
BU
Bournemouth
University

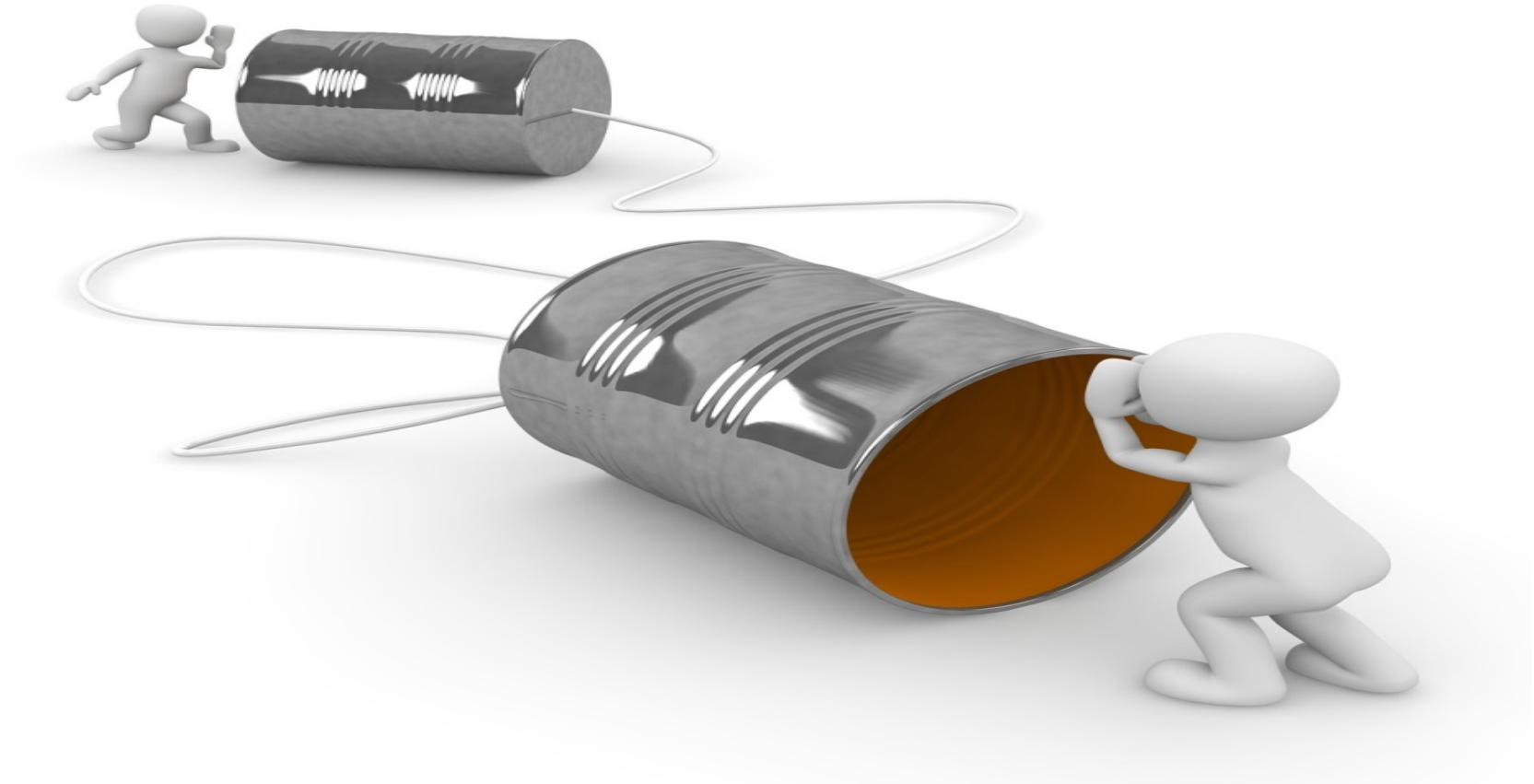
26th IEEE International
Requirements Engineering Conference
The 5th International Workshop on Evolving
Security & Privacy Requirements Engineering
20 August 2018
Banff, Alberta, Canada

Assessing System of Systems Security Risk and Requirements with OASoSIS

Duncan Ki-Aries, Shamal Faily, Huseyin Dogan, Christopher Williams

System of Systems

A Simple System of Systems



Describing Systems

- **Systems** can be described as *'a coming together of people, process, software and hardware, integrated to achieve a purpose'.*
- **System of Systems (SoS)** can be described as *'the coming together of independent systems collaborating for a new or higher purpose'*.
- **Socio-Technical Systems (STS)** are seen as organisational systems that include people, processes and technological systems with complex physical-technical systems and networks of interdependent actors.

Systems and System of Systems

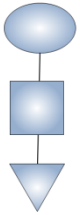
Simple Models of Systems and System of Systems

A System | A Sub-System | A Component System | Independent System Boundary

Systems Interaction | System of Systems Interdependency | System Interconnection

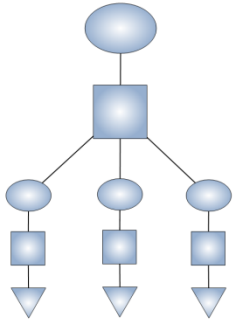
An Independent System

People
Process
Software
Hardware
Integrated to Achieve a Purpose



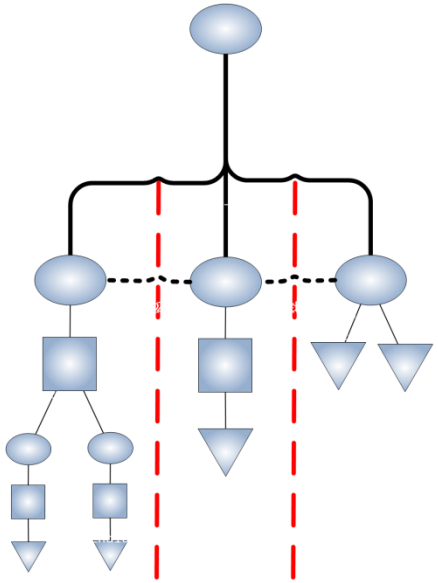
A System with a Sub-System and Component System

Systems Interconnecting



A Complex System

Larger-Scale Systems Interconnecting



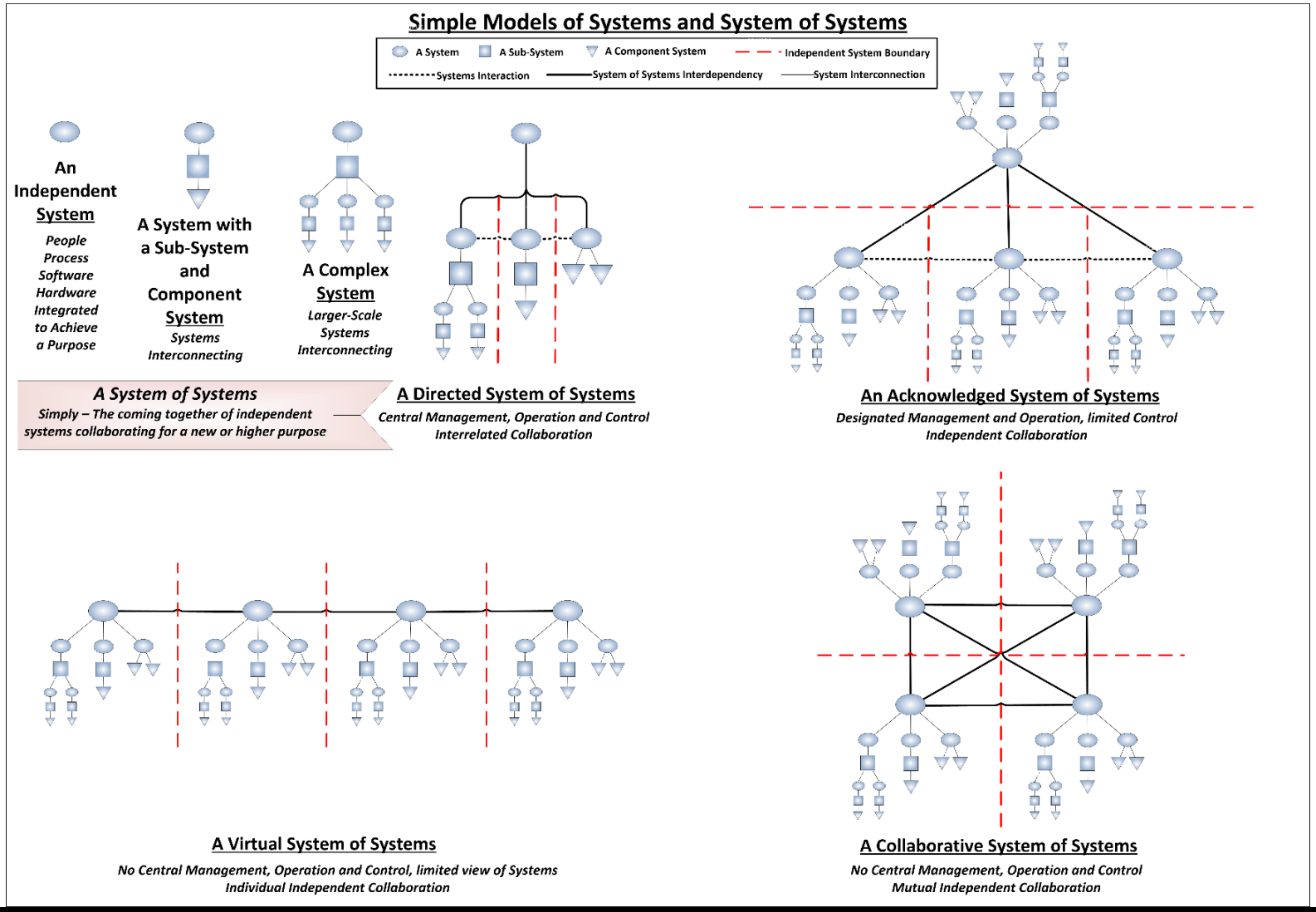
A System of Systems

Simply – The coming together of independent systems collaborating for a new or higher purpose

A Directed System of Systems

Central Management, Operation and Control
Interrelated Collaboration

Systems and System of Systems



Describing Systems of Systems

- **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’.

Bournemouth University

Characterising System of Systems

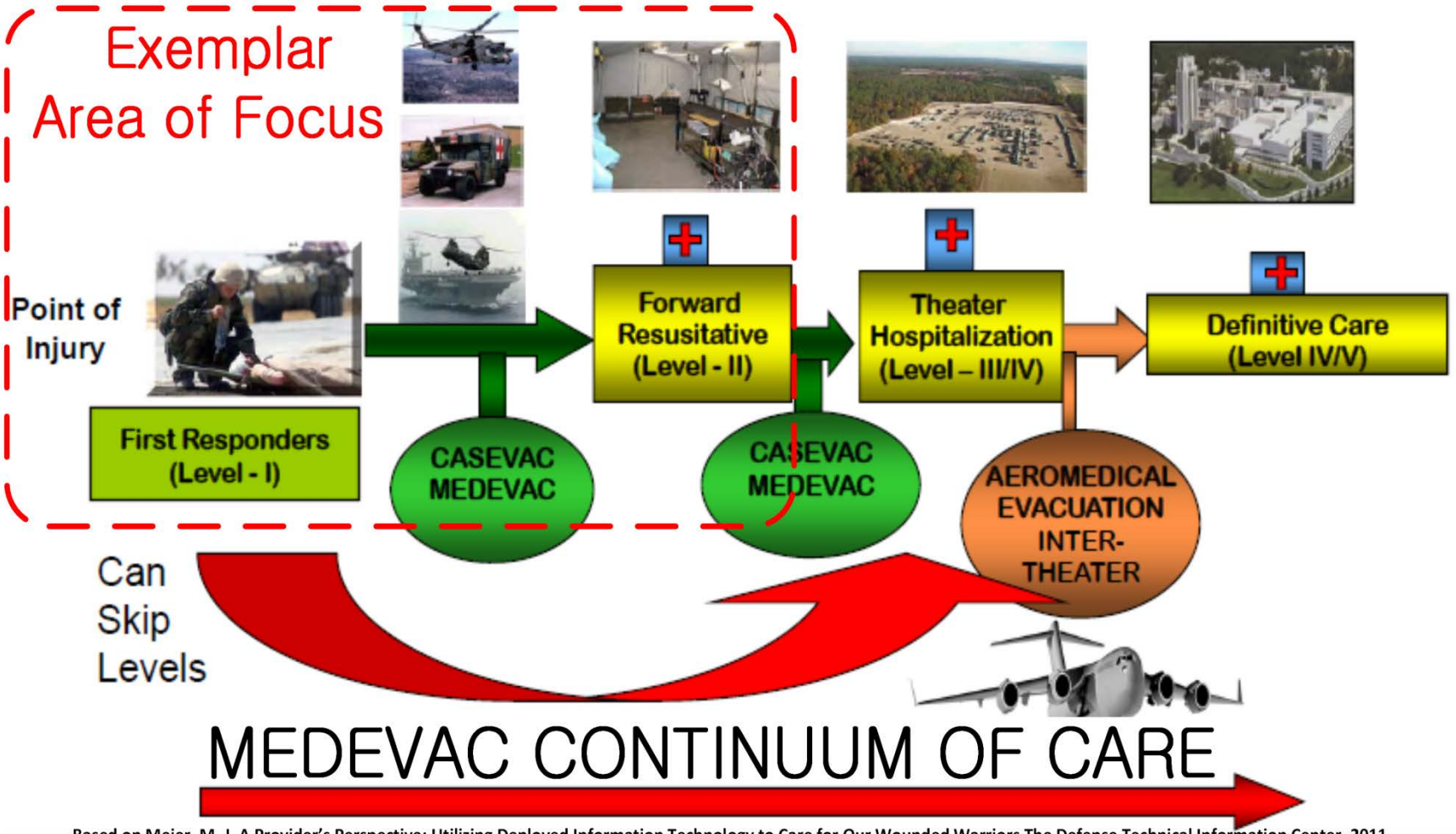
Characterising Systems of Systems

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.

Systems of Systems Questions

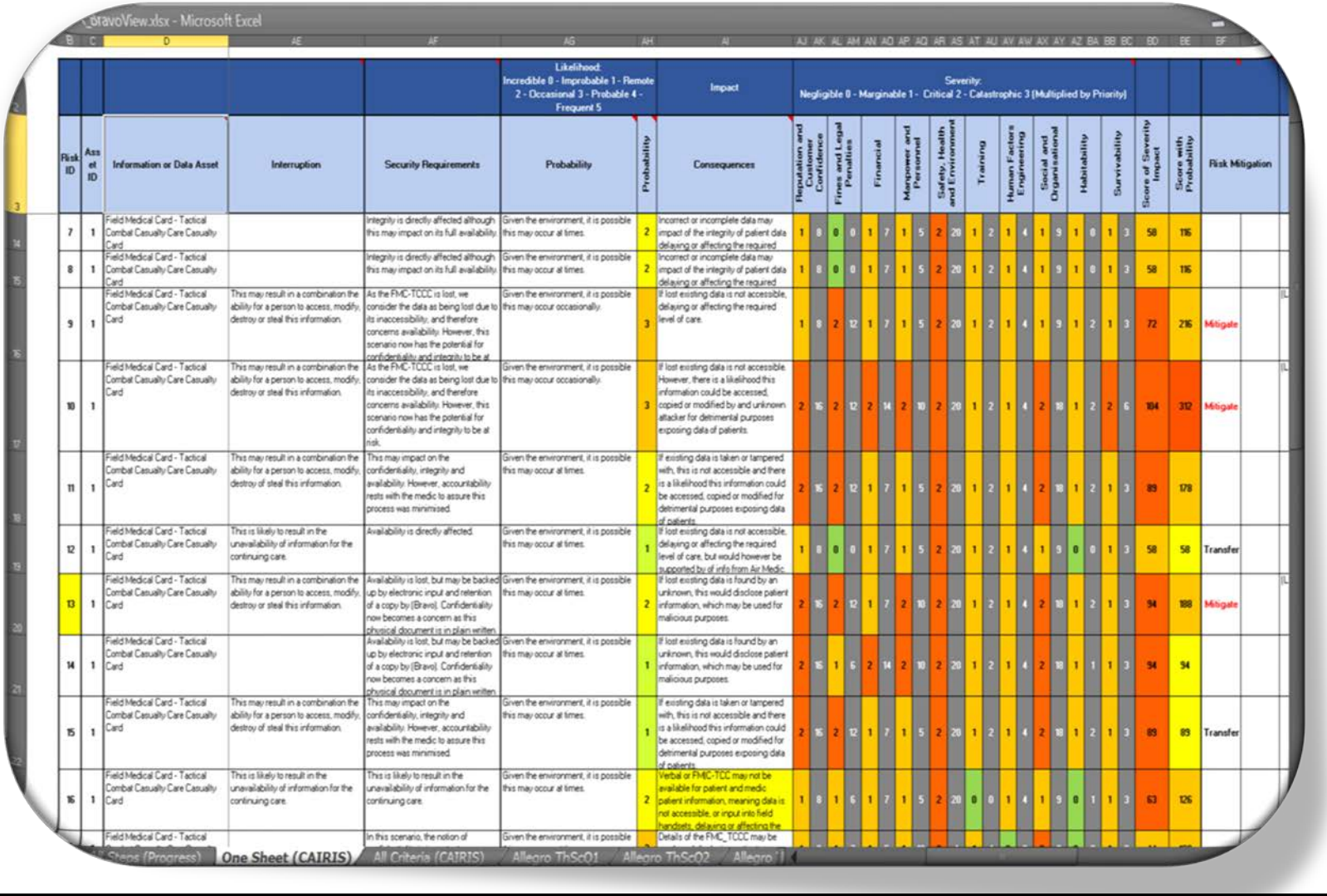
- Who are the high-level stakeholders - the main independent systems of the SoS?
- Who are the other relevant stakeholders important to the SoS achieving its mission?
- Who provides management oversight, governance, funding, and operational control of the SoS?
- Who is responsible for SoS design, development, 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?

MEDEVAC System of Systems

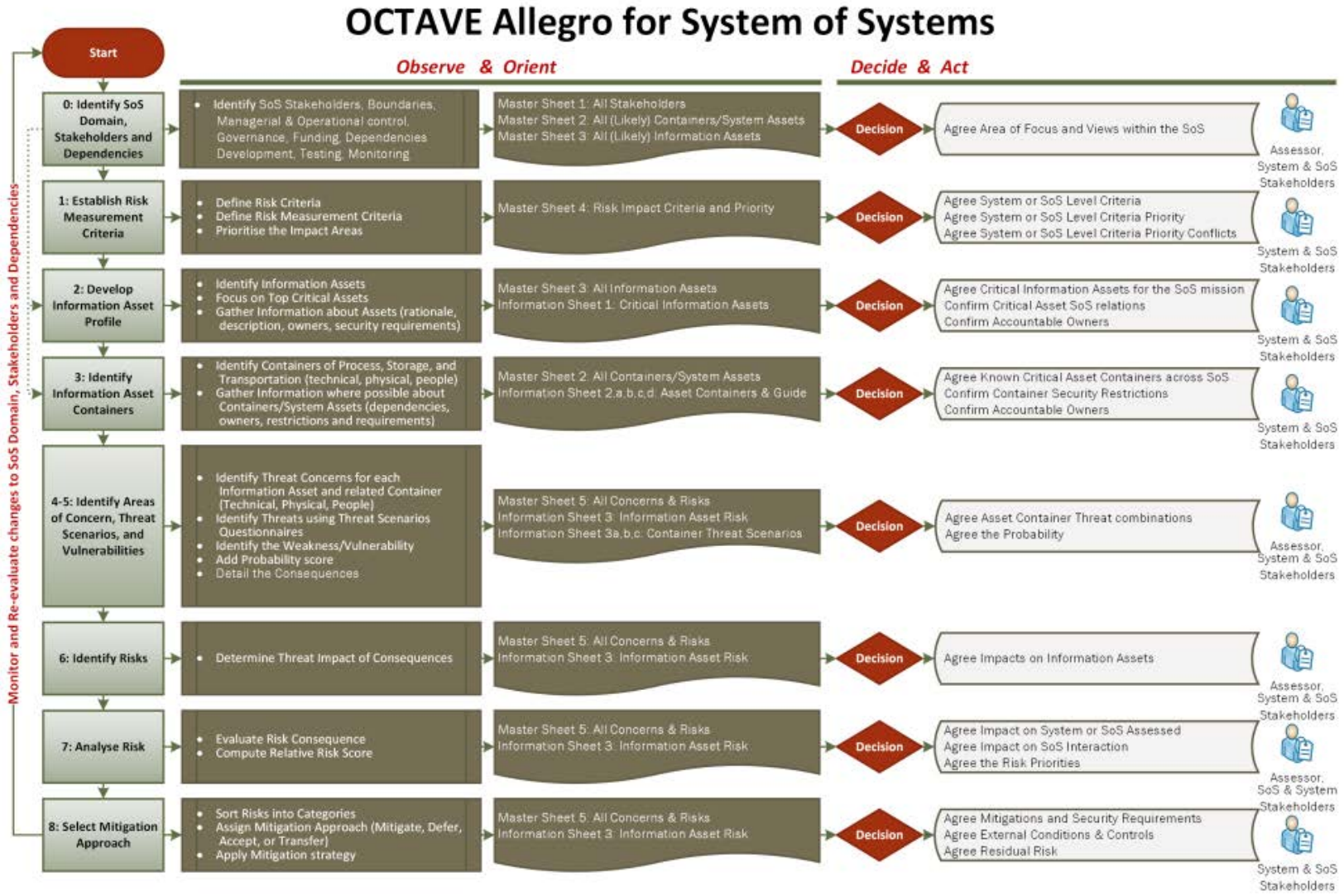


Based on Meier, M. J. A Provider's Perspective: Utilizing Deployed Information Technology to Care for Our Wounded Warriors The Defense Technical Information Center, 2011

Enhancing OCTAVE Allegro

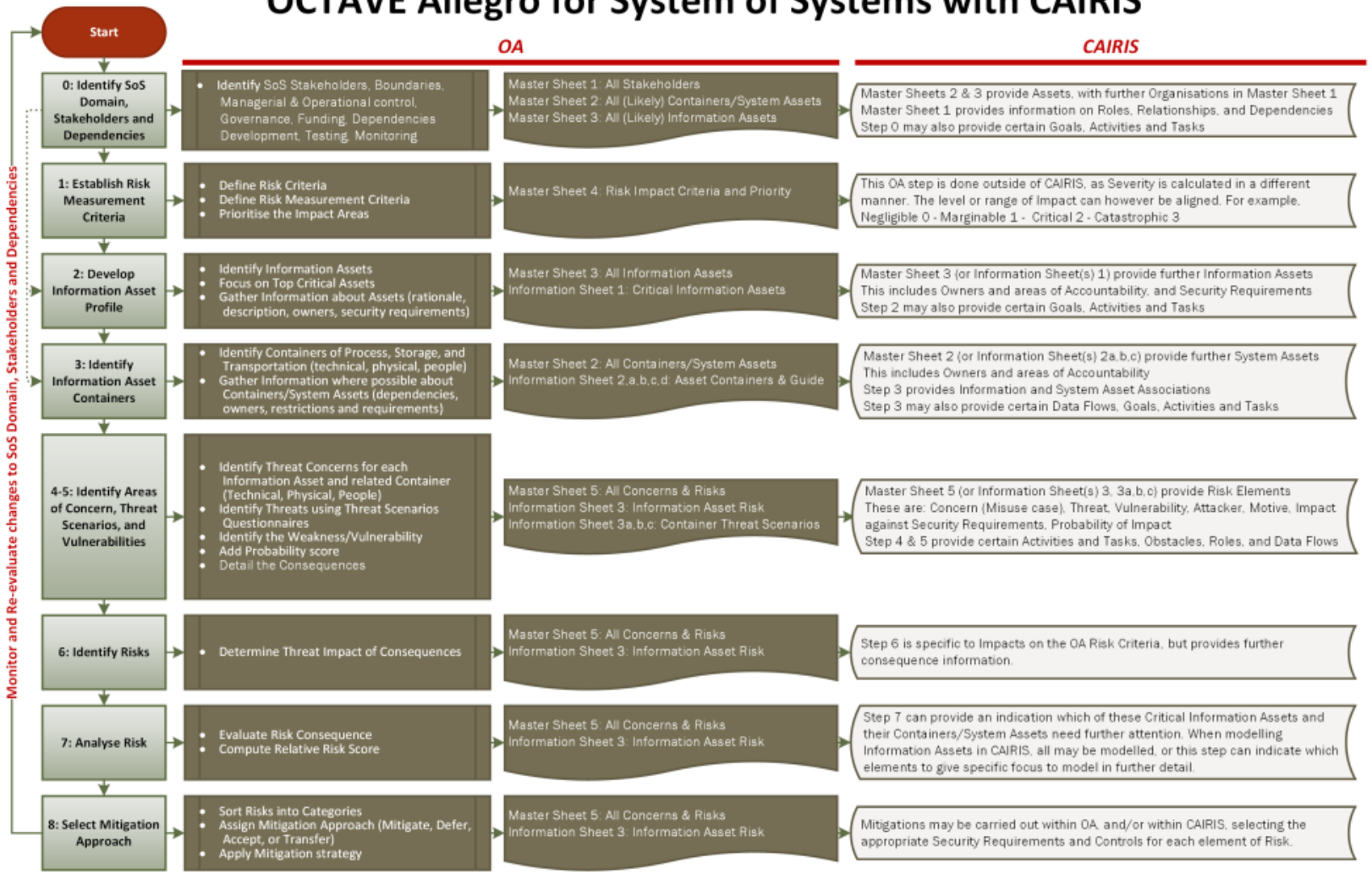


Enhancing OCTAVE Allegro



Enhancing OCTAVE Allegro

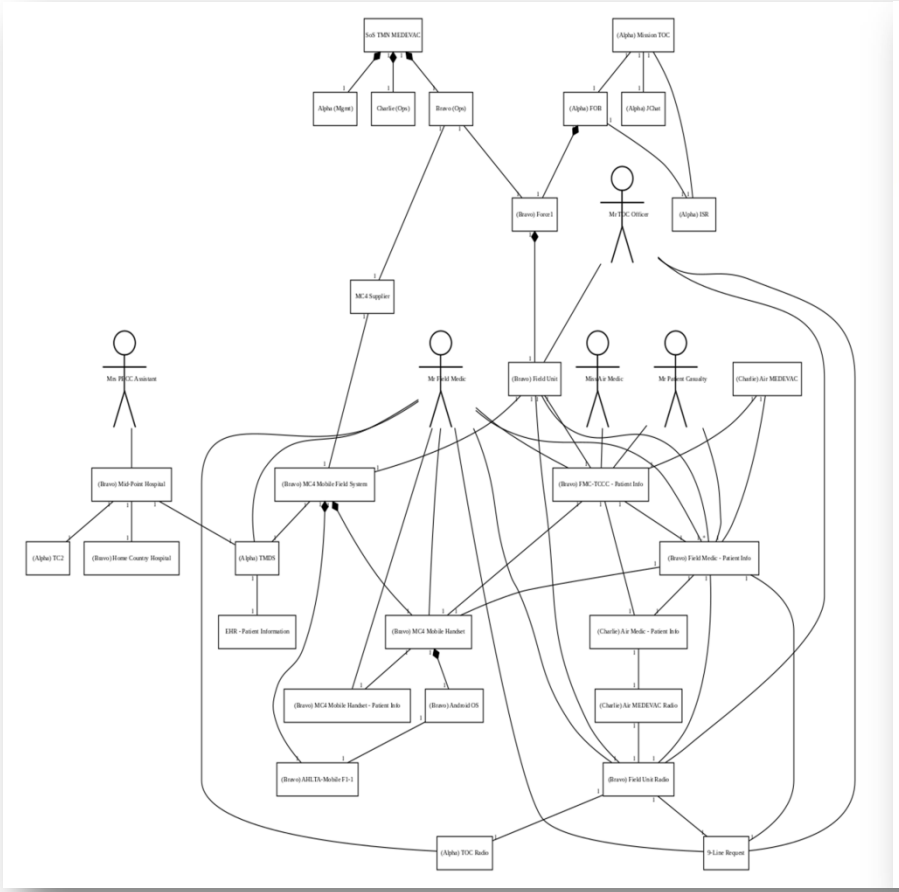
OCTAVE Allegro for System of Systems with CAIRIS

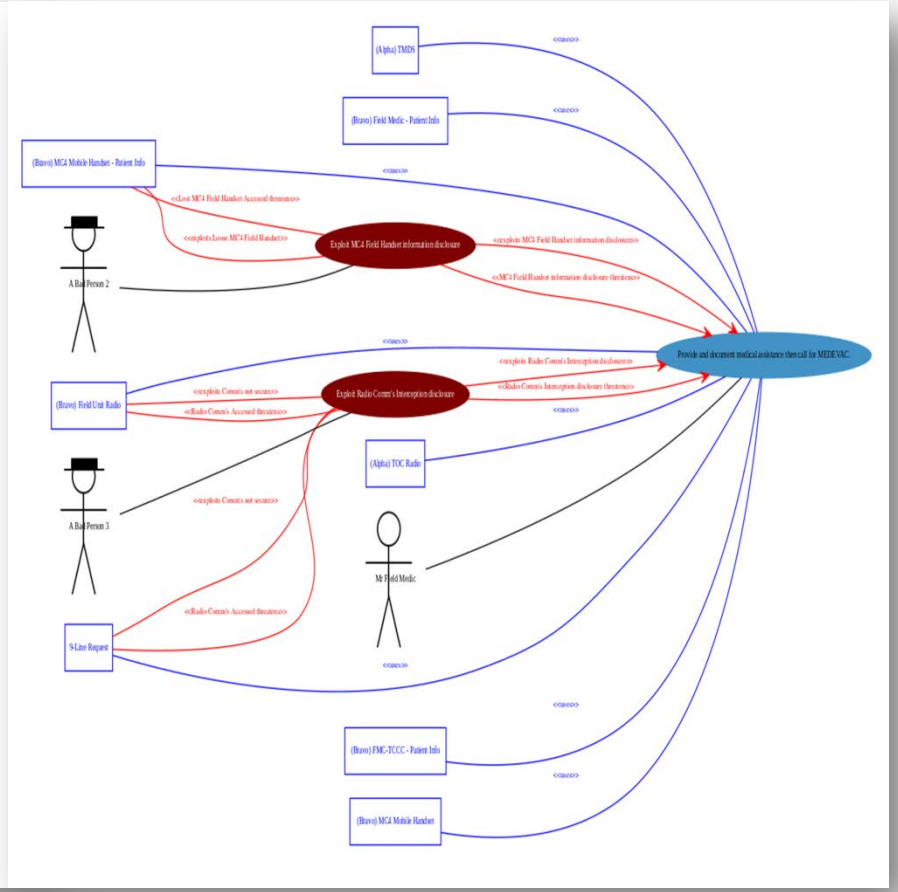


Differences in Assessing Risk

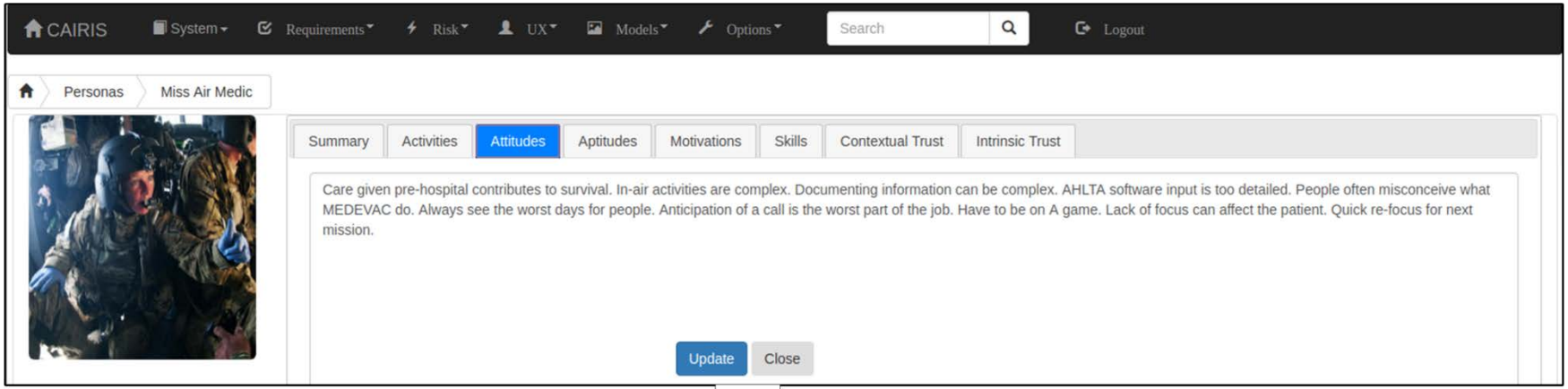
- In a typical assessment, the assessment view takes a top-down approach looking at the protection of assets under the management and control of the organisation for its own business purposes, and outwards towards the third-parties providing services for the organisation.
- When assessing the security risk related to the SoS interaction, the view is flipped. In addition to the organisation and technological systems' 'day job', the assessment now needs to consider the bottom-up interaction into the SoS where the independent system collaborates with other independent systems to achieve a new or higher SoS purpose.
- This is in addition to the day job, or the original purpose it was designed for, relating to the physical, technological, and people elements of each independent system and the interoperations between each.

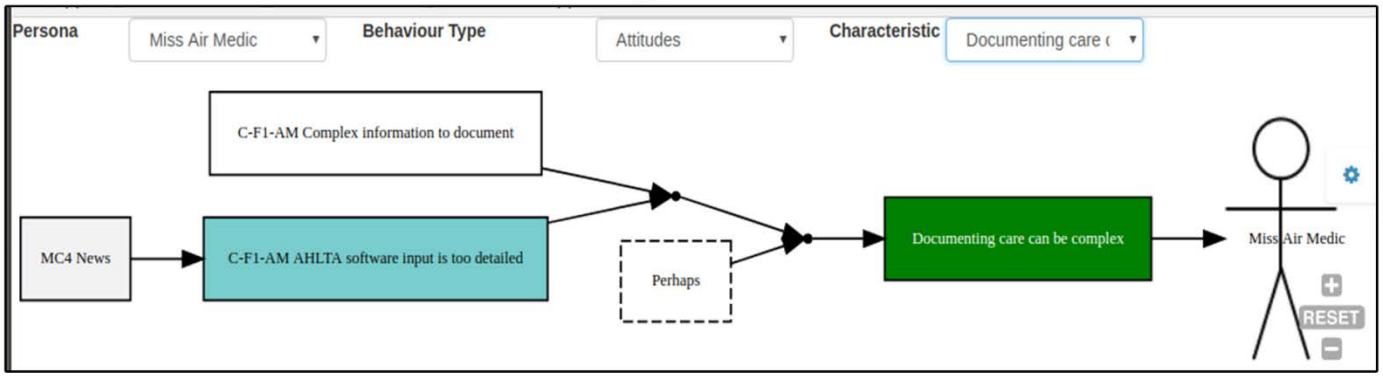
CAIRIS: Asset & Task Models





CAIRIS: Persona Model





CAIRIS

Computer-Aided Integration of Requirements and Information Security

- Enter or import a wide range of security, usability, and requirements data;
- Automatically generate security, usability, and requirements visual models based on connections between concepts that analysts make, and which summarise quantitative and qualitative data analysis;
- Help find new insights ranging from interconnections between requirements and risks;
- Leverage open source intelligence about potential attacks and candidate security architectures to derive risks and attack surface metrics;
- Provide functionally to integrate persona characteristics;
- Generate Volere compliant requirement specifications in different formats

Final Thoughts

- Combining models provided a view for Bravo and their SoS interactions, with additional views added for Alpha and Charlie, highlighting where dependent relations and security risk exists towards fulfilling the continuum of care.
- When modelling multiple systems, naming convention and terms across environments did become a challenge to indicate which element related to each independent system.
- 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 SoS engineering.
- Capturing different stakeholder and user views of the SoS interaction is important towards the modelling process, but the challenge is to understand what the minimum level of information is required to make a satisfactory security risk assessment is of importance.

Questions?

Duncan Ki-Aries

PhD Researcher - Cyber Security

dkiaries@bournemouth.ac.uk

Department of Computing & Informatics
Bournemouth University
Fern Barrow,
Talbot Campus,
Poole
BH12 5BB

Bournemouth University Cyber Security Research group (BUCSR)
https://cybersecurity.bournemouth.ac.uk/

Bournemouth University Human Computer Interaction group (BUCHI)
hci.bournemouth.ac.uk/

CAIRIS – https://cairis.org/


BU
Bournemouth
University