From Requirements to Operation: Components for Risk Assessment in a Pervasive System of Systems

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

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

***Abstract*—Framing Internet of Things (IoT) applications as a System of Systems (SoS) can help us make sense of complexity associated with interoperability and emergence. However, assessing the risk of SoSs is a challenge due to the independence of component systems, and their differing degrees of control and emergence. This paper presents three components for SoS risk assessment that integrate with existing risk assessment approaches: Human System Integration (HSI), Interoperability identification and analysis, and Emergent behaviour evaluation and control measures. We demonstrate the application of these components by assessing a pervasive SoS: a *SmartPowerchair*.**

***Index Terms*—System of Systems, System of Systems Engineering, Security, Risk Assessment, Human System Integration, Interoperability, Emergence, Pervasive Technologies, Assistive Technologies, Internet of Things.**

I. Introduction

To build an Internet of Things (IoT) application, one needs to select and integrate multiple hardware and software components. This includes, sensors, communications modules, and networks, integrated with core systems while applying changes to process and people interaction with technology [1]. For example, smart city sensors monitoring air quality or traffic. However, interoperability and emergence are such intrinsic properties of IoT applications that the classic notion of a *system* is inadequate for dealing with system complexity, and tackling security problems. In recent years, there has been some interest in framing IoT systems as *Systems-of-systems* [2]. A System of Systems (SoS) is an integration of independent and operable constituent systems, networked together to achieve a higher goal [3]. While the notion of SoS can help manage design complexity, there is little work providing guidance for what designing for SoS security entails. Moreover, although some literature exists considering SoS challenges to risk management, there has been little work focusing on risk assessment and security in SoSs.

Risk, the effect of uncertainty on objectives [4], is a key concept in security requirements engineering. Requirements specified need to reflect a system's expected behaviour in the presence of risk. These requirements need to be verified and validated to ensure specified behaviour is in line with stakeholder expectations. Unfortunately, risk assessment can be a challenge in a SoS, where operational and managerial independence exists, with differing degrees of centralised control, and constraints on geographical, environmental, evolutionary, and emergent behaviour adding to SoS complexities. Human interaction and culture can also create obstacles to, or opportunities for interoperability [5].

To understand the interplay between risk assessment and socio-technical SoSs, this paper presents SoS centred components for risk assessment. These are evaluated in a security context, the output of which is intended to inform requirements engineering through to operations. We evaluate these components by considering security risks to an assistive technology *SmartPowerchair* pervasive SoS case study. This was elicited and modelled using the Computer Aided Integration of Requirements and Information Security (CAIRIS) tool [6]. CAIRIS can assist when modelling the socio-technical interaction of the SoS and provides a current view on risks and associated assets, roles, goals, tasks, and other security and usability concepts. The *SmartPowerchair* is a standard powered wheelchair (Powerchair) integrated with existing pervasive technologies. This is comprised of different systems, components, interactions and functions [7] [8], with the aim of enabling independent living, improving quality of life for people with reduced physical abilities.

We introduce the SoS concept in Section II and provide an overview of risk assessment in Section III, presenting our proposed SoS components for risk assessment in Section IV. We then apply our approach to the *SmartPowerchair* case study in Section V, and conclude by discussing findings and implications from our approach and detail directions for future work in Sections VI and VII respectively.

II. System of Systems Concept

Systems Engineering has undergone major changes to extend itself beyond a single system framework towards a class of complex systems whose constituents are themselves complex [3]. A SoS is the concept of the coming together of these complex systems to collectively obtain higher capabilities and performance. The emerging field of System of Systems Engineering (SoSE) requires continued growth in understanding of the discipline [9]. Capability suppliers must integrate many new technical and organisational systems with older legacy systems, within and beyond their own organisational boundary [10].

A SoS exists when there is a majority presence of five characteristics: operational independence, managerial indepen-

dence, 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]. An important element of SoS is Interoperability: the ability of two or more systems or elements to use and exchange information [13]. Given the SoS has a dependency on interoperable systems to fulfil its SoS mission goals, this challenge needs to be addressed early in the development life-cycle considering the scale, complexity and integration challenges, and must be monitored and assessed at an operational level.

As described by [5], a SoS can generally be categorised as one of four types:

Directed SoSs: These are built and managed to fulfil specific purposes; they are centrally managed during long-term operation to continue to fulfil and evolve those purposes. Component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose [11].

Acknowledged SoSs: These have recognised objectives, a designated manager, and resources for the SoS, but constituent systems retain their independent ownership, objectives, funding, as well as development and sustainment approaches. Changes to systems are based on collaboration between the SoS and systems [9].

Collaborative SoSs: These are distinct from Directed SoSs in that the central management organisation does not have coercive power to run the system. The component systems must, more or less, voluntarily collaborate to fulfil the agreed upon central purposes [11].

Virtual SoSs: These lack both central management authority and centrally agreed upon purposes, may exist deliberately or accidentally, and large-scale behaviour emerges, which may be desirable [11]. Participants informally collaborate and manage their own systems to maintain the system as a whole [14].

All SoSs are collaborative in different ways. An important aspect for operations and engineering is to understand and identify characteristics at a system-element level [15], and the relationship and concurrent behaviour amongst systems to understand the SoS as a whole. This is easier in Directed SoSs, but the challenge becomes greater as central management, access and control of constituent systems is reduced in Acknowledged, Collaborative and Virtual SoSs. Consequently, classic approaches for security, risk assessment, human factors, requirements and systems engineering need to evolve to cope with challenges posed by different SoS characteristics [10] [16].

III. Risk Assessment

The goal of any risk assessment is to determine whether a system is acceptable and which measures would provide its acceptability [17]. Risk can be calculated using the formula: Level of Risk (R) = Risk Likelihood (L) $\times$ Risk Impact (I). This is a widely recognised approach applied in a number of risk assessment frameworks, methodologies and standards.

Managing risk in a SoS depends on its type and complexity, and considers a range of risk-based contexts including business, project, technical, safety and security risk. An organisational based SoS is likely to be governed by legal or regulatory requirements meeting certain standards through policy and procedures. An IoT as a SoS may, however, be managed and operated at a single user level integrating with other systems. 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 requirements to operations when addressing the SoS mission needs and goals.

Attending to risk in an engineering context might draw ideas from Systems [18] [19] and SoS [20] engineering guides, security and requirements engineering approaches [21] [22] or a range of other context-specific engineering and operational approaches. At a basic organisational level, Cyber Essentials [23] may be considered, whereas at a higher level of security standards for controls, the most common are the Generally Accepted Principles and Practices for Securing Information Technology Systems [24], and from the ISO 27001+ [25] and NIST Special Publication 800 [26] families, with supporting risk management approaches [27] [4] [28]. Other methodologies such as ISRAM [29] or Octave [30] [31] may also be integrated. Working with this myriad of approaches becomes a challenge where different systems or stages of the development life-cycle use differing approaches to achieve the same goal. Some of these are focused on a single system or organisation context, and scale poorly given SoS collaboration complexity

Despite various definitions and sub-steps associated with risk management, the literature concedes that risk assessment entails three key processes:

- *Risk Identification* develops an in-depth understanding of the system structure and assets. To identify the risks present within the SoS environment, it then identifies threat-sources and vulnerable system elements, controls and potential consequences.
- *Risk Analysis* determines the likelihood and severity of consequences from identified risks impacting on the system element, individual systems and SoS.
- *Risk Evaluation* considers the risk criteria and context, controls and regulatory requirements to make risk-based decisions for future operation. High or unacceptable risks identified are prioritised with potential risk reduction controls considered ahead of risk treatment [4].

Before any risk assessment begins, the context of use, mission goals, boundaries, relevant stakeholders, scope, and risk criteria should be considered.

IV. SoS Components for Risk Assessment

During each of the aforementioned three processes, key SoS components critical to SoS success should be considered. Given the socio-technical nature of a SoS and pervasive technologies, close attention should be paid to human profiles and their relationship with the SoS. Interoperability across different SoS types, constituent systems and components can

also impact aspects of the system influencing risk analysis. Given the unpredictable nature of emergence, it is difficult to capture risks centred on emergent behaviour of SoSs using existing risk assessment approaches. Consequently, we propose considering three components to assist in SoS risk assessment that overlay through identification, analysis and evaluation steps, and have the potential to be utilised alongside existing security and risk approaches, e.g. ISO 27005 [4].

A. Human System Integration Analysis

The first component entails analysing human characteristics involved within the SoS. Human System Integration (HSI) analysis focuses on roles, responsibilities and relationships of manpower and personnel, ownership, stakeholder interaction, training, safety and other factors [32]. HSI is completed at an operational level, or included in requirements engineering and throughout the development life-cycle into operations. Its output and considerations can inform socio-technical aspects that we apply towards security and risk. Engineers or risk managers may adopt a user-centred approach, assisting HSI considerations towards risk identification and analysis, while incorporating evaluation and controls suitable to the SoS and its users. During this stage, we also introduce abstraction stacks [15] for system decomposition, and tool support [33] for eliciting and modelling the SoS.

B. Interoperability Analysis

The second component considers the interoperability impact within the SoS using a qualitative assessment based upon the expertise of system engineers or risk assessors. The impact on SoS goals must be assessed against each risk identified, although not all risks will necessarily have an impact on SoS level interoperability. All details should be taken into consideration with results appropriately documented for further evaluation. Interoperability should be considered during identification, then within analysis to determine system impacts on the SoS.

C. Emergent Behaviour Analysis

Based on analysis, evaluation will consider potential emergent behaviour and relevant countermeasures. Some systems may be used in different contexts due to evolutionary changes, or the emergent behaviour of the users and systems; this may affect the utility of the SoS as a whole. Therefore, the third component incorporates an analysis of emergent behaviour into the evaluation for planning of additional control measures to bring risk to an acceptable level, and be monitored for future feedback of emergent activity.

V. SoS Case Study and Approach

A. SmartPowerchair as a System of Systems

The *SmartPowerchair* is a standard powerchair integrated with existing pervasive technologies consisting of different systems, components, interactions and functions. This is supported by SmartATRS using a Smartphone system to control an Automated Transport and Retrieval System (ATRS) [8]. ATRS is a technically advanced system using robotics technology with Light Detection and Ranging (LIDAR) to autonomously dock a powered wheelchair (Powerchair) onto a platform lift fitted in the rear of a standard Multi-Purpose Vehicle (MPV) system while a disabled driver is seated in the driver's automated Freedom seat.

SmartPowerchair integrates various system components with the Powerchair to meet overall requirements for the SoS as illustrated in Figure 1. For example, the GoVue application is installed on the Smartphone to facilitate use of a rear view camera attached to assist with manoeuvring. SmartATRS is a key system in this SoS supporting interaction between the MPV and the Powerchair systems. SmartATRS improves usability of ATRS keyfobs and hand-held pendants by providing a Smartphone application to control the interaction between the MPV and Powerchair systems.

Integrated into the MPV system is a web server and relay board interfacing between SmartATRS and ATRS components (seat, lift and tailgate). The web server relay connects through Ethernet to a Wi-Fi router that transmits over secure Wi-Fi Protected Access II (WPA2) network. Smartphones or other Wi-Fi enabled devices interact with a GUI by entering the URL or bookmark into a browser. SmartATRS sends commands wirelessly to the relay board, executed by JavaScript. The iPortal system operates via Bluetooth, providing an alternative to the touchscreen interface using Powerchair joystick interaction with the Smartphone and SmartATRS GUI, using left or right for screen navigation and forwards for selection.

The Smartphone is the primary enabling system for control and communication with the user through the interface, Powerchair and joystick controller to receive commands. Other technologies integrated with SmartATRS providing alternative interaction mediums are Head Tracking and Smartglasses. The complexity and number of interactions illustrated in the SmartPowerchair diagram in Figure 1 re-emphasises the importance of identifying SoS risks centred on human and system integration, interoperability and emergent behaviour.

B. HSI, Eliciting and Modelling the SmartPowerchair SoS

Previous work from the SmartATRS project [7] [8] carried out extensive work towards improving usability and interaction. Building on this previous work, we applied the HSI approach by gaining input, clarification and validation from a Powerchair user. We then decomposed the SmartPowerchair SoS using the abstraction stack approach introduced by Simpson and Dagli [15]. For example, starting from its highest level, an abstraction stack of a House is composed of Rooms that consists of floors and walls, which in turn is made up from bricks and mortar. For SoSE, this approach can be used to determine then model and represent individual assets and system elements, understanding their position and relevance in the SoS. We then re-modelled the user interaction with the SoS, as illustrated in Figure 1. Creating this visual model was an important step towards understanding the SoS elements and its interconnections, providing a means of recomposing the system's assets into a SoS model.

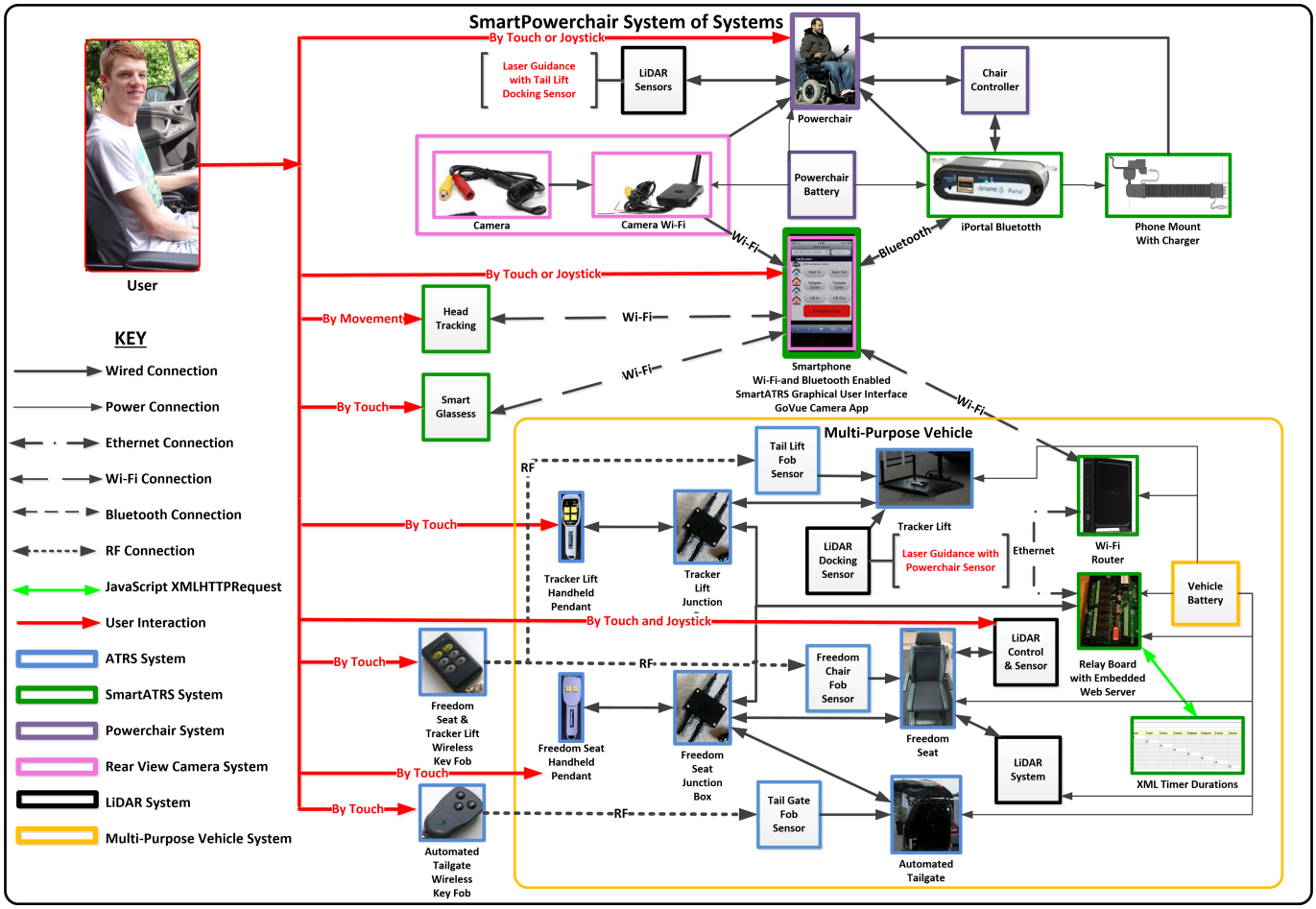

Fig. 1. SmartPowerchair System of Systems Architecture

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

C. HSI, Risk Identification and Analysis

Each system element was entered into CAIRIS as an individual asset. Assets were visualised using CAIRIS asset models illustrated by Figure 2. These models, which are based on UML class diagrams, represent abstraction stacks using composition associations between individual components, systems and the Directed SoS as a whole. Based on the "internet threat model" described in RFC 3552 [34], threats and vulnerabilities carried out by a possible attacker role were added and associated to each system asset while considering their impact on security goals. Availability was considered the primary security goal for this SoS, with Integrity of data processed, stored or transmitted also of value. Although Confidentiality of assets was valued, some trade-offs were considered necessary.

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

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

A version of the GoVue application may also be downloaded from one of many unofficial sources listed on a search engine.

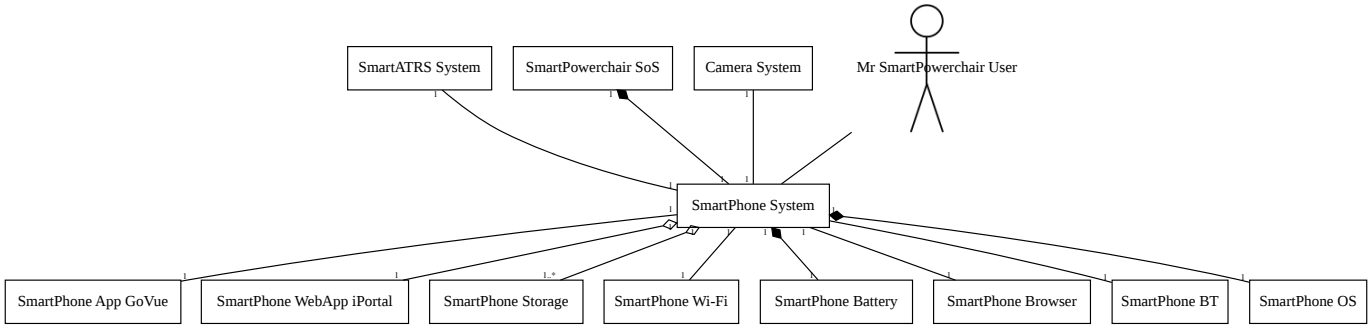

Fig. 2. CAIRIS Asset Model - Smartphone System and relations

We found that the user does not currently consider the risks to security and interoperability of doing this.

D. HSI, Risk Analysis and Interoperability Impact

Despite the Camera system not appearing to demonstrate significant risks or impact on interoperability, it did highlight a specific attack vector due to consistent interactions and dependencies on most systems of the SmartPowerchair SoS. If the Smartphone was compromised in some way, this would have a significant impact on security risks, availability and interoperability at a SoS level.

It is not uncommon for Smartphones to be integrated as a key system in IoT and SoS scenarios, despite the known impact this might have to IoT security [35]. This may contribute to the loss of SoS availability and interoperability if the device or operating system is compromised. Privacy could also be compromised if data theft or location tracking malware is inadvertently installed [36].

An example from our risk assessment findings incorporating the HSI approach, along with interoperability and emergence analysis is shown in Figure 3. For interoperability, this specifically demonstrated where the system asset was at risk of interconnection issues with a majority of the SoS, thus losing the ability to control it.

E. HSI and Evaluation of Emergent Behaviour

SoS interconnections and controls may uncover unexpected emergent behaviour, the consequences of which could increase risk if the SoS mission and security goals are not met. HSI considerations were therefore employed when applying controls and measures to reduce issues arising from emergent behaviour. Emergent behaviour was, however, harder to anticipate due to its unknown and uncertain nature. Feedback included in the evaluation considered a previous operating system update offering enhancements to its security and functionality, but this no longer supported voice interaction functions previously used and tested. We consider other updates by the operating system or application providers outside the SoS boundary, so these may have unexpected consequences.

VI. Discussion

To assist with SoS risk assessment of security in the *SmartPowerchair*, our approach introduced relevant SoS components addressing HSI, interoperability and emergent behaviour that may inform requirements engineering for operational needs. HSI was important towards understanding security concerns of human interaction, and interoperability analysis was found to be significant when determining the overall risk impact level. This approach can be used in requirements engineering through to operations when used with existing repeatable risk approaches. Risk assessment must, however, be based upon informed knowledge of the SoS context, constituent systems and components to ensure key stakeholders, user and system interactions are considered throughout the process.

A. Applying HSI with CAIRIS

Modelling the SoS first using abstraction stacks to decompose the elements of the SoS helped develop a visual representation of the system structure, interconnections and user interaction within the SoS shown in Figure 1. Each of the systems and components were modelled in CAIRIS as assets associated with other relevant system assets composing the SoS. The asset models illustrated in Figure 2 were useful for reviewing and visualising assets and their relations with stakeholders. This indicated how they could be subsequently linked to threats, modelling the related risks specific to the human and system interactions. The asset models were also useful when validating the decomposed elements with stakeholders, as the models helped identify missing systems, components or interrelations.

CAIRIS offered useful tool support for modelling and visualising a Directed SoS with parent-child relationships. It was, however, unclear how this clarity might be achieved with other types of SoS given their differences and reduction in centralised access and control. Additionally, CAIRIS was useful for visualising the SoS assets and modelling its risks. However, CAIRIS does not incorporate any means for evaluating the SoS level impact on interoperability or emergence. Therefore, the assessment reverted to a commonly used spreadsheet for documenting the steps taken. Further analysis and application to case studies in other domains will be useful for validating the effectiveness of CAIRIS as tool support for eliciting and modelling a range of SoSs.

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

Fig. 3. Risk Overview with Interoperability and Emergence analysis

B. Interoperability Analysis

Interoperability impact at SoS level was considered against each potential risk, as demonstrated in Figure 3, providing further consideration towards dependencies and required control measures. For example, if the camera system was no longer interoperable, the SoS would continue to function. However, if the Smartphone system cannot communicate with other constituent systems, the entire SoS ceases to function. Therefore, understanding the impact on interoperability could be critical to achieving its SoS goals.

One option of incorporating interoperability is considering the role of other system models to review its impact. For example, Faily & Fléchais [37] illustrate how Goal-oriented Requirement Language (GRL) models were generated from other models in CAIRIS. The GRL models then identified insights that had previously been missed. GRL could be equally effective when considering interoperability in SoSs to examine the impact of changing system assets, goals, or user processes.

C. Controls and Emergent Behaviour

In a more general context, controls may include data loss prevention and remote wiping tools, certainly where physical theft of the device is a potential risk. Policy, process and security awareness towards permitted usage are other tools that may be incorporated.

However, in our case study example, the SoS is managed and controlled by a single IoT user, which highlights a need to consider security for the user at design stage. This also raises the challenge of introducing basic steps and security awareness for IoT users, particularly when the interoperability of the smartphone becomes a critical element of the SoS success or failure. Suitable control measures and mitigations also need to consider possible outcomes of steps taken for SoS resilience given the emergent behaviour associated with identified risks.

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

In the example described in Figure 3, reviewing future operating system or application updates may be considered. However, updates from third-parties beyond SoS control may be required to ultimately improve system performance and security. This means trade-offs may exist to maintain safety and security in the SoS. Interoperability and emergent behaviour is, however, relatively complex, and requires further analysis and application to other case study domains to understand challenges posed by different SoS types.

VII. Conclusion

In this paper, we presented three components for SoS risk assessment incorporating HSI, interoperability impact analysis, and emergent behaviour evaluation with control measures. We introduced abstraction stacks as a means of decomposing systems, and used CAIRIS for initial risk modelling of security and socio-technical aspects of the SoS. Although the proposed components represent preliminary work, evaluating them provided a holistic view of the SoS from which threat-sources and vulnerabilities to security could be identified. This demonstrated the potential for identifying unacceptable human interactions, interoperability issues and emergent behaviour, thereby allowing appropriate measures to be adopted. This can improve the security and safety of people with reduced physical abilities interacting with assistive technologies.

Future work will conduct further analysis with the *Smart-Powerchair* and other case study domains using CAIRIS for eliciting and modelling a range of SoSs. This aims to identify gaps and opportunities for SoS risk assessment and security.

Acknowledgement

The research described in this paper was funded by Bournemouth University studentship DSTLX1000104780R_BOURNEMOUTH_PhD_RASOS.

REFERENCES

[1] M. Bartolomeo, "Internet of things: Science fiction or business fact," *A Harvard Business Review Analytic Services Report, Tech. Rep*, 2014.

[2] 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.

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

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

[5] 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.

[6] S. Faily and C. Iacob, "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*, ser. ESPRE 2017. IEEE, 2017, to Appear.

[7] P. Whittington and H. Dogan, "Smartpowerchair: A pervasive system of systems," in *System of Systems Engineering Conference (SoSE), 2015 10th*. IEEE, 2015, pp. 244–249.

[8] P. Whittington, H. Dogan, and K. Phalp, "Smartpowerchair: to boldly go where a powerchair has not gone before," in *in Proc. Proceedings of the International Conference on Ergonomics & Human Factors 2015*, 2015, pp. 233–240.

[9] 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.

[10] 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.

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

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

[15] J. J. Simpson and C. H. Dagli, "System of systems: Power and paradox," in *System of Systems Engineering, 2008. SoSE'08. IEEE International Conference on*. IEEE, 2008, pp. 1–5.

[16] C. Ncube, S. L. Lim, and H. Dogan, "Identifying top challenges for international research on requirements engineering for systems of systems engineering," in *Requirements Engineering Conference (RE), 2013 21st IEEE International*. IEEE, 2013, pp. 342–344.

[17] B. Nikolić and L. Ružić-Dimitrijević, "Risk assessment of information technology systems," *Issues in Informing Science and Information Technology*, vol. 6, pp. 595–615, 2009.

[18] International Council of Systems Engineering (INCOSE), *Systems Engineering Handbook*, version 3.1 ed., INCOSE, Aug. 2007.

[19] ISO/IEC, "ISO/IEC 16085, Systems and software engineering — Lifecycle processes — Risk management," 2006.

[20] 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. [Online]. Available: http://www.acq.osd.mil/se/docs/SoS-Summary-PRINT.Format-Duplex.FlipUp.pdf

[21] J. Dahmann, G. Rebovich, M. McEvilley, and G. Turner, "Security engineering in a system of systems environment," in *Systems Conference (SysCon), 2013 IEEE International*. IEEE, 2013, pp. 364–369.

[22] R. Ross, M. McEvilley, and J. C. Oren, "Systems security engineering," *NIST Special Publication*, vol. 800, p. 33, 2016.

[23] Gov.UK, "Cyber essentials scheme: overview." Department for Business, Energy & Industrial Strategy, Gov UK, 2015. [Online]. Available: https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

[24] M. Swanson and B. Guttman, "Sp 800-14. generally accepted principles and practices for securing information technology systems," 1996.

[25] British Standards Institution, "BS ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements [Electronic version]," 2013.

[26] NIST, "Nist special publications," NIST Computer Security Resource Centre, 2017. [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html

[27] ISO, ISO31000, "31000: 2009 risk management–principles and guidelines," *International Organization for Standardization, Geneva, Switzerland*, 2009.

[28] G. Stoneburner, A. Y. Goguen, and A. Feringa, "Sp 800-30. risk management guide for information technology systems," 2002.

[29] B. Karabacak and I. Sogukpinar, "Isram: information security risk analysis method," *Computers & Security*, vol. 24, no. 2, pp. 147–159, 2005.

[30] The CERT Division, "Octave," Carnegie Mellon University, 2017. [Online]. Available: http://www.cert.org/resilience/products-services/octave/

[31] 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.

[32] N. R. Council *et al.*, *Human-system integration in the system development process: A new look*. National Academies Press, 2007.

[33] S. Faily, "CAIRIS web site," http://cairis.org, June 2017.

[34] E. Rescorla and B. Korver, "Guidelines for writing rfc text on security considerations," Tech. Rep., 2003.

[35] M. H. Khan and M. A. Shah, "Survey on security threats of smartphones in internet of things," in *Automation and Computing (ICAC), 2016 22nd International Conference on*. IEEE, 2016, pp. 560–566.

[36] A. Mylonas, S. Dritsas, B. Tsoumas, and D. Gritzalis, "Smartphone security evaluation the malware attack case," in *Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on*. IEEE, 2011, pp. 25–36.

[37] S. Faily and I. Fléchais, "Eliciting and Visualising Trust Expectations using Persona Trust Characteristics and Goal Models," in *Proceedings of the 6th International Workshop on Social Software Engineering*, ser. SSE 2014. ACM, 2014, pp. 17–24.