or accidentally, and large-scale behaviour emerges, which may be desirable [11]. Participants informally collaborate and manage their own systems to maintain the system as a whole [1].

Because they are composed of systems that come together in ways they were not originally designed for, SoSs share two additional elements:

- *Emergence*: the formation of new behaviours due to development or evolutionary processes coming together [8]. Emergent behaviour evolves through the interactions and collaborations that naturally develop within a SoS [11]. Emergent behaviours must be carefully planned, tested, and managed [2], which is a challenge when designing for the SoS. The challenge is to learn how, as the SoS evolves, emergence can flourish, yet retain agility to quickly detect and defend against unintended behaviours [4], while maintaining interoperability and availability.
- *Interoperability*: the ability of two or more systems or elements to use and exchange information [14]. SoSs present an information sharing problem that introduces complexity resulting from interoperability needs across systems [15]. Moreover, the interoperability continuum brings together the importance of governance, standard operating procedures, technology, training and exercises, and usage. Compatible technology alone may not achieve interoperability, as technology, people, and organisational integration all need to be aligned to achieve interoperability [16]. Therefore, Sommerville et al. [17] argue a system's components and their relationships need to be thoroughly understood, otherwise predictions cannot be made as the scale and complexity increases.

Typical examples of SoSs may range from larger-scale military operations, to smaller examples with fewer direct stakeholders [18] [19]. For example, the Smartphone is a common system integrated into personal and work environments that could be considered a SoS. Many Smart device and Internet of Things (IoT) systems are likely to be SoSs [20] [21] where strategic principles are required for design and operation [22]. Utilising the Internet, software applications on a Smart device may be operated by users to connect to and control other smart systems such as home security, communications systems, or assistive technology [23].

An emergency response unit as a SoS brings together independently owned and managed systems and services such as fire, police, ambulance, hospitals and other facilities collaborating to deliver a service on which reliance is placed to achieve the SoS level objective or mission [15] [24]. Further reliance may also be found when considering the over-arching role of critical infrastructure. For example, where the health infrastructure on a national level has an operational and managerial dependence upon hospitals, medical centres, communication systems, power systems and networks, transportation, health insurance and finance networks to operate as a complex interconnected infrastructure [25].

Stakeholder needs and input are a vital consideration in addition to the system interconnections and boundaries of the SoS. For example, the ownership and operation of constituent systems within a SoS by independent stakeholders may lead to limitations on the exchange of information [24]. Security risks will likely increase where stakeholders are not always recognised across the SoS, or stakeholders of individual systems may have little interest, or resist the SoS demands on their system giving lower priority to the SoS [2].

Trust mechanisms are an important factor throughout the entire SoS life-cycle. Although there are a number of documented types of trust [26], trust is the willingness to be vulnerable, based on the positive expectations about the actions of others [27], and it is an individual's reliance on another party under conditions of dependence and risk [28]. Trustworthiness of the flow of information, the security of the service provision and the protection of the supporting systems of the SoS need

to be taken into account [29]. However, a trust relationship is a dynamic relationship that may change over time [17], and may span across multiple systems, boundaries and people, leading to varied assumptions, perceptions, expectations and appetite. Through transparency and trust, active participation should be focused on areas specifically related to the systems and the SoS as a whole [30].

Security risk is likely to be present across most types of SoS, with security risk assessment conducted at different levels. For example, at the operational level, carried through to the development life-cycle, where security requirements should begin with asset analysis and the context in which they are in [31]. This should also continue to focus on related human factors and interoperability critical for the SoS operation. However, program risk management in systems engineering programs is also a factor where organisational design information requires consideration and protection [32].

A range of risk assessment approaches may be used, but articulating a clear and consistent risk statement to identify possible adverse effects is always a core component [33]. In the current context, risk assessment should rely on modelling, and be repeatable, measureable, and auditable [34]. However, before any SoS risk assessment begins, elements and factors such as the context of use, mission goals, boundaries, relevant stakeholders, scope, and risk criteria should be considered. A grounded SoS characterisation therefore becomes a critical prerequisite to a SoS security risk assessment.

III. Approach

As discussed, the term *System of Systems* can be applied to a number of scenarios with differing scale or complexity of interconnected systems, or geographical boundaries. SoSs were mentioned decades ago [35] [36], perhaps in a slightly different context, but it was Maier [11] that really gave a more modern categorisation of SoSs, along with Dahmann and Baldwin [13] a decade later bringing together the main four categories that hold today. However, over those forty or more years to present day, SoSs have changed considerably, for example, with the concept of IoT and Smart devices, vehicles, grids and cities. This is something that was perhaps not accounted for in past work, and more unlikely in previous years where the technical considerations were more mechanical and machine-based.

Through our research [19] [37], it has also become evident that use of a common less-technical language of security and risk can assist multi-level stakeholder understanding. Moreover, it is useful for operational stakeholders to first align with the concept of SoSs before its complexity can be identified and appreciated. Therefore, based on findings from the review of literature and case-study implementations, to assist the communication bridge between operations and requirements engineering, a clearer SoS distinction and description is proposed. An example using simple models is demonstrated in Figure 1. This is provided to ground the SoS concept, definition and description, and provide a baseline for continuing research between domains. This links directly to current work designed to classify and characterise a SoS, which began with work characterising the Afghan Mission Network (AMN) [18].

Systems can be considered as *'a coming together of people, process, software and hardware, integrated to achieve a purpose'*. From an operational or design perspective, these systems are likely to be composed of supporting sub-systems and component systems interconnecting to fulfil system needs. As these interconnections grow in scale, complexity increases with evolutionary, geographical, environmental, cultural, organisational and technical demands. Systems may, therefore, generally be considered as being small-scale, large-scale and at times complex. A small-scale system could, however, still be described as having complexity with software and hardware interactions, which in a different context could itself be described as large-scale and complex. For example, when considering the quantity of lines of code in software, interoperating with seamless background services to provide functional applications. In either case, a large-scale complex system may not always be a SoS. Furthermore, research suggests the term *System of Systems* could equally apply to smaller scale independent system collaborations with less complexity. This difference is evident with examples ranging from basic IoT applications, through to software dependant systems up to large-scale governmental or military and defence SoSs.

A distinction may also be drawn where a single system designed for an original purpose may evolve overtime, but may only be an adaptation of itself to meet changing environmental and cultural needs. This example may not qualify as a SoS. However, it is also true within a SoS, an independent system or lower-level systems designed for a different purpose, could permanently become a component system of a SoS; it could return to its original state, but may serve a greater purpose in its new context.

SoSs can be described as containing independent systems designed for a purpose different to that of the SoS as a whole. Each upper-level individual system is one part of the whole. SoSs may also contain systems which themselves are SoSs. Evolution may have led to the need and creation of the SoS that will likely continue to evolve and adapt for resilience until which point it ceases to exist as a whole. This may be due to the nature of the SoS only forming when required, e.g. an emergency response unit. Alternatively, this may relate to the permanent disbanding or disposal of the SoS.

We therefore propose an improved description to simply define a *System of Systems* as being *'the coming together of independent systems collaborating for a new or higher purpose'*. Independent collaboration must be in place by one means or another for the SoS to exist, otherwise they would simply be independent systems. A Directed SoS seemingly has the most in common with the genetic make-up of a single independent system, usually with a top-down input, but still requires bottom-up input to function. Evolutionary and geographical challenges in present day exist in systems, and so is not unique to SoSs, whereas emergence is more likely within SoSs. The level of central control and oversight of the

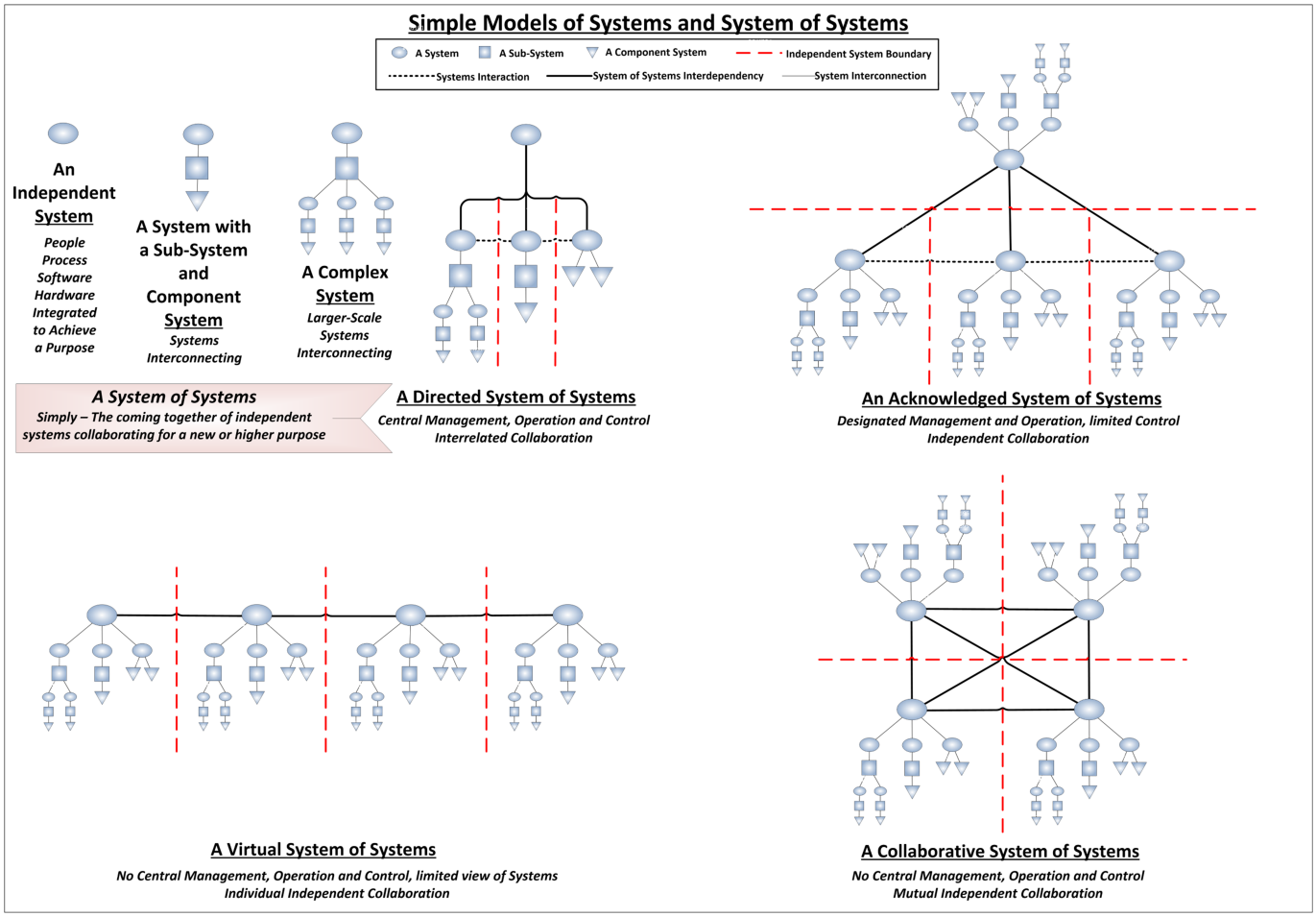

Fig. 1. Simple Models for Systems and System of Systems

functional and operational SoS appears to be the overarching feature, combined with the type and level of collaboration from independent systems, their sub-systems, and varying trust boundaries. We further propose that:

- A Directed SoS can be described as possessing *'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 as a whole'*;
- A Collaborative SoS has *'no central management, so operation and control must be formed and agreed as a mutual independent collaboration'*;
- A Virtual SoS has *'individual independent collaboration with no central management, operation or control of the SoS as a whole'*.

These refined descriptions may continue to align with other research of SoSs [38] [11] [13] [1], and will be used within the future SoS characterisation process for security risk assessment. For example, previous work [18] considered an approach using a candidate SoS to characterise and frame the AMN as an Acknowledged SoS. We continue with this approach originally based on work described by Dahmann and Baldwin [39] drawing comparisons between a system and Acknowledged SoS using systems engineering terminology. As articulated in Figure 2, we modify and expand on this work to consider subtle differences between other SoSs types as a means to classify a given example in a likely SoS environment. This is to assist the initial steps of a SoS security risk assessment approach using a tool-supported framework [40], which is intended to act as a further bridge between operations and engineering environments.

IV. Case Study Example: A MEDEVAC SoS

In previous work with the AMN SoS, we identified a range of services and mission threads vital to its operation. One in particular supported medical evacuation (MEDEVAC) operations that we believe can also be considered a SoS given the joint-force collaboration to provide a MEDEVAC service. Therefore, inspired by operations of that nature, supported by available literature, we implement a reduced-scale exemplar of the typical interconnections of a MEDEVAC SoS. This will be used as a case-study to apply and test a SoS security risk assessment approach in on-going work.

Characterising Systems of Systems					
Types	**Aspect**	**Directed SoS**	**Acknowledged SoS**	**Collaborative SoS**	**Virtual SoS**
SoS Types	**Description**	A Directed SoS can be described as possessing *'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**	• Stakeholders are at system and SoS levels; • Interrelated independent system owners; • Some competing interests and priorities; • May have limited interest in the SoS; • Most stakeholders are likely to be recognised.	• Stakeholders are at system and SoS levels; • Independent system owners; • Competing interests and priorities ; • May have no vested interest in the SoS; • Some stakeholders may not be recognised.	• Stakeholders are at system level mutually collaborating at SoS level; • Independent system owners; • Competing interests and priorities; • May have no vested interest in the SoS; • Some stakeholders may not be recognised.	• Stakeholders are at system and SoS levels; • Independent system owners may not have direct interactive collaboration; • May have no vested interest in the SoS or systems; • Many stakeholders may not be recognised.
	Governance	• Some levels of complexity with central management and funding for both the SoS and interrelated collaboration of systems; • The SoS does have authority over all the systems.	• Added levels of complexity due to designated management and funding for both the SoS and individual systems; • With independent collaboration, the SoS does not have authority over all the systems.	• Further levels of complexity due to the mutual independent collaboration of SoS management with funding only at or from individual system level; • The SoS does not have authority over all the systems.	• Increased levels of complexity and uncertainty due to no central management and funding for the SoS limited to individual system level; • Systems do not have authority over the SoS as a whole.
Operational Environment	**Operational Focus**	• Directed collaboration to meet a set of operational objectives; • Systems' objectives may or may not align with the SoS objectives.	• Designated collaboration to meet a set of operational objectives; • Systems' objectives may or may not align with the SoS objectives.	• Mutually agreed collaboration to meet a set of operational objectives; • Systems' objectives may or may not align with the SoS objectives.	• Individually aligned to meet a set of operational objectives; • Direct and indirect systems objectives may or may not be known or align with the SoS objectives.
Implementation	**Acquisition**	• Complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems; • Stated capability objectives up-front, which may provide basis for requirements; • Benefits from central control to establish and integrate system needs.	• Complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems; • Stated capability objectives up-front, which may provide basis for requirements; • Designated management and independent system needs are established.	• Complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems; • Stated capability objectives up-front, which may provide basis for requirements; • Mutually agreed independent system needs are established.	• Complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems; • Stated capability objectives based on limited needs may be noted up-front, which may provide some basis for requirements; • Individual independent system needs may not establish needs of other systems.
	Test & Evaluation	• Some challenges due to the difficulty of synchronising across multiple systems' life cycles; • Complexity of all the moving parts and potential for unintended consequences.	• More challenging due to the difficulty of synchronising across multiple systems' life cycles; • Complexity of all the moving parts and potential for unintended consequences.	• Complete testing is more challenging due to the difficulty of synchronising across multiple systems' life cycles; • Complexity of all the moving parts and potential for unintended consequences.	• Testing cannot be completed in full and is challenge due to the difficulty of synchronising across multiple systems' life cycles; • Limited access and complexity of all the moving parts and potential for unintended consequences.
Engineering and Design Considerations	**Boundaries & Interfaces**	• Focus is on identifying the independent systems within direct management and control that contribute to the SoS objectives, functionality and data flow.	• Focus is on identifying the independent systems and designated management and control that contribute to the SoS objectives, functionality and data flow.	• Focus is on identifying the independent systems and mutually agreed management and control that contribute to the SoS objectives, functionality and data flow.	• Focus is on identifying the independent systems and expected indirect collaborations and control that contribute to the SoS objectives, functionality and data flow.
	Performance & Behaviour	• Directly managed and monitored at SoS level to satisfy SoS user needs; • Balancing needs of the systems benefits from direct co-ordination.	• Designated management and monitoring at SoS and system levels to satisfy SoS user needs; • Balancing needs of the systems benefits from designated co-ordination.	• Mutually agreed management and monitoring at systems level to satisfy SoS user needs; • Balancing needs of all systems is reliant on mutual co-ordination.	• Direct and indirect management and monitoring at systems level to satisfy SoS user needs; • Balancing needs of the systems and indirect systems may not be achieved.

Fig. 2. SoS Characteristics - extended from work by Dahmann and Baldwin [39]

However, prior to its risk assessment, we must determine the scope of the independent system collaboration and its interdependencies. The main focus is likely to be on identifying where SoS managerial and operational control is in place, if at all. When characterising a SoS with Figure 2, this helps us consider initial questions that may 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?

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. This may be a challenge for some systems or types of SoS where there is a weak collaboration or trust relationships providing limited information.

A. Considering a Joint-Force MEDEVAC as a SoS

In this scenario, the MEDEVAC operation contains three independent system examples that can be loosely attributed to the interaction of NATO operations with two Troop Contributing Nations (TCNs) to perform a continuum of care through medical evacuation. We consider these as Alpha, Bravo, and Charlie, coming together as independent systems collaborating to achieve higher purpose.

To illustrate this interaction, consider a call raised for a MEDEVAC, initiated by Bravo using a *9-Line request*; this is a template for the basic information needed for a medical evacuation. Once received by a Tactical Operations Centre (TOC) Officer, this is processed with the Patient Evacuation Co-ordination Cell (PECC) who together initiate MEDEVAC. The initial mission goal is to transport a patient to a Forward Surgical Team (FST) within one hour – *The Golden Hour* – from the Point of Injury (PoI). A first-stage Forward Air MEDEVAC is called to transfer in-field casualties to a suitable Forward Operating Base (FOB) FST. A Patient Movement Request (PMR) is used for Tactical Air MEDEVAC patient transfer from the FST to a next stage HQ hospital. Strategic Air MEDEVAC is 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 [41] [42].

B. Characterising MEDEVAC as a SoS

MEDEVAC Management and Oversight

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

Governance: Governance is provided by Alpha, with support of 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 [41] [42].

MEDEVAC Operational Environment

Operational Focus: In this scenario, Bravo has a limited role, but is the initiator of the process. A Bravo Field Unit's Medic provides in-field medical care, requesting the MEDEVAC and documents care given, creating a chain of patient information. Trust mechanisms are likely to be in place, supported by technical measures to ensure this data flow is maintained. Charlie has a greater role and depends upon more than one system to achieve its mission, each individually operated to fulfil the process, further managing patient care and documentation stored in Alpha's shared data repository. Bravo and Charlie, therefore, each retain a level of autonomy with some competing interests. However, operations are driven by Alpha command levels and the MEDEVAC operation, specifically through the PECC. Mission needs are guided by a Common Operational Picture (COP) of tactical and medical Situational Awareness (SA) to achieve its mission safely and securely [41] [42] [43].

MEDEVAC Implementation

Acquisition: Some system and security requirements may be mandated by Alpha for participation, however, Bravo and Charlie would be responsible for capturing these needs within their differing requirements to ensure interoperability. Alpha provides an 'as is' set up 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. 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. Bravo use in-field handsets with AHLTA-Mobile, whereas Charlie use Laptops with AHLTA-Theater 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 [43].

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

MEDEVAC Engineering and Design Considerations

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

Performance & Behaviour: Alpha continue to provide command and control with SA provided to all throughout the continuum of care. This allows for on-going feedback to improve their own capabilities, whilst providing input for independent systems to align and balance SoS needs against system demands. Performance may also be monitored at casualty level, with reduction of issues and rates of survival from critical golden hour care and transportation [41].

V. Discussion

A. MEDEVAC as a SoS

As the MEDEVAC scenario is loosely based around a NATO Joint-Force operation acting as one force, early assumptions could indicate some alignment with a Directed SoS description. Despite Alpha mandating standard operating agreements (STANAGS), each independent system operates with its own autonomy. For example, Alpha has no direct link to Charlie Air Corp, who have operational and managerial control of Air MEDEVAC. However, Alpha, Bravo, and Charlie are reliant on each other to fulfil the coming together, which could perhaps lean towards a Collaborative SoS. From the review, it is, however, evident the MEDEVAC would be considered an Acknowledged SoS given its high-level distinction of designated management by Alpha, with limited control over the independent collaboration of Bravo and Charlie.

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 [43]. 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 [44].

Additional considerations such as these may only become apparent once systems information has been gathered and assessed. By following the steps illustrated, this provides a simple process for a SoS level stakeholder to identify specific characteristics of an inter-connected systems environment, and potentially classify it as a SoS based on this output, clarifying where managerial and operational independence and control are in place. This in-turn directs future assessment of areas of dependency and complexity, or specific areas of risk.

Although we have demonstrated the ease in which questions may be applied to a potential SoS scenario using the refined descriptions, answers may differ when considering from whose view the SoS is being assessed. We have provided a general overview of the MEDEVAC SoS as a whole. However, this may be closer to Alpha's view, whereas, the view of Bravo may be minimal given the limited interaction it has with many Alpha or Charlie sub-systems.

B. Assessing SoS Security Risk

The MEDEVAC example demonstrates some key challenges to SoS environments where interoperability is vital to the SoS success, yet it is not always possible to have visibility or direct knowledge and interaction with all systems. When relating this to data flow and information security, potential risks may be overlooked. A system may also have visibility of another system, but have limited knowledge in which to base a security risk assessment. It is, therefore, critical to identify the main context of a given SoS and its characteristics, identifying relevant independent systems and stakeholders in a top-down manner, decomposed into its systems, before being able to appreciate the complexity and input from the bottom up.

The proposed baseline understanding of SoSs helps set the likely type of SoS, its characteristics, management and control boundaries. However, there are other considerations to account for when assessing security risk in SoS, certainly when considering the development life-cycle of the SoS and constituent systems, and the supply chain throughout. Boundaries also cross many domains, such as land, sea, air, space and cyber, networks, the physical or electronic realms, cultural, organisational or geographical and environmental, all of which may be constrained by changing trust equations, legal and regulatory requirements. This places a greater reliance on requirements engineering to reduce system and SoS risk. As a result, the SoS would benefit from consistent approaches to risk from operations to requirements, helping to reduce gaps where risks may otherwise evolve or be unaccounted for within differing areas and contexts of engineering or indeed at an individual or organisational level.

VI. Conclusion

In this paper, we considered the diversity of small and large-scale SoS examples in the present day, each in a different context. Our research has identified confusion exists for multi-level stakeholders when defining and classifying interconnected systems as a SoS. For example, SoSs range from being a single person interacting with systems, to large or national scale organisational collaborations. Individually, these may have quite different standards and policies in place, if at all, to achieve its independent purpose in addition to its SoS function. An IoT as a SoS may be managed and operated at a single user level integrating with other systems. Whereas, an organisational SoS is likely governed by legal or regulatory requirements, meeting these through policy and procedures.

Identifying the level of managerial and operational independence, control and governance required for the SoS interconnectivity is important to achieve its new or higher purpose. To address this and aid multi-stakeholder communication and understanding, this paper has provided a simple repeatable process and questions, using a baseline approach as a prerequisite to address important initial considerations supporting a SoS security risk assessment approach. This process was applied to an example MEDEVAC case-study, where information from these questions helped to characterise and define the SoS collaboration, its context and environment. For example, where the SoS has a dependency on secure and interoperable systems to fulfil its SoS mission goals.

These needs should be addressed early in the development life-cycle. The scale and complexity of interacting systems towards integration and operational challenges must be accounted for, as detailed as possible considering all needs and requirements to satisfy stakeholder and SoS mission needs. This should assist continual monitoring and assessment at an operational level to meet stakeholder needs, security, interoperability, or vital situational awareness supporting resilience and risk reduction. Modelling, engineering and operating SoSs is therefore a challenge for engineering, security and human factors communities, where gaps were identified lacking in formal approaches applied in a SoS security and risk context.

Our current and future work will continue to address these areas to test and validate a security risk assessment approach for SoSs using a tool-supported framework. Current work, for example, integrates a modified OCTAVE Allegro risk approach [45] integrated with the use of CAIRIS [40] for modelling and visualisation of security risk in the MEDEVAC SoS, whilst demonstrating the benefits of model-driven approaches for SoSs. The challenge however remains, identifying the minimum level of information in which a SoS assessment can be based on from its varied relationships and interconnections.

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

[1] I. Sommerville, *Software Engineering*, 10th ed. Pearson, 2015.

[2] 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*, 1st ed., Washington, DC: ODUSD(A&T)SSE, 2008, 2008.

[3] R. Staker, "Decision support for complex systems-of-systems," in *Proceedings of the 16th National Conference of the Australian Society for Operations Research*. Citeseer, 2001.

[4] J. Boardman and B. Sauser, "System of Systems-the meaning of of," in *2006 IEEE/SMC International Conference on System of Systems Engineering*. IEEE, 2006, p. 6.

[5] Director of Systems Engineering, *Systems Engineering Guide for Systems of Systems: Summary*, Department of Defense, Office of the Director, Defense Research and Engineering, Washington, D.C., Dec. 2010.

[6] K. Baldwin, J. Dahmann, and J. Goodnight, "Systems of Systems and Security: A Defense Perspective," *Insight*, vol. 14, no. 2, pp. 11–14, 2011.

[7] J. A. Lane and D. Epstein, "What is a System of Systems and why should I care?" *University of Southern California*, 2013.

[8] V. Chiprianov, L. Gallon, M. Munier, P. Aniorte, and V. Lalanne, "Challenges in Security Engineering of Systems-of-Systems," in *Troisième Conférence en IngénieriE du Logiciel*, 2014, p. 143.

[9] M. Jamshidi, *System of systems engineering: innovations for the twenty-first century*. John Wiley & Sons, 2011, vol. 58.

[10] C. Harvey and N. A. Stanton, "Safety in System-of-Systems: ten key challenges," *Safety science*, vol. 70, pp. 358–366, 2014.

[11] M. W. Maier, "Architecting principles for systems-of-systems," in *INCOSE International Symposium*, vol. 6, no. 1. Wiley Online Library, 1996, pp. 565–573.

[12] G. B. Dyson, *Darwin among the machines: The evolution of global intelligence*. Basic Books, 2012.

[13] J. S. Dahmann and K. J. Baldwin, "Understanding the current state of US defense systems of systems and the implications for systems engineering," in *Systems Conference, 2008 2nd Annual IEEE*. IEEE, 2008, pp. 1–7.

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

[15] H. Dogan, S. A. Pilfold, and M. Henshaw, "The role of Human Factors in addressing Systems of Systems complexity," in *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1244–1249.

[16] Homeland Security, "The System of Systems Approach for Interoperable Communications [online]," 2017, Available From: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2458&file=SOSA pproachforInteroperableCommunications_02.pdf [Accessed 4 October 2017].

[17] I. Sommerville, D. Cliff, R. Calinescu, J. Keen, T. Kelly, M. Kwiatkowska, J. Mcdermid, and R. Paige, "Large-scale complex IT systems," *Communications of the ACM*, vol. 55, no. 7, pp. 71–77, 2012.

[18] D. Ki-Aries, S. Faily, H. Dogan, and C. Williams, "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, May 2017.

[19] D. Ki-Aries, H. Dogan, S. Faily, P. Whittington, and C. Williams, "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, 2017, pp. 83–89.

[20] P. Maia, E. Cavalcante, P. Gomes, T. Batista, F. C. Delicato, and P. F. Pires, "On the Development of Systems-of-Systems Based on the Internet of Things: A Systematic Mapping," in *Proceedings of the 2014 European Conference on Software Architecture Workshops*, ser. ECSAW '14. ACM, 2014, pp. 23:1–23:8.

[21] F. Alkhabbas, R. Spalazzese, and P. Davidsson, "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, 2016.

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

[23] P. Whittington and H. Dogan, "SmartPowerchair: Characterization and Usability of a Pervasive System of Systems," *IEEE Transactions on Human-Machine Systems*, 2016.

[24] C. B. Nielsen, P. G. Larsen, J. Fitzgerald, J. Woodcock, and J. Peleska, "Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions," *ACM Comput. Surv.*, vol. 48, no. 2, pp. 18:1–18:41, Sep. 2015.

[25] M. Branagan, R. Dawson, and D. Longley, "Security Risk Analysis for Complex Systems." in *ISSA*, 2006, pp. 1–12.

[26] D. H. McKnight and N. L. Chervany, "The meanings of trust," 1996.

[27] D. E. Zand, "Trust and managerial problem solving," *Administrative science quarterly*, pp. 229–239, 1972.

[28] S. C. Currall and T. A. Judge, "Measuring trust between organizational boundary role persons," *Organizational behavior and Human Decision processes*, vol. 64, no. 2, pp. 151–170, 1995.

[29] C. Richardson, "Bridging the air gap: an information assurance perspective," Ph.D. dissertation, University of Southampton, 2012.

[30] J. Dahmann, K. J. Baldwin, and G. Rebovich, "Systems of systems and net-centric enterprise systems," in *7th Annual Conference on Systems Engineering Research*, 2009.

[31] D. G. Firesmith, "Analyzing and specifying reusable security requirements," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep., 2003.

[32] G. Rebovich Jr. and M. Authors, *MITRE Systems Engineering Guide [online]*. MITRE Corporation, 2014, available From: https://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf [Accessed 10 October 2016].

[33] I. Böröcz, "Risk to the Right to the Protection of Personal Data," *European Data Protection Law Review*, vol. 2, no. 4, pp. 467–480, 2016.

[34] A. Jones, "A framework for the management of information security risks," *BT technology journal*, vol. 25, no. 1, pp. 30–36, 2007.

[35] R. L. Ackoff, "Towards a system of systems concepts," *Management science*, vol. 17, no. 11, pp. 661–671, 1971.

[36] M. C. Jackson and P. Keys, "Towards a system of systems methodologies," *Journal of the operational research society*, pp. 473–486, 1984.

[37] D. Ki-Aries and S. Faily, "Persona-Centred Information Security Awareness," *Computers & Security*, vol. 70, pp. 663–674, 2017.

[38] P. Boxer and S. Garcia, "Limits to the use of the zachman framework in developing and evolving architectures for complex systems of systems," CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, Tech. Rep., 2009.

[39] J. S. Dahmann, G. Rebovich Jr, and J. A. Lane, "Systems Engineering for Capabilities," DTIC Document, Tech. Rep., 2008.

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

[41] Col. Dr. I. Hartenstein, "Medical Evacuation in Afghanistan: Lessons Identified Lessons Learned [online]," Tech. Rep., 2008, available From: https://stopthemedevacmadness.files.wordpress.com/2012/02/nato-medical-evacuation-in-afghanistan-mp-hfm-157-05.pdf[Accessed 19 January 2018].

[42] Col. Dr. I. Hartenstein, "Medical Evacuation Policies in NATO: Allied Joint Doctrine for Medical Evacuation [online]," Tech. Rep., 2008, available From: https://stopthemedevacmadness.files.wordpress.com/2012/02/nato-medical-evacuation-policies-in-nato-mp-hfm-157-01.pdf [Accessed 19 January 2018].

[43] M. J. Meier, "A providers perspective: Utilizing deployed information technology to care for our wounded warriors," The Joint Staff, J4/HSSD. presented at the 2011 Military Health System Conference, January 24-27, National Harbor, Maryland: The Defense Technical Information Center, 2011, available From: http://www.dtic.mil/dtic/tr/fulltext/u2/a556202.pdf [Accessed 19 January 2018].

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

[45] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the information security risk assessment process," DTIC Document, Tech. Rep., 2007.