31st Annual INCOSE international symposium

virtual event

July 17 - 22, 2021

Using Security Views in UAF

www.incose.org/symp2021

Presenters

- Matthew Hause,
  Principal
  System Security Innovation
  - MHause@SystemXI.com

- Lars-Olof Kihlström,
  Principal Consultant
  Syntell AB
  - Lars-Olof.kihlstrom@syntell.se

Agenda

1. The importance of security
2. The UAF architecture framework and the grid
3. Why Add Security?
4. A UAF security model example
5. Conclusions

Syntell

The Importance of Security

Cyber-security

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

MBSE is

- 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).
- MBSE ***must*** deal with security issues in general including cyber-security.
- Security handling is a cross-cutting concern that affects the system definition in its entirety.

The Unified Framework Architecture Grid

- Looking at the architecture of an enterprise in a grid was originally defined by Zachmann.
- The importance of aspects such as What needs to be done, How and Why and When were used in his grid but has an even older use.

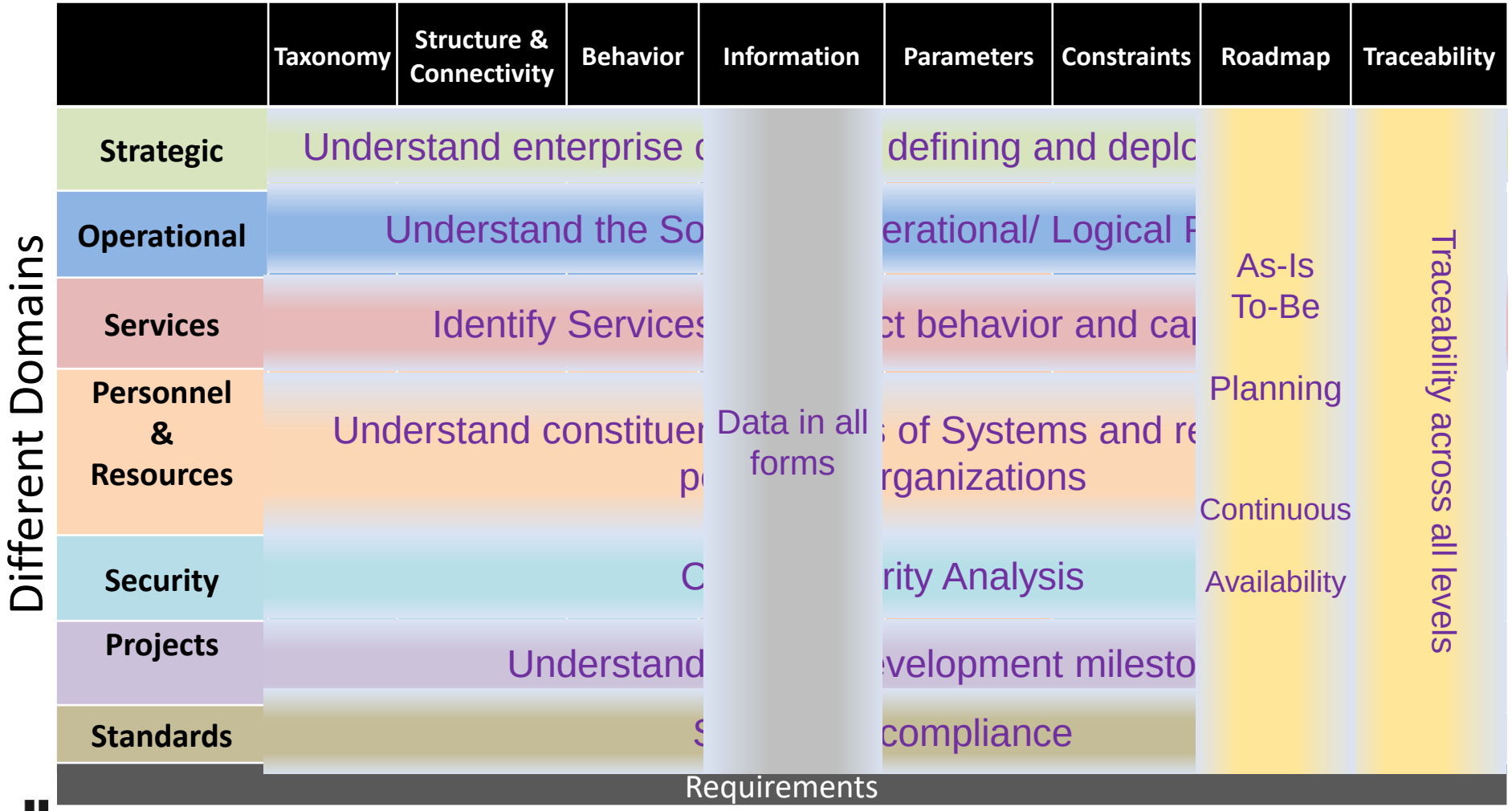
I KEEP six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who.
I send them over land and sea,
I send them east and west;
But after they have worked for me,
I give them all a rest.

The Elephant's Child

Rudyard Kipling

UAF Grid

Standard means of expression – model kinds



	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 Rs-Is	Physical schema, real world results	Measurements Pm-Me	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	-	-			Security Constraints Sc-Ct	-	-
Projects Pj	Project Taxonomy Pj-Tx	Project Structure Pj-Sr	Project 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											

Agenda

1. The importance of security
2. The UAF architecture framework and the grid
3. Why Add Security?
4. A UAF security model example
5. Conclusions

Why Add Security Views?

- The need for security is ubiquitous
  - People, infrastructure, electrical and electronics systems, networks, cyber, physical, social, etc.
- Security is a system aspect, not a component
  - Embedded, cross cutting, integrated
- Security spans the lifecycle
  - system concept inception to implementation, updates, maintenance, and disposal
- Not currently in DoDAF
  - The UAF views are based on the Canadian DNDAF with a number of additions

Security Aspects Dealt with in UAF

Stakeholders:

- Security Architects, Security Engineers. Systems Engineers, Operational Architects.

Concerns:

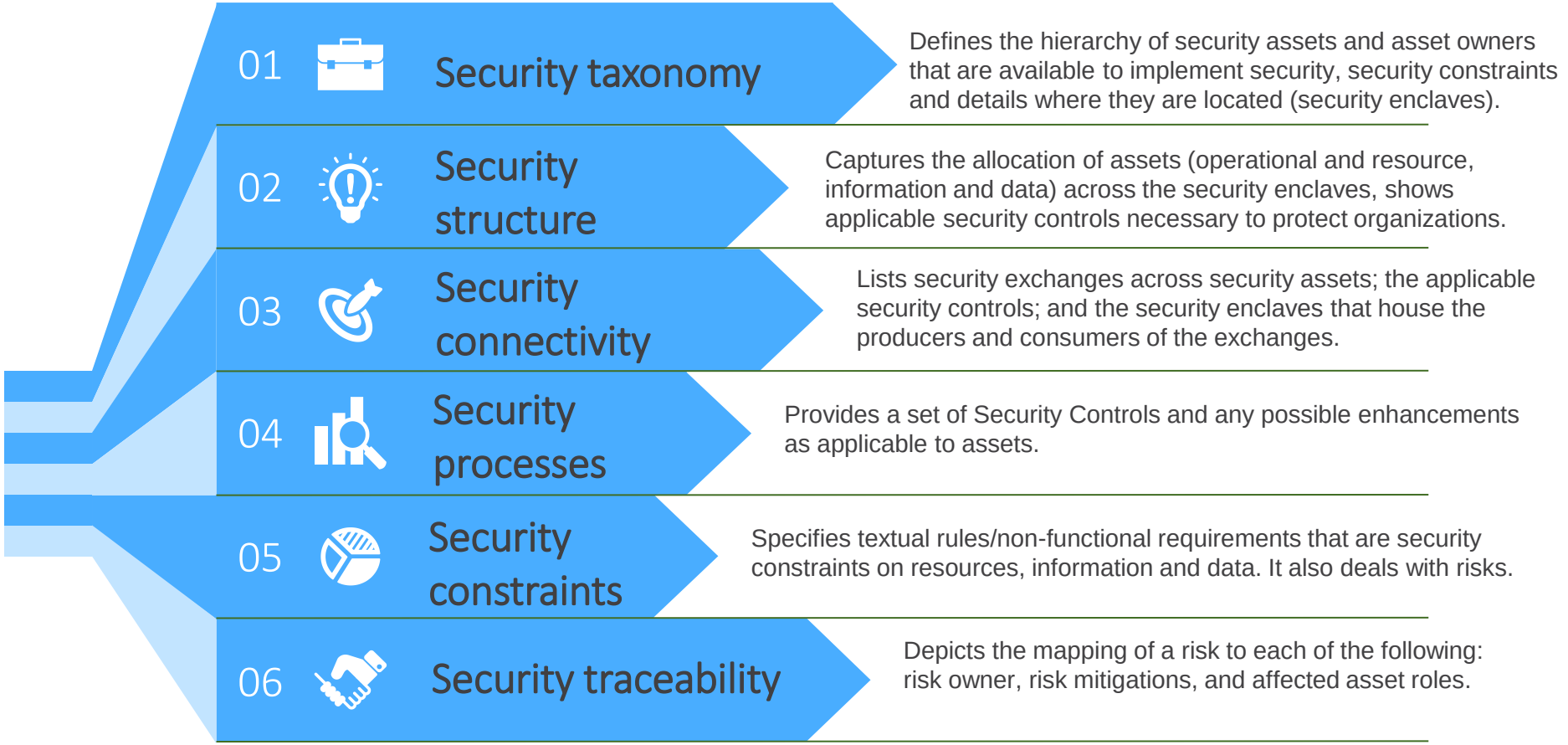
- Addresses the security constraints and information assurance attributes that exist on exchanges between resources and Operational Performers

Definition:

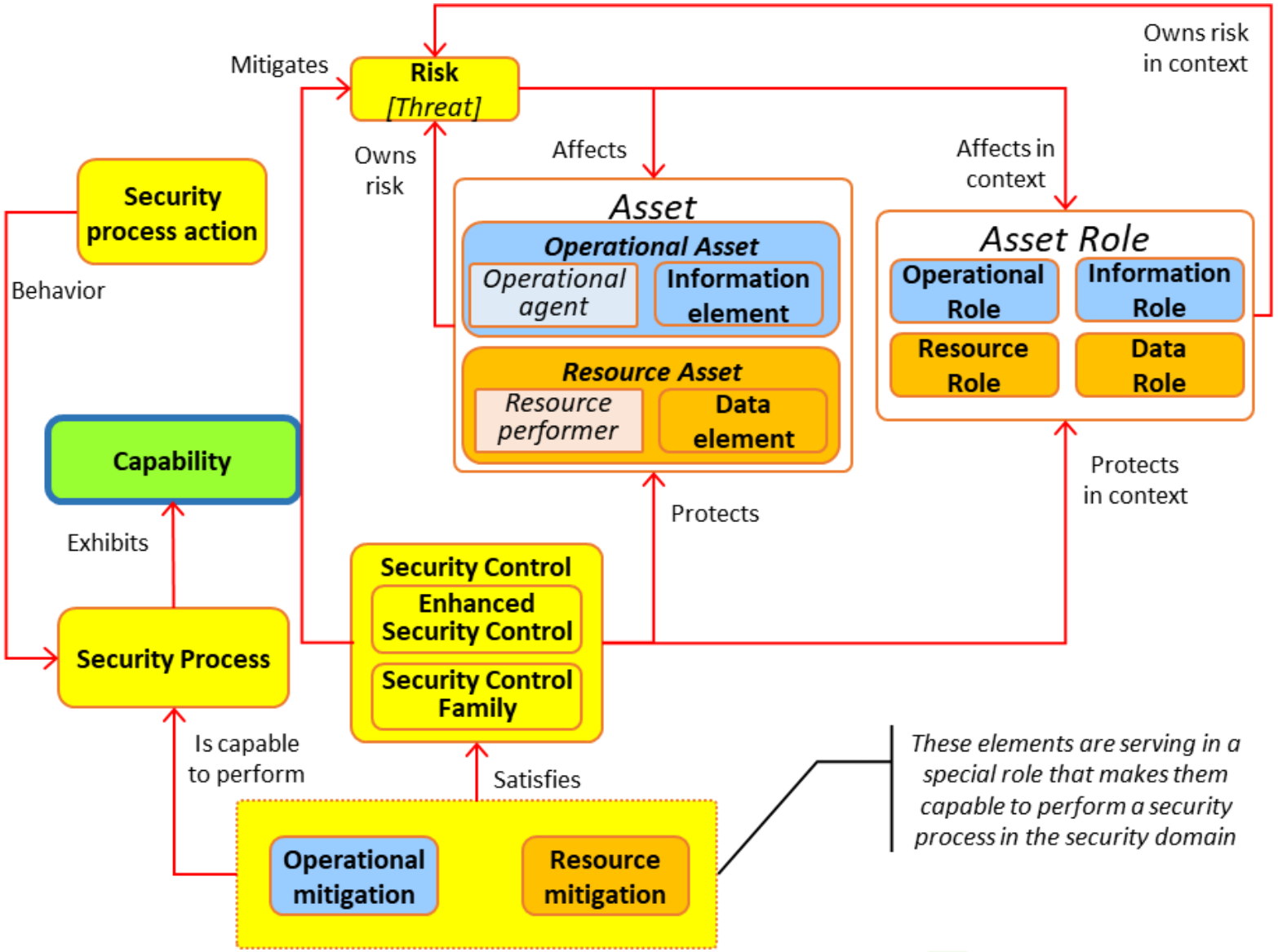
- Definition: illustrates the security assets, security constraints, security controls, families, risks, mitigations, interactions, processes, and measures required to address specific security concerns.

Views for Security in UAF

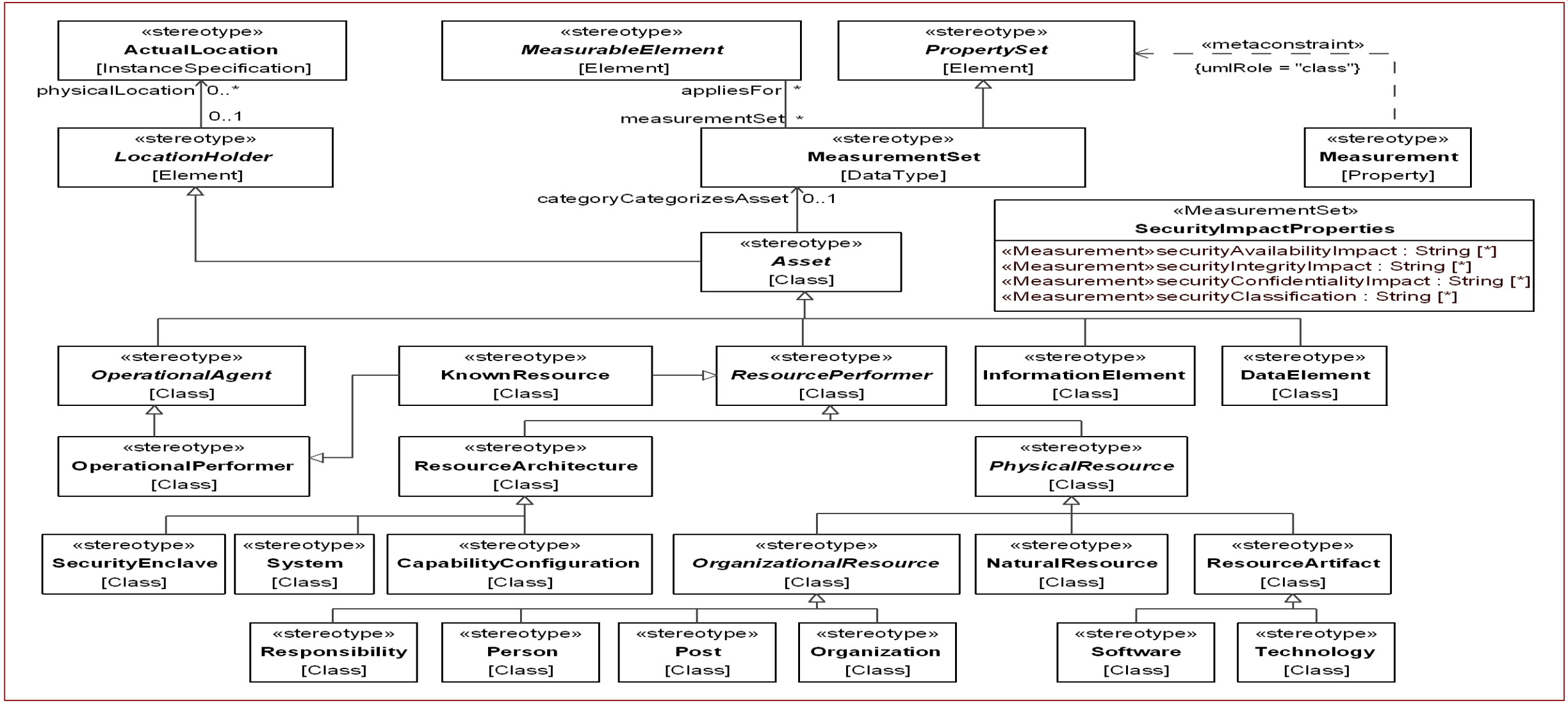
Security views in UAF



Security Taxonomy Example



Security Taxonomy Example Profile



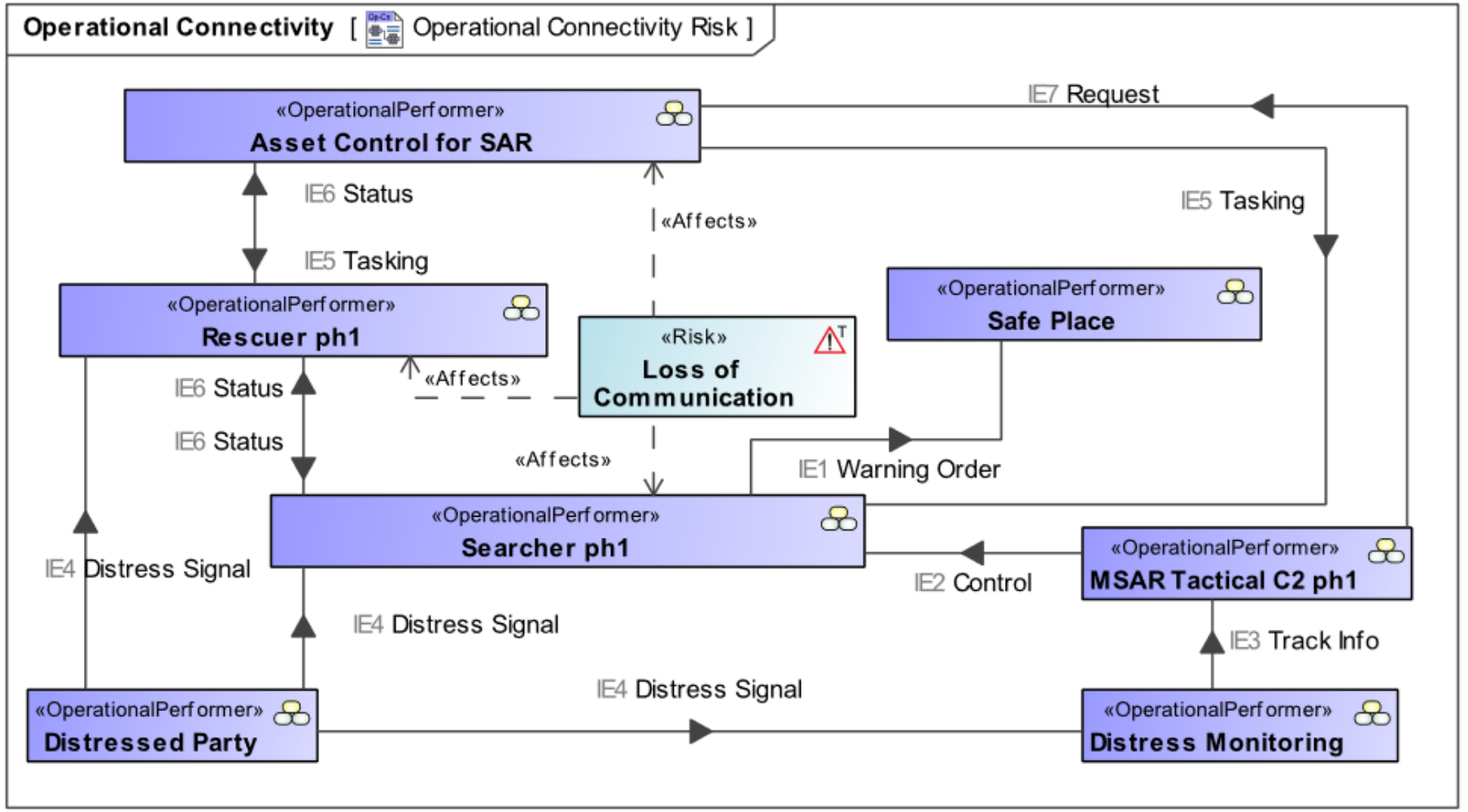
Agenda

1. The importance of security
2. The UAF architecture framework and the grid
3. Why Add Security?
4. A UAF security model example
5. Conclusions

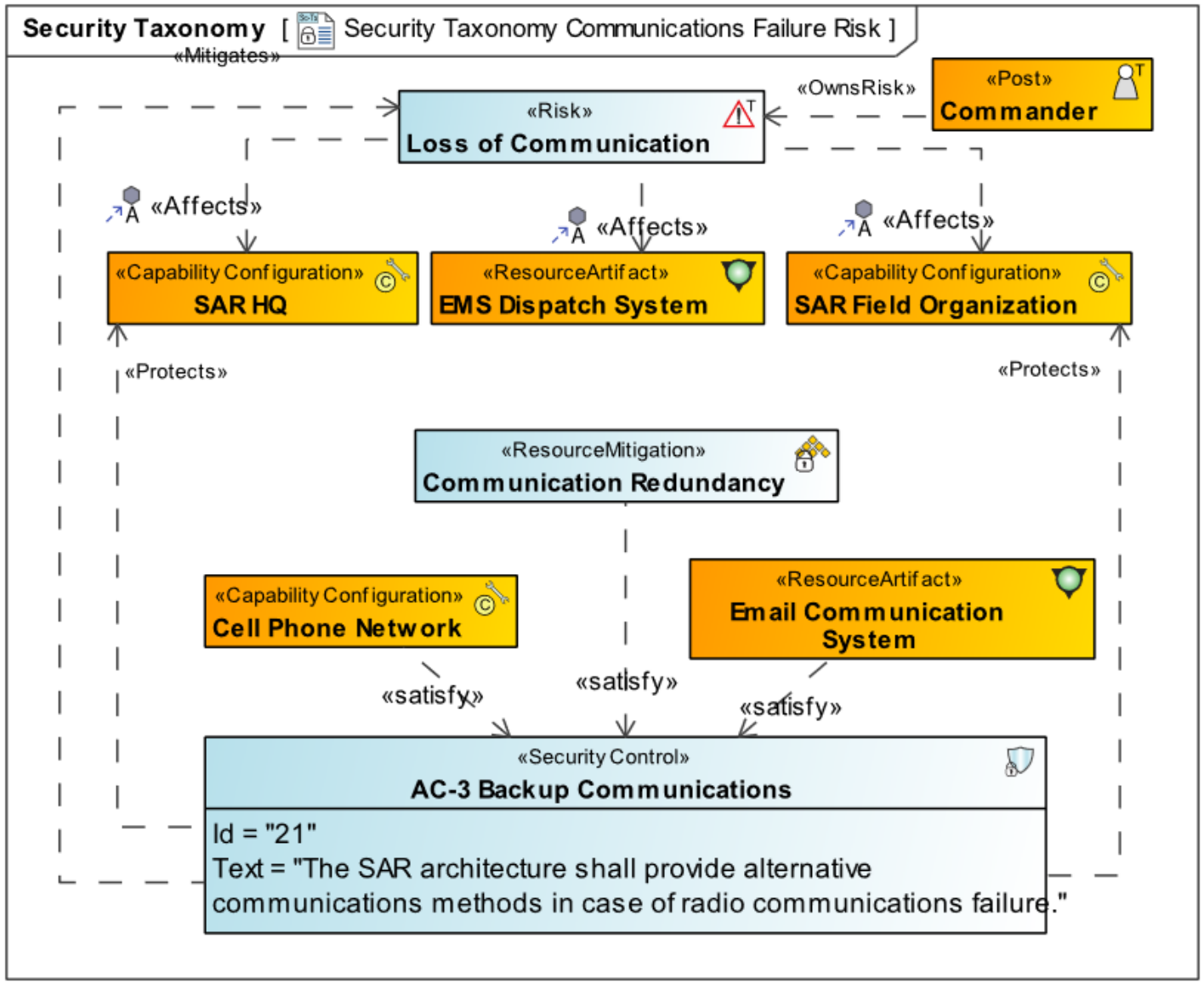
An example

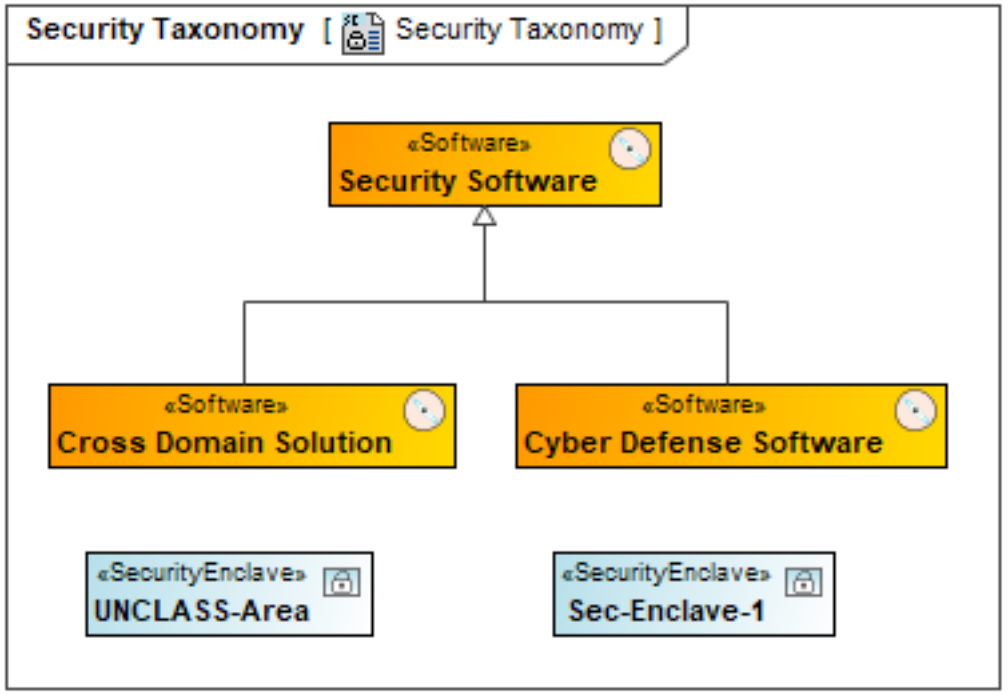
- A model example that deals with security is used in this presentation (Search and rescue) and the integration in UAF views of security elements with operational elements and resource elements are demonstrated.
- Operational issues also needs to be dealt with from a security aspect and risks can be associated with an operational description.

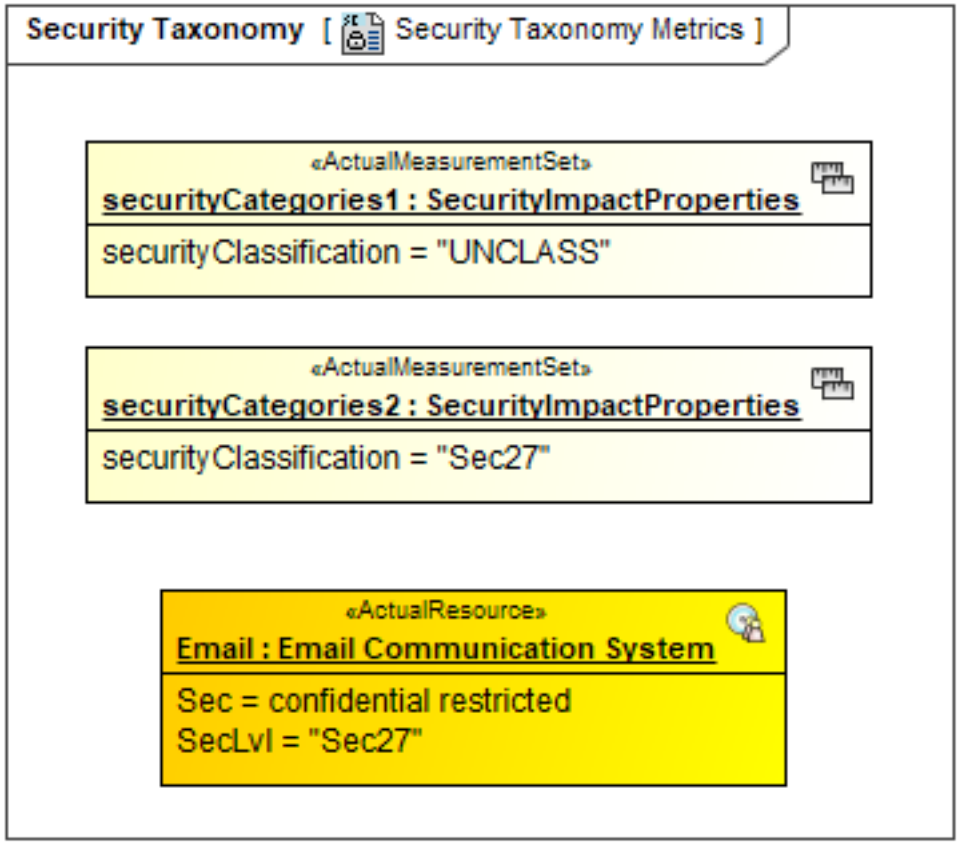
Operational Connectivity and Risk



Resulting Resource Risk Handling







Security Taxonomy

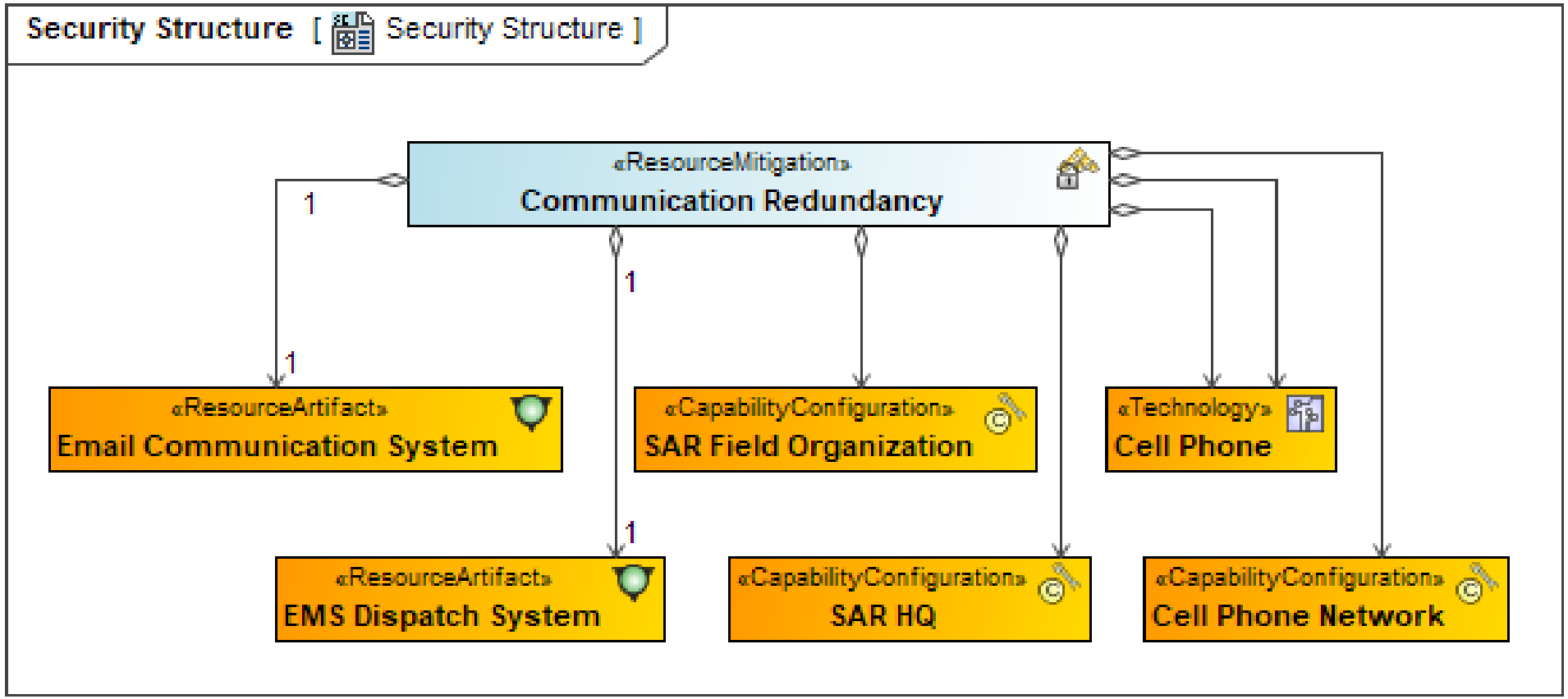
Defines the assets across security domains and their locations. Includes hardware, software, systems, operational.

Security Measurements

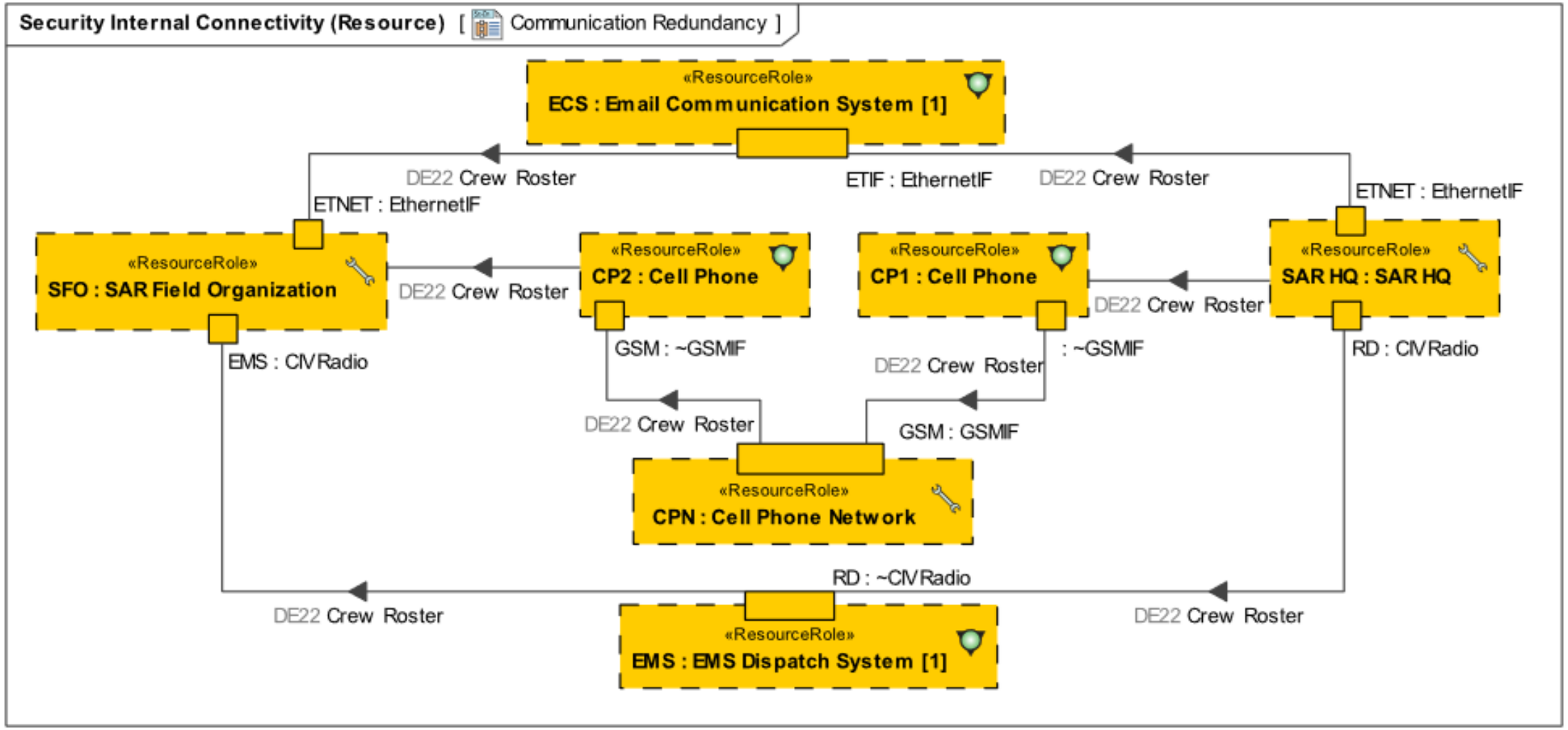
Actual security classifications that will be used in the model.

Security Structure (Sc-Sr)

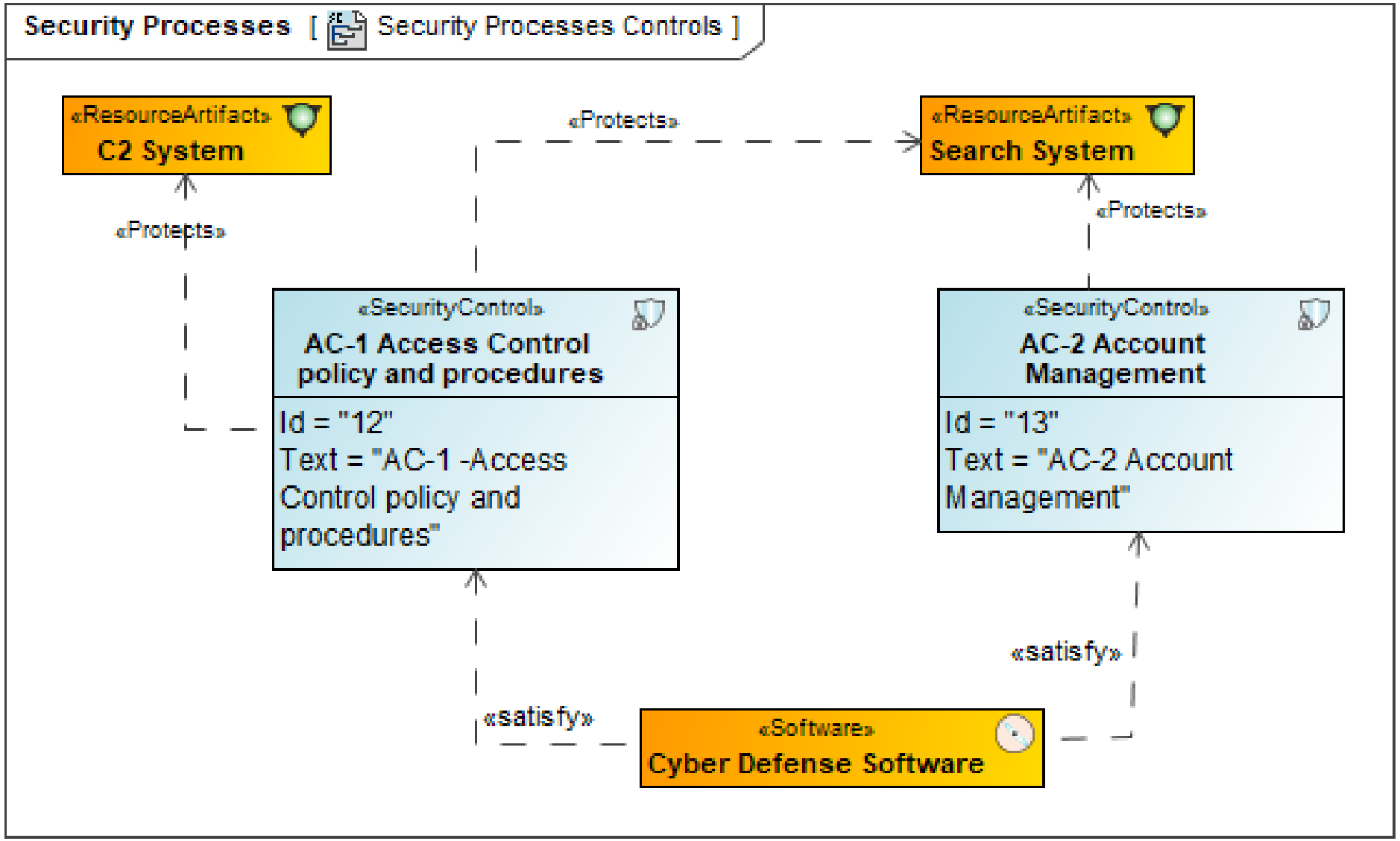
- Shows structure of security systems and information and where it is used



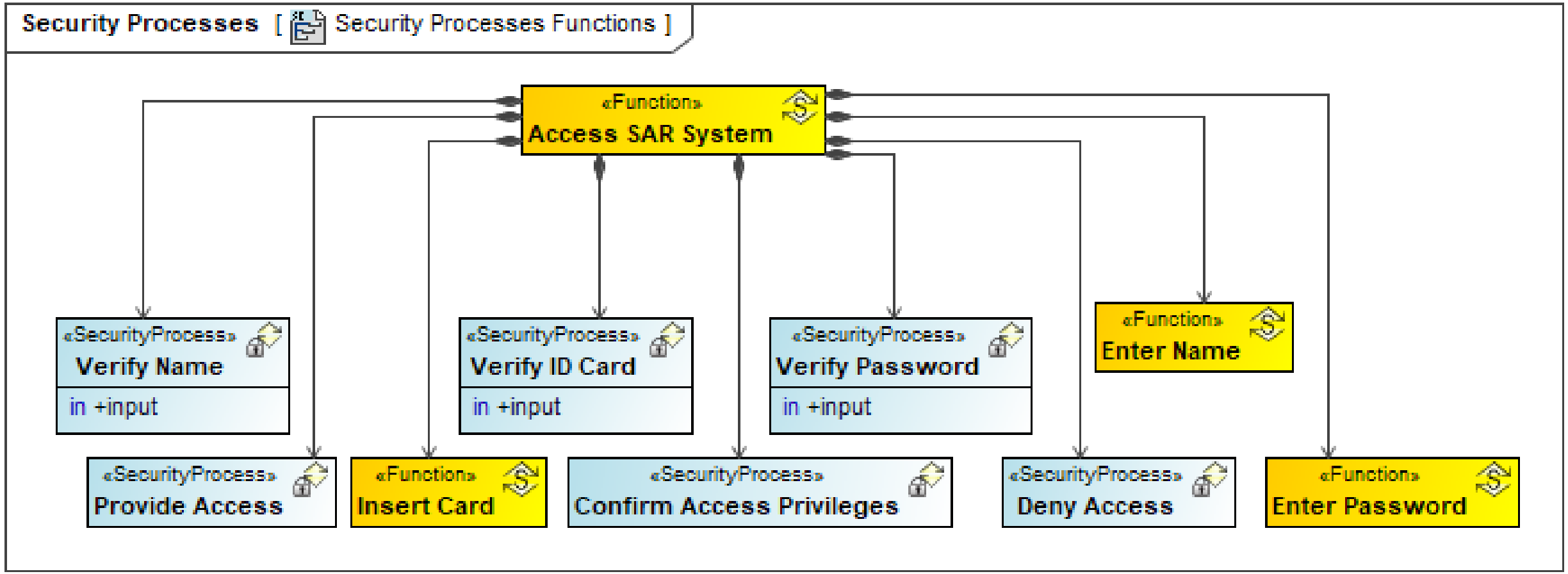
Security Structure (Sc-Sr)



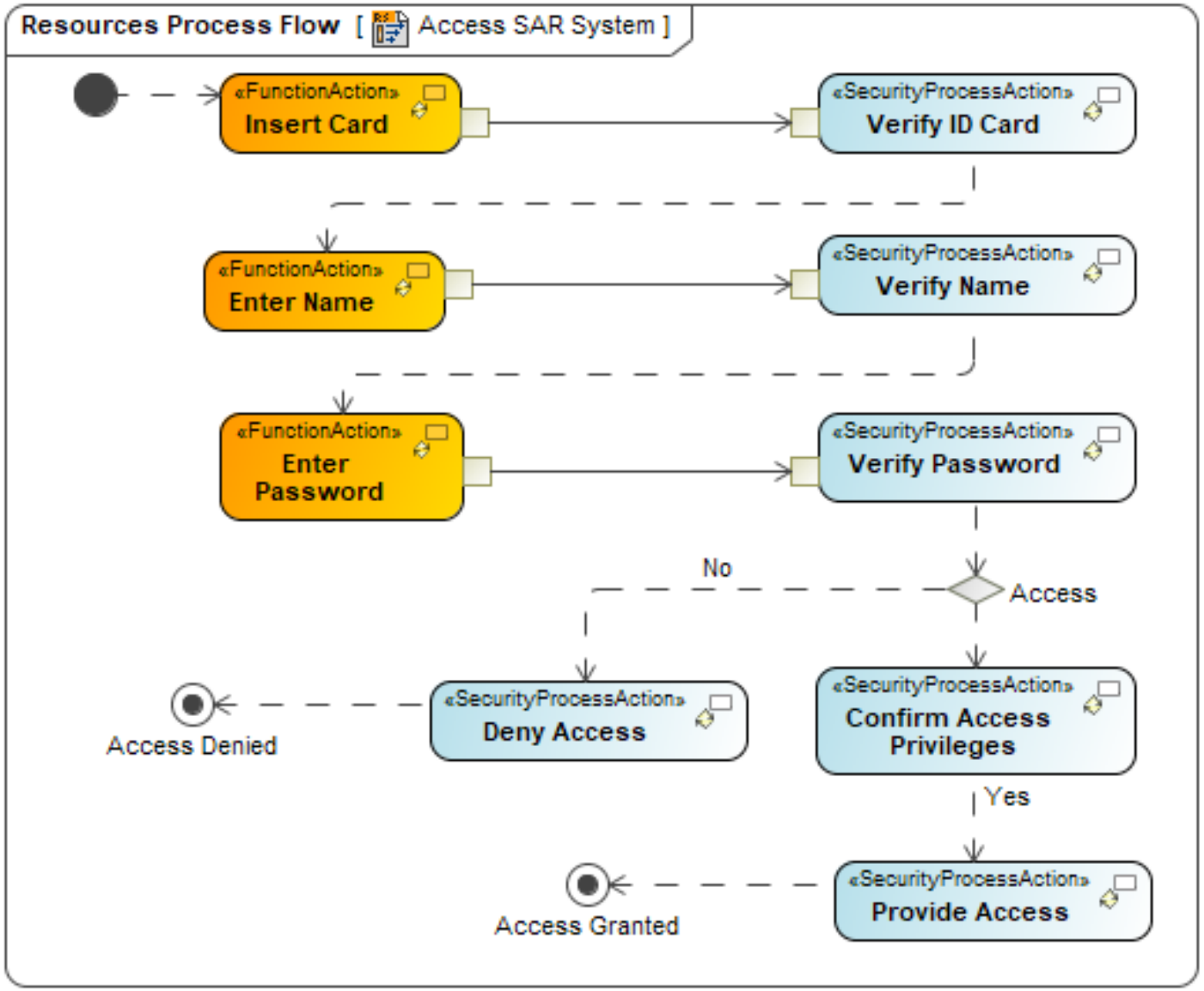
Security Controls



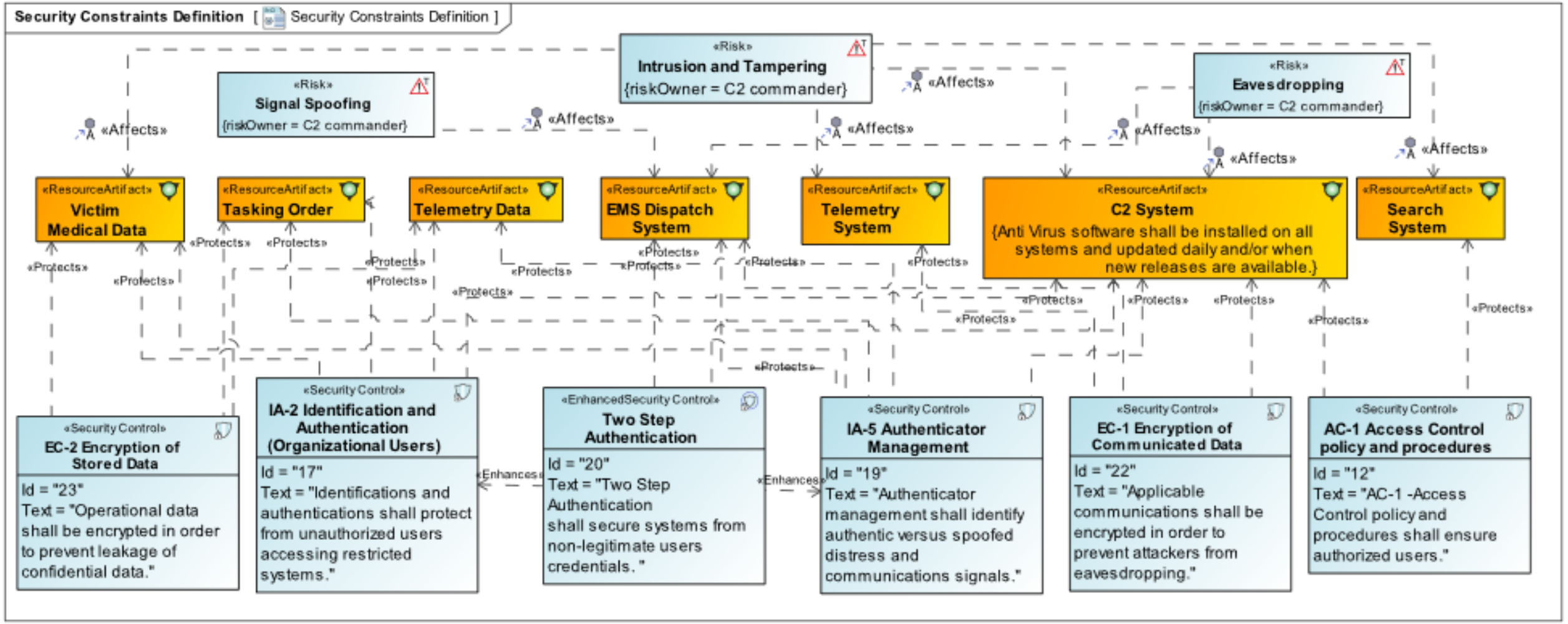
Security Process (Sc-Pr)



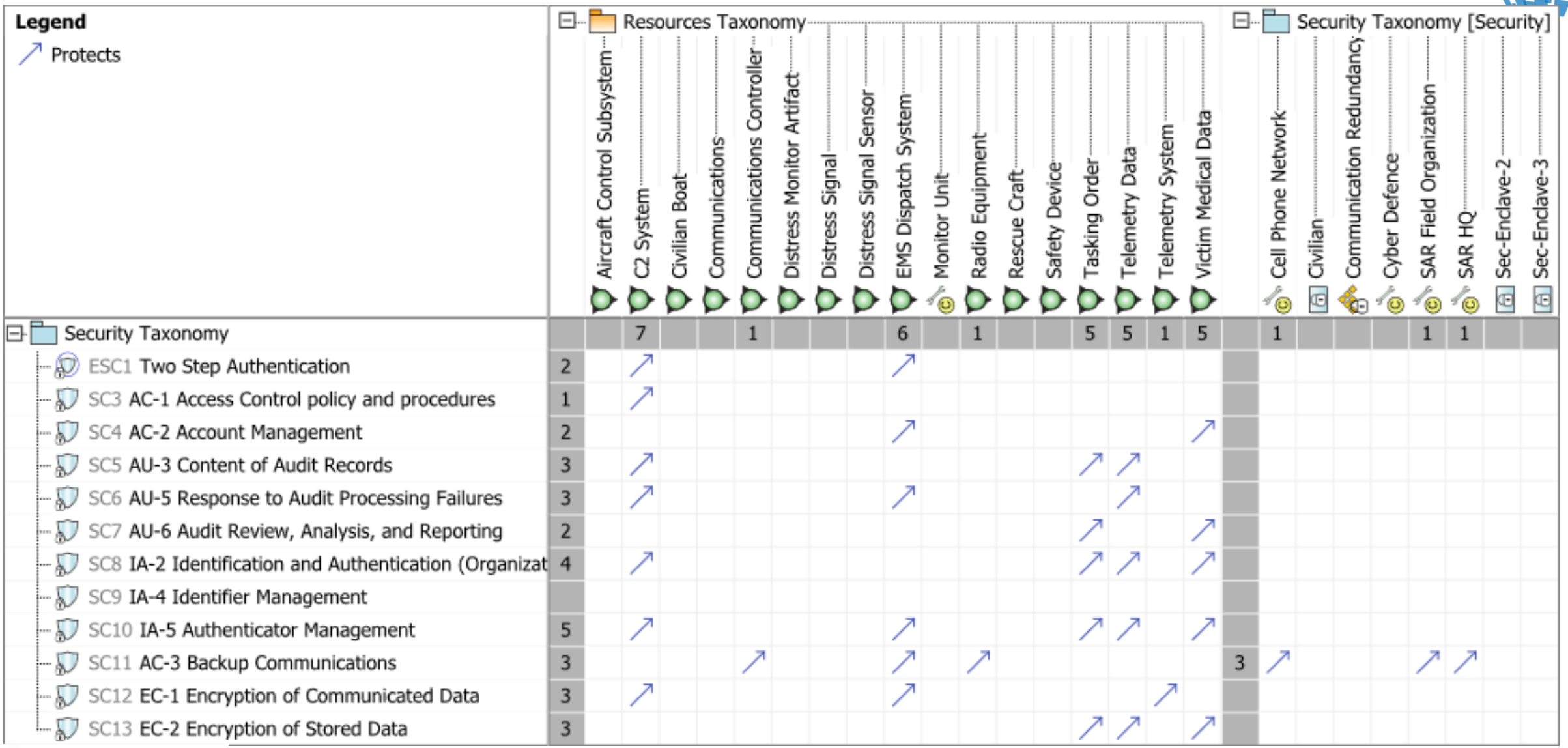
Security Process (Sc-Pr)



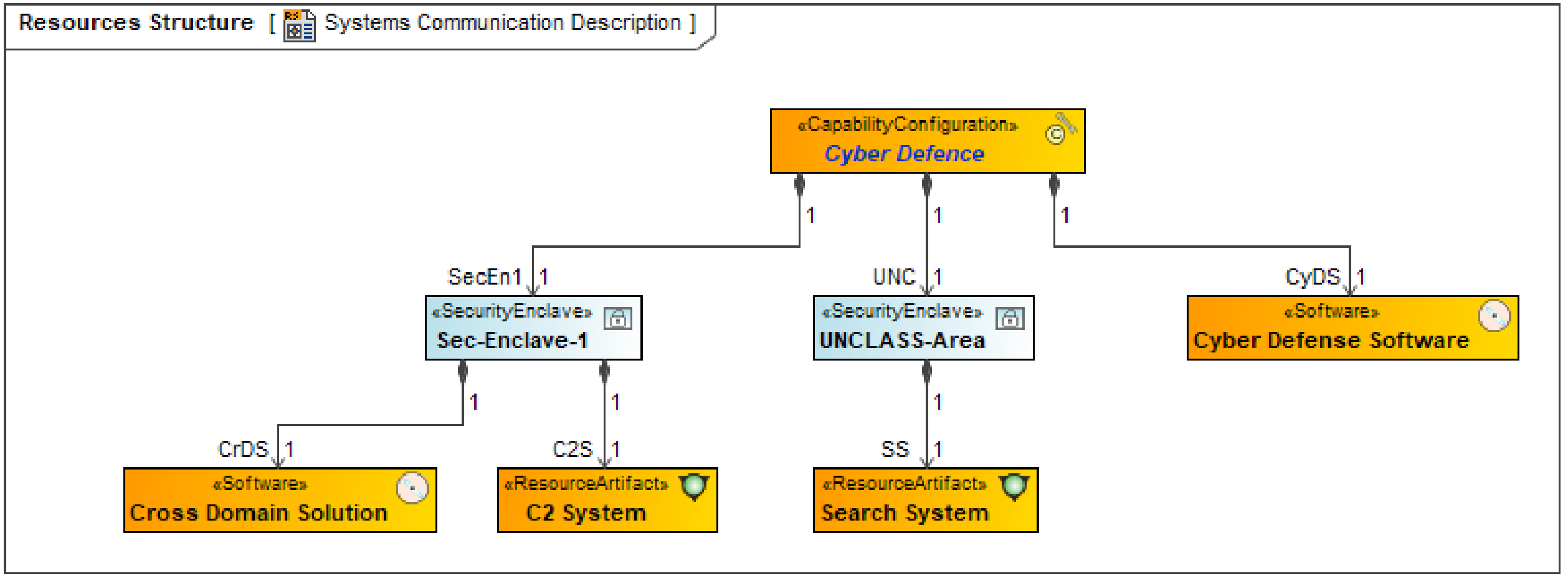
Security Constraints (Sc-Ct)



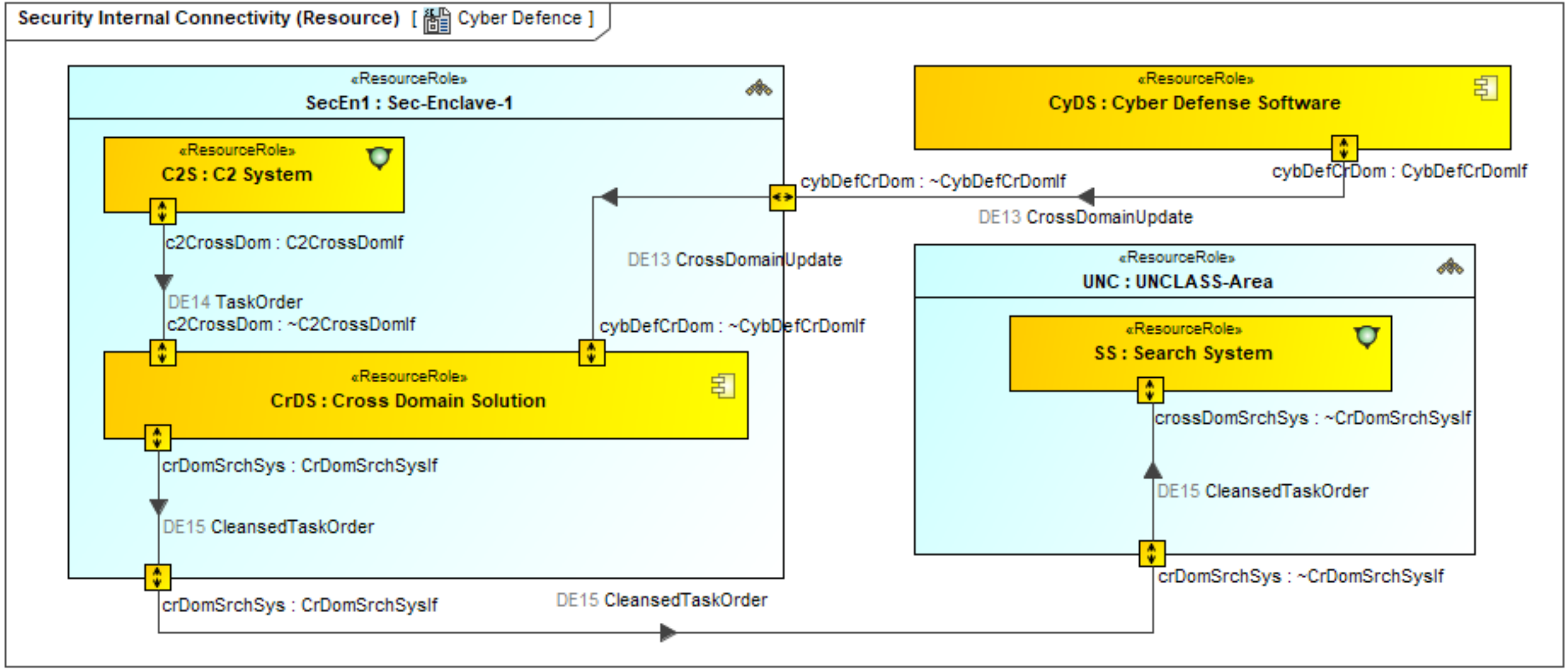
Security Traceability (Sc-Tr)



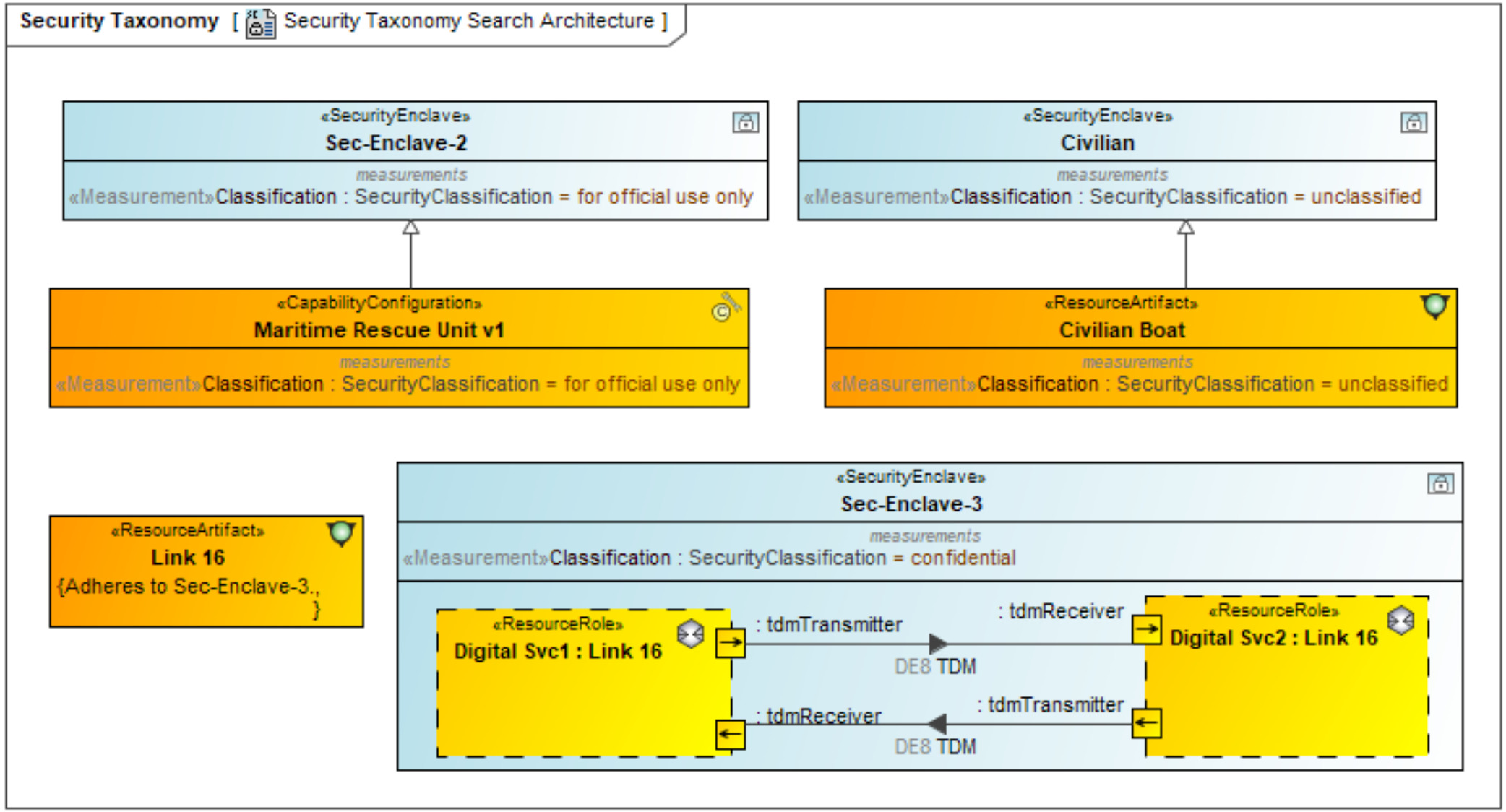
Security Integrated into Other Views



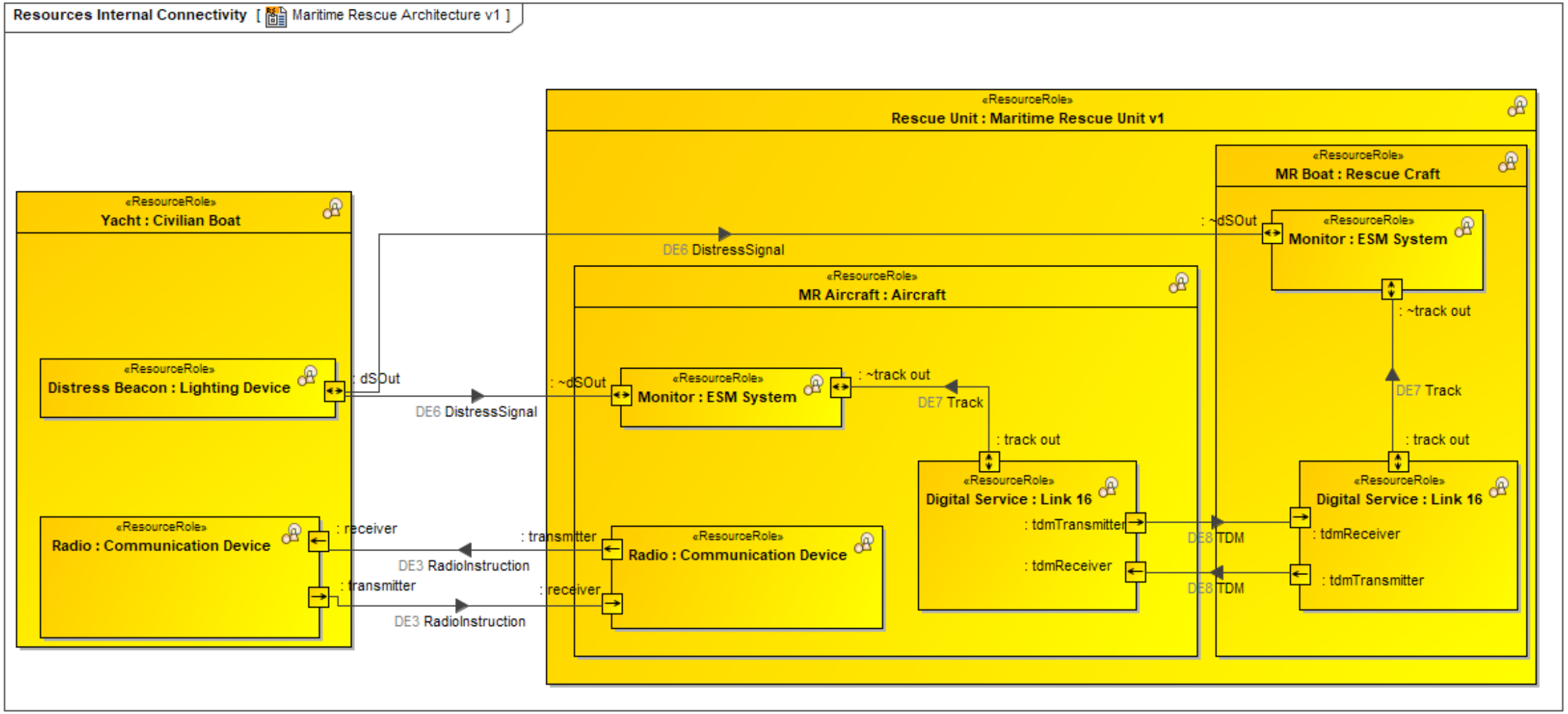
Security Integrated into Other Views



An Approach to Handle Security Enclaves



The Example Resource Architecture



KDM Analytics

Working Together to Build Confidence

Risks Analysis

Djenana Campara

Chief Executive Officer

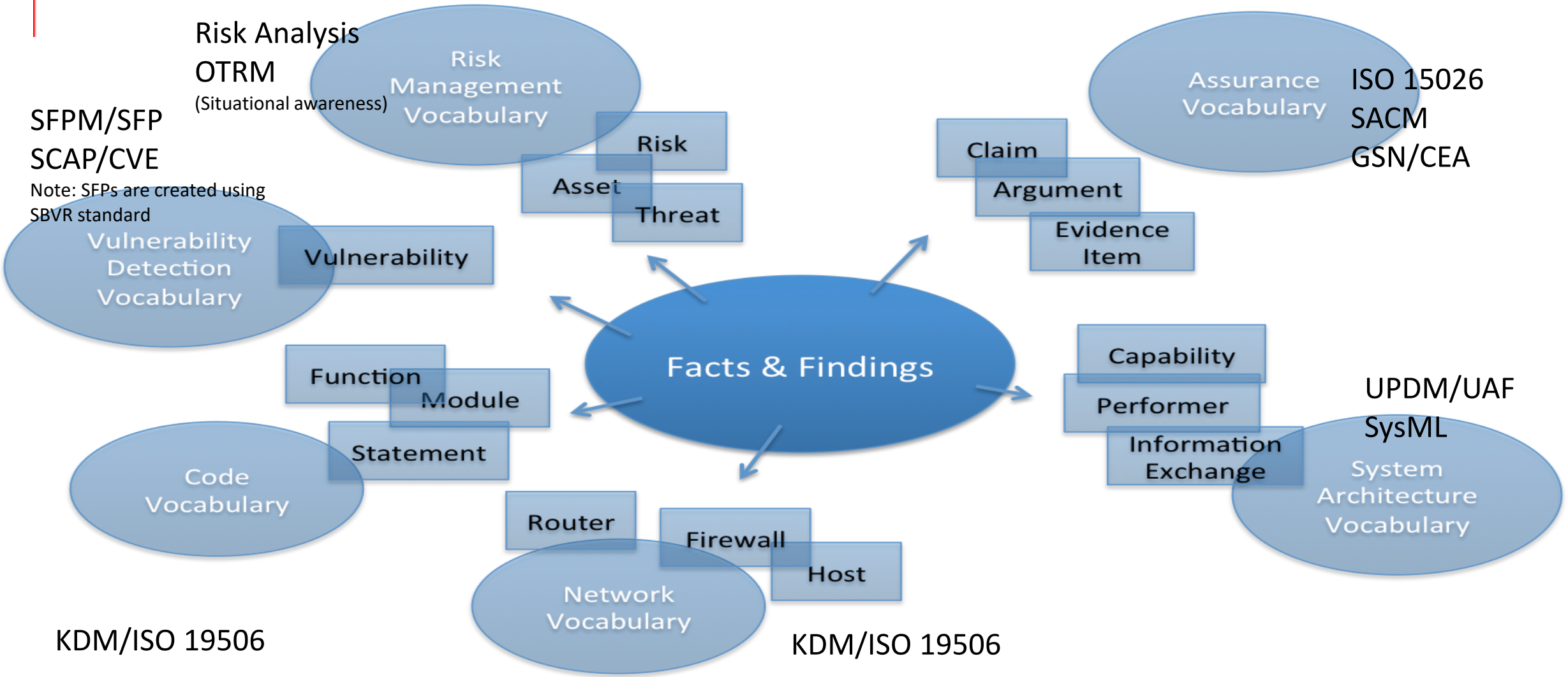
Member, Object Management Group Board of Directors

Chair, System Assurance Task Force

Syntell

Ecosystem Foundation: Common Fact Model

Data Fusion & Semantic Integration



Tools integration possible only through standards

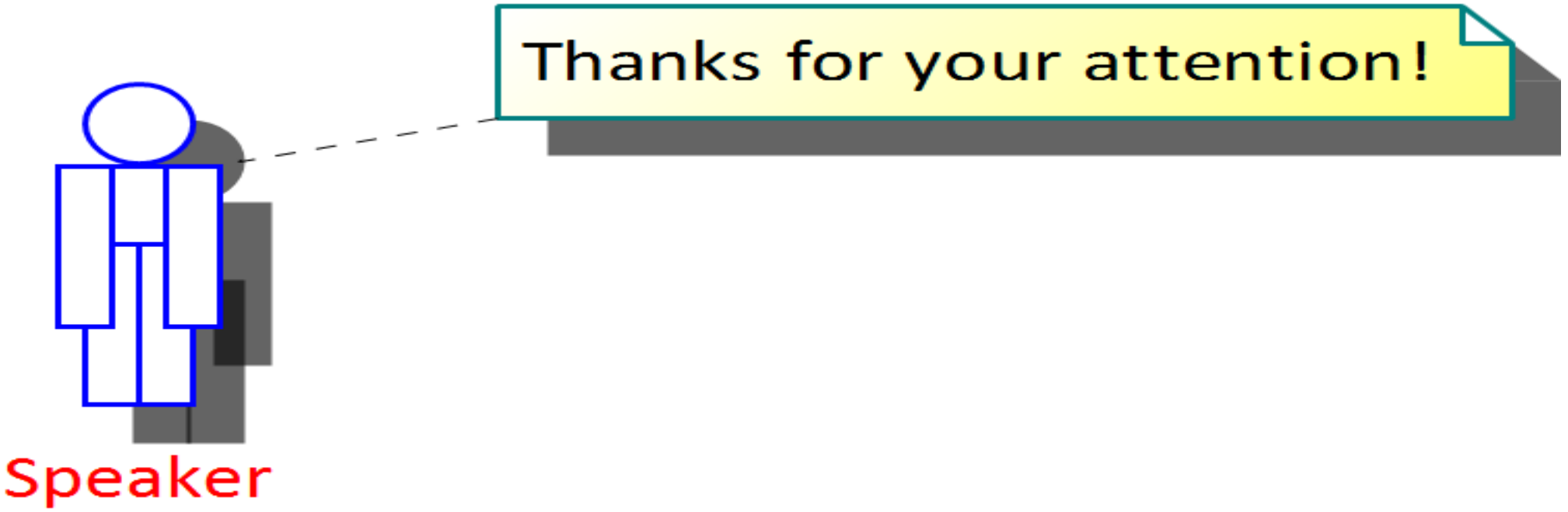
Agenda

1. The importance of security
2. The UAF architecture framework and the grid
3. Why Add Security?
4. A UAF security model example
5. Conclusions

Conclusions

- The UAF defines enterprise architectures
  - At various levels of abstraction
  - From multiple viewpoints
- The UAF implements DoDAF, NAF and MODAF in SysML
  - Traces to systems engineering
  - Provides multiple forms of trade-off analysis
- Security Views have been integrated into the UAF
- This will enable system security to be modeled and dealt with as part of the enterprise architecture.
- Cross-cutting concerns can be handled in the model without complicating a specific model.

Questions and Answers



Syntell

SSI

31st Annual INCOSE international symposium

virtual event

July 17 - 22, 2021

www.incose.org/symp2021

www.incose.org/symp2021