31st Annual INCOSE international symposium
Honolulu, HI, USA
July 17 - 22, 2021

Using the Security Views in UAF

Matthew Hause
Systems Solutions Inc (SSI)
3208 Misty Oaks Way, Round Rock, Texas, USA
+1 917 514 7581
mhause@systemxi.com

Lars-Olof Kihlström
Syntell AB
PO Box 10022, SE-10055 Stockholm, Sweden
+46 706661978
lars-olof.kihlstrom@syntell.se

Abstract. Architectures, systems, subsystems, and the data that they contain, are valuable assets. Systems engineers and architects must plan for system security from concept inception to retirement to ensure that security is embedded into every part of every process, procedure, system and component as well as in the mindset of the people in the enterprise. While the various DoDAF views contain attributes of security, there are no views for defining system security goals, threats, risks, mitigating elements, etc. and demonstrating how these are integrated and implemented into the operational, system, standards and services views. The Unified Architecture Framework (UAF) has integrated a set of security views that provide engineers a means of defining security goals and requirements and demonstrating how these are implemented throughout the architecture.

Introduction

Given the connected nature of our world and our systems, cyber-security has risen to the forefront of system architecture, design, development, deployment, operations, maintenance, and even retirement. Hacking of computer systems is ubiquitous, almost inevitable, and has a long history. Consider the 3 August 2011 story by Ars Technica, "Operation Shady RAT: five-year hack attack hit 14 countries". The article states that "So widespread are the attacks that Dmitri Alperovitch, McAfee Vice President of Threat Research, said that the only companies not at risk are those who have nothing worth taking, and that of the world's biggest firms, there are just two kinds: those that know they've been compromised, and those that still haven't realized they've been compromised." The article further states that “The governments of the United States, Canada, and South Korea, as well as the UN, the International Olympic Committee, and 12 US defense contractors were among those hacked in a five-year hacking campaign. Many of the penetrations were long-term, with 19 intrusions lasting more than a year, and five lasting more than two.” (Ars Technica, 2011).

The website purplesec.uc lists several sobering statistics. Among these:

- In 2017, cyber crime costs accelerated with organizations spending nearly 23% more than 2016 — on average about $11.7 million.
- By 2020, we expect IT analysts covering cyber security will be predicting five-year spending forecasts (to 2025) at well over $1 trillion.
- The average cost of a malware attack on a company is $2.4 million.

- The Equifax breach cost the company over $4 billion in total.
- 67% of financial institutions reported an increase in cyber-attacks over the past year.
- Ransomware attacks worldwide rose 350% in 2018.
- Ransomware attacks are estimated to cost $6 trillion annually by 2021.
- 50% of a surveyed 582 information security professionals do not believe their organization is prepared to repel a ransomware attack.

Things have not slowed down in 2020 with Cybercrime up 600%. The website states that "Due to the COVID-19 outbreak an uptick in sophisticated phishing email schemes by cybercriminals has emerged. Malicious actors are posing as the Center for Disease Control and Prevention (CDC) or World Health Organization (WHO) representatives." (Purplesec.us, 2020) Sadly, it appears that we will be undermanned in the fight for defense of our systems. In Morgan (2019) the 2019/2020 Official Annual Cybersecurity Jobs Report states that there will be a "350 percent growth in open cybersecurity positions from 2013 to 2021". The New York Times reports that "A stunning statistic is reverberating in cybersecurity: An estimated 3.5 million cybersecurity jobs will be available but unfilled by 2021, according to predictions from Cybersecurity Ventures and other experts." (Perhach, 2018). With fewer trained people we will need to work smarter.

The US Department of Defense is taking this seriously. In an article in Breaking Defense, entitled "Starting Dec. 1, Cybersecurity Is No Longer Optional", Katie Arrington says "This is the start of a new day in the Department of Defense where cybersecurity, as we've been saying for years is foundational for acquisitions, we're putting our money where our mouth is. We mean it," (Atherton, 2020). Under previous recommendations, it was enough for a company to meet some of the 110 NIST benchmark standards, so long as they claimed they were working towards compliance with the rest. That meant companies could compete for contracts without having to prove compliance. "Cybersecurity Maturity Model Certification (CMMC) is going to be a go/no-go decision. When audited, you're either level 1 or not," said Arrington.

Innovative techniques are being proposed and studied. Dove & Willett (2020) suggested a new approach in a paper entitled "Techno-Social Contracts for Security Orchestration in the Future of Systems Engineering". (Dove, Willett, 2020) "The cyber-physical-social aspects of systems engineering are gaining attention in the social dimension principally for human-human and human-technology interaction. This paper suggests that systems and systems of systems can be viewed as social communities of technical elements, where security of the community and its technical members can benefit from collective and distributed mutual protection behaviors." As systems engineering is concerned with all aspects of systems, cyber security is necessarily one of them. And it needs to start with architectures.

Model-Based Systems Engineering (MBSE)

The INCOSE SE Vision 2025 defines model-based systems engineering (MBSE) as "the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases (INCOSE 2007)." The Systems Modeling Language (SysML) is the most widely used standardized modeling language and notation for representing properties and characteristics of systems. It is used to model systems in both the abstract and concrete (logical and physical) views that include behavioral, structural, parametric and requirements views. (OMG,

2017) For enterprise modeling, an architecture framework is required to understand systems of systems and how they change over time. DoDAF is the Department of Defense Architecture Framework (DoD, 2012) and MODAF is the Ministry of Defence Architecture Framework (MOD, 2020). The MOD has lately adopted NAF version 4. (NATO, 2018) The Unified Architecture Framework (UAF) is built on top of SysML and is used to define the overall goals, strategies, capabilities, interactions, standards, operational and systems architectures, systems patterns and so forth (UAF, 2019). Security and human factors (personnel) views were added to the UAF to improve the coverage of these areas of concern. The UAF was previously called the Unified Profile for DoDAF and MODAF (UPDM) and was ratified by the Object Management Group (OMG). Several papers have been written on the UAF and its support of SoS modeling including (Hause, Dandashi 2015) and (Hause 2014). The full details of SysML and UAF are not included here for space reasons. Please see the above references for more information. The purpose of this paper is to describe the UAF security views and how they can be used for applying security throughout the enterprise and over time.

UAF Views

Before modeling a system or system of systems (SoS), one needs to understand the purpose of the system as well as the purpose of the model. UAF has a set of views for defining a set of capabilities over its life-cycle phases. These are used to define the goals, vision, enterprise phases, evolution over time and the capabilities and how these are realized by systems and subsystems. The UAF provides traceability from these elements to the other UAF views including the operational architecture, which is used to define the abstract, logical and solution-independent expression of the system as intended to be used in operations. This defines what needs to be done and traces directly to the systems views that define how these capabilities and operational architecture will be realized. To use an analogy, the operational view could define a need to generate power, and the resources views define fossil fuel, solar, wind, tidal and other means of providing the power. Standards views are used to define system standards and systems that conform to them, services views define services to be implemented by systems and the project views define when the systems will be deployed and retired. In addition, the latest version of the UAF also defines security and human factors views. Work is also being done with the systems assurance group at the OMG to integrate threat and risk analysis as a set of cross cutting concerns.

Architecture Cross Cutting Concerns

Cross cutting concerns are those characteristics of an architecture that cannot be modular and cut across other aspects. A simple example would be vehicular safety. When a car is designed there is no specific component of the car that is the safety module. Safety needs to be inherent and intrinsic to the car design and implementation or the car will not be safe. Furthermore, overall safety performance must also be attributed to the vehicle operator, as well as the environment in which the vehicle operates. In the same way, a system of systems contains a variety of cross cutting concerns we must address. These include security, safety, resilience, flexibility, robustness, and others. Defining the points of vulnerability for security and resilience allows engineers to perform trade-off and threat and risk analysis on the entire architecture. Integrating the analysis tools with the UAF architecture provides a means of defining the problem, designing possible solutions, and then performing trade-off analysis to determine the best fit. These possible solutions can be narrowed to one or more solutions that will be implemented in the final system.

The UAF Security Views

Security views were lacking in DoDAF and MODAF. These were added to the UAF to provide a means of defining requirements, strategies, implementations and solutions for security of all forms throughout the enterprise. They were based on a variety of sources including the Canadian Department of National Defense Architecture Framework, work done at the DoD, MOD and NATO, and industry best practice. They were developed by experts from the DoD, DND, Mitre, industry, DISA and OMG tool vendors. The UAF security views illustrate the security assets, enclaves, security constraints, security controls, families, and measures required to address specific security concerns. Their purpose is to address the security constraints and information assurance attributes that exist on exchanges between systems and operational elements as well as the elements themselves. The stakeholders for these views include security architects, security engineers, systems engineers, and operational architects. Figure 1 shows an overview of many of these concepts and relationships. For a full specification of the UAF metamodel ontology, see (OMG, 2019)

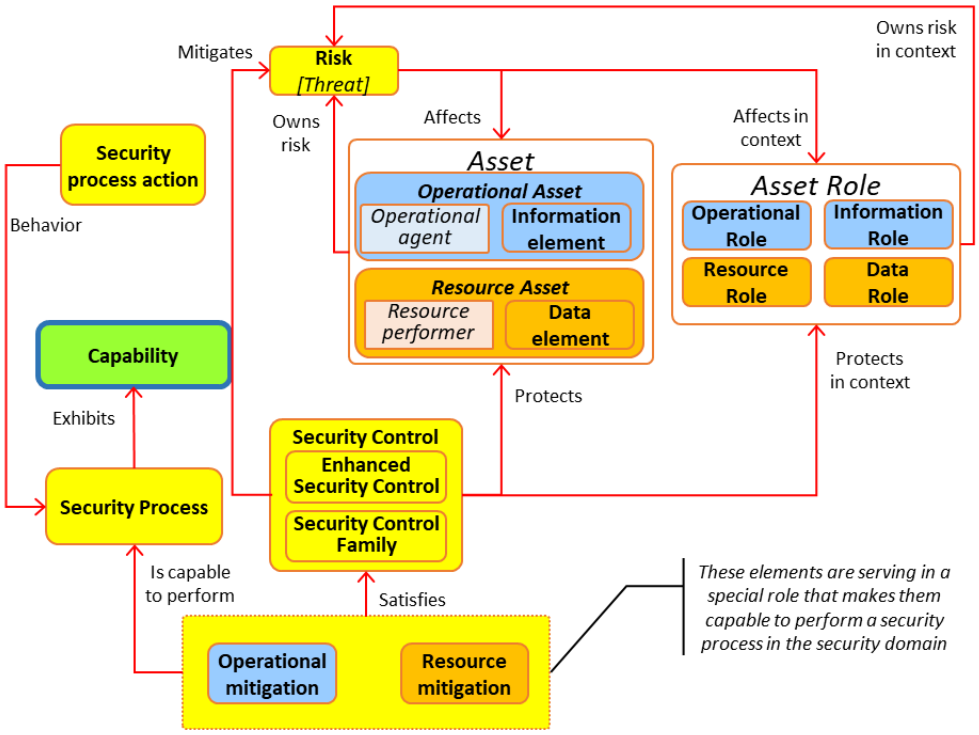

Figure 1 Portion of the Security View Meta-Model

Many of the aspects in Figure 1 directly or indirectly point to risk. This is deliberate as it is via the identification of risk that drives the need for security controls and other aspects of security. In systems engineering, requirements drive system development. In security engineering it is risk.

The Example Model

The example model shown below applies the UAF to a common scenario in civilian maritime Search and Rescue (SAR) operations -- a Yacht in distress. A Monitor Unit picks up the Distress Signal from the Yacht and passes it on to the Command and Control (C2 Center). The C2 Center coordinates the search and rescue operation among the Rescue Helicopters, Naval Ships and

Rescue Boats. The system contains a set of systems with different stakeholders, owners, command hierarchies, purposes, security and safety levels and constraints, etc. In short it is a complex system of systems. Communications and interactions involve naval vessels and helicopters, first responders, civilian and federal government vessels and vehicles. There is a need to communicate and cooperate, but also a need to ensure security of systems, personnel and communications. The example model is fully described in the UAF specification. For the other views in the model, refer to the example model document. (OMG, 2019). This paper augments the UAF security views from the UAF example SAR Architecture to demonstrate how they can be used to define a secure architecture. Their purpose is to illustrate the concepts rather than to describe a complete, detailed, solution. These additions will be included in the next version of UAF, planned for 2021.

The Security Taxonomy (Sc-Tx)

The Security Taxonomy (Sc-Tx) view shows the security assets and security enclaves. A Security Enclave is a collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location. The diagram is used to define the hierarchy of security assets and asset owners that are available to implement security, security constraints (policy, guidance, laws and regulations) and details where they are located (security enclaves). In addition to the security elements, system resources can also be defined in the Security Taxonomy diagram and associated with other security elements. In this way the different security elements can be grouped in the same diagram and package hierarchy. Since the UAF does not constrain where elements can be defined and stored, this contributes to more modular architectures.

This main emphasis in this paper will be the integration between the resource and security views, to demonstrate risk mitigation solutions and traceability. Security and operational views can also be linked. For example, operational performers and activities can be linked to risks, constraints and security controls as shown in Figure 2. This allows architects to identify risk early on in the development cycle and take steps to ensure that solution-based elements take these into account.

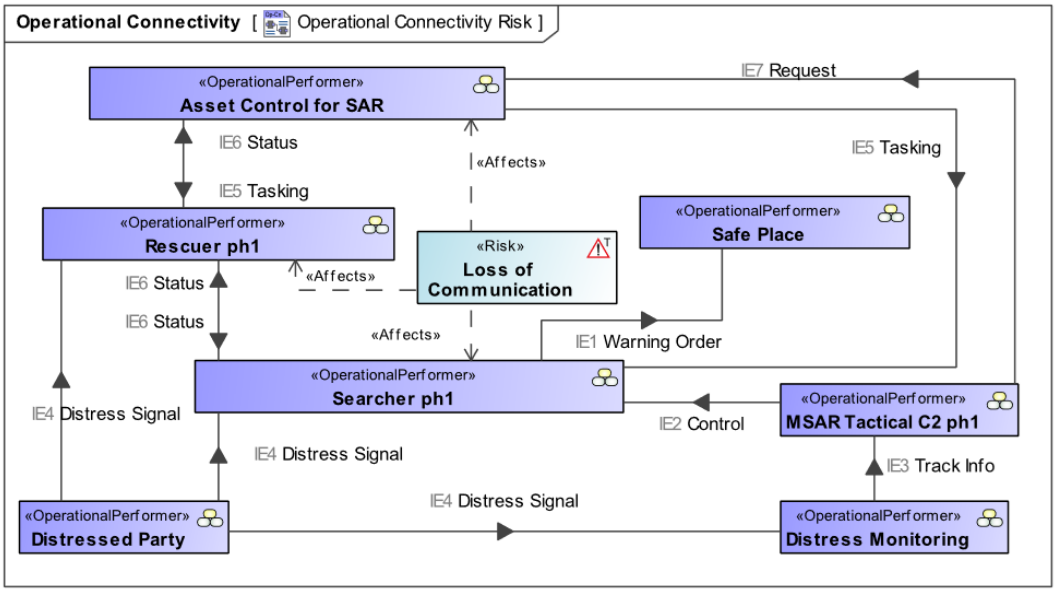

Figure 2 Operational Connectivity with Risk Links

Figure 2 shows the operational connectivity for the search and rescue context with traceability to the loss of communication risk. The Rescuer, Searcher and Asset Controller communicate together to coordinate operations. Without this ability to communicate, the commands, controls, tasking, status updates and other aspects cannot take place. These elements are implemented by the SAR HQ and SAR Field Organization among others. To fulfill their duties, SAR HQ communicates with the SAR Field Organizations via an EMS Dispatch System. This allows them to coordinate and communicate tasks, orders, crew rosters, etc. A risk analysis expert has analyzed the SAR architecture and realized that this is a single point of failure: loss of comms = loss of mission capability. The analysis is shown in Figure 3.

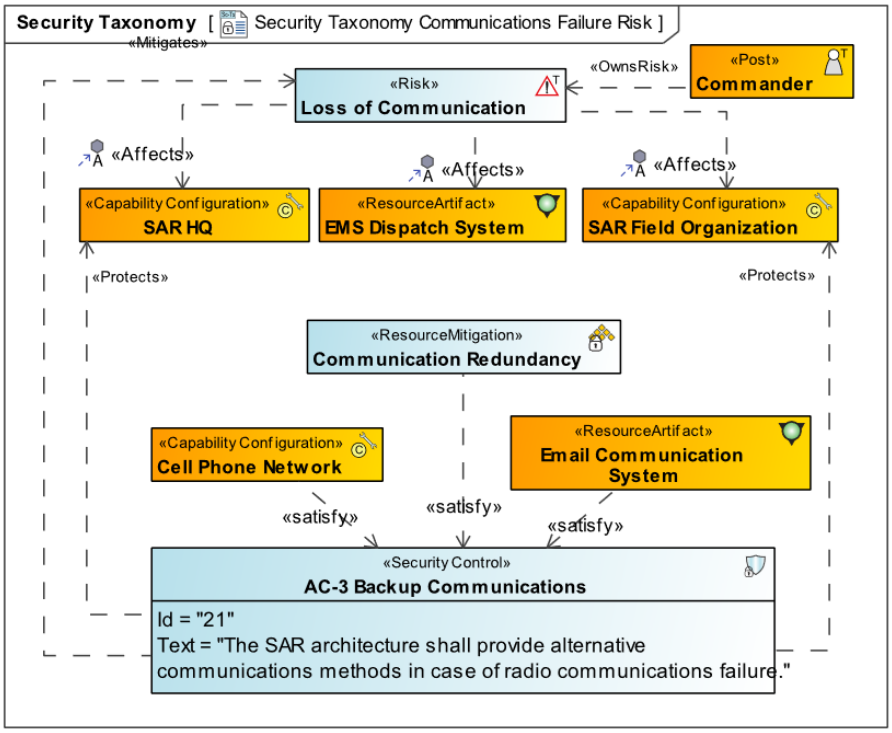

Figure 3 - Security Taxonomy Loss of Communication Risk Elements

The Loss of Communication risk affects the SAR HQ and SAR Field Organization's ability to communicate. The Commander owns this risk and takes responsibility for implementing a solution. Security Controls represent the management, operational, and technical control (i.e., safeguard or countermeasure) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. The AC-3 Backup Communications Security Control is a subtype of a SysML requirement. It defines the requirement for mitigating the Loss of Communications risk and protecting the SAR HQ and SAR Field Organization. The Cell Phone Network and Email Communications systems provide backup communications abilities.

A Resource Mitigation is a set of security measures intended to address specific cyber risks. It comprises a subset of Tailored Security Controls that are used to protect the asset at resource. The Communication Redundancy Resource Mitigation and the backup systems satisfy the Security Control by providing the required alternative communications systems. Other elements such as security processes will be defined to describe failover between systems, failure indications and several other elements. This set of elements and relationships provides the core of the security

view concepts that define how the security views can be used define risks, analyze risk mitigation elements and demonstrate how these provide system security. These and other concepts are further defined in the subsequent sections. Figure 4 shows two security enclaves along with software resource elements used to implement security measures.

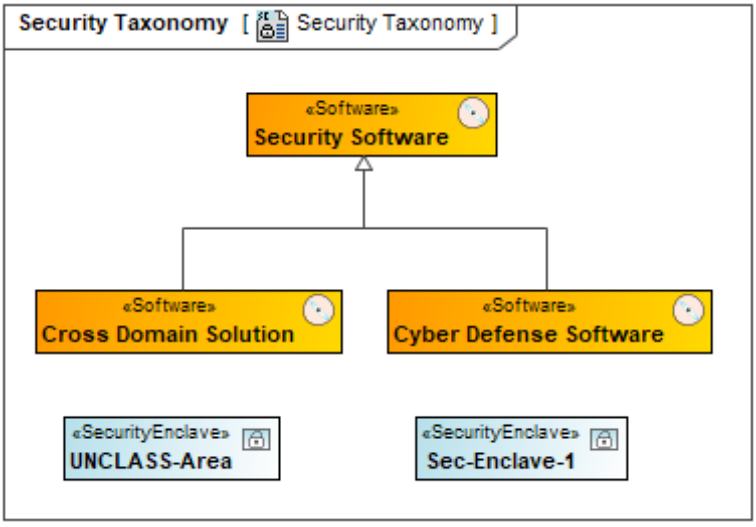

Figure 4 - Security Taxonomy for the Search and Rescue Architecture

Security Structure (Sc-Sr)

The Security Structure view captures the allocation of assets (operational and resource, information and data) across the security enclaves, shows applicable security controls necessary to protect organizations, systems and information during processing, while in storage, and during transmission. It also captures Asset Aggregation and allocates the usage of the aggregated information at a location as shown in Figure 5.

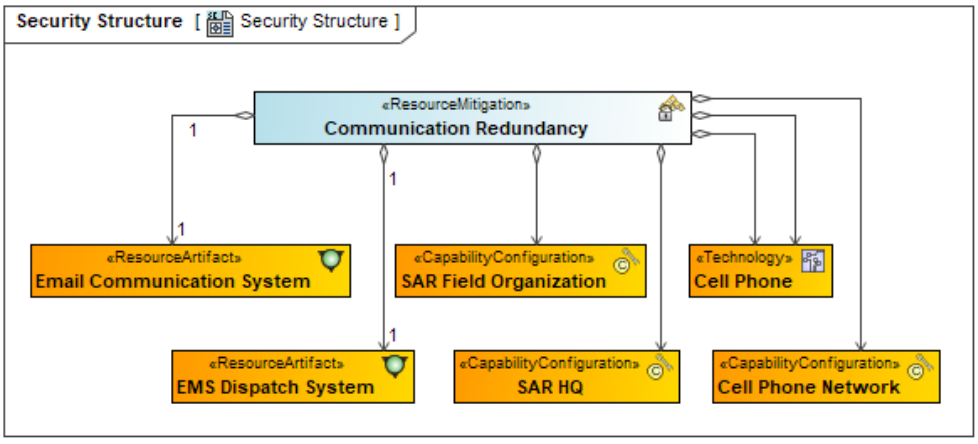

Figure 5 - Security Structure for Communication Redundancy

In this case, Communication Redundancy Resource Mitigation defined earlier is comprised of the SAR Field Organization, SAR HQ and communication technology. The communication technology choices are the email communication system, EMS dispatch system and the cell phone

network. Not all these systems may be used in the final configuration but are included at this stage as they will be compared during trade-off analysis. Along with performance, cost, etc., security controls, levels and methods can be used in the evaluation to compare the efficacy of the communication methods. For example, it may not be financially viable to provide all three systems, all three systems may not be available at all locations, etc.

Security Connectivity (Sc-Cn)

The Security Connectivity view lists security exchanges across security assets; the applicable security controls, resource interfaces and the security enclaves that house the producers and consumers of the exchanges. Figure 6 shows the internal structure for the communication redundancy resource mitigation.

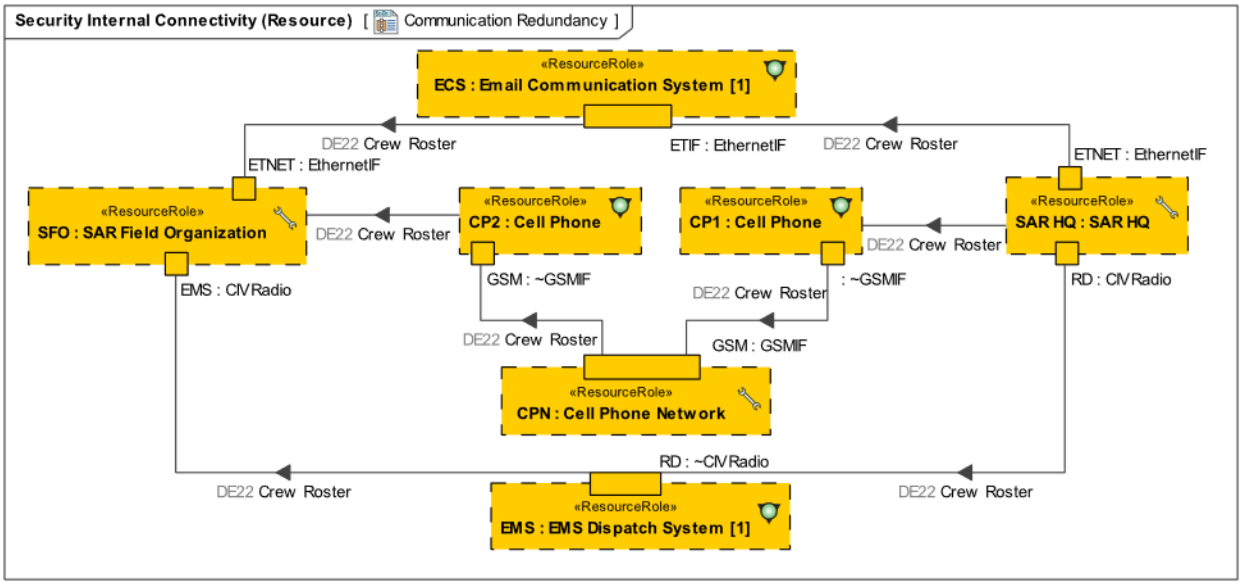

Figure 6 - Internal View of Communication Redundancy

Figure 5 was used to describe the structural breakdown of communication redundancy. Figure 6 shows how they are configured and connected and how the parts communicate. The resource roles are shown as dashed boxes as they also are part of the SAR architecture. The Communication Redundancy resource mitigation is effectively a virtual architecture defined for the resource mitigation demonstrating elements within its domain. In this case the crew roster needs to be distributed from the SAR HQ to the SAR Field Organization. Figure 6 shows the communication paths at a very high level. For example, the crew roster travels from the SAR HQ to the cell phone, to the cell phone network, to the Field Organization, and through the other cell phone. Several other systems have been elided for clarity.

Figure 7 shows the internal structure of the Cyber Defense architecture. These elements were defined in Figure 4, describing the elements on the Security Taxonomy diagram. The Search System communicates with the C2 System to receive tasking orders. The Search System is a civilian system and is in an unclassified enclave.

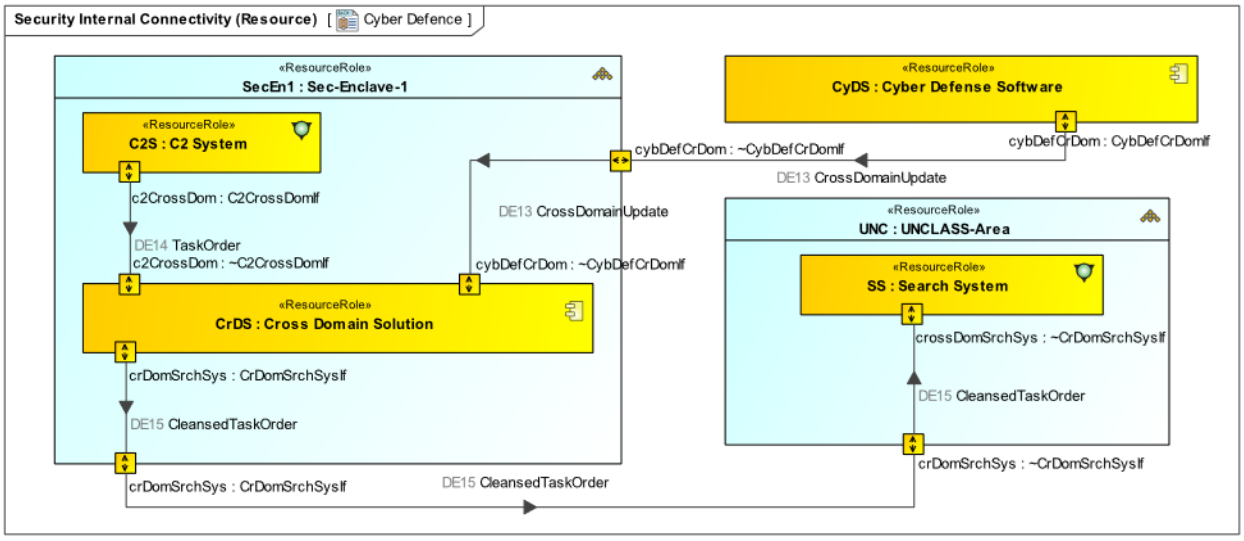

Figure 7 Cyber Defense Architecture

The cross-domain solution is an information assurance system composed of software and hardware, that provides a controlled interface to manually or automatically enable and/or restrict the access or transfer of information between two or more security domains based on a predetermined security policy. The goal of a cross domain solution is to allow interchange without introducing security threats. They are designed to enforce domain separation and typically include some form of content filtering, specifying which information can be transferred between security domains or levels of classification, in this case Sec-Enclave-1 and UNCLASS-Area. Interaction between elements in the architecture can be automatically generated in table form. An example is shown in Table 1.

Table 1 – Security Connectivity Table

#	Exchang ID	Resource Exchange Item	Sending Resource	Receiving Resource	Realized By	securityClass
1	RI10	DE13 CrossDomainUpdate	Cyber Defense Software	Sec-Enclave-1	Resource Connector[CyDS.cybDefCrDom - Secl	Classified
2	RI11	DE13 CrossDomainUpdate	Sec-Enclave-1	Cross Domain Solution	Resource Connector[cybDefCrDom - CrDS.cybI	Classified
3	RI12	DE14 TaskOrder	C2 System	Cross Domain Solution	Resource Connector[C2S.c2CrossDom - CrDS.(	Classified
4	RI13	DE15 CleansedTaskOrder	Cross Domain Solution	Sec-Enclave-1	Resource Connector[CrDS.crDomSrchSys - crD	Classified
5	RI14	DE15 CleansedTaskOrder	Sec-Enclave-1	UNCLASS-Area	Resource Connector[SecEn1.crDomSrchSys - U	Unclassified
6	RI15	DE15 CleansedTaskOrder	UNCLASS-Area	Search System	Resource Connector[crDomSrchSys - SS.cross	Unclassified

The table shows item flows between the systems, the sending and receiving resource, the connector as well as the security classification.

Security Measurements (PM-Me)

Measurement definitions and actual measurements can be defined and reused throughout the architecture. They can be linked to systems, activities and interactions as well as directly integrated into systems as shown in Figure 8.

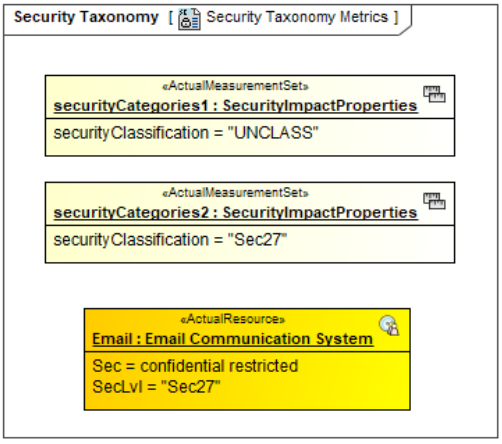

Figure 8 – Actual Security Measurements and Actual Resource with Measurements

Figure 8 shows an actual measurement set defining the security categories of unclassified and security classification Sec27. It also shows the actual resource of the email communication system with its security category and the security classification level.

Security Processes (Sc-Pr)

Security Process sequences view can be defined that execute behaviors associated with security as shown in Figure 9.

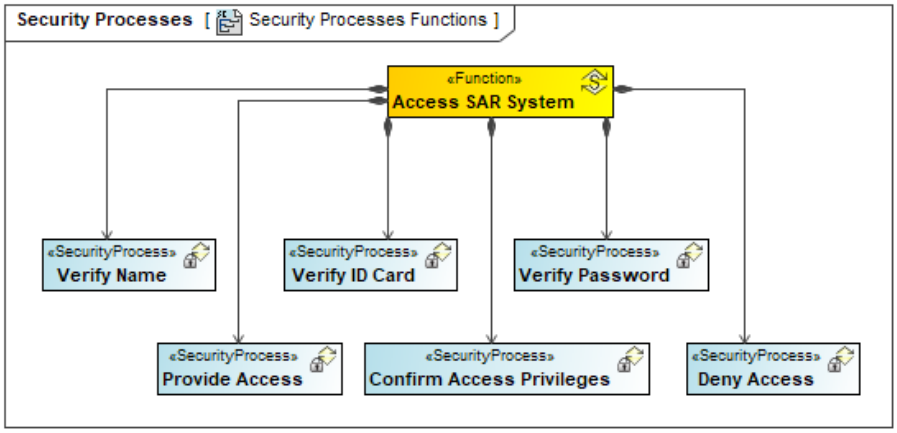

Figure 9 - Security Behavior as part of System Functions

Figure 9 shows a set of security processes that take place to access the SAR system. These can be added to operational or resource activity diagrams to demonstrate logical security measure requirements as well as system function activity diagrams to describe specific security measures and technologies. They can also be shown on state diagrams to describe state-based security behavior.

The SysML activity diagram describes operational or resource level processes that apply (operational level) or implement (resource level) security controls/enhancements to assets located in enclaves and across enclaves. This demonstrates interactions crossing security levels and going in and out of systems. The security processes can be used to demonstrate how the data is protected as well as the assets themselves. These can be used in conjunction with resource functions as shown in Figure 10.

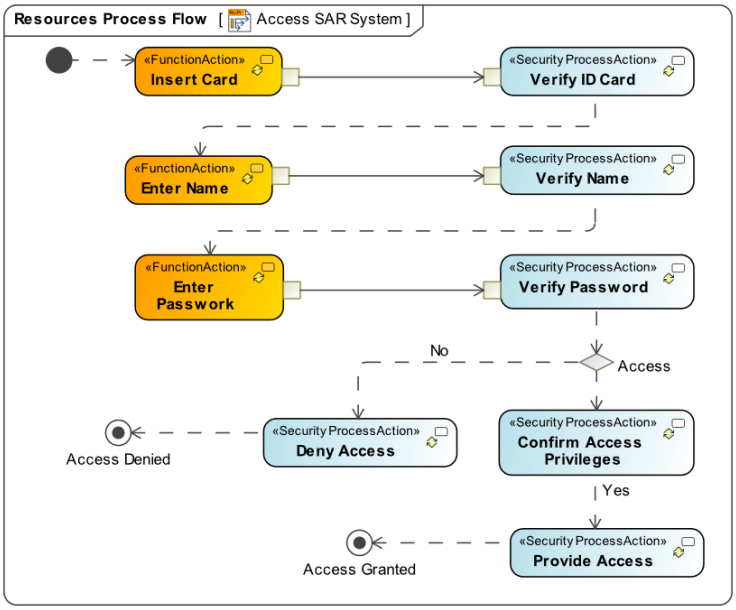

Figure 10 – Access SAR System process Flow Diagram

The activity diagram shown in Figure 10 would be an initial mock-up of the security and functional steps needed to access the SAR system. The final diagram would have swim lanes added corresponding to the implementing systems.

Security Constraints (Sc-Ct)

The Security Constraints view specifies textual rules/non-functional requirements that are security constraints on resources, information and data (e.g. security-related in the form of rules (e.g. access control policy). It identifies risks, specifies risk likelihood, impact, asset criticality, and other measurements that enable risk assessment. Figure 11 shows the security constraints and controls and their relationships to the systems and software. Figure 11 also shows some of the risks (Signal Spoofing, Intrusion and Tampering, and Eavesdropping) and the systems that they affect as well as the person who owns the risks. An enhanced security control demonstrates how additional security can be added. In this case two-step authentication added to the authentication control policy and procedures. This is by no means an exhaustive set of risks and security controls. NIST (2020) lists over 1400 different security controls in its Risk Management Framework RMF SP 800-53. However, this does demonstrate the mechanisms available for the identification of risks and the security controls intended to prevent and mitigate them.

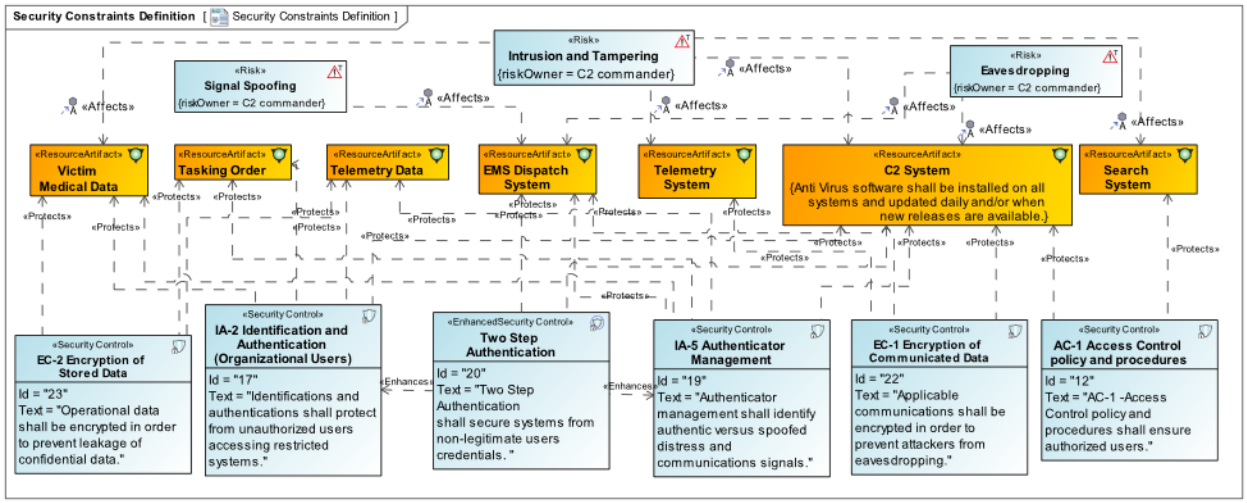

Figure 11 – Security Controls & Constraints for the Search and Rescue

When there is such a multiplicity of relationships on a diagram it is difficult to follow them and visualize them. For this reason, the UAF provides a set of built-in traceability views.

Security Traceability

The Security Traceability (Sc-Tr) domain depicts the mapping of a risk to each of the following: risk owner, risk mitigations, and affected asset roles. The Security Traceability (Sc-Tr) view is represented by: Security Controls to Risks Mapping matrix shows which operational or resource asset roles mitigate risks. The Risks to Assets Mapping matrix shows which risks are applicable to Asset Roles. These are automatically generated from the model. Table 2 is a matrix showing the relationships between the security controls and the elements that they protect.

Table 2 – Protected Resources Matrix

Legend: Protects	Resources Taxonomy: Aircraft Control Subsystem	C2 System	Civilian Boat	Communications	Communications Controller	Distress Monitor Artifact	Distress Signal	Distress Signal Sensor	EMS Dispatch System	Monitor Unit	Radio Equipment	Rescue Craft	Safety Device	Tasking Order	Telemetry Data	Telemetry System	Victim Medical Data	Security Taxonomy [Security]: Cell Phone Network	Civilian	Communication Redundancy	Cyber Defence	SAR Field Organization	SAR HQ	Sec-Enclave-2	Sec-Enclave-3
Security Taxonomy		7			1				6		1			5	5	1	5	1				1	1		
ESC1 Two Step Authentication	2	↗							↗																
SC3 AC-1 Access Control policy and procedures	1	↗																							
SC4 AC-2 Account Management	2								↗								↗								
SC5 AU-3 Content of Audit Records	3	↗												↗	↗										
SC6 AU-5 Response to Audit Processing Failures	3	↗							↗						↗										
SC7 AU-6 Audit Review, Analysis, and Reporting	2													↗			↗								
SC8 IA-2 Identification and Authentication (Organizat	4	↗												↗	↗		↗								
SC9 IA-4 Identifier Management																									
SC10 IA-5 Authenticator Management	5	↗							↗					↗	↗		↗								
SC11 AC-3 Backup Communications	3				↗				↗		↗							3	↗			↗	↗		
SC12 EC-1 Encryption of Communicated Data	3	↗							↗							↗									
SC13 EC-2 Encryption of Stored Data	3													↗	↗		↗								

The elements across the top represent the protected resources. The elements along the left represent the security controls defined in Figure 11. The arrows in the matrix represent a resource that is protected by a security control.

Security Integrated into Other views

As stated earlier, security is a cross cutting construct. As a result, it needs to be integrated into the architecture. This was demonstrated in Figures 5 & 9. Security elements can also be included in the other UAF views. Figure 12 shows elements of the SAR architecture and their security enclaves.

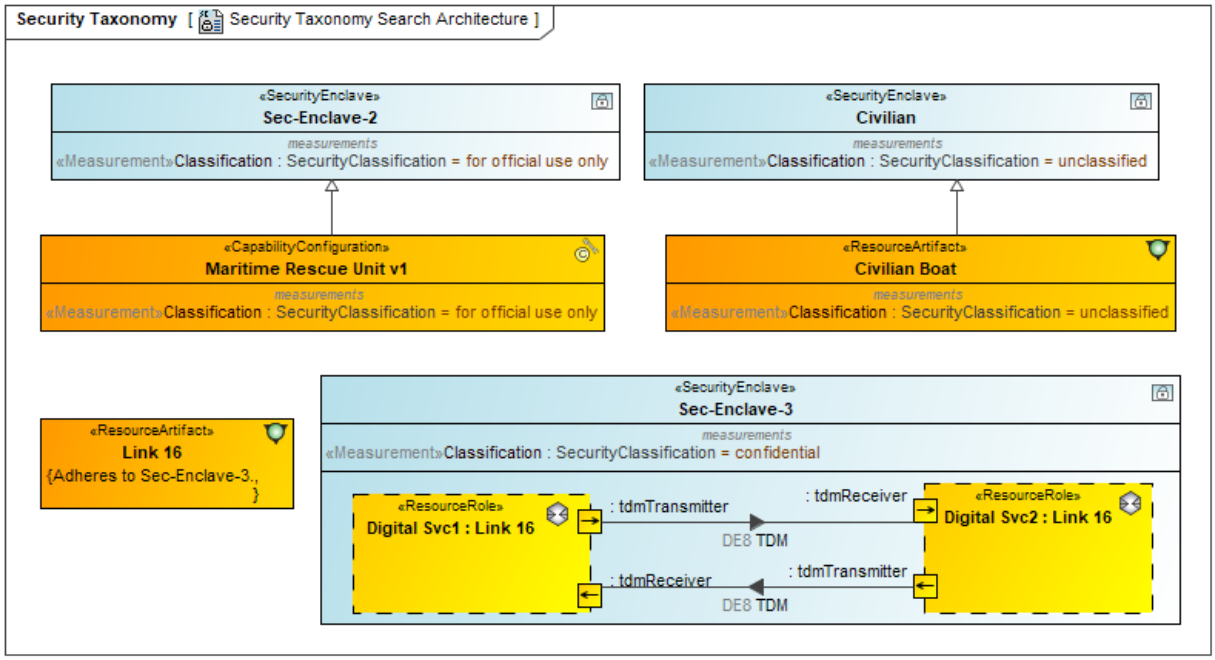

Figure 12 Security Enclaves for SAR Elements

By means of inheritance, the Maritime Rescue Unit has been placed in the Sec-Enclave-2 and the Civilian Boat in the Civilian enclave. This avoids placing the enclave elements within the total architecture as resource roles which essentially just adds one more layer of abstraction within the overall resource architecture without any additional data except for an indication of a given security policy. Using enclaves within a complete resource architecture can have problematic consequences. It could well be that the part of the system containing the two Link 16 tactical radios have another security classification as regards their internal communication but that they both have a way to cross a classification boundary when dealing with the ESM system. Note that as Link 16 is an encrypted technology they comply with the security controls defined in Figure 11. It would be problematic to include a security enclave around the tactical radios in the architecture since they have been placed in different elements here (the helicopter and the rescue ship). A Sec-Enclave-3 enclave has been defined that shows two tactical radios communicating with one another under a defined classification. The mere fact that security is crosscutting indicates that there is a need to be able to handle enclaves separately from a concrete resource architecture. Therefore, a security enclave for increased security for the tactical radios would only show them communicating. The port with the external interface towards the ESM system would not be visible in this security enclave definition.

Figure 13 shows the Maritime Rescue Architecture and its enclosed systems. The civilian boat, personnel and communication systems are shown on the left. The rescue systems, personnel and communication systems are shown on the right.

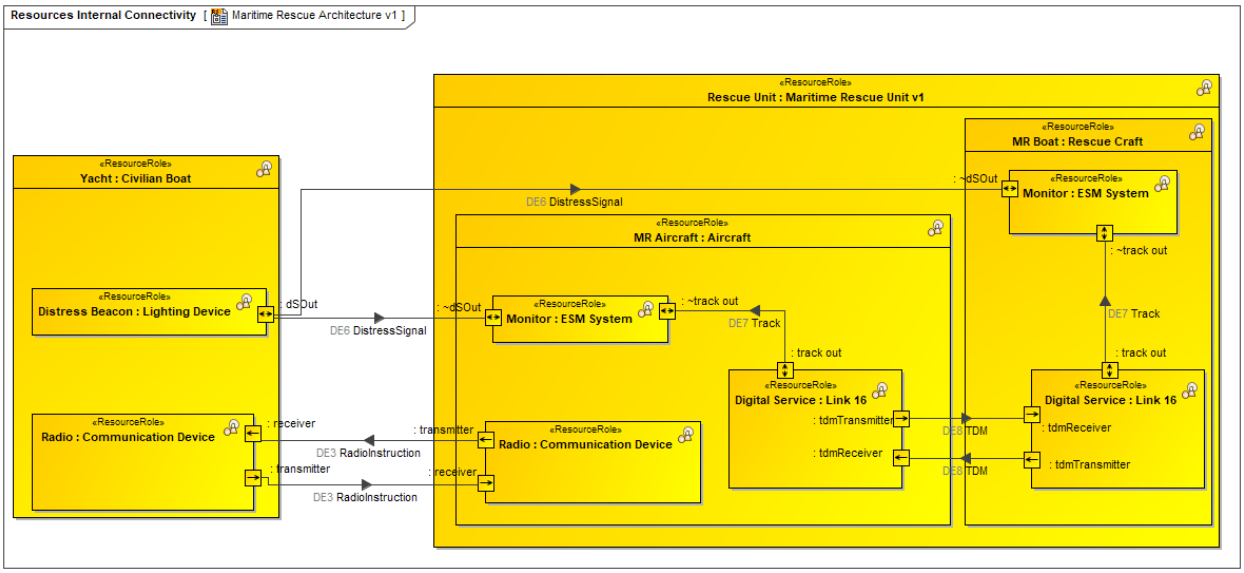

Figure 13 – Maritime Rescue Architecture Internal View

Figure 13 shows the internal structure of the Maritime Rescue Architecture. The previously defined security controls and elements will allow the two systems to communicate and collaborate without security issues. Risks have been identified and mitigated and the architecture is secure.

Summary and Conclusions

The UAF describes enterprise and system architectures as well as an integrated set of security views. The security views provide a means of defining the security requirements and issues at the start of the project in a set of separate views. They also provide a means of integrating security into the different views to highlight security vulnerabilities and demonstrate how they may be mitigated. These security views provide the architecture options that can be expressed to assist in trade off analysis and evaluation of alternatives. The UAF views promote a proactive treatment of cyber security, cyber resilience, risk analysis, security measures, vulnerability management, and incident response planning in the architecture while it is being developed. Resource mitigation defines the alternatives for mitigating security risks in the architecture. The measures shown in the UAF sample problem show the benefit of addressing vulnerabilities while the architecture is being developed. These provide a quantitative and qualitative means of analyzing security alternatives. In addition to cyber security issues, the UAF has been used on various projects to identify and analyze other types of risk such as project risk, physical security risk, system and safety risk. Having identified these risks, they are then handed over to specialist and specialty tools to perform the detail analysis and mitigation. By identifying them early and at the enterprise level, they can be addressed in a more effective, economical and system-wide manner. It is this type of systems thinking and systems of systems thinking that that the UAF was developed for and will continue to be used. These views will be updated in the example architecture in the example model for the UAF to ensure that users will get the guidance necessary to provide safe and secure systems. In

addition, changes are being planned for UAF 1.2 to expand the use of risk and address other security domain issues.

References

Ars Technica, “Operation Shady RAT: five-year hack attack hit 14 countries”, 3-Aug-2011, available from https://arstechnica.com/information-technology/2011/08/operation-shady-rat-five-year-hack-attack-hit-14-countries/

Atherton, 2020, "Starting Dec. 1, Cybersecurity Is No Longer Optional", Available at https://breakingdefense.com/2020/11/starting-dec-1-cybersecurity-is-no-longer-optional/

Dahmann, J., G. Rebovich, J. Lane, R. Lowry. 2010. “System Engineering Artifacts for SoS.” Paper presented at the 4th Annual IEEE Systems Conference, San Diego, US-CA, 5-8 April.

Department of Defense (DoD). 2013. Defense Acquisition Guidebook. http://at.dod.mil/docs/DefenseAcquisitionGuidebook.pdf

DoDAF DoD CIO, 2012, DoD Architecture Framework Version 2.02, DoD Deputy Chief Information Officer, Available online at http://dodcio.defense.gov/dodaf20/dodaf20_pes.aspx, accessed June, 2014.

Dove, R, Willett, K, 2020, “Techno-Social Contracts for Security Orchestration in the Future of Systems Engineering”, presented at the INCOSE 30th Annual Symposium in Capetown, July 18-23, 2020.

Hause, M. 2014. “SOS for SoS: A New Paradigm for System of Systems Modeling.” Paper presented at the IEEE, AIAA Aerospace Conference, Big Sky, US-MT, 1-8 March.

Hause, M., F. Dandashi, 2015. “UAF for System of Systems Modeling , Systems Conference (SysCon).” Paper Presented at the 9th Annual IEEE Systems Conference, Vancouver, CA-BC, 13-16 April.

Hause, M., 2020, Integrating Security into Enterprise Architecture with UAF and PLE, Published in INCOSE Insight Magazine.

INCOSE SE Vision 2020. 2007. http://www.incose.org/ProductsPubs/pdf/SEVision2020_20071003_v2_03.pdf.

Morgan, S, 2019, "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021" available at: https://cybersecurityventures.com/jobs/

MOD Architectural Framework, Version 1.2, 2020, Office of Public Sector Information, https://www.gov.uk/guidance/mod-architecture-framework/

NATO Architecture Framework Version 4, January 2018, Architecture Capability Team Consultation, Command & Control Board

NIST, 2020, NIST Risk Management Framework RMF SP 800-53 available at: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1

Object Management Group (OMG). 2013. OMG2013-08-04:2013. Unified Profile for DoDAF/MODAF (UPDM) V2.1, http://www.omg.org/spec/UPDM/2.1/PDF

———————————. 2012. OMG2012-06-01.OMG Systems Modeling Language (OMG SysML™), V1.3, http://www.omg.org/spec/SysML/1.3/PDF/.

Object Management Group (OMG), 2019, The Unified Architecture Framework, (UAF) Available from https://www.omg.org/spec/UAF

Perhach, P, Nov 7, 2018, “The Mad Dash to Find a Cybersecurity Force”, Published in the NY Times, available at https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html0

Purplesec.us, 2020, 2020 “Cyber Security Statistics, The Ultimate List Of Stats, Data & Trends”, available from: https://purplesec.us/resources/cyber-security-statistics/#:~:text=Nearly%2060%20million%20Americans%20have,target%20for%20targeted%20cyber%20attacks.

Biography

Lars-Olof Kihlström. Lars-Olof Kihlström is a principal consultant at Syntell AB where he has worked since 2013, primarily in the area of MBSE. He has been a core member of the UAF group within the OMG since its start as the UPDM group. He was involved in the development of NAF as well as MODAF. He has worked with modelling in a variety of domains such as telecommunications, automotive, defence as well as financial systems. He is specifically interested in models that can be used to analyze the behavior of system of systems.

Matthew Hause. Matthew Hause is a principal consultant at SSI, a member of the UAF group, and a member of the OMG SysML specification team. He has been developing multi-national complex systems for almost 40 years as a systems and software engineer. He worked in the power systems industry, command and control systems, process control, SCADA, military systems, and many other areas. His role at SSI includes consulting, mentoring, standards development, specification of the UAF profile and training.