33rd Annual INCOSE international symposium
hybrid event
Honolulu, HI, USA
July 15 - 20, 2023

Model-Based Cybersecurity at the Enterprise and Systems Level

Mitchell Brooks: System Strategy Inc.

Matthew Hause: System Strategy Inc.

Introduction to the Authors

- Mitchell Brooks
  - Cyber Systems Engineer for Systems Strategy, Inc.
  - Degree in Cybersecurity from Stevens Institute of Technology
  - MBA from Saint Mary's College of California

- Matthew Hause
  - Principal Systems Engineer for Systems Strategy, Inc.
  - Decades of systems engineering experience
  - Chair of the OMG UAF Group, member of SysML V2 specification team

Agenda

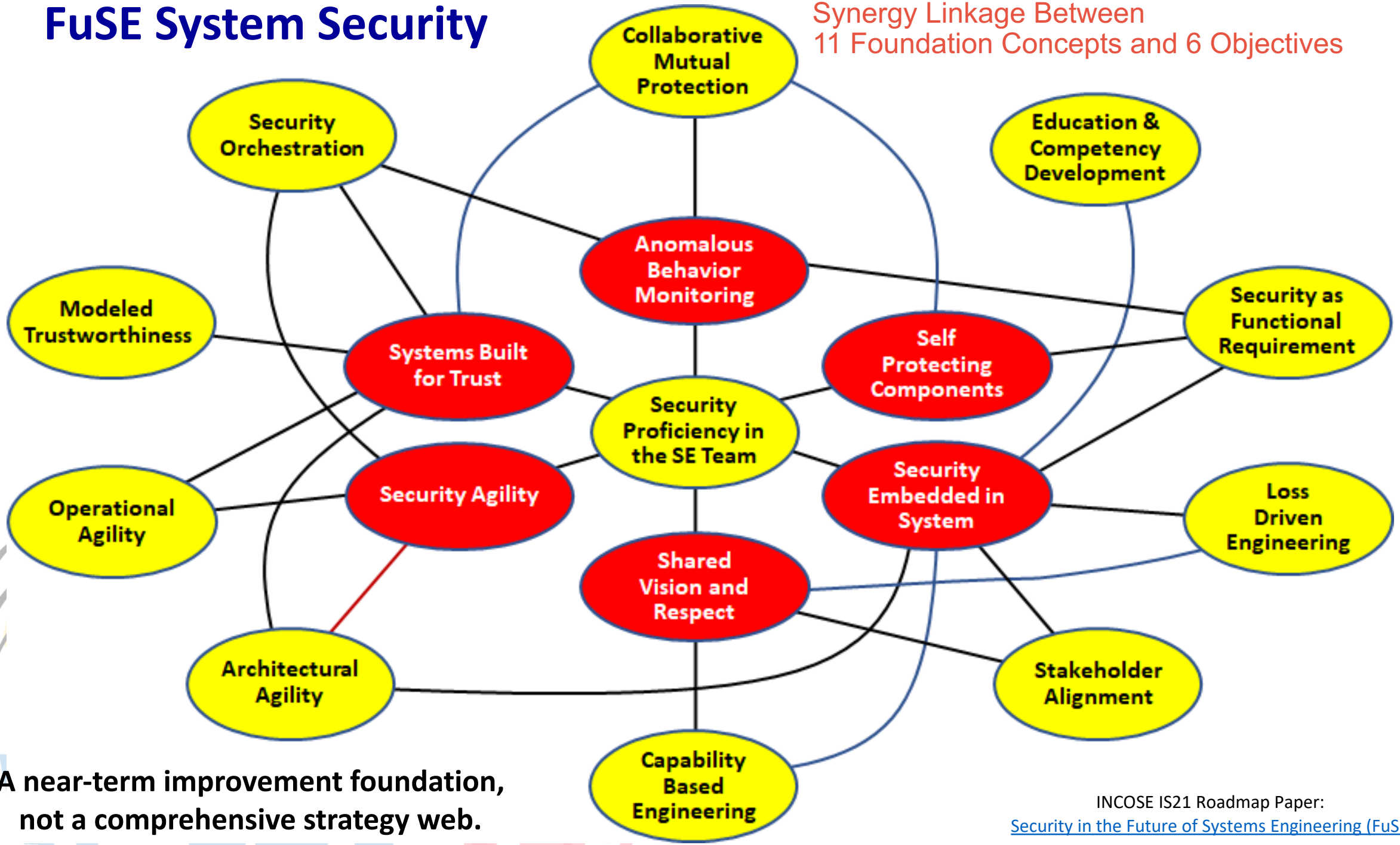
- Introduce main ideas
- Why model cybersecurity?
- Common drawbacks and pitfalls of current cybersecurity modeling
- Brief introduction to UAF
- Main benefits of utilizing UAF
- The importance of capability-based engineering
- Cybersecurity in the digital thread
- Conclusion
- Q/A

Main Ideas

- Using MBSE to model cybersecurity of IT systems helps to provide clearer and more effective solutions to the most common problems faced by cybersecurity and IT professionals
- Capability-based engineering ensures desired outcomes are met
- When modeling IT Systems and their security, UAF provides clear benefits
  - The ability to treat cybersecurity as an enterprise
  - The systems of systems view can be used to model both cybersecurity *within* IT systems and the cyber systems themselves
  - The specialized security viewpoints

FuSE System Security

Synergy Linkage Between
11 Foundation Concepts and 6 Objectives



A near-term improvement foundation, not a comprehensive strategy web.

INCOSE IS21 Roadmap Paper:
Security in the Future of Systems Engineering (FuSE)

Why do we need to model Cybersecurity?

- Cybersecurity is both very complex and misunderstood, even among those in tech
- The decision makers for cybersecurity are often not the subject matter experts
- Even cybersecurity experts don’t always speak the same “language”
- Utilizing a common language which is accessible to both SMEs and decision makers leads to better outcomes
- Helps overcome the issues of “problemeering” and “solutioneering” and drives towards capability-based engineering

Common pitfalls when modeling cybersecurity

- Implementation based approach
  - Often overly idealistic
- Functional based approach
  - Specific actions and services are laid out, no connection to the real world
- Both too often sequester and isolate security
- Solutioneering”
  - Make the predefined solution fit the requirements
- “Problemeering”
  - Concentration on the requirements without recognizing true need.
  - What customers want is not often what they need
  - Henry Ford vs. Steve Jobs
    - Faster horses and anticipating customer needs

Unified Architecture Framework (UAF)

- The UAF is an implementation of DoDAF, MODAF, NAF, and DNDAF frameworks in SysML with additional security views.
- The UAF is used for architecting enterprises, systems of systems, family of systems, and individual systems
- It is focused on the scope, needs, strategy, expectations, stakeholders, and long-term plans
- It is built on SysML, so has built-in traceability to system development in SysML.
- Not ***just*** defense focused, but applicable to commercial as well

Great for organizations to figure out what they are doing and why.

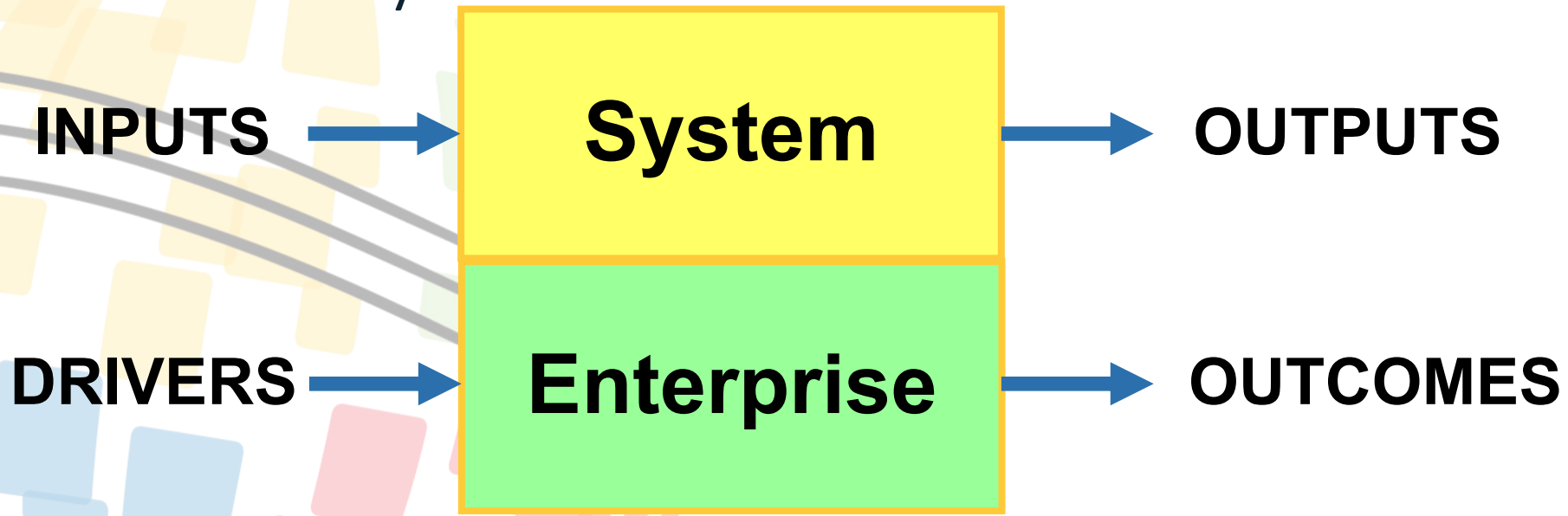
UAF
OMG UNIFIED ARCHITECTURE FRAMEWORK™

	Taxonomy Tx	Structure Sr	Connectivity Cn	Processes Pr	States St	Interaction Scenarios Is	Information If	Parameters Pm	Constraints Ct	Roadmap Rm	Traceability Tr
Metadata Md	Metadata Taxonomy Md-Tx	Architecture Viewpoints [a] Md-Sr	Metadata Connectivity Md-Cn	Metadata Processes [a] Md-Pr	-	-			Metadata Constraints [a] Md-Ct		Metadata Traceability Md-Tr
Strategic St	Strategic Taxonomy St-Tx	Strategic Structure St-Sr	Strategic Connectivity St-Cn	-	Strategic States St-St	-			Strategic Constraints St-Ct	Strategic Deployment, St-Rm Stategic Phasing St-Rm	Strategic Traceability St-Tr
Operational 0p	Operational Taxonomy Op-Tx	Operational Structure Op-Sr	Operational Connectivity Op-Cn	Operational Processes Op-Pr	Operational States Op-St	Operational Interaction Scenarios Op-Is			Operational Constraints Op-Ct	-	-
Services Sv	Service Taxonomy Sv-Tx	Service Structure Sv-Sr	Service Connectivity Sv-Cn	Service Processes Sv-Pr	Service States Sv-St	Service Interaction Scenarios Sv-Is	Conceptual Data Model,	Environment Pm-En	Service Constraints Sv-Ct	Service Roadmap Sv-Rm	Service Traceability Sv-Tr
Personnel Pr	Personnel Taxonomy Pr-Tx	Personnel Structure Pr-Sr	Personnel Connectivity Pr-Cn	Personnel Processes Pr-Pr	Personnel States Pr-St	Personnel Interaction Scenarios Pr-Is	Logical Data Model,		Competence, Drivers, Performance Pr-Ct	Personnel Availability, Personnel Evolution, Personnel Forecast Pr-Rm	Personnel Traceability Pr-Tr
Resources Rs	Resource Taxonomy Rs-Tx	Resource Structure Rs-Sr	Resource Connectivity Rs-Cn	Resource Processes Rs-Pr	Resource States Rs-St	Resource Interaction Scenarios			Resource Constraints Rs-Ct	Resource evolution, Resource forecast Rs-Rm	Resource Traceability Rs-Tr
Security Sc	Security Taxonomy Sc-Tx	Security Structure Sc-Sr	Security Connectivity Sc-Cn	Security Processes Sc-Pr	-	-	world results	Measurements Pm-Me	Security Constraints Sc-Ct	-	-
Projects Pj	Project Taxonomy Pj-Tx	Project Structure Pj-Sr	Connectivity Pj-Cn	-	-	-			-	Project Roadmap Pj-Rm	Project Traceability Pj-Tr
Standards Sd	Standard Taxonomy Sd-Tx	Standards Structure Sd-Sr	-	-	-	-			-	Standards Roadmap Sr-Rm	Standards Traceability Sr-Tr
Actuals Resources Ar		Actual Resources Structure, Ar-Sr	Actual Resources Connectivity, Ar-Cn	Simulation [b]					Parametric Execution/ Evaluation [b]	-	-
Dictionary * Dc											
Summary & Overview SmOv											
Requirements Rq											

Benefits of Utilizing UAF

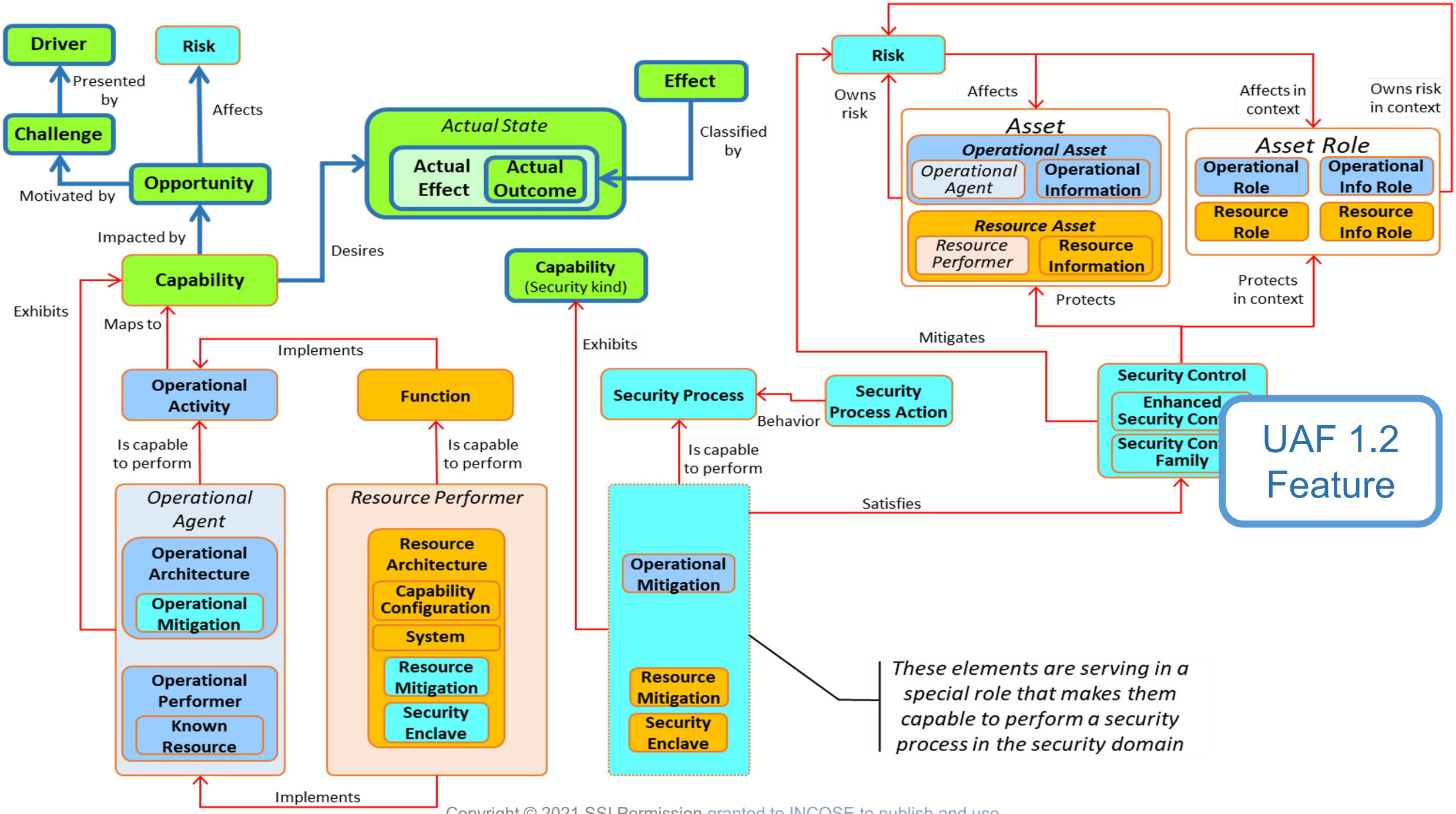
Benefit #1 - Security as an Enterprise

- Cyber is too often treated as a system part
- The solution? Think of it as an enterprise
  - "a human undertaking or venture that has explicit and clearly defined mission, goals, and objectives to offer products or service, or to achieve a desired project outcome or business outcome" (ISO 15704).
- UAF is specifically designed to help model these enterprises
  - Allows the ability to model across time



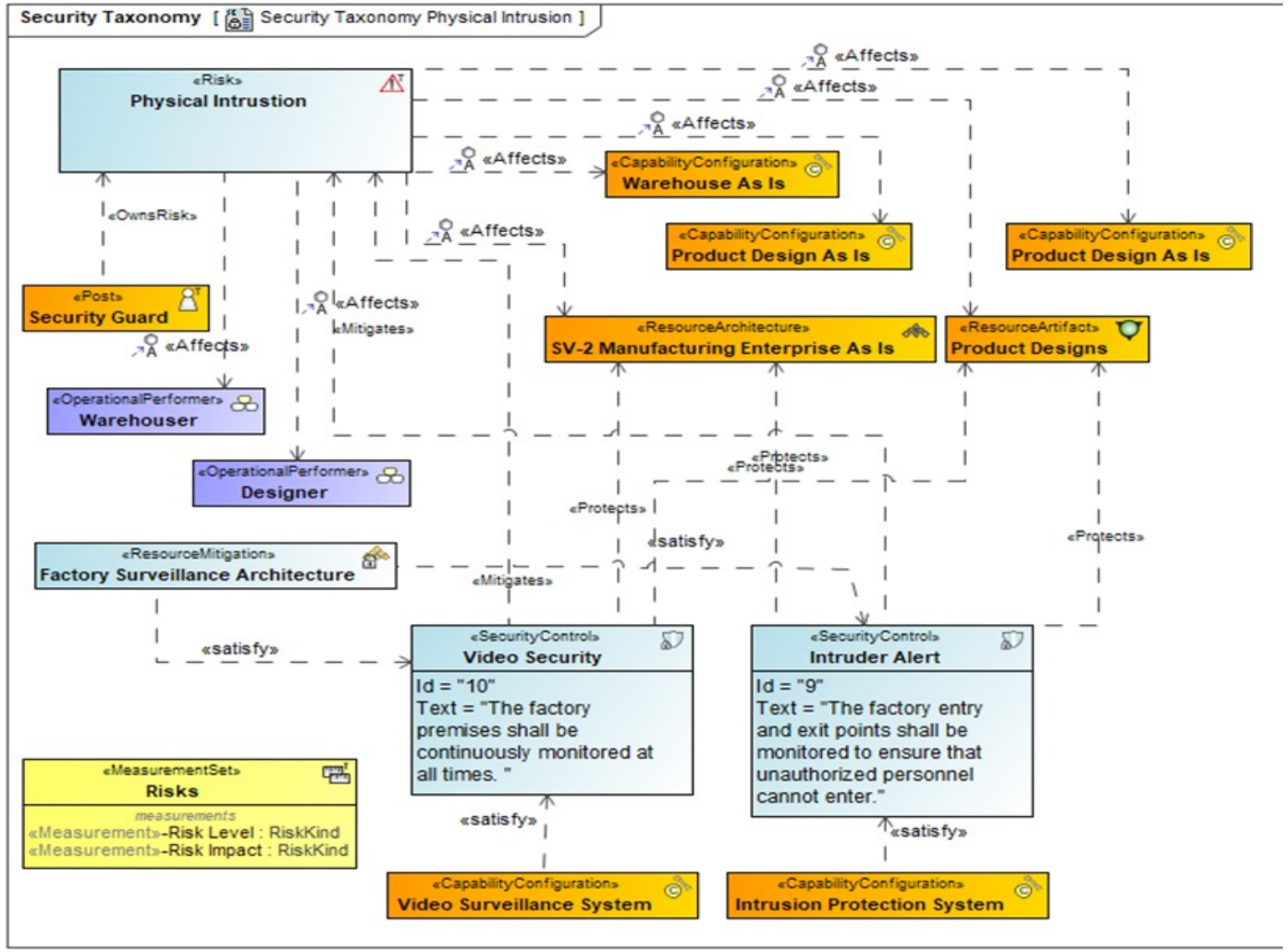
Benefit #2 – Security as a System of Systems

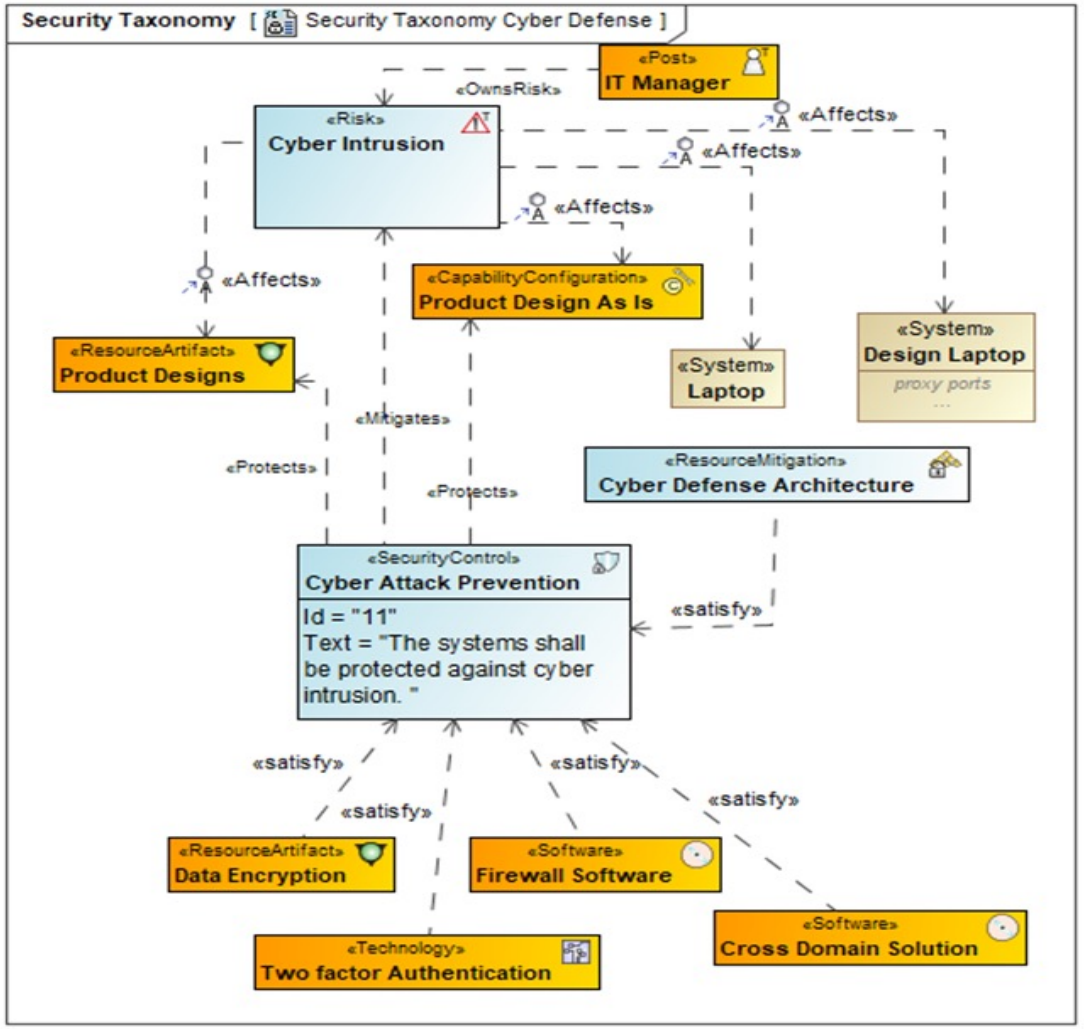
- Most IT systems are a patchwork of smaller technologies and systems
  - The average IT department utilizes an average of 75 products just to secure their network (CSO Online)
- UAF is perfectly designed to help capture these quirks
- Modeling interactions and relationships between these systems is quite literally what UAF was built to do



Risks, Mitigations and Controls

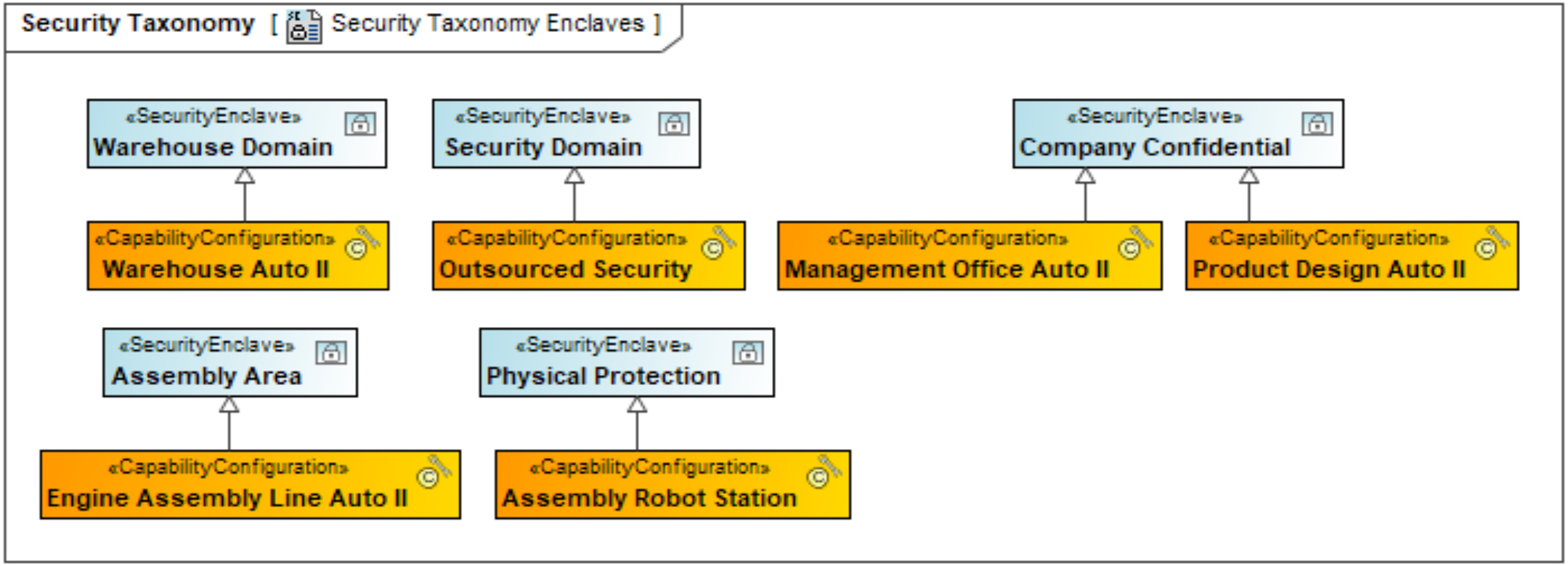
- Physical and Cyber risks are identified along with applicable security controls, modeled as requirements
- Mitigations and owners identified and risks are further quantified.





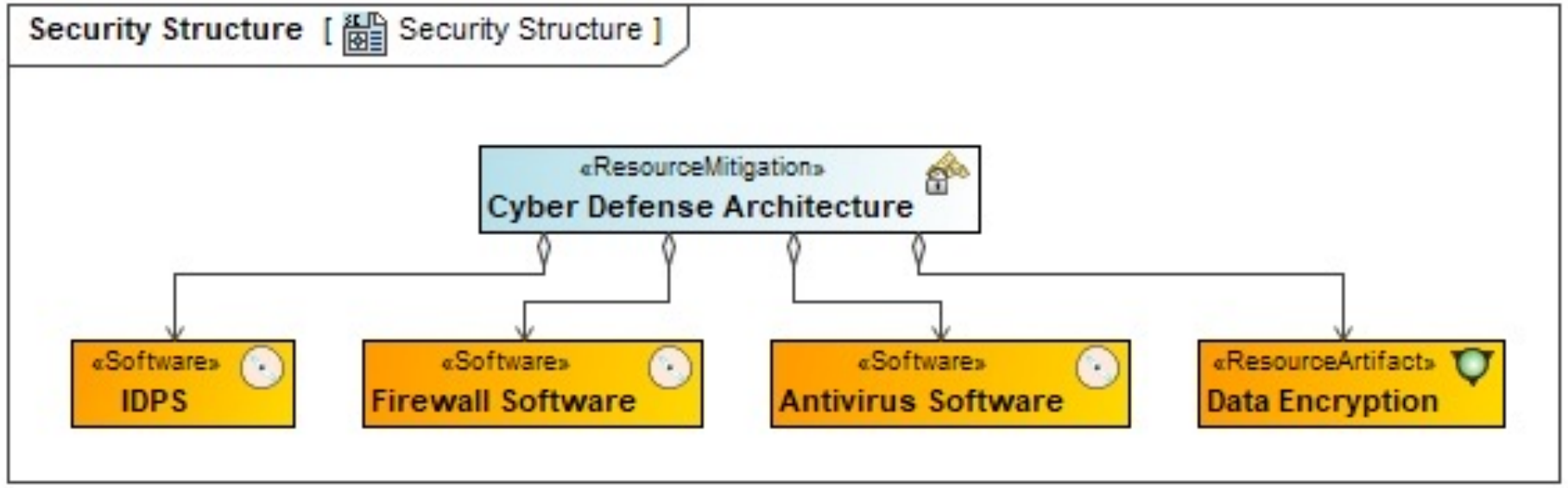
Security Enclave Defined

- Security enclaves are identified for the defined systems and physical areas
- Defined enclaves can combine all three security capabilities if required
  - The assembly area will need physical, IT and personnel safety
  - Security control implementations defined earlier are owned by the enclave and inherited by the systems
  - Common response to common problems and risks



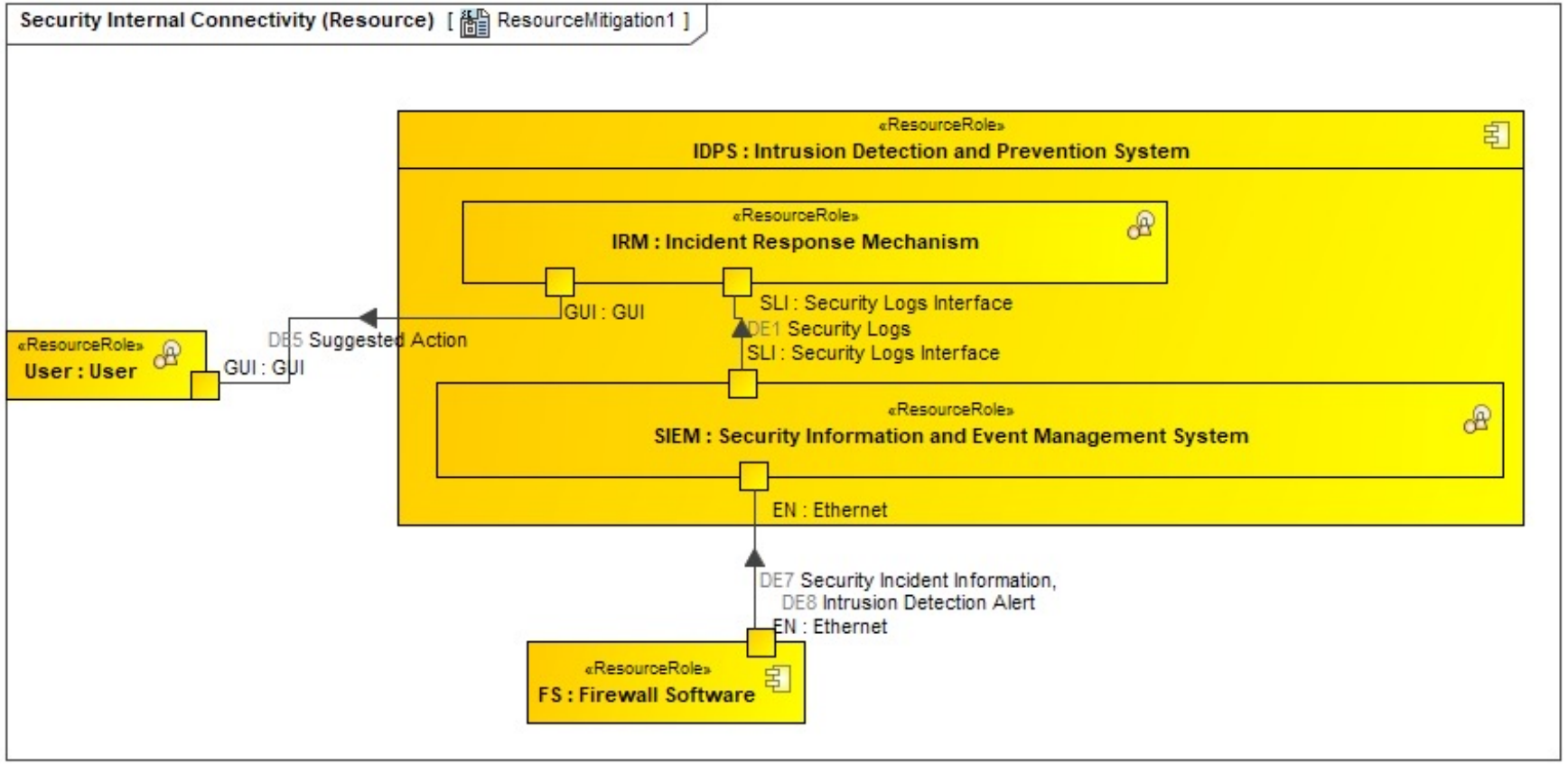
UAF Security Viewpoint – Security Structure

- Having defined the risks, we create a breakdown of the cyber defense architecture, allowing us to logically group the systems contained within the IT infrastructure to mitigate the risk



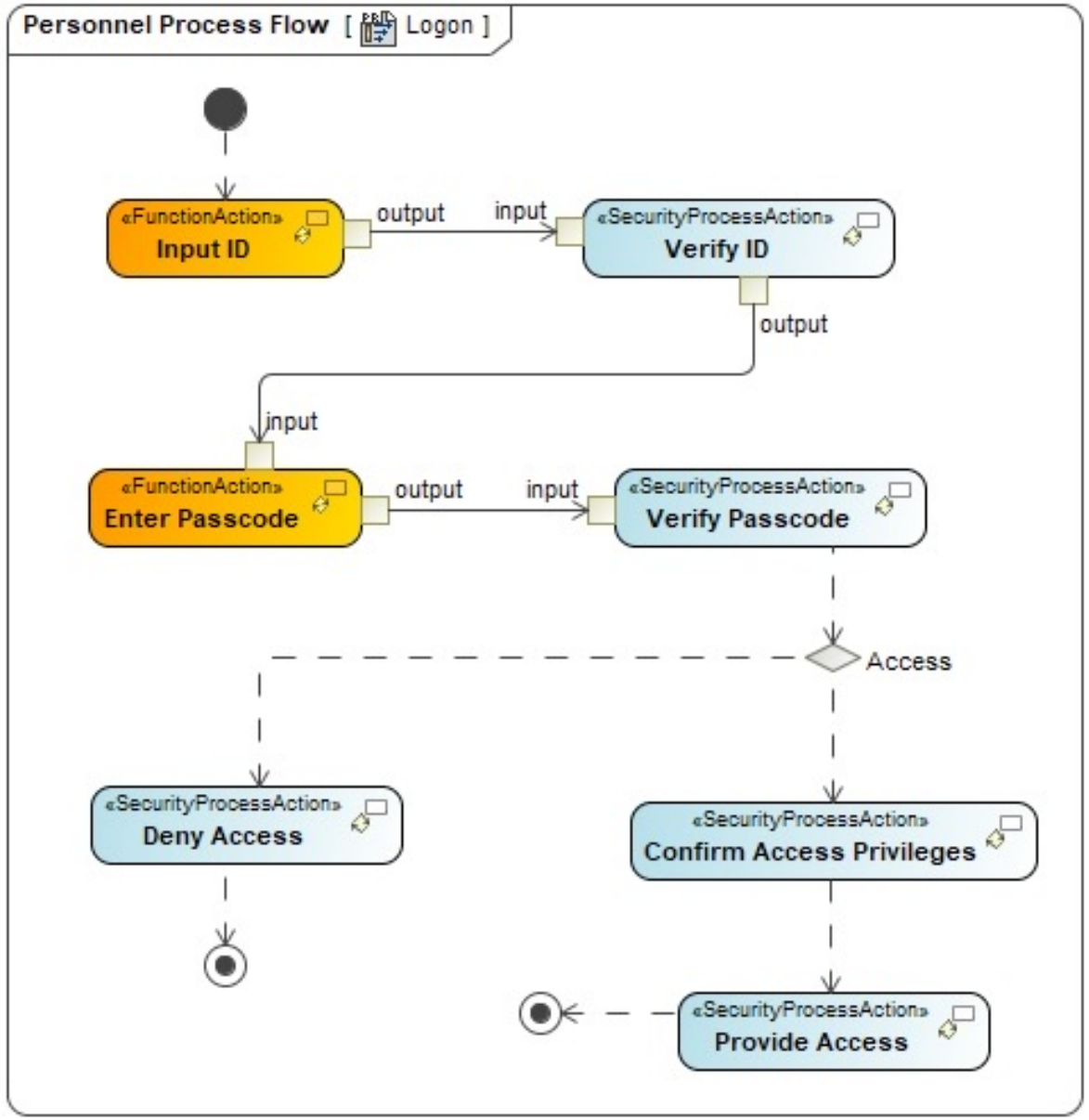
UAF Security Viewpoint – Security Internal Connectivity

- The aforementioned 75 technologies that are included within the average IT system are often implemented without regard to how they interact.
- By modeling these systems, we ensure that the interfaces, communications, and interactions between these systems are possible and achieve their desired effects



UAF Security Viewpoint – Security Processes

- Implements security as a functional requirement (FuSE)
- This diagram provides a gray-box view by showing how a user will interact with the security elements
- The processes are implemented by the previously defined systems



Benefit #4 UAF is Mandated

Defense Information Standards Registry (**DISR**) record

Standard Reference Number	Standard Identifier	Standard Title	Standard Class	DoD Status
301131	OMG UPDM v2.1	Unified Profile for the Department of Defense Architecture Framework (DoDAF) and the Ministry of Defence Architecture Framework (MODAF), Version 2.1, formal/2013-08-04	DISR	Retired
302737	OMG UAFP v1.0	Unified Architecture Framework Profile (UAFP) v1.0, OMG formal/2017-12-01, November 2017 including all normative appendices.	DISR	Emerging

Mandated November 10, 2021

Benefit #5 UAF Implements Industry Best Prac

Infor

Cameo Enterprise Architecture 19.0 - NIST SP 800-53r5 Security Controls.mdzip [C:\Users\MatthewHause\Downloads\]

File Edit View Layout Diagrams Options Tools Analyze Collaborate Window Help

Preview: - no preview - | Full Model | Perspective: UAF Architect | Create Diagram

Containment | Diagrams

Containment

- Model «ModelLibrary»
  - Security
    - Security Taxonomy
      - AC - Access Control
        - AC Enhancements
          - Relations
          - AC Enhancements Table
          - Access Control Decisions | No User or Process Identi
          - Access Control Decisions | Transmit Access Authoriz
          - Access Control for Mobile Devices | Full Device or Cc
          - Access Control for Mobile Devices | Restrictions for (
          - Access Enforcement | Assert and Enforce Applicatior
          - Access Enforcement | Attribute-based Access Contrc
          - Access Enforcement | Audited Override of Access Cc
          - Access Enforcement | Controlled Release «Enhancec
          - Access Enforcement | Discretionary Access Control «
          - Access Enforcement | Discretionary and Mandatory A
          - Access Enforcement | Dual Authorization «Enhanced
          - Access Enforcement | Individual Access «EnhancedS
          - Access Enforcement | Mandatory Access Control «Er
          - Access Enforcement | Restrict Access to Specific Infc
          - Access Enforcement | Revocation of Access Authoriz
          - Access Enforcement | Role-based Access Control «E
          - Access Enforcement | Security-relevant Information
          - Account Management | Account Monitoring for Atypi
          - Account Management | Automated Audit Actions «Er
          - Account Management | Automated System Account I
          - Account Management | Automated Temporary and E

Security Controls Table

Add New | Add Existing... | Delete | Remove From Table

Criteria

Element Type: Security Control,Security Control Fa ... Scope (optional): Security Taxonomy ... Filter:

#	Id	Name	Enhanced Security Control
1		AC - Access Control	
2	AC	AC - Access Control	
3	AC-1	Access Control Policy and Procedures	
4	AC-2	Account Management	Account Management | Account Monitoring for Atypical Usage Account Management | Automated Audit Actions Account Management | Automated System Account Management Account Management | Automated Temporary and Emergency Account Managem Account Management | Disable Accounts Account Management | Disable Accounts for High-risk Individuals Account Management | Dynamic Account Management Account Management | Dynamic Privilege Management Account Management | Inactivity Logout Account Management | Privileged User Accounts Account Management | Restrictions on Use of Shared and Group Accounts Account Management | Usage Conditions
5	AC-3	Access Enforcement	Access Enforcement | Assert and Enforce Application Access Access Enforcement | Attribute-based Access Control Access Enforcement | Audited Override of Access Control Mechanisms Access Enforcement | Controlled Release Access Enforcement | Discretionary Access Control Access Enforcement | Discretionary and Mandatory Access Control Access Enforcement | Dual Authorization Access Enforcement | Security-relevant Information

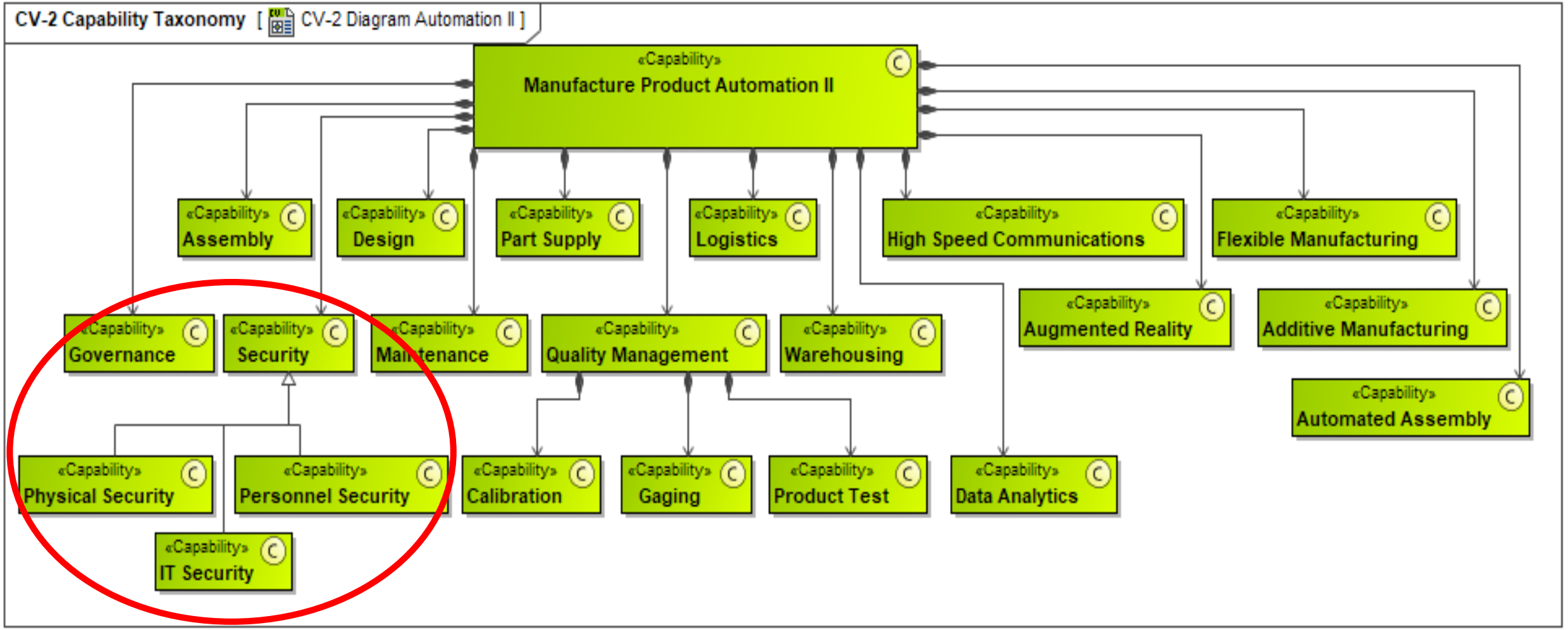
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

OSE to publish and use.

Capability Based Engineering

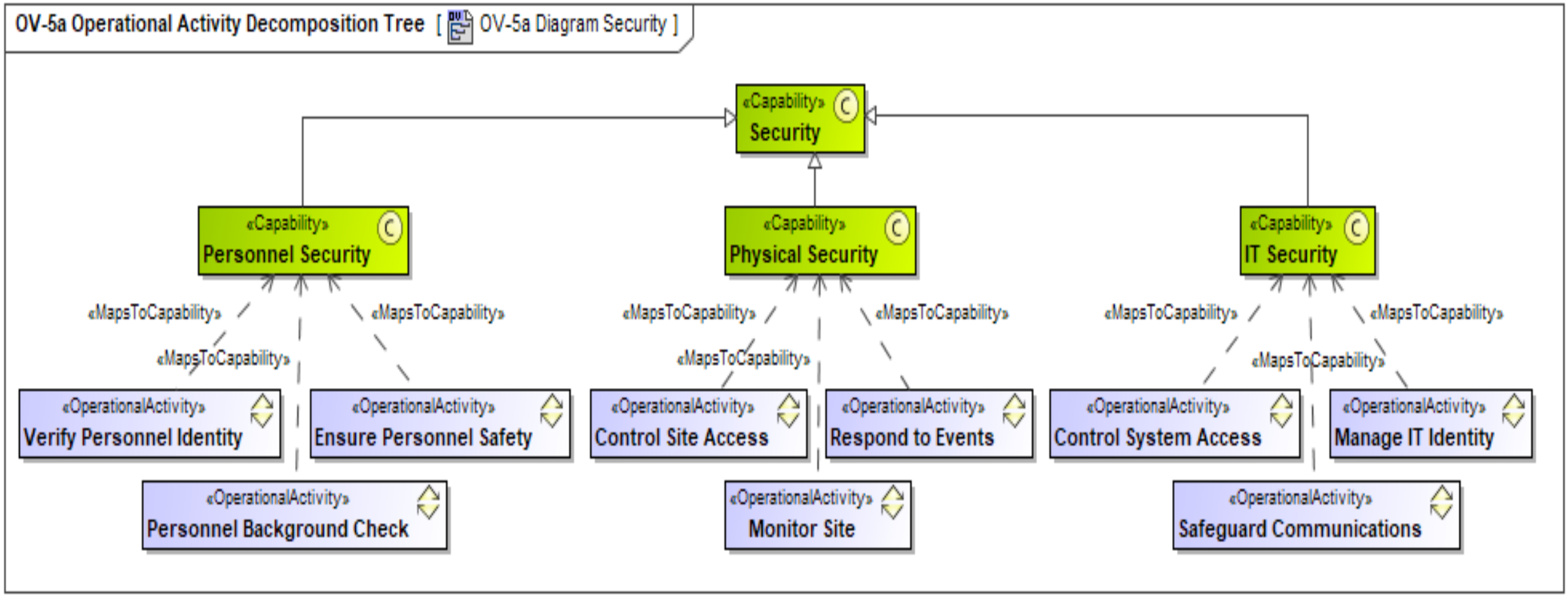
Factory Capability Taxonomy

- Automotive enterprise has multiple capabilities
- Security has Physical Security, Personnel Security and IT Security



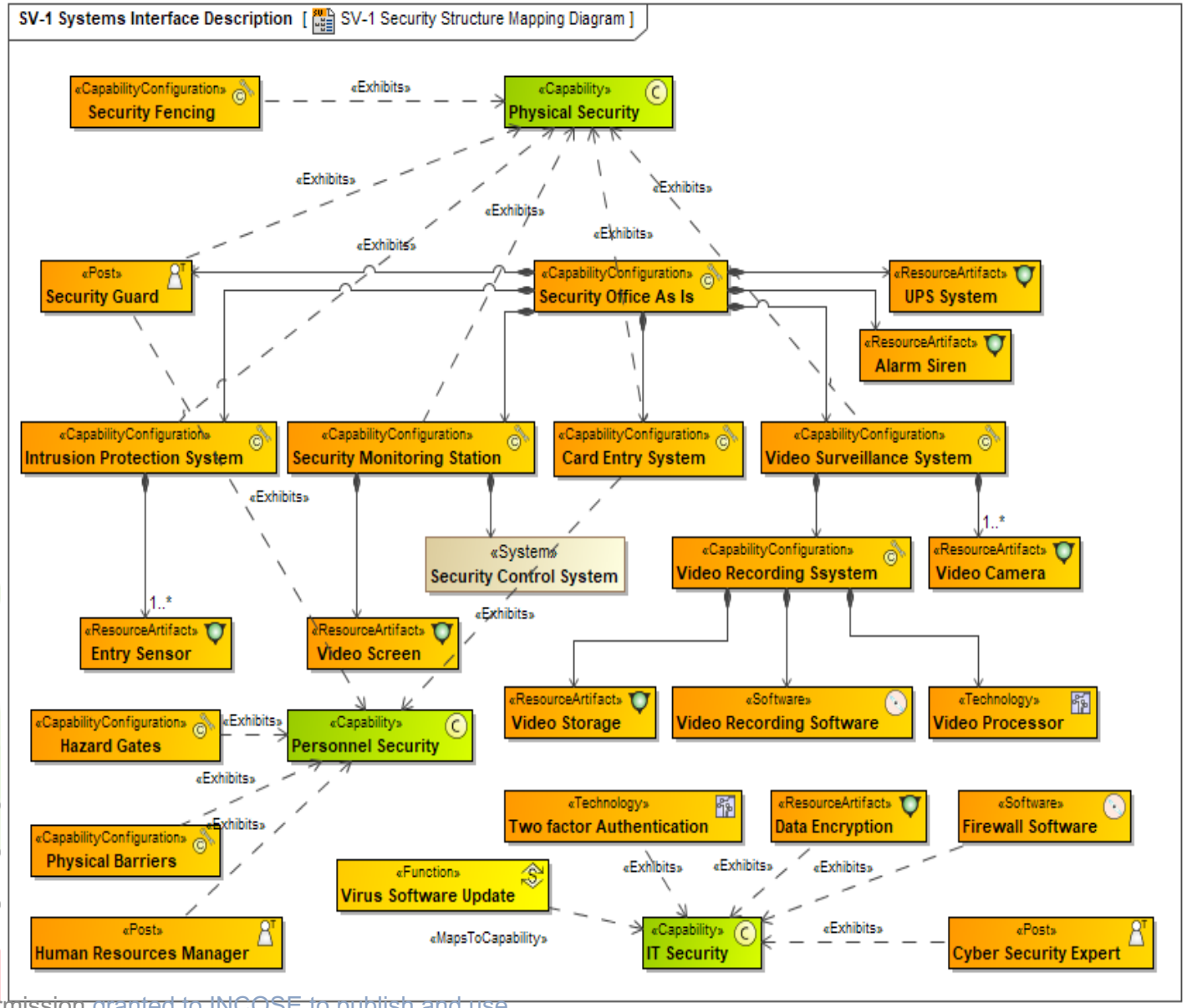
Operational Activities

- Operational activities solution independent describe business used to elaborate capabilities
- These are further described as detailed activity diagrams.
- Structural elements are then mapped to these



Capabilities and the System and Security Architecture

- Capabilities are then mapped to solution elements
  - Systems, software, technology, personnel
  - Security behavior is defined
  - Security systems are integrated into the solution architecture.
- Requirements are traced to the model elements to ensure a complete solution
- Additional derived requirements are created



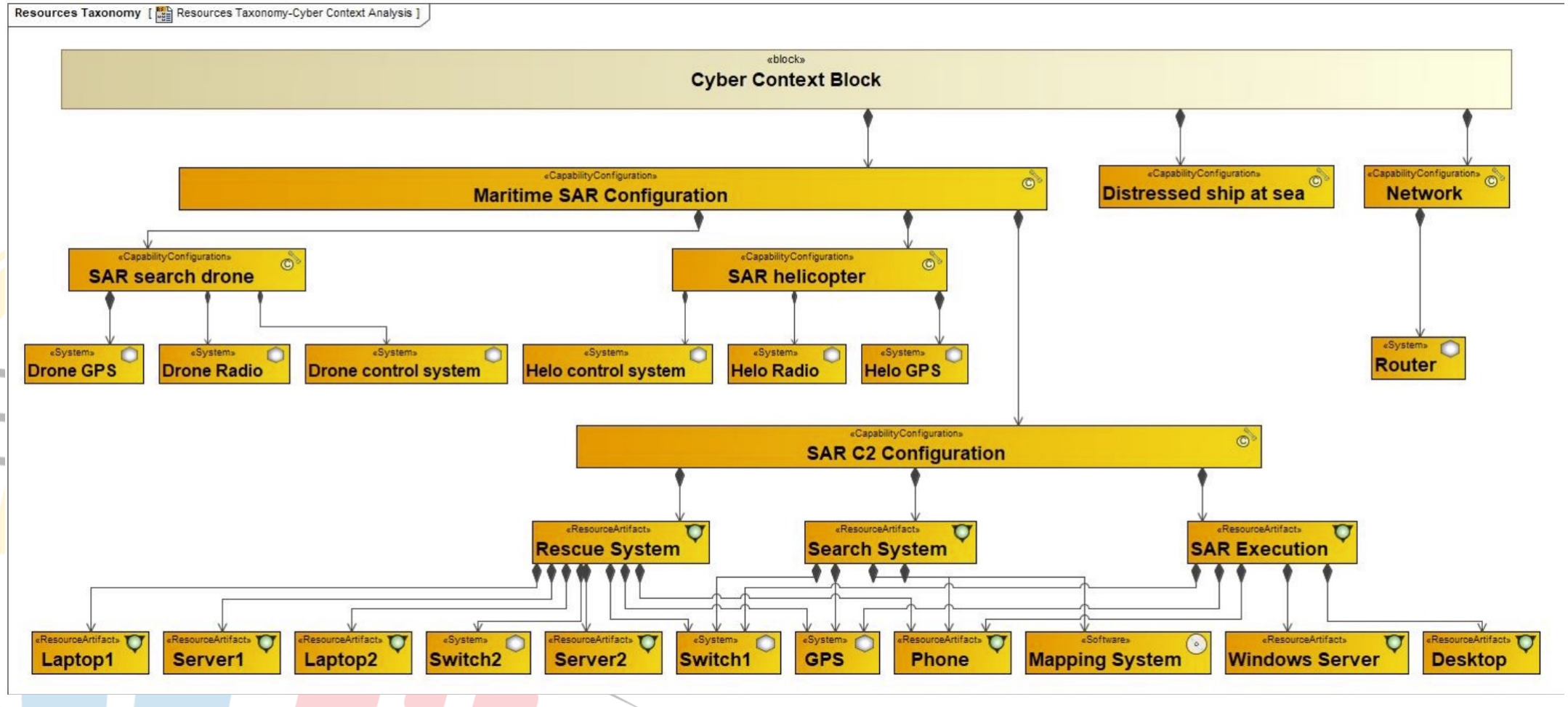
Cybersecurity in the Digital Thread

RAAML Integration

- As RAAML is integrated with SysML, this same integration can be used by the UAF
- A team from Mitre also provided an example making use of RAAML to examine the benefits of using Fault Tree Analysis (FTA).
  - "The structure and connectivity of the Fault Tree (FT) is constructed through analysis of the systems, system functions, and potential system failures. Based on such an analysis, the FT is created by identifying the events that can lead to each undesired system behavior which may lead to a system failure. Based on the structure of system resources identified, the system components that are vulnerable are identified. In the sample SAR model, the leaf level model elements are identified as the first point of attack from an external (internet) connection." (Dansashi 2022)

The Systems, Hardware, And Software Components For Cyber Resiliency Analysis

Image from Dandashi, F., 2022, Modeling Security Views with Unified Architecture Framework, Risk Assessment and Analysis Modeling Language, and Systems



Fault Tree For Cyber Resiliency Analysis

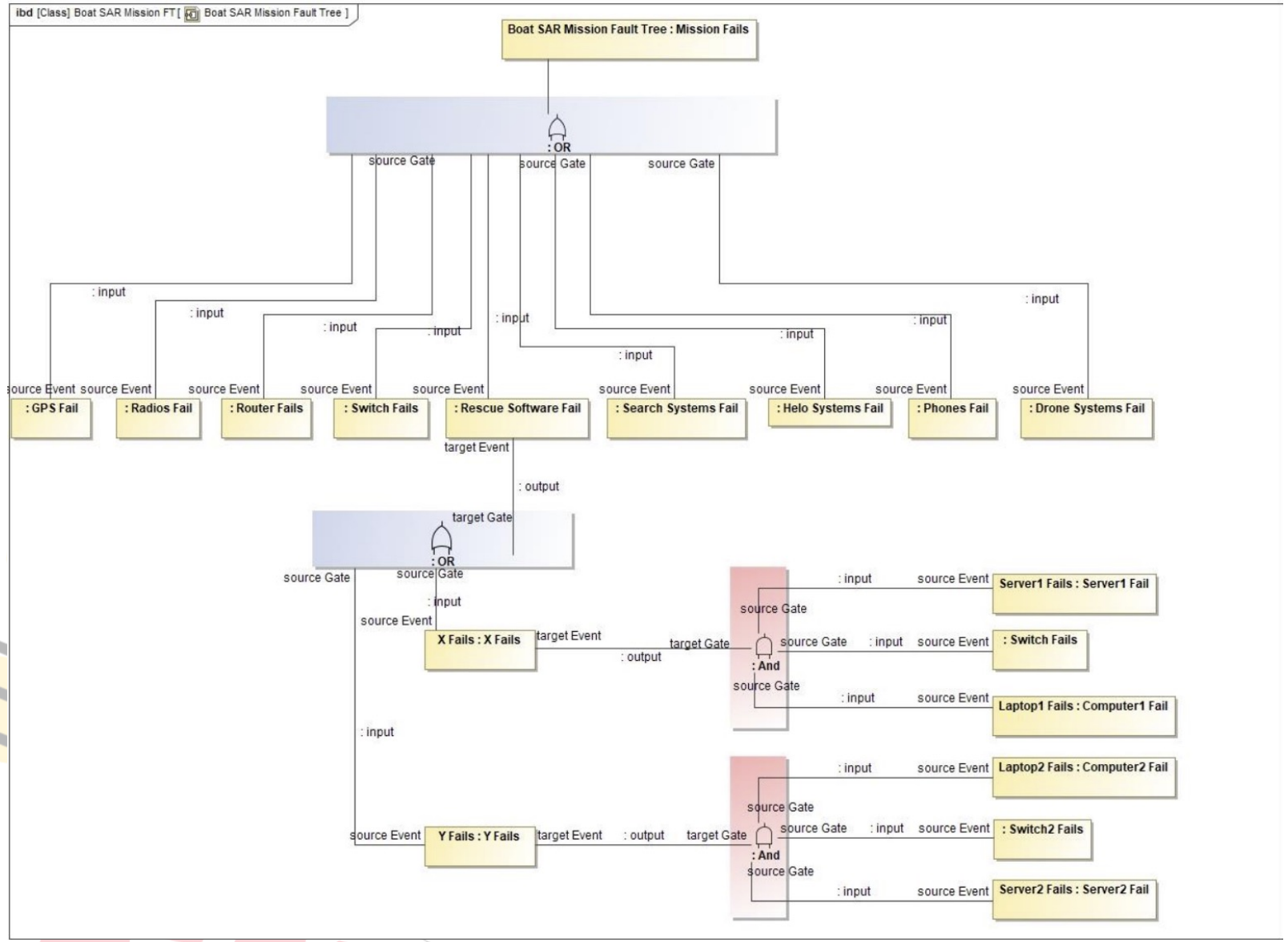


Image from Dandashi, F., 2022, Modeling Security Views with Unified Architecture Framework, Risk Assessment and Analysis Modeling Language, and Systems

About blade RiskManager

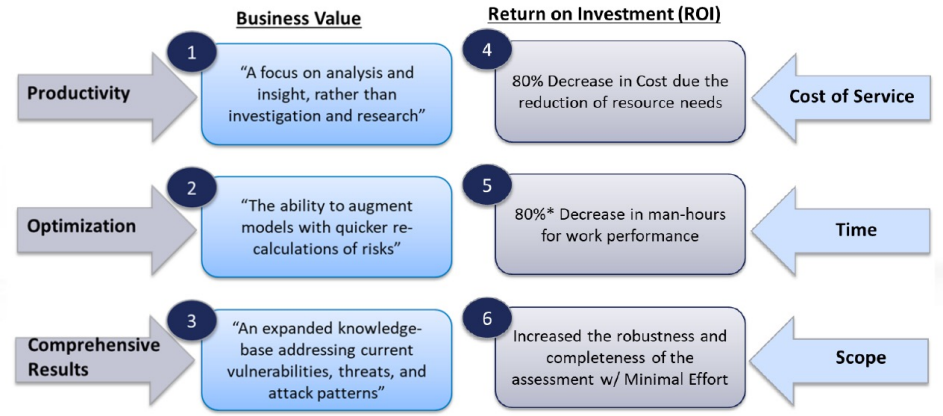
KDM Analytics

Fully automated risk assessment and measurement platform

Enables organizations to identify, prioritize, and focus their risk mitigation efforts to the most critical assets of a system

Its value proposition allows organizations to:

- Reduce requirements of highly specialized knowledge
- Save Time
- Save Resources
- Increased ROI



*Using the blade RiskManager, we were able to provide **'More Insight'** with **'Less Effort'**.*

DR. TONY D BARBER, Principal Consultant, ADS

NORTHROP GRUMMAN

BOEING

BAE SYSTEMS

U.S. AIR FORCE

Services publics et Approvisionnement Canada | Public Services and Procurement Canada

tenable

DELL EMC

Delivers Digital Risk Assessment at industrial-scale for Cyber and Cyber-Physical systems

Delivers fully automated (objective & repeatable) risk analysis by utilizing digital engineering framework/MBSE

- Support for UPDM, UAF, SysML, CSV/MS Word Tables
- Validate model's fitness for purpose (e.g. Correctness, Completeness)
- Supports MOSA approach by utilizing mul. module imports & merge

Provides system visualization & modeling platform

- Auto-generates interactive view of system model from documents, and
- Provides platform for creating system model

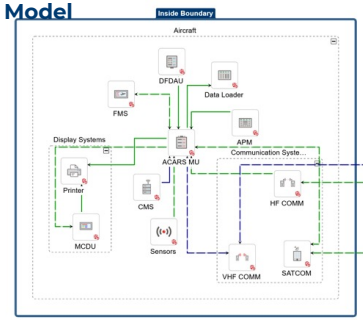
Auto-generates Threat Model with Customizable Threat Environment

- Automated identification of attack paths and corresponding vulnerabilities
- Calculates fully quantifiable and prioritized initial, mitigated, compliance and residual risk
- Enables what-if scenario with auto-mitigation capability

Support for Multiple Standardized Frameworks, Catalogues & documentation

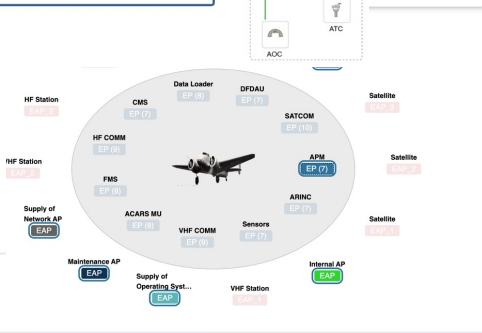
- NIST RMF, CSF, Cyber Survivability Attributes (CSA) KPP
- NIST 800-53; CNSSI 1253, ITSG-33
- MITRE ATT&CK, CAPEC, SFP/CWE
- Auto-generated Customizable Reports & ATO pkg

Auto-generated Interactive System Model



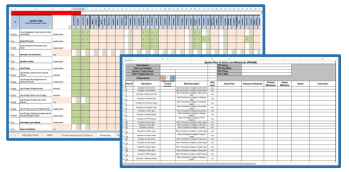
Visualization

Automated Analysis



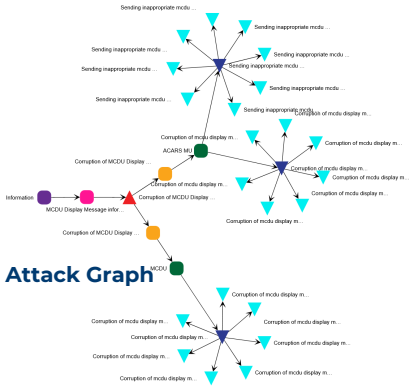
Auto-generated Reports

Security Traceability Matrix



Prepopulated POA&M

Auto-generated Attack Graph



MITRE's TRACE

- Mitre's TRACE considers likelihood and impact to mission, and ties asset failures to mission impact using FT analysis
- The tool uses sources such as MITRE's Adversarial Tactics Techniques & Common Knowledge (ATT&CK®) and overlays probability data from a Threat Concept Database and conducts Monte Carlo analysis to identify vulnerabilities and provides a list of Security Controls as output. TRACE ingests OMG's XMI® (Dandashi, 2022).
- This process is repeated until the system is deemed secure

Conclusion

- The diagrams shown are a small part of a complex model.
- UAF integrates security into the model rather than stand-alone
- UAF can be used by IT professionals and systems engineers to
  - Identify the most common problems and unmitigated risks faced by IT systems
  - Model existing security enterprises and identify security holes, superfluous security systems and software, and rectify incompatibilities
- Start with capabilities and trace them down to systems ensure that the true capabilities required by the customer are met
- Needs and capabilities ensure that the right system is built right.
- Standards based-security ensures best practices

References

- Brooks M., Hause M., 2022, Making the Puzzle Pieces Fit - Utilizing UAF to Model a Cybersecurity SoS, published in INCOSE Insight, 2022
- Campara, D, 2020, Blade RiskManager (BRM) by KDM Analytics suite, KDM Analytics: automated risk frameworks for operational technology, online, Available from: https://kdmanalytics.com/wp-content/uploads/2020/06/KDM-Automated-NIST-Risk-Management-Framework-06-09-20-R3-web.pdf
- Dandashi, F., 2022, Modeling Security Views with Unified Architecture Framework, Risk Assessment and Analysis Modeling Language, and Systems Modeling Language, MITRE Technical Report MTR220019
- Friedenthal S., Moore A., Steiner S. (2014). A Practical Guide to SysML: The Systems Modeling Language, 3rd Edition. Ny, Ny: Elsevier.
- Hause, M., Brooks M., 2022, Capability Engineering vs. “Problemeering” and “Solutioneering” - Prioritizing Stakeholder Needs over Requirements, published in INCOSE Insight 2021
- Hause, M and Kihlström, L. 2021. “Using the Security Views in UAF.” Presented at the 31st Annual INCOSE, July 17-22, 2021
- Hause M., Adejokun A., Brooks M., 2023, Preserving and Sharing Knowledge – Extending the UAF Security Views with Libraries, Patterns and Profiles, presented at the 33rd Annual INCOSE International Symposium, July 15-20, 2023 in Honolulu Hawaii.
- INCOSE, 2021, The Future of Systems Engineering, available from https://www.incose.org/about-systems-engineering/fuse
- ISO 15704:2019, Enterprise modelling and architecture — Requirements for enterprise-referencing architectures and methodologies, Available online from https://www.iso.org/standard/71890.html
- Maier, M.W. 1998. "Architecting Principles for Systems-of-Systems." Systems Engineering. 1 (4): 267-284
- NIST Special Publication (SP) 800-160 Vol 2, “Developing cyber resilient systems: a systems security engineering approach,” November 2019, https://doi.org/10.6028/NIST.SP.800-160v2 [5] NIST SP 800-53 Rev. 4, “Security and privacy controls for federal information systems and organizations,” April 2013, https://doi.org/10.6028/NIST.SP.800-53r4
- OMG 2019, Systems Modeling Language, Version 1.6, Object Management Group, https://www.omg.org/spec/SysML/About-SysML/.
- OMG, 2022a, Object Management Group, March 2022, Risk Analysis and Assessment Modeling Language (RAAML) v1.0 FTF, OMG Document -- ptc/21-01-01 (Risk Analysis and Assessment Modeling Language (RAAML), v1.0 beta 2) online available from https://www.omg.org/spec/RAAML/
- OMG, 2022b, Unified Architecture Framework Specification Version 1.2. (2022). Retrieved 31 January 2022, from https://omg.org/spec/UAF/About-UAF/
- Maier, M.W. 1998. "Architecting Principles for Systems-of-Systems." Systems Engineering. 1 (4): 267-284
- Mitre, 2022, Traversal-driven Risk Assessment of Composite Effects GitHub - MITRE/trace: Traversal-driven Risk Assessment of Composite Effects
- Zurkus, K. (2022). Defense in depth: Stop spending, start consolidating. Retrieved 31 January 2022, from https://www.csoonline.com/article/3042601/defense-in-depth-stop-spending-start-consolidating.html

Questions?

Mitchell Brooks:

mbrooks@systemxi.com

Matthew Hause:

mhause@systemxi.com