33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

Preserving and Sharing Knowledge – Extending the UAF Security Views with Libraries, Patterns and Profiles

Ademola Adejokun: Lockheed Martin Aeronautics

Matthew Hause: System Strategy Inc.

Mitchell Brooks: System Strategy Inc.

Problem

- Knowledge and experience are gained during the execution of every project. This knowledge remains in the heads of the engineers, but often is not distributed more widely.

- In Model-Based Systems Engineering (MBSE) projects, this knowledge can include problem solving techniques, algorithms, libraries of types, patterns, interfaces, components, etc.

- Patterns publicly provided as a curated, searchable, solution set library could be leveraged by projects and augmented over time, preserving their Intellectual Property (IP) and knowledge assets.

- One of the ways to preserve this knowledge is by creating libraries of these reusable assets.
  - For example, the newest version of Unified Architecture Framework (UAF) included a library developed by Mitre of 1200 different security controls defined in National Institute of Standards and Technology (NIST) standard 800-53r5.
  - These controls can be referenced on projects to mitigate many common security risks.
  - Each defined control can be integrated with the corresponding risks, security metrics, mitigating elements, solutions, and so forth. All these elements could then be used to construct Security Patterns showing risks that the security controls can mitigate as well as abstract solutions that can satisfy these controls.

Knowledge and Skills Pattern

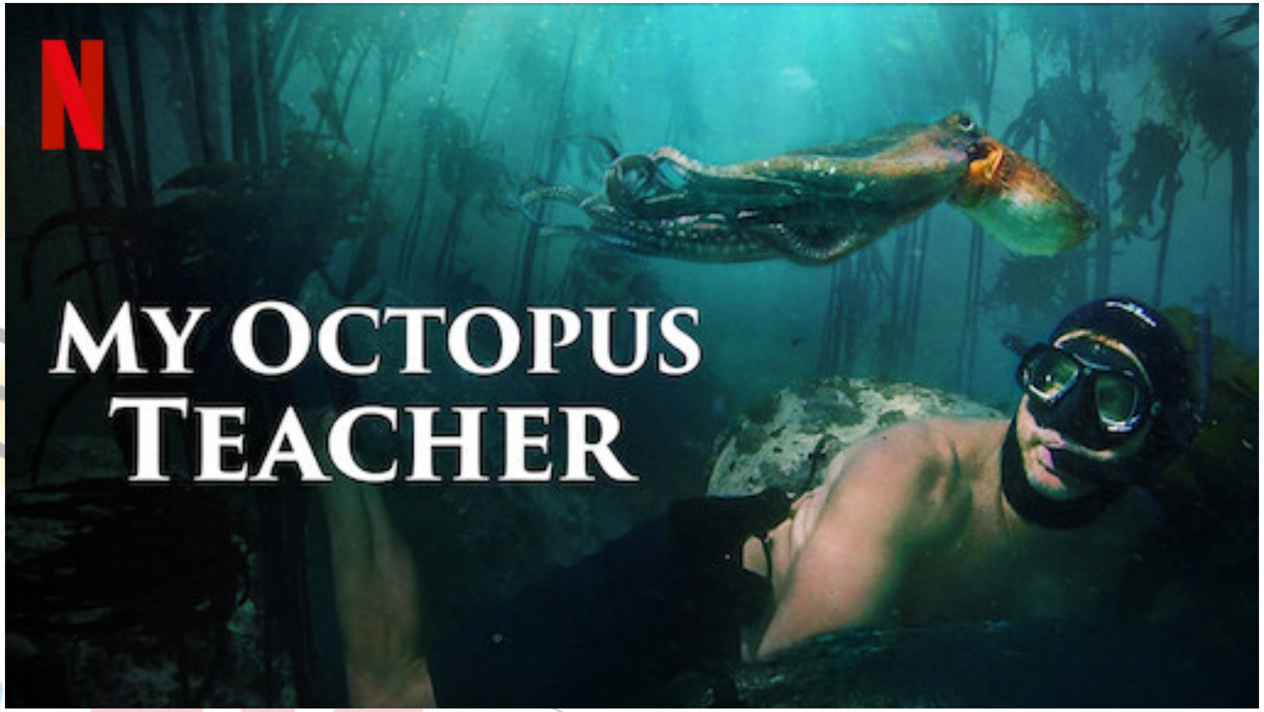
Knowledge and Skills in Animals

- Knowledge and skills transfer is essential for survival for all animals
  - Hunting for food
  - Evading predators
  - Recognizing poisonous plants
- Complex Social Skills
  - Dominant male behavior
  - Social bonding
  - Acceptable play
- Transfer Methods
  - Copying behavior (monkey see, monkey do)
  - Positive and negative reinforcement
  - Natural Instinct/DNA
- In person, in the moment, and synchronous
  - Lost knowledge is costly to reaquire




Example: The Octopus

- Intelligent, excellent at problem solving, uses tools, etc.
- Solitary, with no means of knowledge transfer
- Information skills acquired by one octopus is lost when it dies



Knowledge and Skills in Humans

- Synchronous Methods
  - Animal methods previously listed
  - Spoken Language (Epic poems, Conversations, etc.)
  - Apprenticeships
  - Song and social events
  - Schools and education
- Asynchronous Methods
  - Written language (Scrolls, Books, Letters, Notes, etc.)
  - Libraries – general, technical, philosophy, architecture, science, etc.
  - The internet – All human knowledge and information both true and false
  - Preserves knowledge across generations.

Building on Past Knowledge

- "If I have seen further [than others], it is by standing on the shoulders of giants." (Newton, 1675)
- Science and Engineering
  - CAD Models
  - Complex computer simulations
  - Technical journals and presentations
  - Ontologies
  - Systems Engineering models
  - SysML profiles and domain specific languages
  - UAF NIST Security Controls Library
  - SysML libraries and patterns (QUVD for instance)
    - SysML V2 emphasizes libraries over profiles

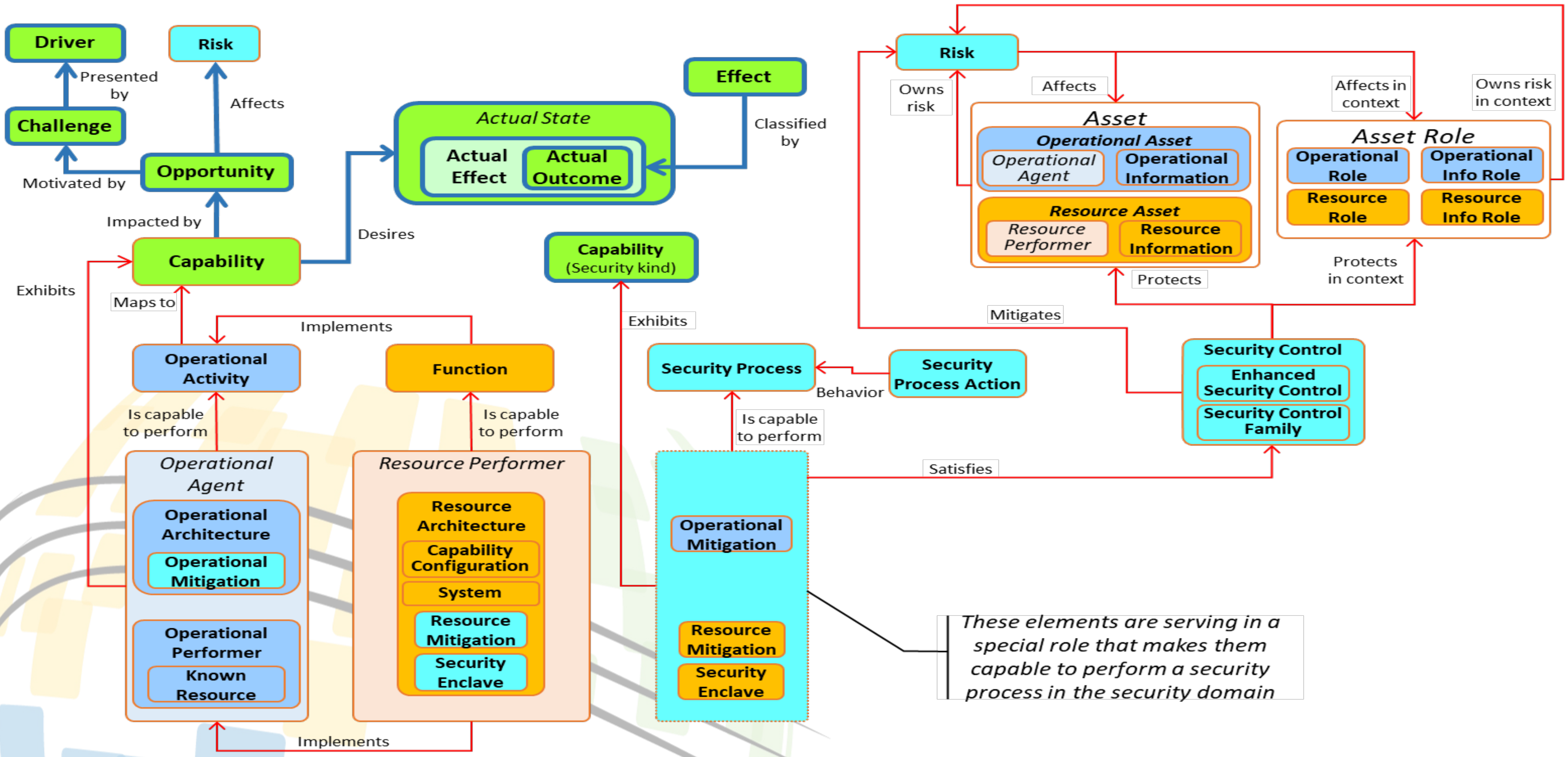
https://www.prime1studio.com/mini-minions-in-laboratory-pcfmini-03.html

Octopus Security

- A big gap in the libraries on the previous slides is that there are no security libraries or means of reuse
- We are having to relearn/reteach/reinvent security concepts whenever systems need to be secure – which is every system

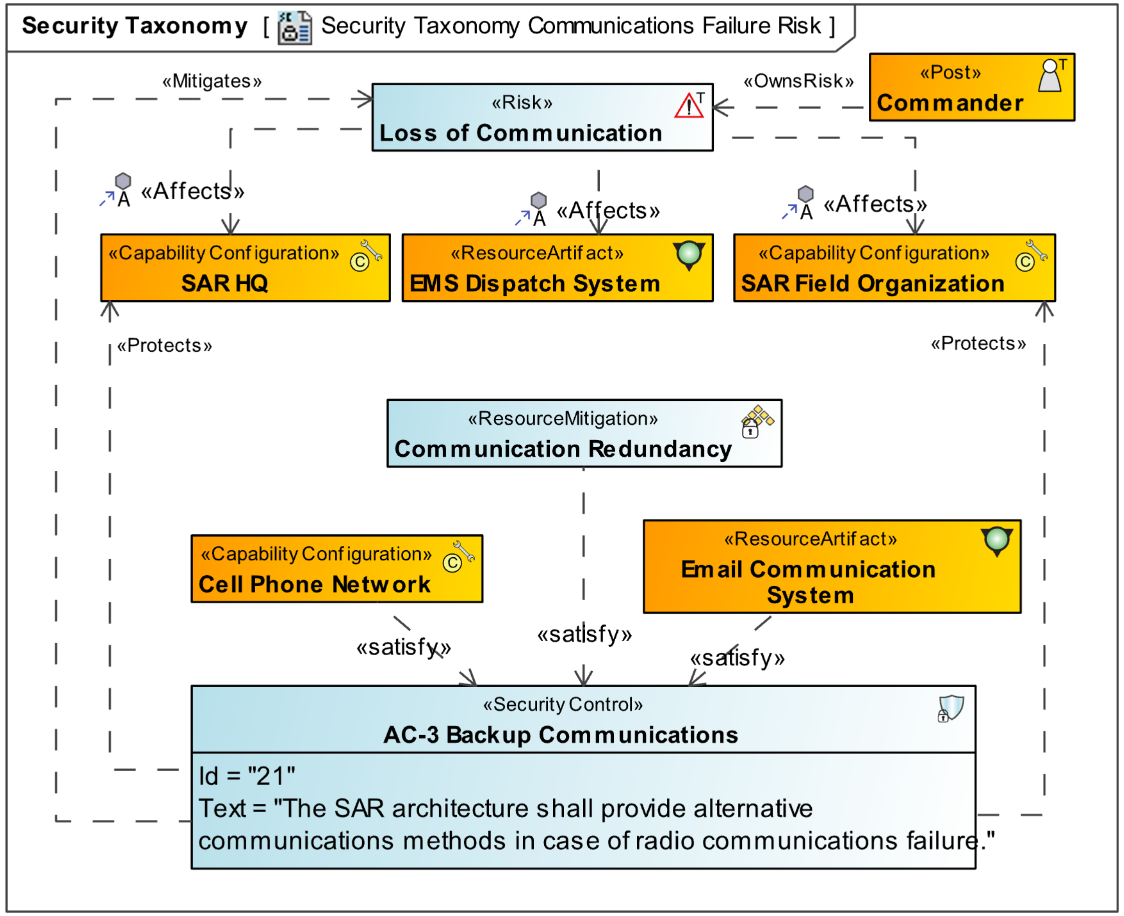
UAF Security Libraries

UAF Security Views Conceptual Meta-Model



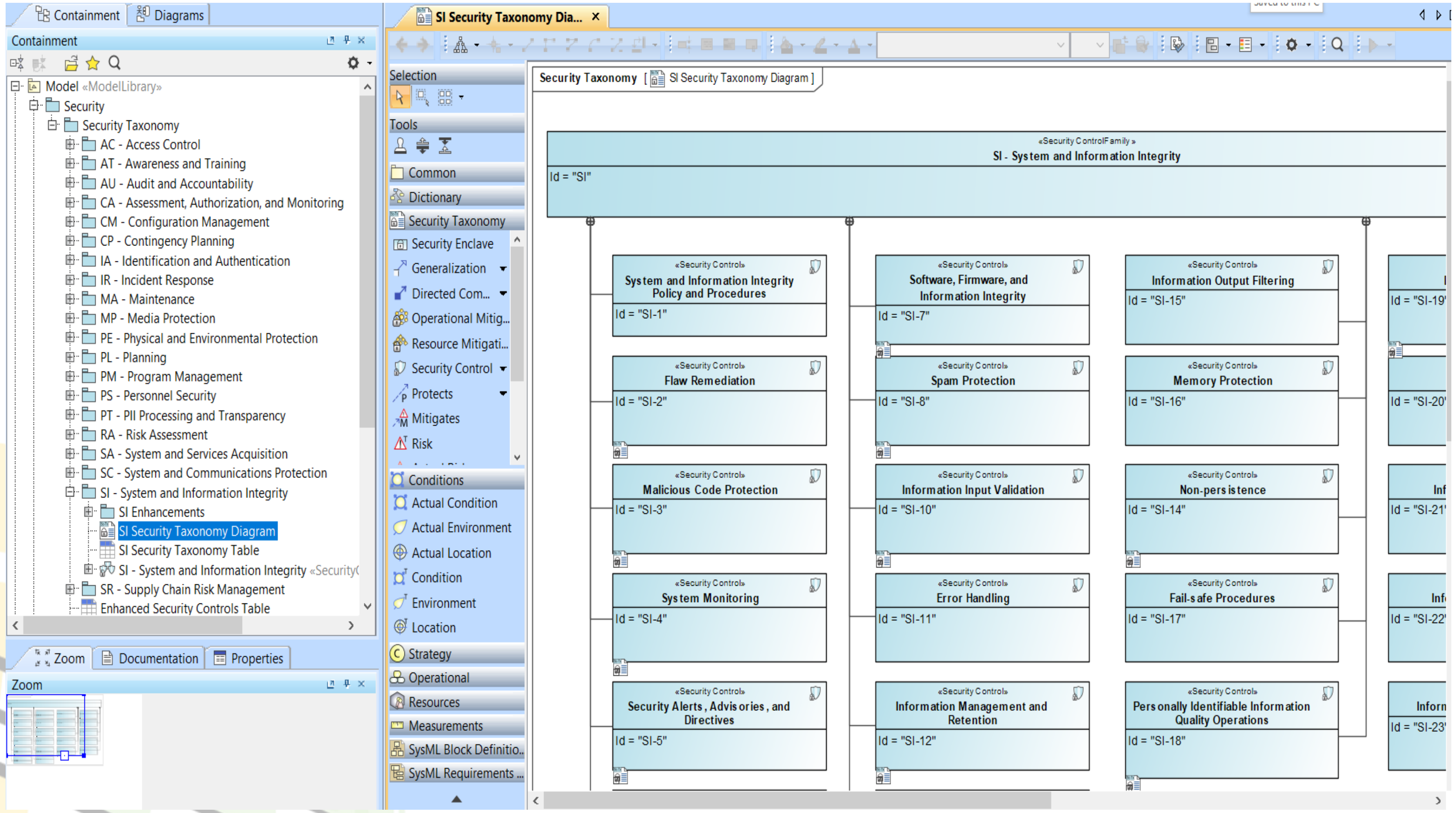
Sc-Tx Security Taxonomy

- **This figure shows the taxonomy for some of the security elements**
- **Risks are the possibility of an adverse effect and its likelihood of occurrence**
  - Risks affect resource artifacts, capability configurations, etc.
- **Security Controls are a management, operational, or technical control (e.g., safeguard or countermeasure) which Protects an asset.**
  - They mitigate risks and protect assets
- **Resource Mitigations are a set of performers established to manage operational or resource Risks.**
  - They are represented as an overall strategy or through techniques (mitigation configurations) and procedures (Security Processes)and other assets to satisfy security controls



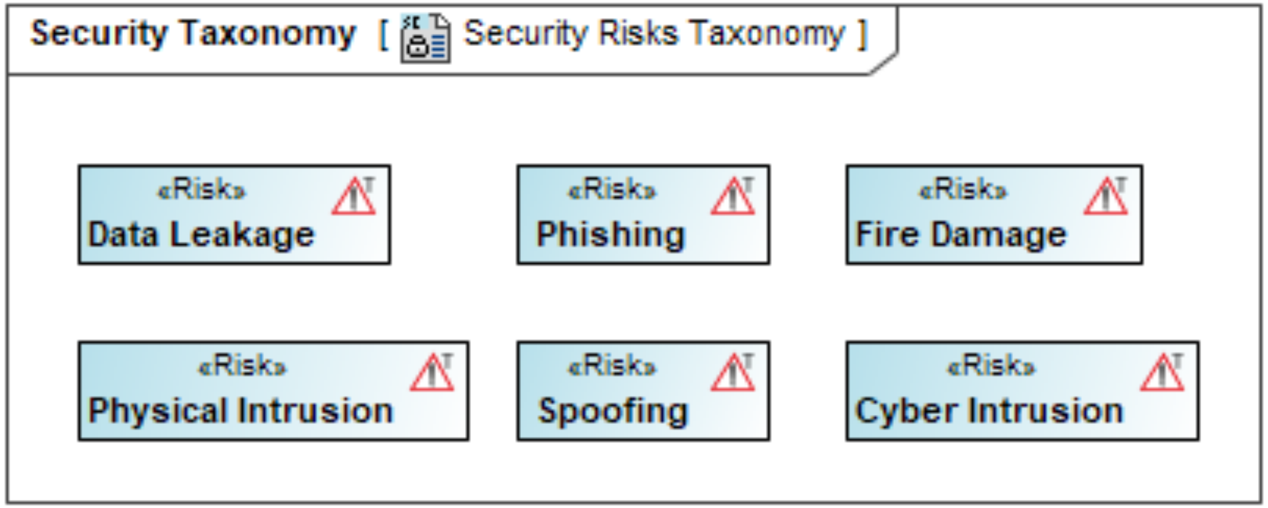
NIST SP 800-53 Security Controls Library

- UAF Reference Library
- Captures Security Controls, Families, Enhanced, Etc.
- No risks, mitigations, solutions – How can we add these?



Security Risks Taxonomy

- Sample of risks used in the sample model
- Can be built up over time with complete descriptions
- Links added to mitigations
- Examples of affected elements

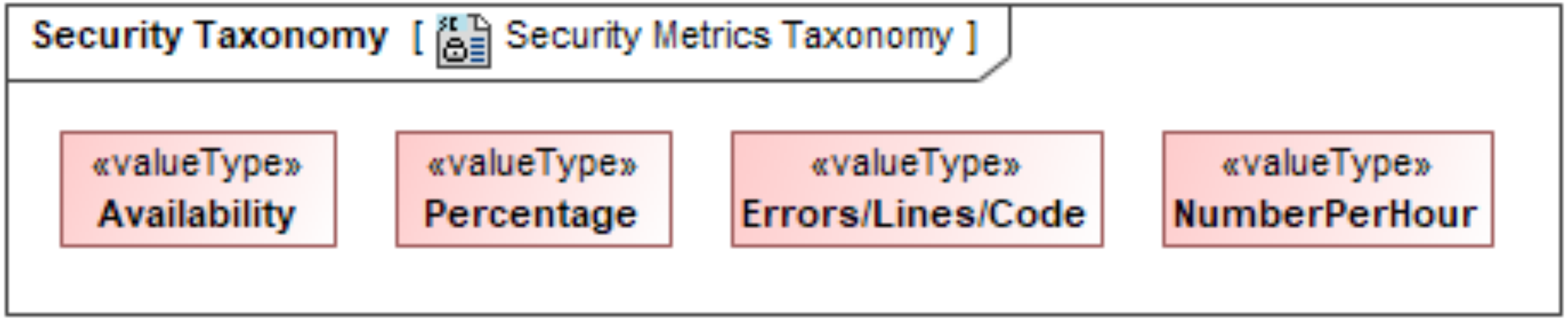


Security Measurements

Measures Type	Definition	Measure	Category
Implementation	Measure execution of security policy	System and Communications Protection System and Information Integrity Awareness and Training Configuration Management	Situational awareness
Effectiveness / Efficiency	Metrics used to monitor results of security control implementation for a single control or across multiple controls	Vulnerability Management System and Information Integrity Access Control Audit and Accountability Certification, Accreditation, and Security Assessments Identification and Authentication Incident Response) Maintenance Media Protection Physical and Environmental Risk assessment	Incident response system vulnerabilities, Mitigation attack or threat severity situational awareness
Impact	Metrics used to convey the impact of the information security program on the institution's mission, often through quantifying cost avoidance or risk reduction produced by the overall security program	Security Budget	Situational awareness

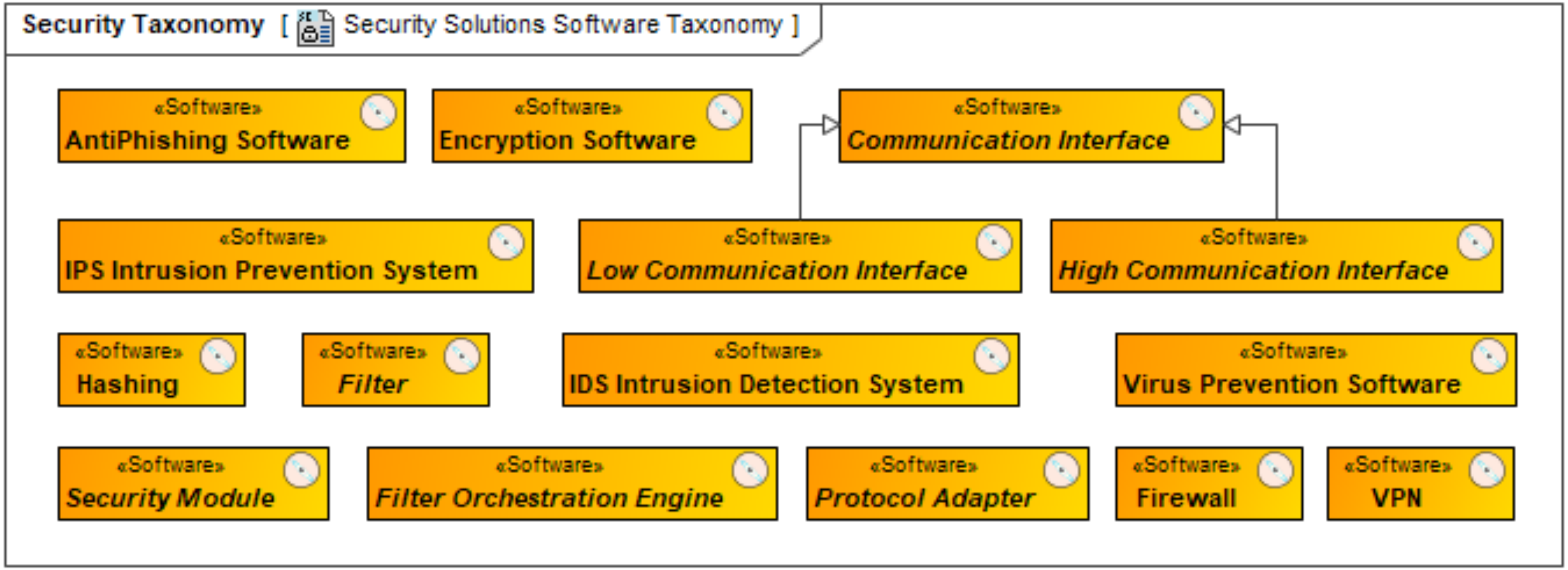
Value Types Library

- Having defined the measurements, it is necessary to define types.
- Many will be in the SysML libraries
- These can be reused throughout the model



Security Solutions Library

- Library of elements that can mitigate risks
- Can be both abstract (solution independent) or concrete



Security Patterns Orchestration

Introduction to Patterns

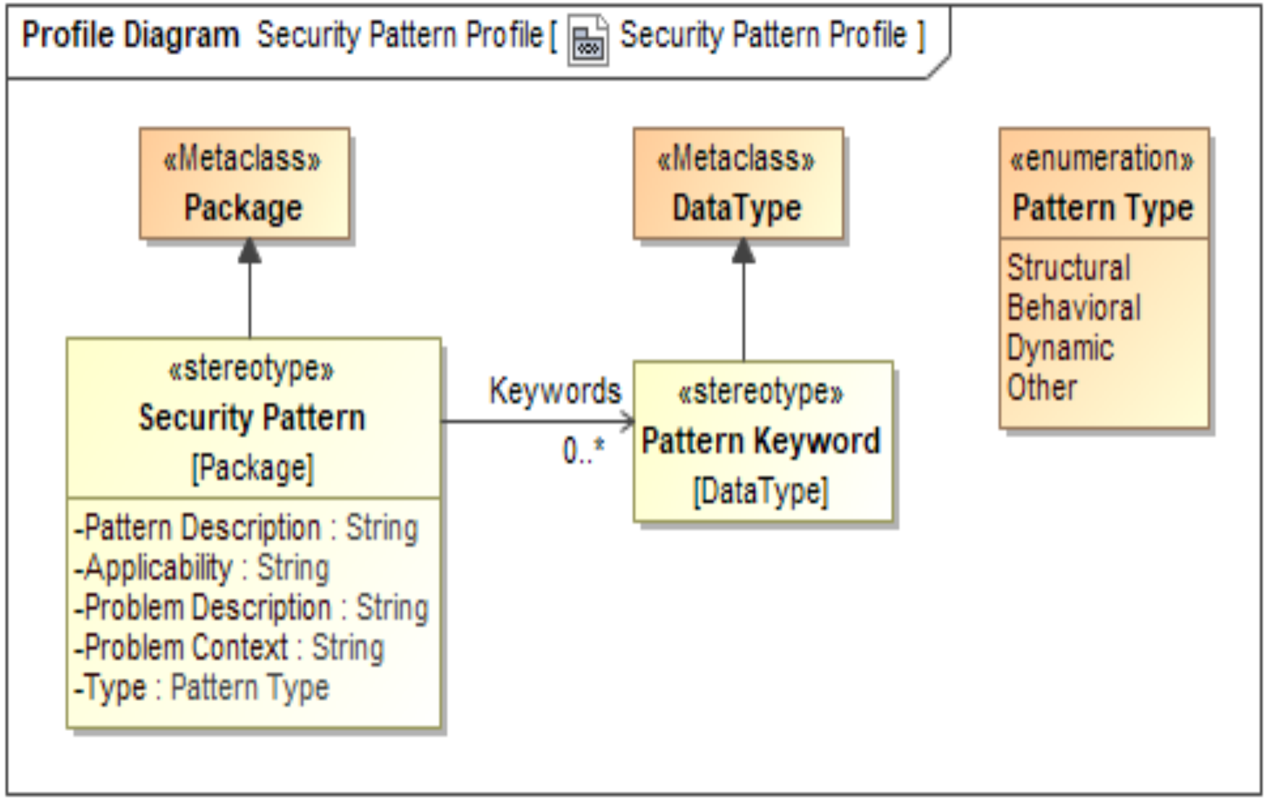
- Pattern recognition describes a cognitive process that matches information from a stimulus with information retrieved from memory. (Eysenck at al, 2003)
- Information from the environment is received and entered into short-term memory, causing automatic activation of a specific content of long-term memory.
- Semantic memory, which is used implicitly and subconsciously is the main type of memory involved with recognition. (Snyder, 2000)
- In engineering, pattern recognition is the automated recognition of patterns and regularities in data.
- Modern approaches include the use of machine learning, due to the increased availability of big data and a new abundance of processing power. (Mattson, 2014)

Model-Based Design Patterns

- Enables a solution to a specific problem that commonly occurs in the programming process (Alexander, 1979).
- The Gang of Four (GOF) defined Design Patterns in software engineering. Provides specific and effective solutions for software design and architecture scenarios. (Gamma, Helm , et al. 1994)
- Design patterns are classified according to their applicability and purposes.
  - Creational Design patterns,
  - Structural Design patterns and
  - Behavioral Design patterns (Gamma et al, 1994).
- Douglas (2002) further extended the design patterns into real-time software and systems engineering using UML.

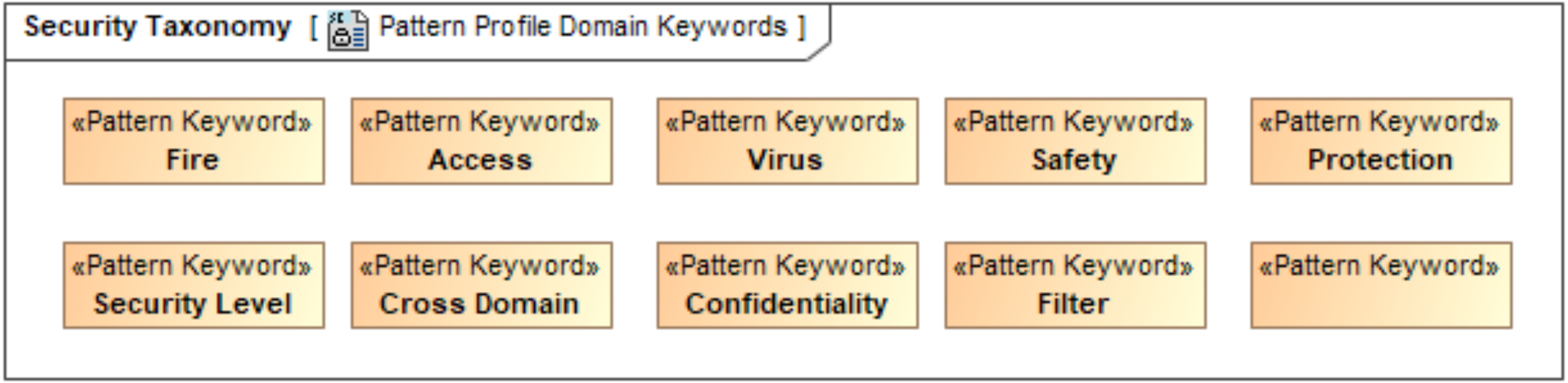
Security Pattern Profile

- Patterns are contained within a package
- Attributes include:
  - Description
  - Applicability
  - Problem Description
  - Problem Context
  - Pattern Type
  - Keywords
- Patterns are reusable and shareable



Security Pattern Keywords

- Keywords allow for searching for patterns
- Applicable keyword library will expand over time

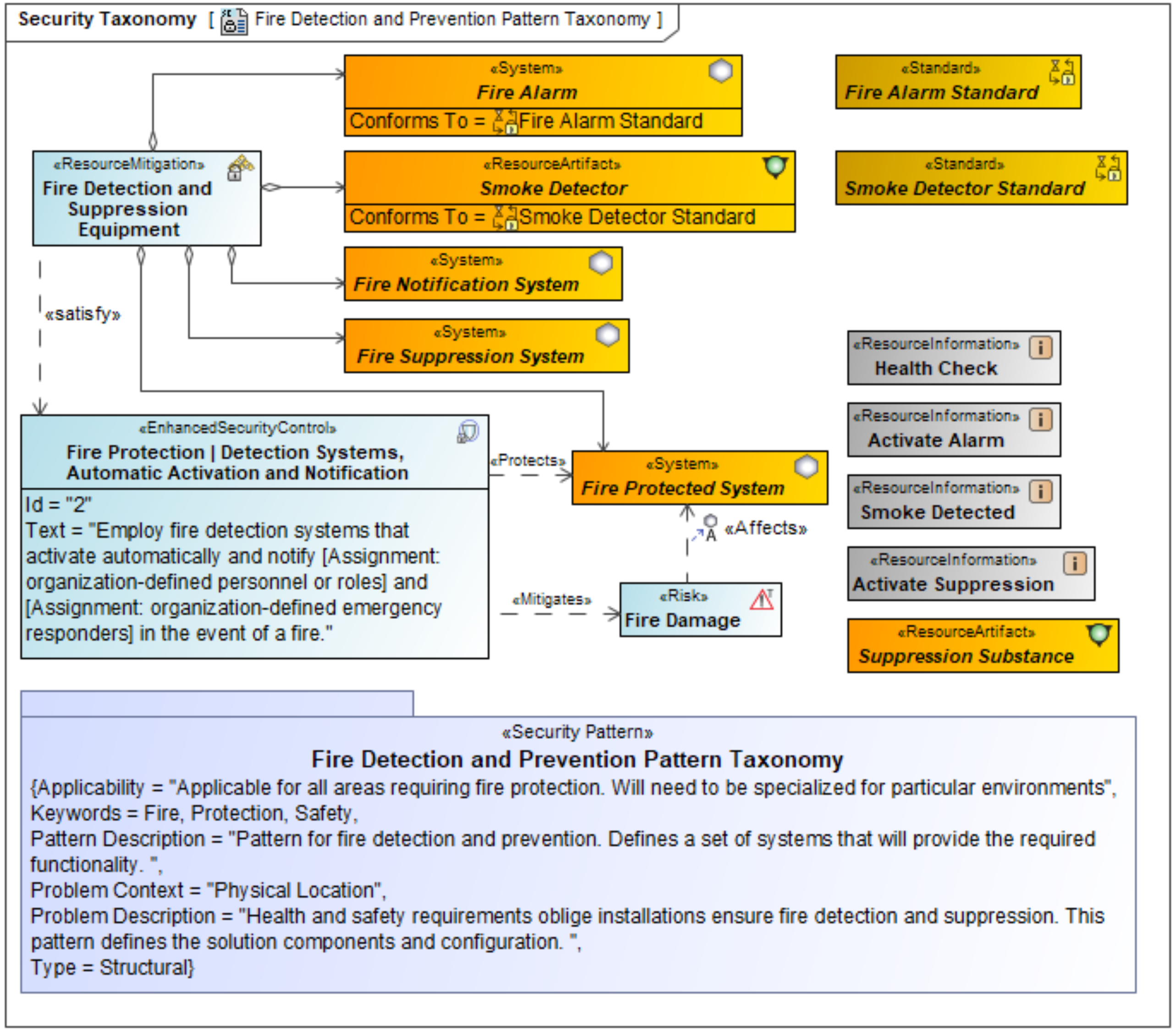


Sample text

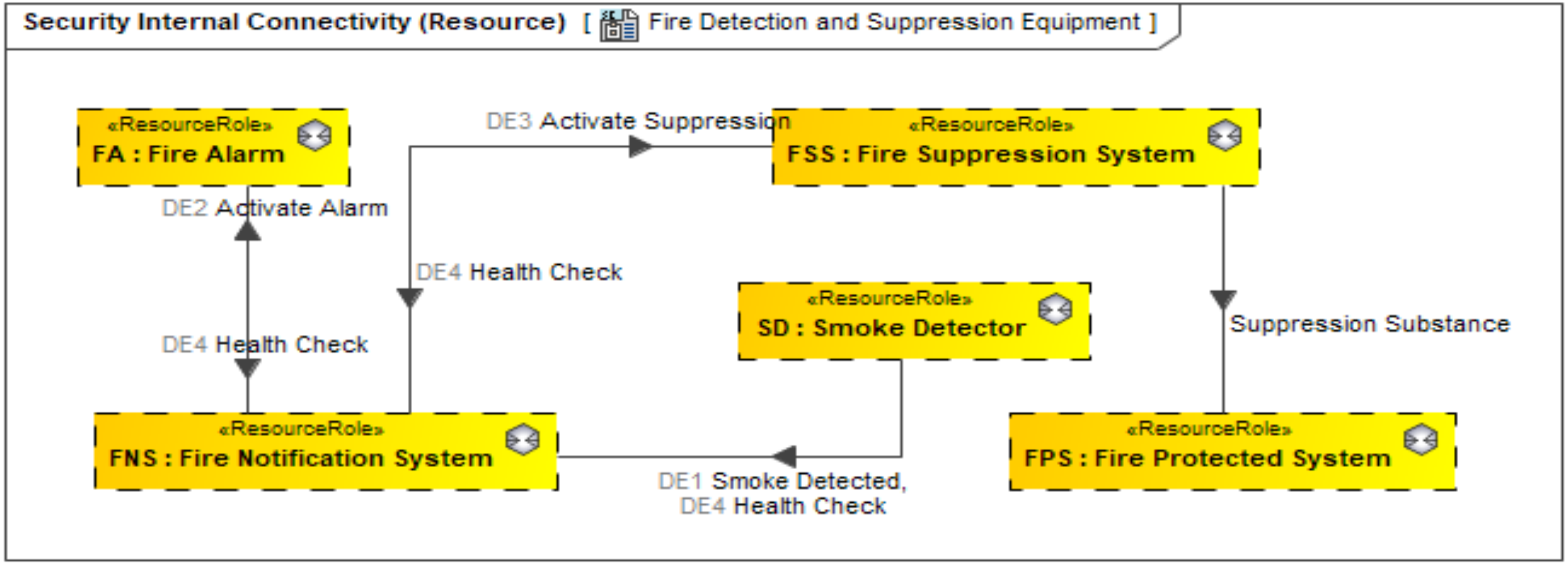
Pattern Example 1

Fire Detection and Prevention Pattern

Fire Detection and Prevention Pattern Specification



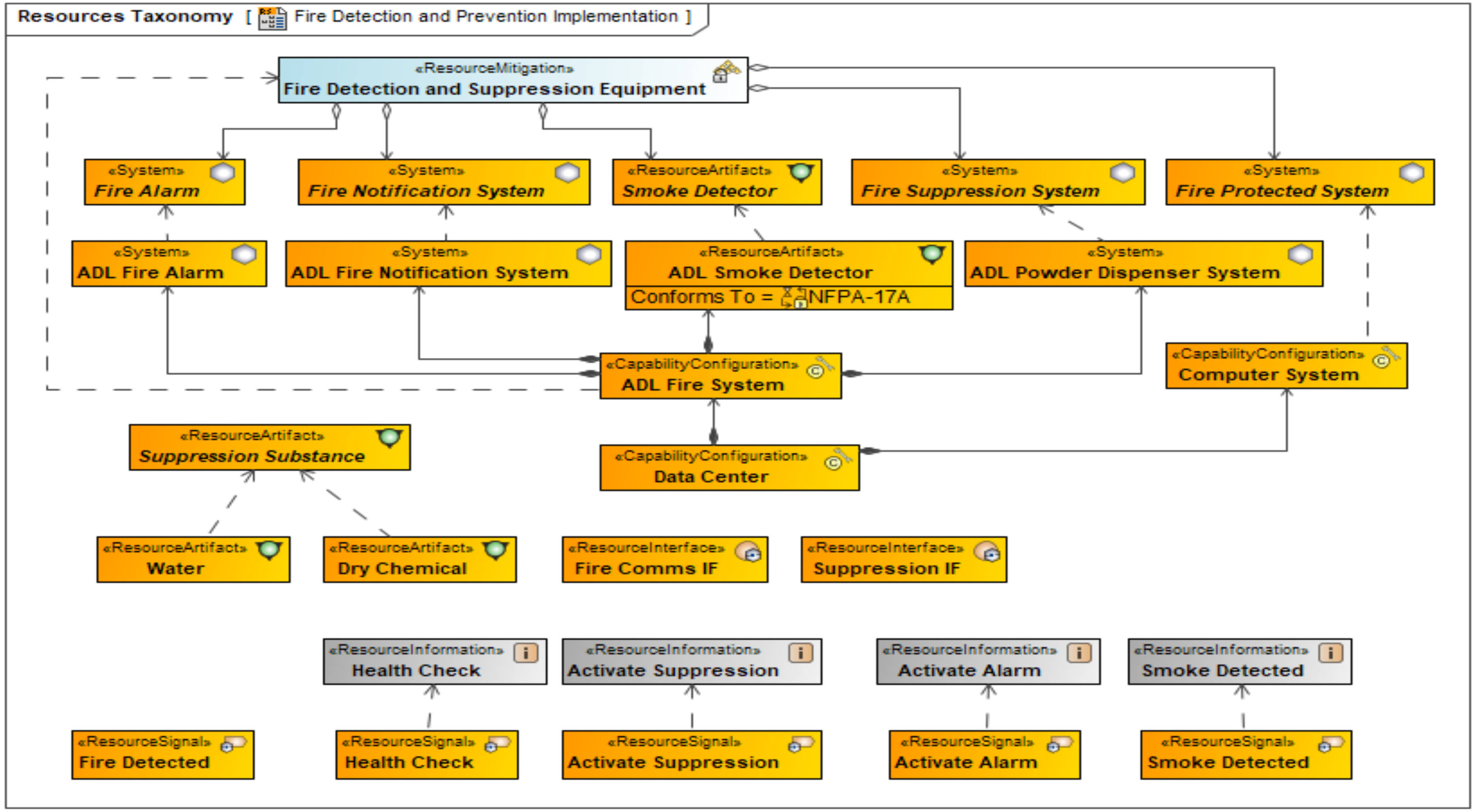
Fire Detection and Suppression Resource Mitigation Abstract Definition



Fire Detection and Suppression Implementation and Mapping to Abstract Solution

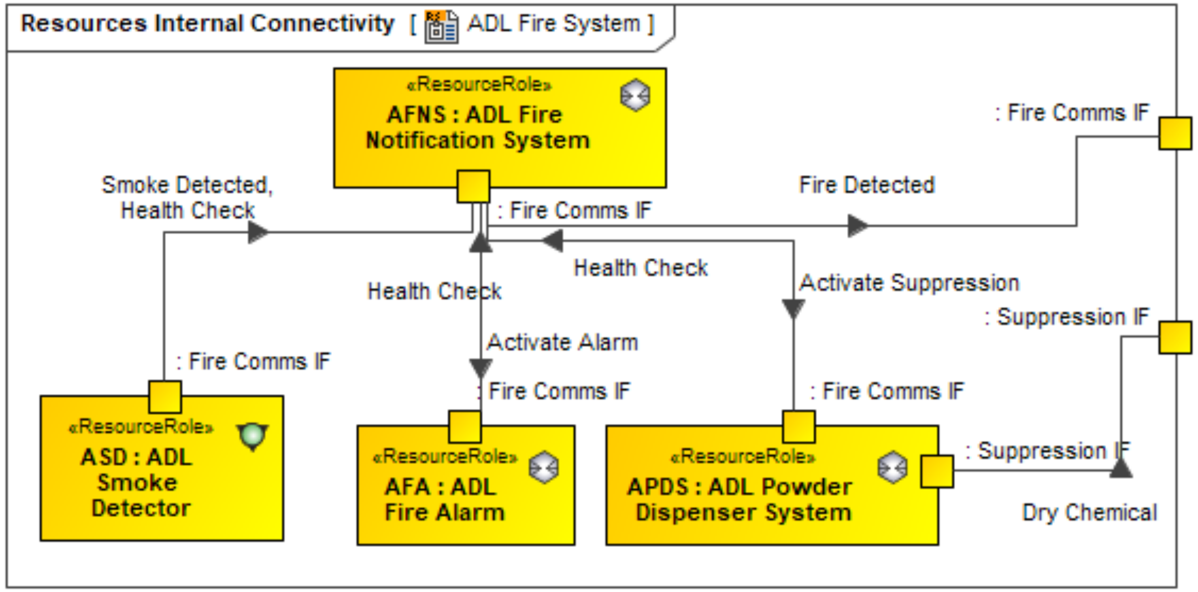
- Here, we map the pattern from its abstract elements down to its concrete elements

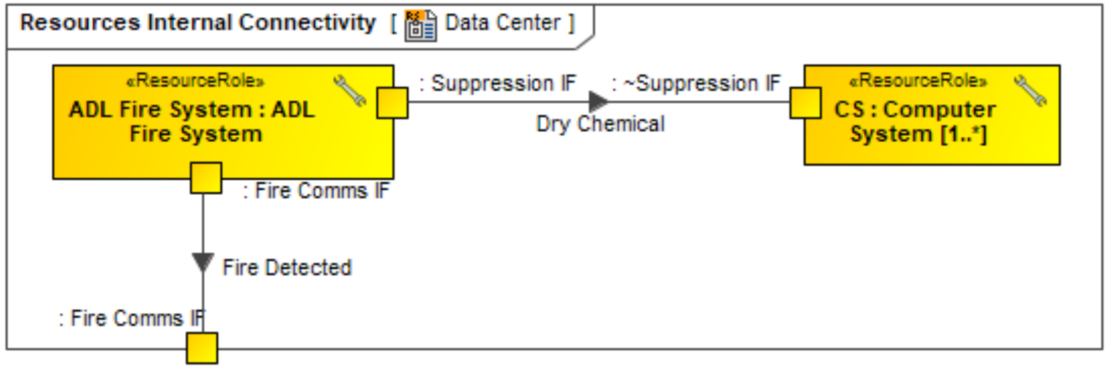
- ADL system implementation protects a Computer System using Powder Dispenser system



Fire Detection and Suppression Implementation

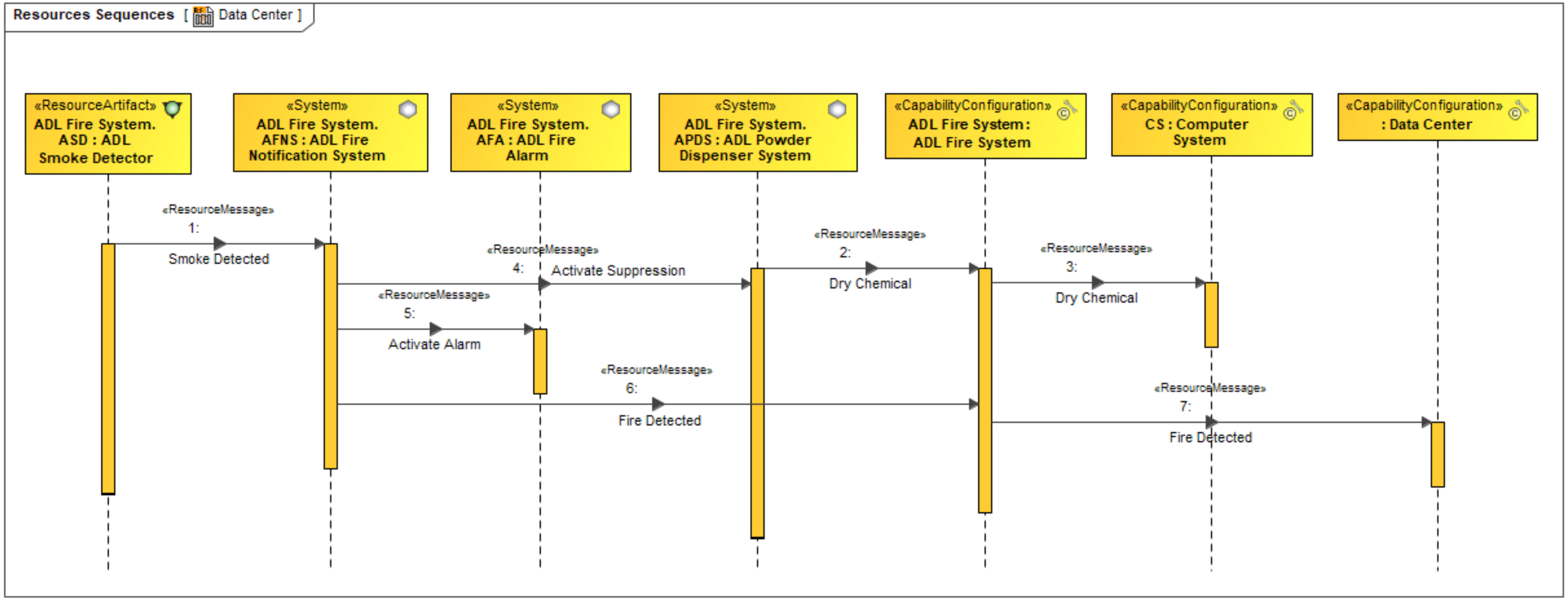
- Details the internal implementation of the system as well as external context.





Fire Detection and Suppression Implementation

- Fire Suppression Execution Sequence



Pattern Example 2

Cross Domain Solution Pattern

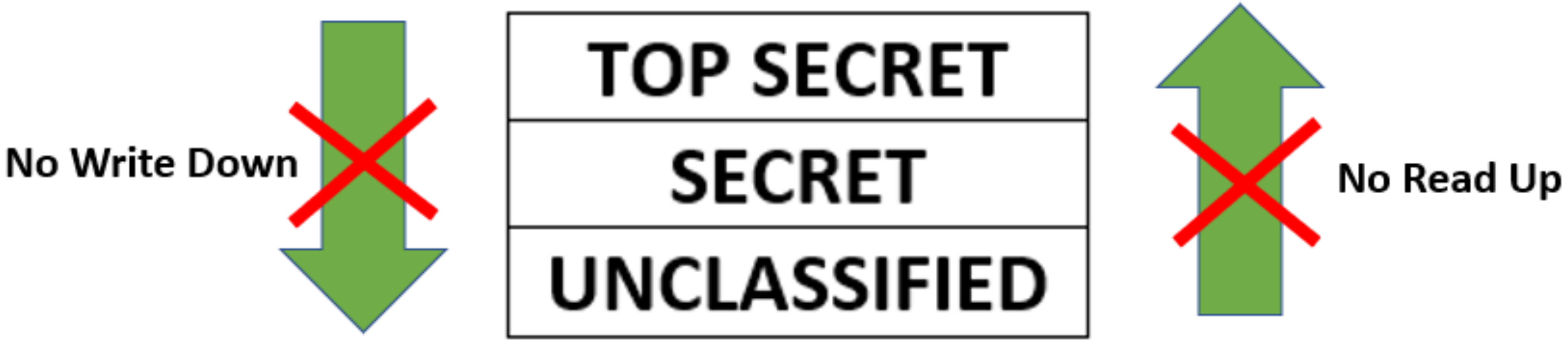
Cross Domain Solution Principle

- A Cross Domain Solution (CDS) is an information transfer and assurance system with software and hardware appliances.
- Enables secure exchange of data across isolated network enclaves with different levels of security classification.
- Governed by an established security policy and information assurance standards.
- Implemented as unidirectional or a bidirectional
- In a multi-level security environment, a unidirectional flow is the only valid configuration.

Information flows Security Policy Models

Confidentiality Policy ()

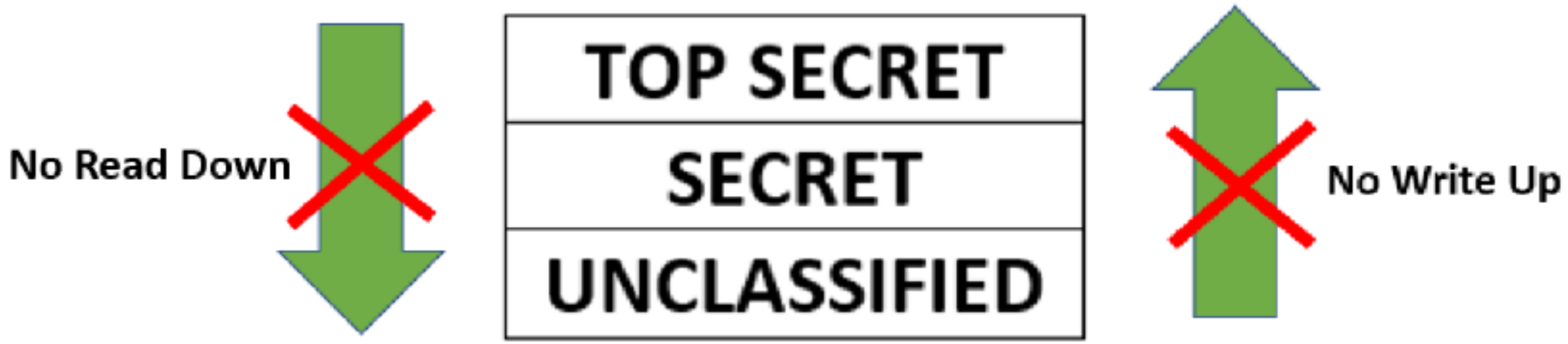
– Bell-LaPadula Modell: prevent the unauthorized disclosure of information.



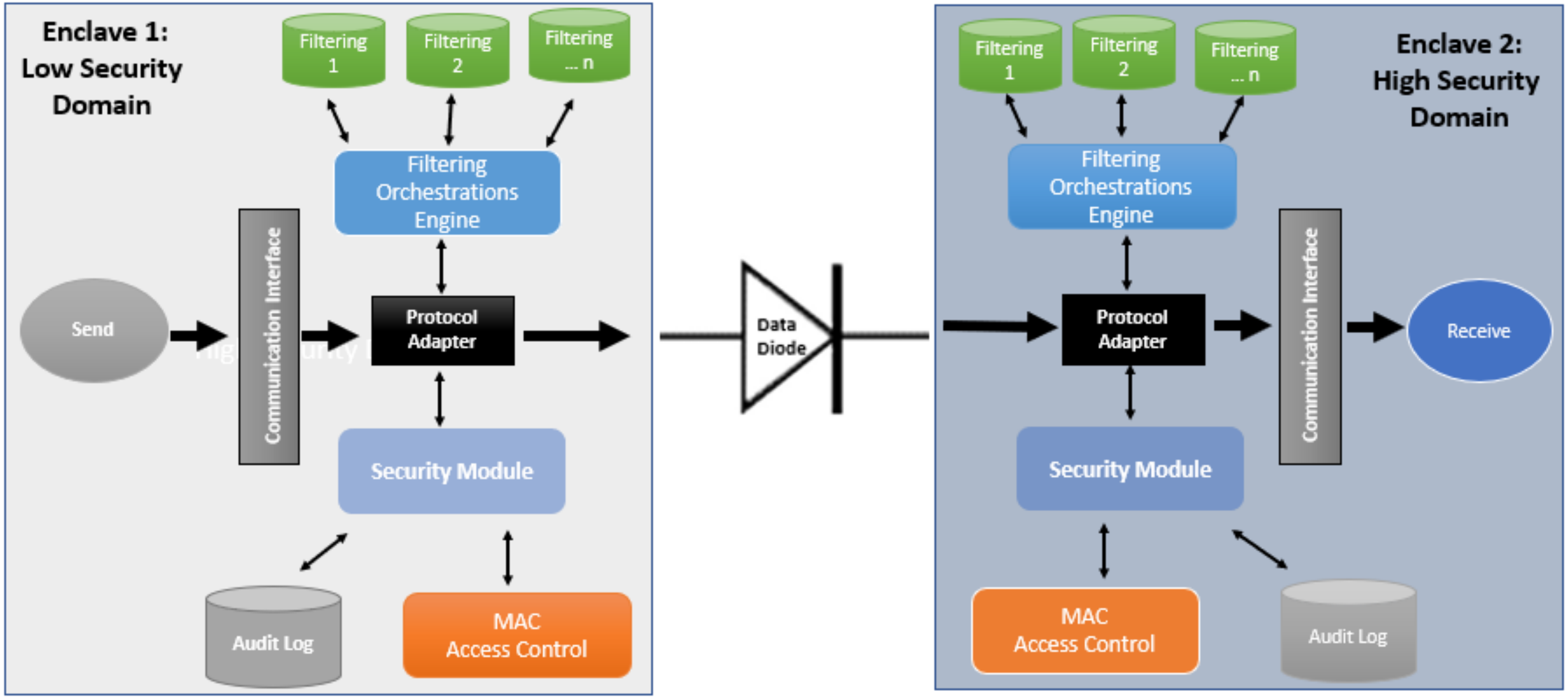
Information flows Security Policy Models

Integrity Policy Requirements

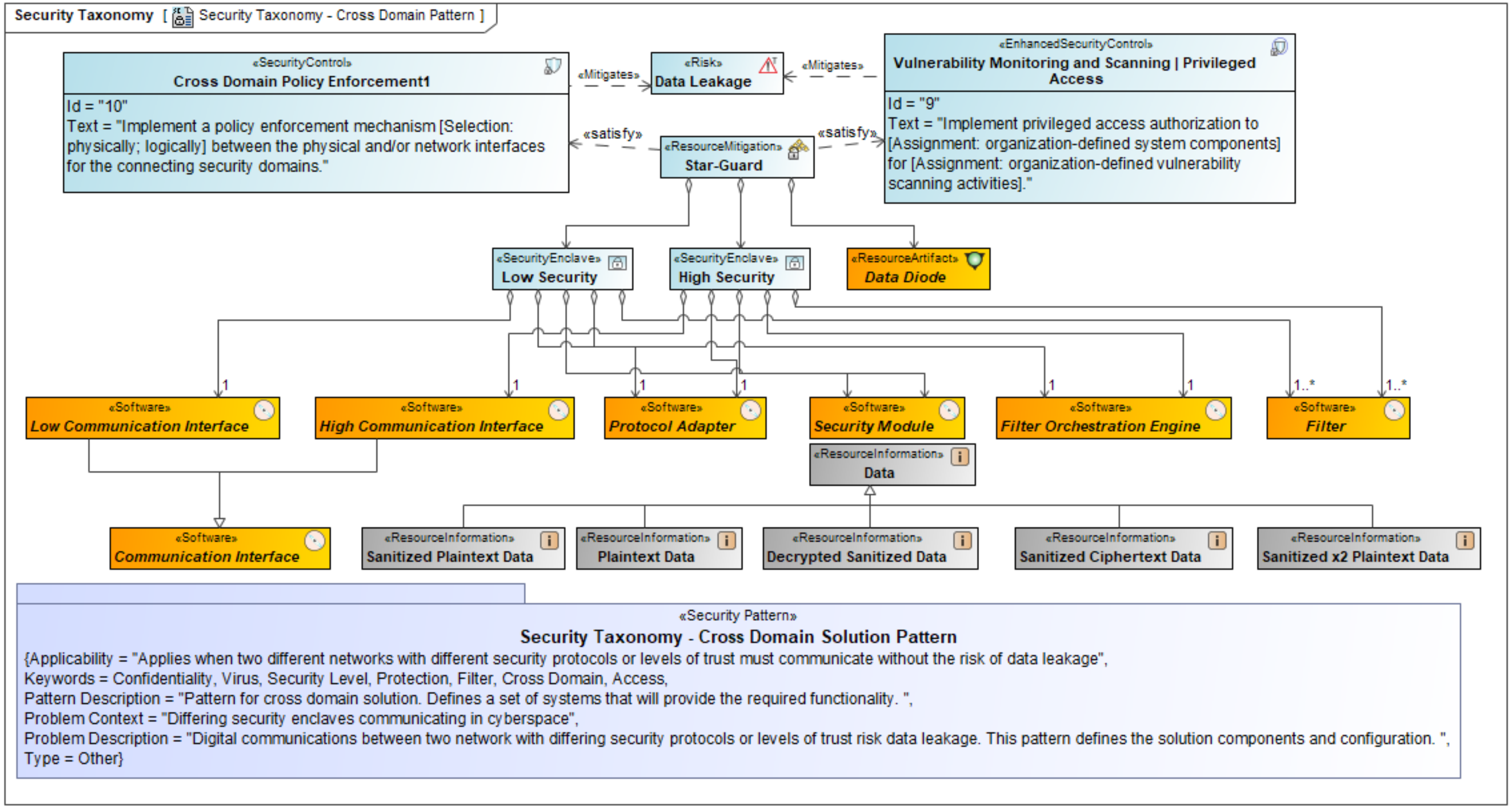
- Biba Integrity Model- protect high levels from less trustworthy low levels



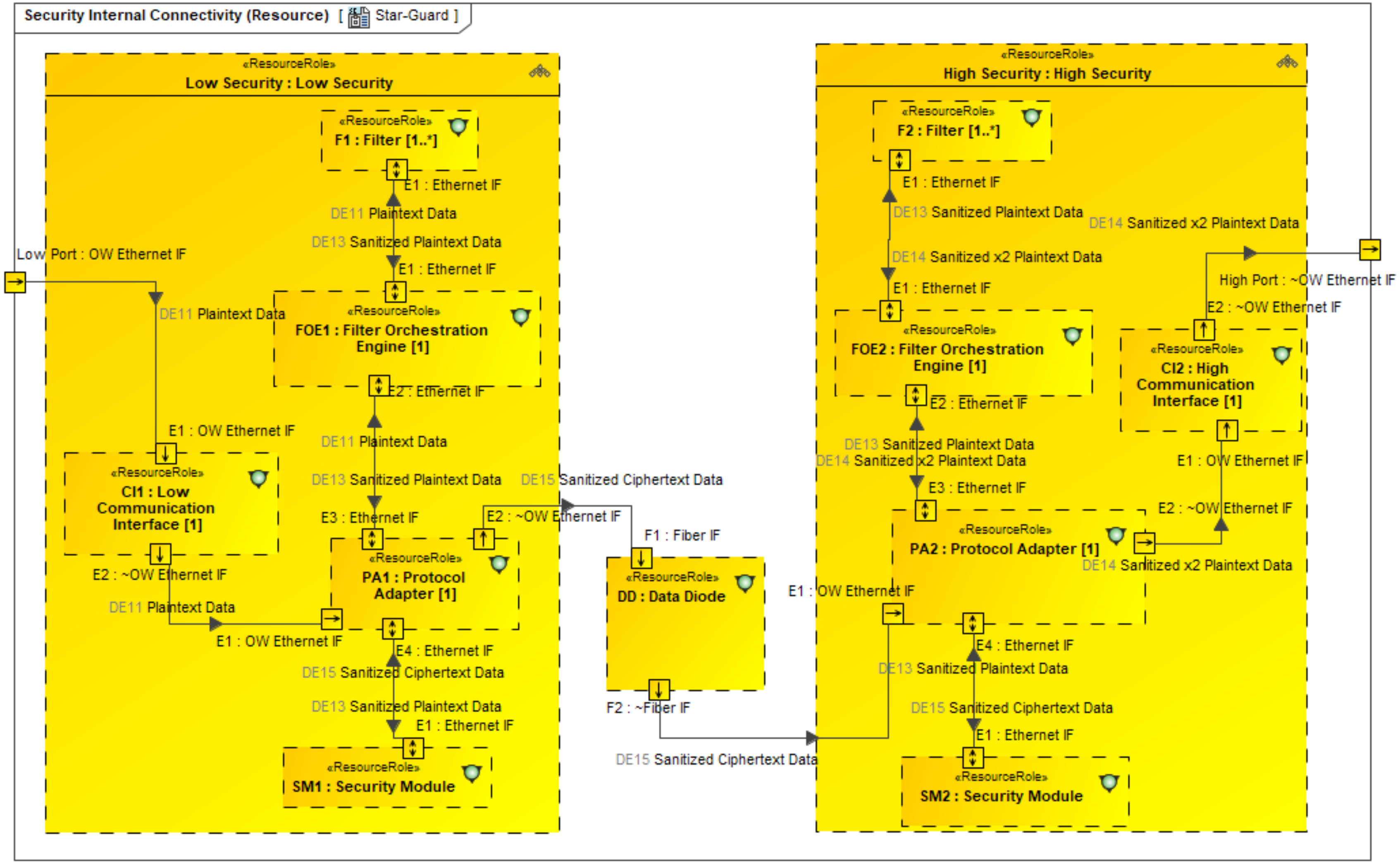
Cross Domain Solution Architecture



Cross Domain Solution Pattern Specification



Cross Domain Solution Internal Connectivity

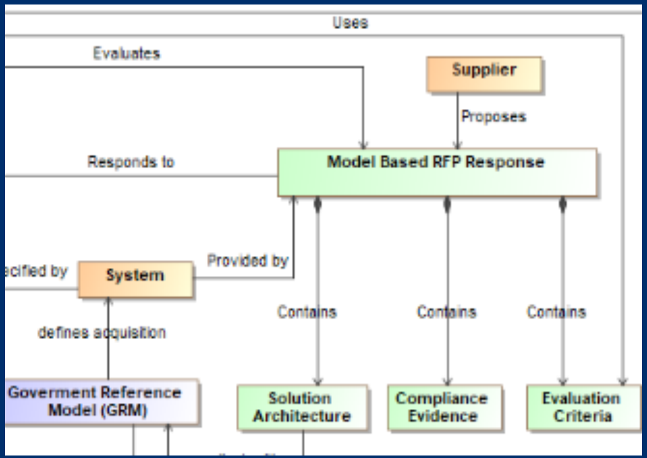


Model Curation & Model-Based Acquisition

BLUF: Model-Based Acquisition (MBAcq)

About MBAcq

Model-based acquisition is the Technical approach to acquisition that uses models and other digital artifacts as the primary means of information exchange, rather than document-based information exchange.



Why MBAcq Matters

Customers are increasingly specifying MBSE in RFPs
Customers are increasingly requiring models in proposals
Lack of standardization raises proposal learning curves

MBAcq standardization minimizes acquisition risk while improving communication across industry

OMG MBAcq User Group

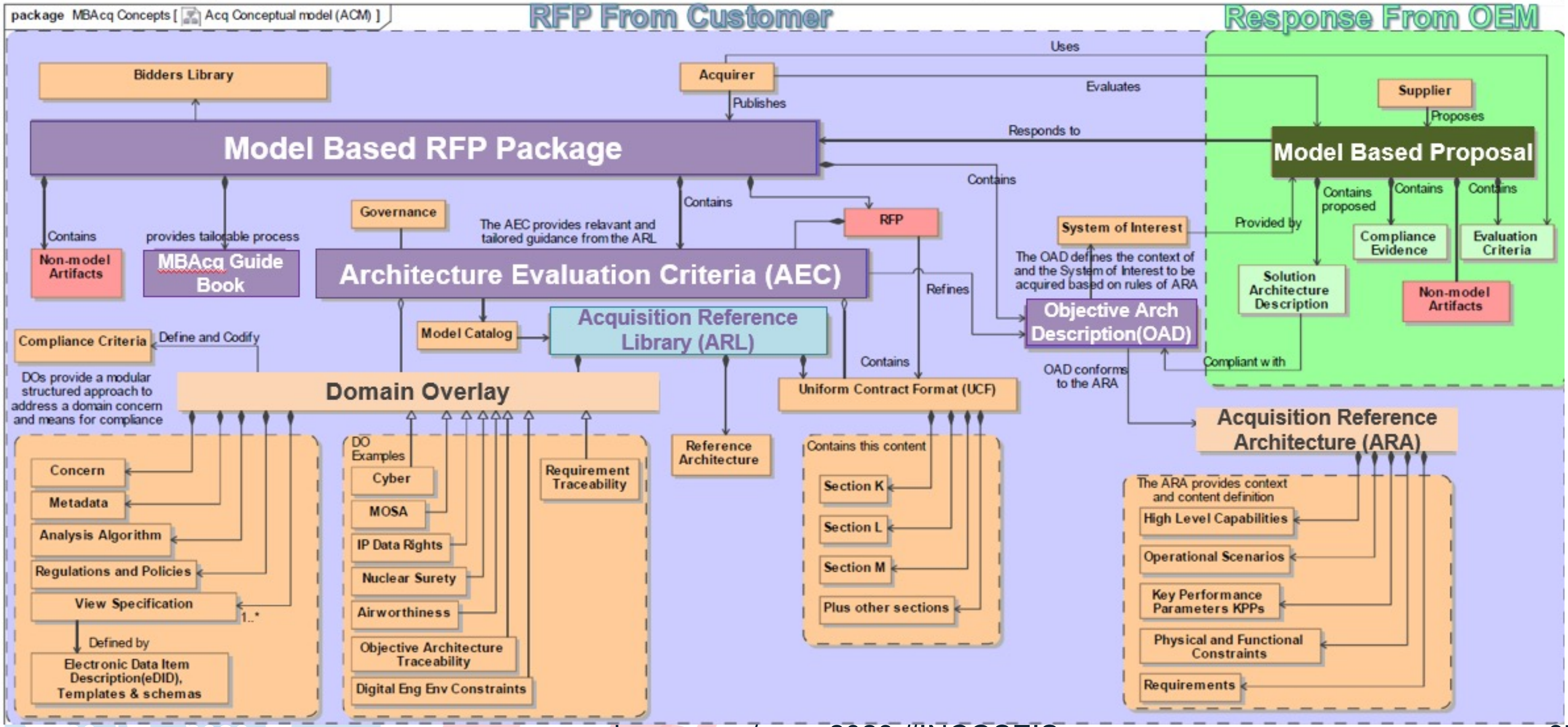
Is a broad industry body with participation from OMG, INCOSE, Armed Services, OUSD, DoD CIO, NDIA, DAU, FFRDCs and many industry suppliers such as Boeing, Northrop Grumman, Lockheed Martin, etc. working together to create the standards and guidance to successfully deploy MBAcq to the larger community.

Expected Timeline

2022: Formed Team & Framework
2023: Q4 Govt Ref Arch
2024: Q2 Acquisition Users Guide
Q2/3 DAU Acquisition Training
Q4 Acquisition Model Example

MBAcq Future State

Bringing it all together!



Domain Overlays (DOS)

Domain Overlay (DO) Description: A collection of constructs needed to support analysis for a **domain specific concern** using a standardized modular approach. Typical construct elements include:

Previously called Aspect Viewpoint Overlays (AVO)

- A set of regulations, constraints, rules… driving the analysis (i.e. MOSA, safety, certification, airworthiness, Space …)These could be provided as an instrumented lib
- A set of Data/Metadata required to address or support analysis, compliance or fit-for-purpose. Implementation example (Domain model/profile)
- Logic/algorithm needed to perform analysis using the metadata and regulations
- A set of Viewpoints to support various analysis (Certification plan, coverage, design trades, schedule and resources…)

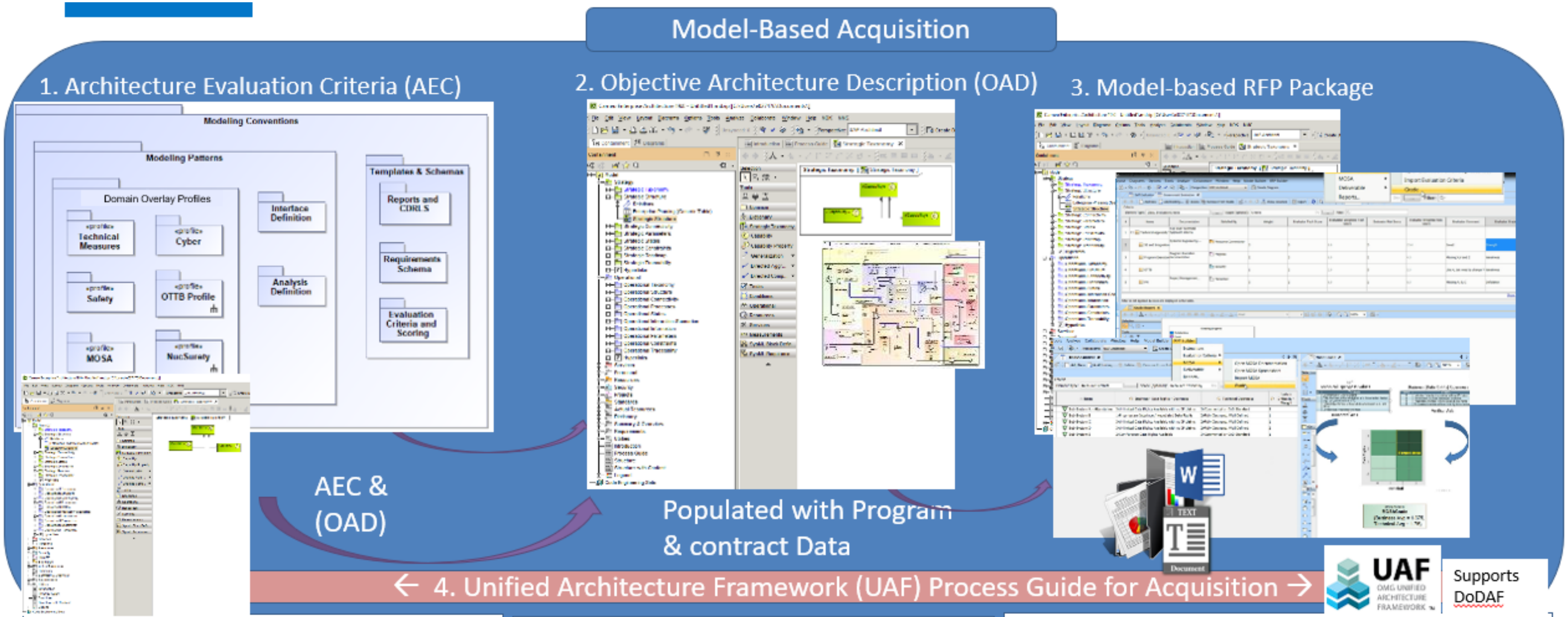
Characteristics

- Usually has associated regulations, governance that can be treated as pseudo requirements or constraints
- Cross-cutting both viewpoints/rows & aspects/columns
- Supports specific analysis associated with a Domain-Specific concern
- Can be created independent of a specific solution architecture description
- Can be applied or removed from a specific architecture description without impacting the AD, hence an overlay

Based on NDIA Actionable Architecture Using Aspect Modeling, L Hart 2018

Modular structured pattern to support standardization

Model Based Acquisition



1. The AEC provides model structure for RFP content and evaluation tools:

- Modeling Patterns
  - DO Profiles (i.e. MOSA, Data Rights, certs)
  - Interface & Analysis Definitions
- Templates & Schemas
  - Evaluation Criteria & Scoring (Section K, L, M)
  - Reports & CDRLS

2. The OAD is a descriptive model containing the program requirements, constraints and context

- High-level Capabilities, mapped to Operational scenarios, traced to requirements (e.g. CDD, SRD, Conops)
- Technical performance measures (i.e. KPPs, KSAs, MOEs..)
- Any required architectural partitioning including structural and functional

(Based on UAF acquisition process guide and template)

3. The Model-based RFP model contains the populated OAD&AC providing **RFP evaluation content, CDRL definitions** for documentation generation and **scoring tools** for solution validation and evaluation

4. UAF Process Guide provides the Acquisition Guidance for using MBAcq **to create, respond and evaluate a Model-based RFP.**

Model Curation

- "If we build it they will come." *Field of Dreams*
  - However, "they" need to know that it exists.
  - For a library to be of any use, It needs to be available and cataloged in public domain:
  - Catalogue must be available for update and improvement

Model Curation – The Status Quo

- Rouse (2015) stresses that "the wealth of existing models is often not used because of a lack of knowledge of these resources and the difficulty in accessing them.
- Lack of access to models, mistrust of models, and perception of legitimacy of models are all barriers in model reuse and longevity.
- Reymondet et al. (2016), 'model expertise is largely resident in individuals, and the ability to select and compose sets of models is typically limited to the original use. Lack of a centralized leadership authority results in models being owned and managed primarily at a local level.
- Rhodes & Ross (2015 "Modeling efforts are often duplicated across programs, and the individual programs may lack model experts preventing benefit from the collected wisdom of the enterprise.
- Models have been employed for numerous purposes in recent years (McBurney, 2011) and it is likely that digital engineering transformation may extend model use even further.
- A question arises as to whether a model curation function at the enterprise level could lead to more effective use of models and digital assets at all levels." (Rhodes, 2019)

Model Curation – The Future

- Wu et al (2021) describes a maturity assessment of Systems Engineering reusable assets to facilitate MBSE adoption, basically a Capability Maturity Model (CMM) for model and asset reuse.
- Hause (2014), defines how the OMG Reusable Asset Specification (RAS) was used to build an asset library to harvest, curate, and share SysML model assets to promote and enable model asset reuse.
- The OMG RAS was published in 2005 and provides a means of categorizing assets for reuse.
  - The PTC Asset Library is the only implementation the authors are aware of that is still in use.
  - The solution may be a standard for a library for sharing these reusable assets, whether they are for security or any other purpose.
  - The authors will be proposing this to INCOSE and the OMG.
  - We will continue to build and promote these patterns as a means of improving system security and promoting reuse of model assets.
  - Could also be added to the OMG UAF standard page as are other documents and models.

Summary and Conclusion

- **Design patterns serve as a building block for promoting reusable knowledge.**
- **Reusable patterns enable architectural solutions for system design and architecture problems.**
- **Patterns enables system thinking and accelerate system design and development while promoting reusability.**
- **Contribution to the foundation of the design pattern concept has crafted new design patterns for both physical (fire prevention and detection) and cyber-security (CDS).**
- **Concept of System library are key enabler for catalog of solution elements of security pattern libraries.**
- **UAF Modeling Language (UAFML) standard serves as the primary modeling approach to realize the design of the security patterns presented.**

Don’t be an Octopus; Share Your Knowledge!

https://rare-gallery.com/108495-finding-dory-hank-nemo-fish-octopus-animation.html

Questions

About the Authors

Matthew Hause is an SSI Principal and MBSE Technical Specialist, a former PTC Fellow, a co-chair of the UAF group and a member of the OMG SysML specification team. He has been developing multi-national complex systems for over 45 years as a systems and software engineer. He started out working in the power systems industry and has been involved in military command and control systems, process control, manufacturing, factory automation, communications, SCADA, distributed control, office automation and many other areas of technical and real-time systems. His roles have varied from project manager to developer. His role at SSI includes mentoring, sales presentations, standards development, presentations at conferences, specification of the UAF profile and developing and presenting training courses. He has written over 100 technical papers on architectural modeling, project management, systems engineering, model-based engineering, and many other subjects.

Ademola (Peter) Adejokun has over 20 years' experience in systems and software engineering; he currently works as a cyber systems security engineer at Lockheed Martin Aeronautics in Fort Worth, Texas. Ademola is a licensed professional engineer in Texas, an INCOSE ESEP, Six Sigma Black Belt, a certified PMP. Ademola is a senior member of the IEEE and ACM. He serves on the Object Management Group UML Testing Profile, UAF and System Assurance Task Force. He also serves on the National Council of Examiners for Engineering and Surveyors (NCCEES) Software and Electrical/Computer Engineering PE Licensure Exam Committees.

Mitchell Brooks is a cyber systems engineer at SSI, specializing in modeling cybersecurity aspects of larger systems. He also instructs a course designed to introduce systems engineers to UAF. He has previously been included on research teams helping to examine how we approach IT security in order to improve efficiency and effectiveness. He holds a degree in cybersecurity from Stevens Institute of Technology and an MBA from Saint Mary's College of California.

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

www.incose.org/symp2023
#INCOSEIS