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
• **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

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

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**
- Simplicity - The coming together of independent systems collaborating for a new or higher purpose

**A Directed System of Systems**
- Central Management, Operation and Control
- Interrelated Collaboration

**An Acknowledged System of Systems**
- Designated Management and Operation, limited Control
- Independent Collaboration

**A Virtual System of Systems**
- No Central Management, Operation and Control, limited view of Systems
- Individual Independent Collaboration

**A Collaborative System of Systems**
- No Central Management, Operation and Control
- Mutual Independent Collaboration
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’.
## Characterising Systems of Systems

<table>
<thead>
<tr>
<th>Types</th>
<th>Aspect</th>
<th>Directed SoS</th>
<th>Acknowledged SoS</th>
<th>Collaborative SoS</th>
<th>Virtual SoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SoS Types</td>
<td>Description</td>
<td>A Directed SoS can be described as possessing 'interrelated collaboration, with central management, operation and control over the SoS as a whole'</td>
<td>An Acknowledged SoS has 'designated management, but limited control over the independent collaboration of the SoS'.</td>
<td>A Collaborative SoS has 'no central management, so operation and control must be formed and agreed as a mutual independent collaboration'.</td>
<td>A Virtual SoS has 'individual independent collaboration with no central management, operation or control of the SoS as a whole'.</td>
</tr>
<tr>
<td>Stakeholder Involvement</td>
<td>• Stakeholders are at system and SoS levels;</td>
<td>• Interrelated independent system owners;</td>
<td>• Competing interests and priorities;</td>
<td>• May have no vested interest in the SoS;</td>
<td>• Most stakeholders are likely to be recognised.</td>
</tr>
<tr>
<td>Stakeholder Involvement</td>
<td>• Interrelated independent system owners;</td>
<td>• Independent system owners;</td>
<td>• Competing interests and priorities;</td>
<td>• May have no vested interest in the SoS;</td>
<td>• Some stakeholders may not be recognised.</td>
</tr>
<tr>
<td>Governance</td>
<td>• Some levels of complexity with central management and funding for both the SoS and interrelated collaboration of systems;</td>
<td>• The SoS does have authority over all the systems.</td>
<td>• Added levels of complexity due to designated management and funding for both the SoS and individual systems;</td>
<td>• With independent collaboration, the SoS does not have authority over all the systems.</td>
<td>• Further levels of complexity due to the mutual independent collaboration of SoS management with funding only at or from individual system level.</td>
</tr>
<tr>
<td>Operational Environment</td>
<td>• Direct collaboration to meet a set of operational objectives;</td>
<td>• Systems’ objectives may or may not align with the SoS objectives.</td>
<td>• Designated collaboration to meet a set of operational objectives;</td>
<td>• Systems’ objectives may or may not align with the SoS objectives.</td>
<td>• Mutually agreed collaboration to meet a set of operational objectives;</td>
</tr>
<tr>
<td>Acquisition</td>
<td>• Complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems;</td>
<td>• Stated capability objectives up-front, which may provide basis for requirements;</td>
<td>• Benefits from central control to establish and integrate system needs.</td>
<td>• Designated management and independent system needs are established.</td>
<td>• Mutually agreed independent system needs are established.</td>
</tr>
<tr>
<td>Implementation</td>
<td>• Complexity from multiple system lifecycles, new developments, technology, acquisition programs, developmental and legacy systems;</td>
<td>• Stated capability objectives up-front, which may provide basis for requirements;</td>
<td>• Benefits from central control to establish and integrate system needs.</td>
<td>• Designated management and independent system needs are established.</td>
<td>• Mutually agreed independent system needs are established.</td>
</tr>
<tr>
<td>Test &amp; Evaluation</td>
<td>• Some challenges due to the difficulty of synchronising across multiple systems’ life cycles;</td>
<td>• Complexity of all the moving parts and potential for unintended consequences.</td>
<td>• More challenging due to the difficulty of synchronising across multiple systems’ life cycles;</td>
<td>• Complexity of all the moving parts and potential for unintended consequences.</td>
<td>• Testing cannot be completed in full and is challenge due to the difficulty of synchronising across multiple systems’ life cycles;</td>
</tr>
<tr>
<td>Engineering &amp; Design Considerations</td>
<td>• Focus is on identifying the independent systems within direct management and control that contribute to the SoS objectives, functionality and data flow.</td>
<td>• Designated management and monitoring at SoS and system levels to satisfy SoS user needs;</td>
<td>• Balancing needs of the systems benefits from direct co-ordination.</td>
<td>• Mutually agreed management and monitoring at systems level to satisfy SoS user needs;</td>
<td>• Direct and indirect management and monitoring at system level to satisfy SoS user needs;</td>
</tr>
<tr>
<td>Performance &amp; Behaviour</td>
<td>• Directly managed and monitored at SoS level to satisfy SoS user needs;</td>
<td>• Designated management and monitoring at SoS and system levels to satisfy SoS user needs;</td>
<td>• Balancing needs of the systems benefits from designated co-ordination.</td>
<td>• Balancing needs of all systems is reliant on mutual co-ordination.</td>
<td>• Balancing needs of the systems and indirect systems may not be achieved.</td>
</tr>
</tbody>
</table>
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

Exemplar Area of Focus

Point of Injury

First Responders (Level - I)

CASEVAC MEDEVAC

Forward Resusitative (Level - II)

CASEVAC MEDEVAC

Theater Hospitalization (Level – III/IV)

AEROMEDICAL EVACUATION INTER-THEATER

Definitive Care (Level IV/V)

Can Skip Levels

MEDEVAC CONTINUUM OF CARE

Based on Meier, M. J. A Provider’s Perspective: Utilizing Deployed Information Technology to Care for Our Wounded Warriors The Defense Technical Information Center, 2011
<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Asset ID</th>
<th>Information or Data Asset</th>
<th>Interruption</th>
<th>Security Requirements</th>
<th>Probability</th>
<th>Consequences</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>Integrity is directly affected although this may impact on its full availability.</td>
<td>Given the environment, it is possible this may occur at times.</td>
<td>2</td>
<td>Incorrect or incomplete data may impact the integrity of patient data and may affect the required training.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>Integrity is directly affected although this may impact on its full availability.</td>
<td>Given the environment, it is possible this may occur at times.</td>
<td>2</td>
<td>Incorrect or incomplete data may impact the integrity of patient data and may affect the required training.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>This may result in a combination of loss of the ability for a person to access, modify, destroy or delete this information.</td>
<td>As the HSCIC, this loss could be due to its accessibility, and therefore concerns availability. However, this scenario now has the potential for confidentiality and integrity to be at risk.</td>
<td>1</td>
<td>If existing data is not accessible, this information could be accessed.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>This may result in a combination of loss of the ability for a person to access, modify, destroy or delete this information.</td>
<td>As the HSCIC, this loss could be due to its accessibility, and therefore concerns availability. However, this scenario now has the potential for confidentiality and integrity to be at risk.</td>
<td>1</td>
<td>If existing data is not accessible, this information could be accessed.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>This may result in a combination of loss of the ability for a person to access, modify, destroy or delete this information.</td>
<td>This may impact on the confidentiality, integrity and availability. However, it is possible this process was minimised.</td>
<td>1</td>
<td>If existing data is not accessible, this information could be accessed.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>This may result in a combination of loss of the ability for a person to access, modify, destroy or delete this information.</td>
<td>Available data is directly affected.</td>
<td>1</td>
<td>If existing data is not accessible, this information could be accessed.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>This may result in a combination of loss of the ability for a person to access, modify, destroy or delete this information.</td>
<td>Available data is lost, but may be backed up if necessary.</td>
<td>1</td>
<td>If existing data is not accessible, this information could be accessed.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
<tr>
<td>14</td>
<td>14</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>This may result in a combination of loss of the ability for a person to access, modify, destroy or delete this information.</td>
<td>Available data is lost, but may be backed up if necessary.</td>
<td>1</td>
<td>If existing data is not accessible, this information could be accessed.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
<tr>
<td>15</td>
<td>15</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>This may result in a combination of loss of the ability for a person to access, modify, destroy or delete this information.</td>
<td>Available data is lost, but may be backed up if necessary.</td>
<td>1</td>
<td>If existing data is not accessible, this information could be accessed.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>Field Medical Card - Tactical Combat Casualty Casualty Card</td>
<td>This may result in a combination of loss of the ability for a person to access, modify, destroy or delete this information.</td>
<td>Available data is lost, but may be backed up if necessary.</td>
<td>1</td>
<td>If existing data is not accessible, this information could be accessed.</td>
<td>1</td>
<td>Inevitable - Improbable - Remote - Occasional - Probable - Frequent</td>
<td>Catastrophic - Critical - Significant - Minor</td>
</tr>
</tbody>
</table>

Enhancing OCTAVE Allegro
Enhancing OCTAVE Allegro

OCTAVE Allegro for System of Systems

**Observe & Orient**

- Start
- 0: Identify SoS Domain, Stakeholders and Dependencies
  - Identify SoS Stakeholders, Boundaries, Operational control, Governance, Funding, Dependencies, Development, Testing, Monitoring

- 1: Establish Risk Measurement Criteria
  - Define Risk Criteria
  - Define Risk Measurement Criteria
  - Prioritize the Impact Areas

- 2: Develop Information Asset Profile
  - Identify Information Assets
  - Focus on Top Critical Assets
  - Gather Information about Assets (rationale, description, ownership, security requirements)

- 3: Identify Information Asset Containers
  - Identify Containers of Process, Storage, and Transportation (technical, physical, people)
  - Gather Information where possible about Containers/Systems Assets (information, owners, restrictions and requirements)

- 4-5: Identify Area of Concern, Threat Scenarios, and Vulnerabilities
  - Identify Threat Concerns for each Information Asset and Related Container (technical, physical, people)
  - Identify Threats using Threat Scenarios
  - Gather Information where possible about Information Assets (information, owners, restrictions and requirements)

- 6: Identify Risks
  - Determine Threat impact of Consequences

- 7: Analyze Risk
  - Evaluate Risk Consequence
  - Compute Relative Risk Score

- 8: Select Mitigation Approach
  - Sort Risks into Categories
  - Assign Mitigation Approach (Mitigate, Defend, Accept, or Transfer)
  - Apply Mitigation Strategy

**Decide & Act**

- Master Sheet 1: All Stakeholders
- Master Sheet 2: All Information Assets
- Master Sheet 3: All Information Asset Containers

- Master Sheet 4: Risk Impact Criteria and Priority

- Master Sheet 5: All Information Assets
- Master Sheet 2: All Information Assets

- Information Sheet 3: Information Asset Risk

- Information Sheet 4: Critical Information Assets

- Information Sheet 2: Asset Containers and Guide

- Information Sheet 1: Critical Information Assets

- Information Sheet 5: Container Threat Scenarios

- Decision
  - Agree Area of Focus and Views within the SoS
  - Assessors: System & SoS Stakeholders

- Decision
  - Agree System of SoS Level Criteria
  - Assessors: System & SoS Stakeholders

- Decision
  - Agree System of SoS Level Criteria Priority
  - Assessors: System & SoS Stakeholders

- Decision
  - Agree Critical Information Assets for the SoS mission
  - Confirm Critical Asset SoS mission
  - System & SoS Stakeholders

- Decision
  - Agree Known Critical Asset Containers across SoS
  - Confirm Container Security Restrictions
  - Confirm Accountable Owners
  - System & SoS Stakeholders

- Decision
  - Agree Asset Container Threat combinations
  - Agree the Probability
  - Assessors: System & SoS Stakeholders

- Decision
  - Agree Impacts on Information Assets
  - Assessors: System & SoS Stakeholders

- Decision
  - Agree Impact on System or SoS
  - Assessors: SoS & System Stakeholders

- Decision
  - Agree Mitigations and Security Requirements
  - Agree External Conditions & Controls
  - Agree Residual Risk
  - System & SoS Stakeholders
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.
Care given pre-hospital contributes to survival. In-air activities are complex. Documenting information can be complex. AHLTA software input is too detailed. People often misconceive what MEDEVAC do. Always see the worst days for people. Anticipation of a call is the worst part of the job. Have to be on A game. Lack of focus can affect the patient. Quick re-focus for next mission.
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.
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/