33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

Patrick Meharg – Chief Architect, Noblis Inc.

Transforming Perimeter Cybersecurity to a Zero Trust Strategy Using Model Based System Engineering (MBSE)

Overview

- What is Zero Trust (ZT)?
- What are the available Zero Trust Architectures (ZTA)?
- How to approach modeling Zero Trust?

Strategy and Architecture

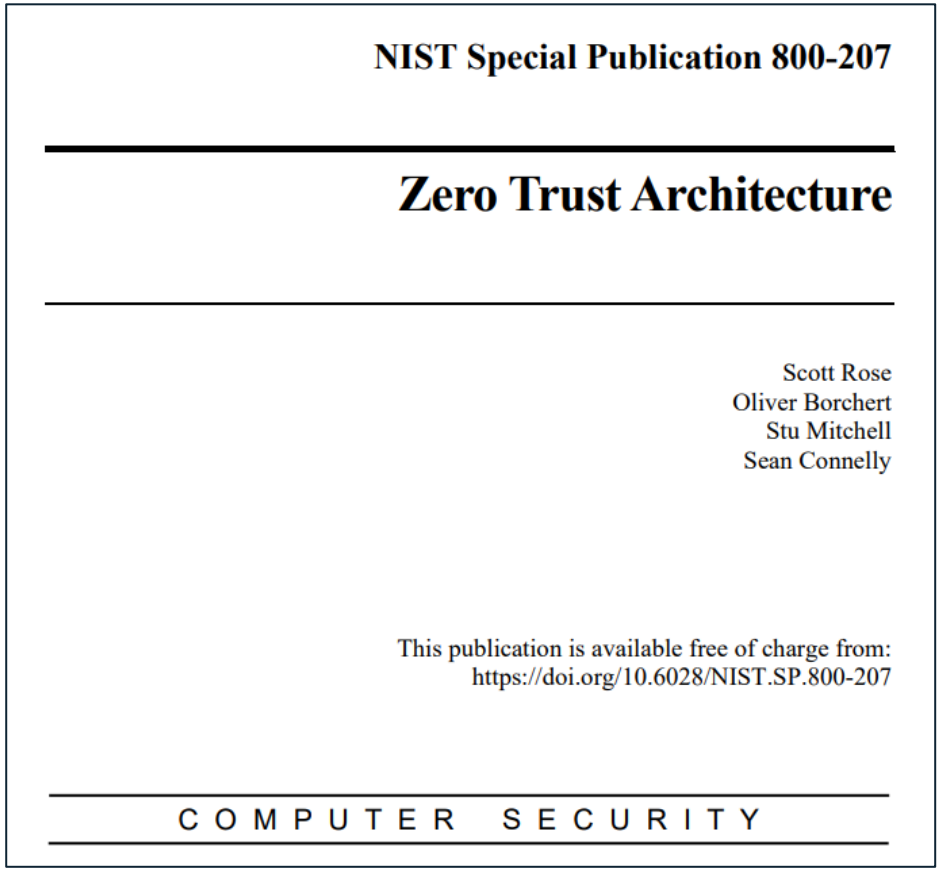
What is Zero Trust?

Zero Trust – What is it?

- "Zero Trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."

- Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the Internet) or based on asset ownership (enterprise or personally owned)."

- The classic perimeter/defense-in-depth cybersecurity strategy shows limited value against well-resourced adversaries and is an ineffective approach to address insider threats.


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

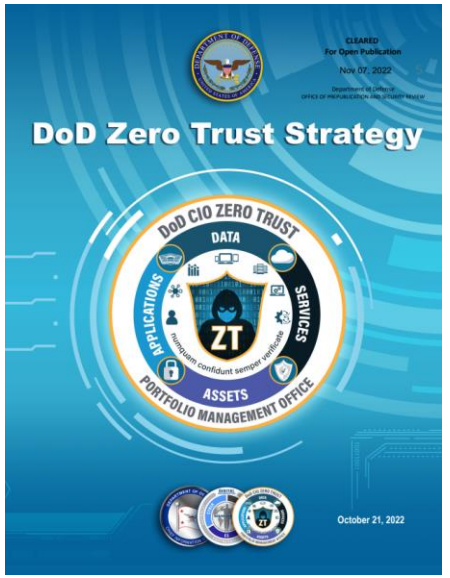
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

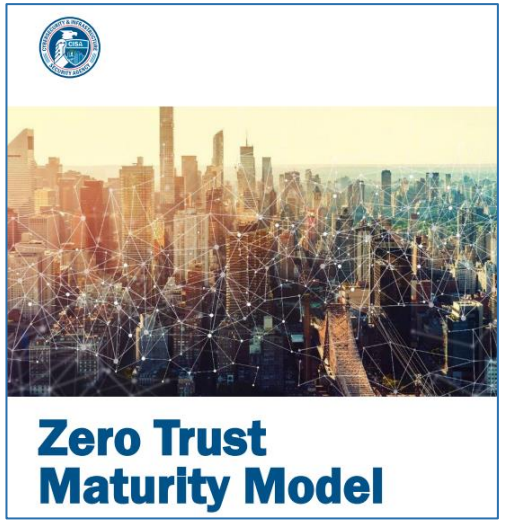
COMPUTER SECURITY

Zero Trust Strategies and Architectures

The DoD Zero Trust Strategy and CISA Zero Trust Maturity Model approaches were chosen as the reference for the modeling approach.

- The challenge government agencies face today is how to transition to a Zero Trust Architecture without impeding operations or compromising security.

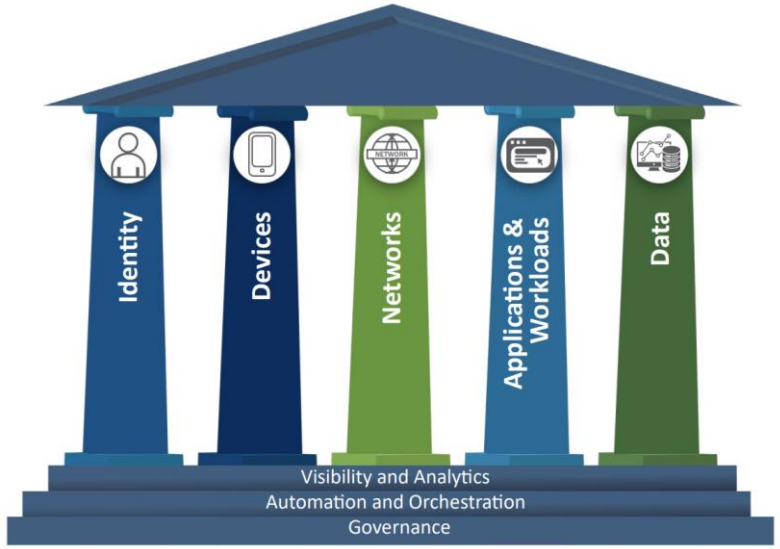




Applying a model-based approach provides a formalized method for the transition to a Zero Trust Architecture by creating reusable elements (requirements, structure, behavior, references, and analysis) used throughout the product lifecycle.

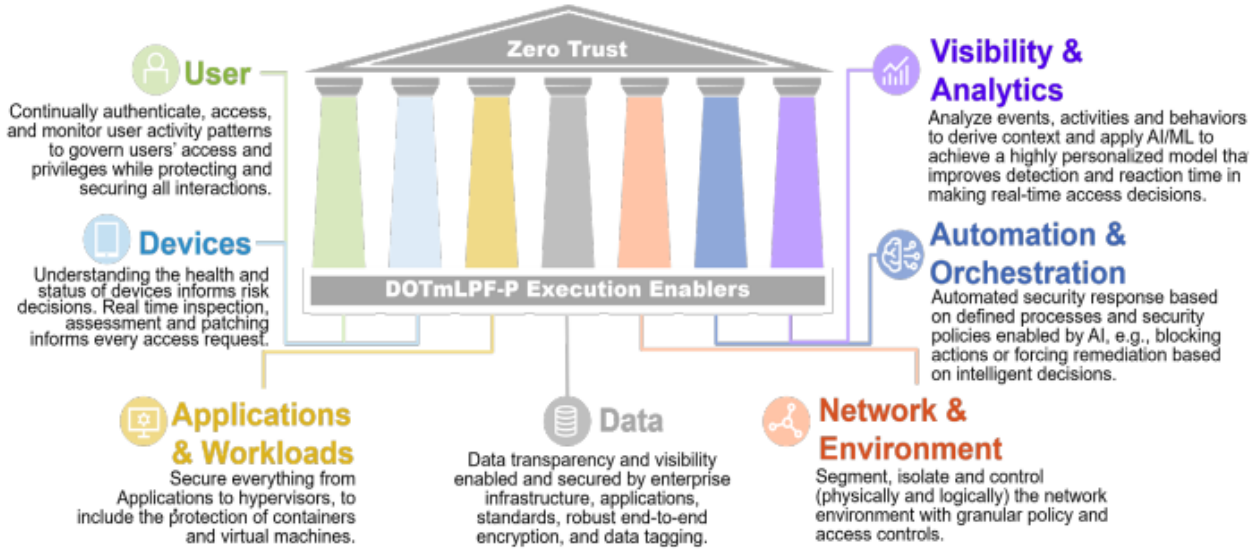
Comparing CISA and DoD Strategies

CISA Approach



- 5 Pillars / 3 Cross Cutting Capabilities
- 160 Lower-Level Functions
- 4 Levels of Implementation

DoD Approach



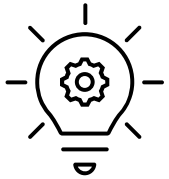
- 7 Pillars
- 152 Lower-Level Functions
- 3 Levels of Implementation

NIST.SP 800-53 Security and Privacy Controls - (20 Families = 1190 Total Controls)

Model-based solutions for complex, scalable, and reusable designs.

How to Approach Modeling Zero Trust

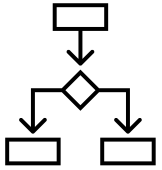
Goals and Products of the Modeling Activity



Create a modeling approach defining and describing stakeholder needs (what)' from the viewpoint of a new acquisition and/or an upgrade of legacy systems.

Goal 1

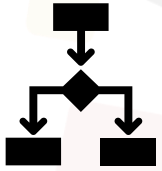
- Establish modeling approach.
- Identify traceability approaches.
- Develop modeling approach for requirements, behaviors, interfaces, structure, references and analysis.

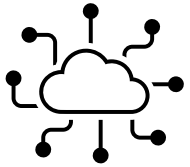


Transform the reference strategies and architectures (document based) to digital artifacts (model based) to establish an Authoritative Source of Truth (ASoT).

Goal 2

- Identify IT infrastructure and tools.
- Create Unified Architecture Framework (UAF). enterprise level model(s).
- Create system level model(s) (SysML).





Explore using a monolithic (single model) architecture or federated (models of models) architecture or a combination of both.

Goal 3

- Create a monolithic system level model.
- Create a federated system level model.
- Conduct trade study for the pros and cons of each approach.

Explore using a Product Line Engineering (PLE) approach to re-use the system model for any System of Interest (SOI). (scalability and reusability).

Goal 4

- Implement root feature groups and variation points.
- Determine scalability and re-usability constraints.
- Explore 3rd party software PLE integration.

Use the model to define early verification and validation approaches using a digital twin modeling approach to drive prototyping.

Goal 5

- Create test cases.
- Establish digital threads.
- Identify existing solutions (vendors) to optimize designs based on ZT modeled capabilities.

Goal 1

Model Traceability and Transformation Overview

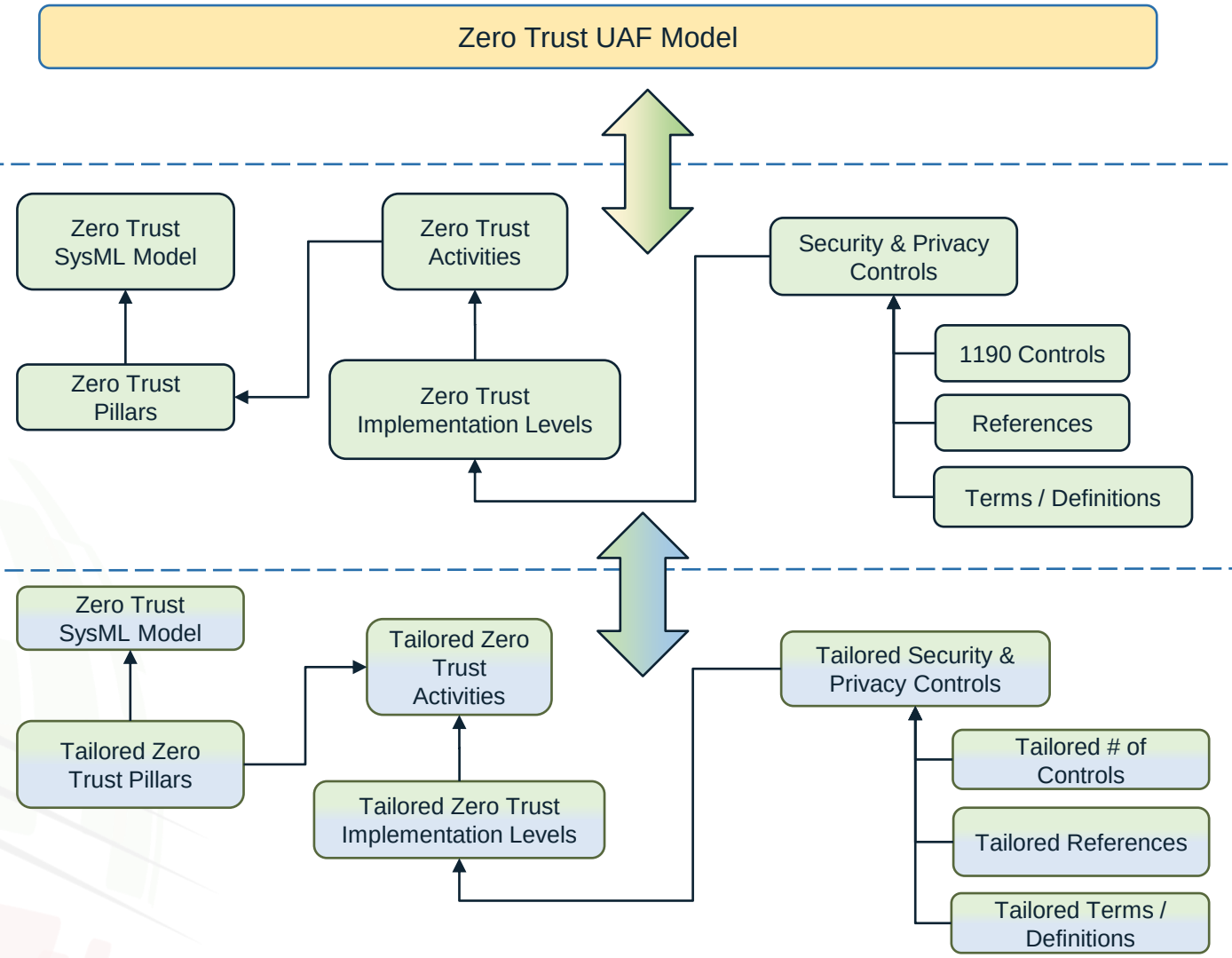
Enterprise Level UAF Model – Tailored to specific needs of Zero Trust (ex. Enterprise Level Capabilities and Execution Timelines)

Product Line Engineering Level Model (150%) – SysML Model

- Reusable library of Requirements, Behavior, Interfaces, Structures, References and Analysis Artifacts

Program Level Models Tailored to Specifically Meet Individual Implementation Needs

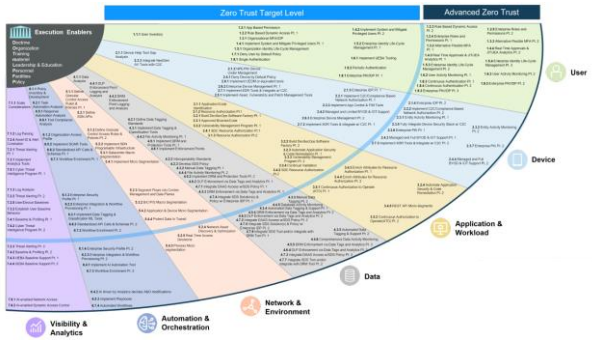
- Models containing tailored set of Requirements, Behavior, Interfaces, Structures, References and Analysis Artifacts

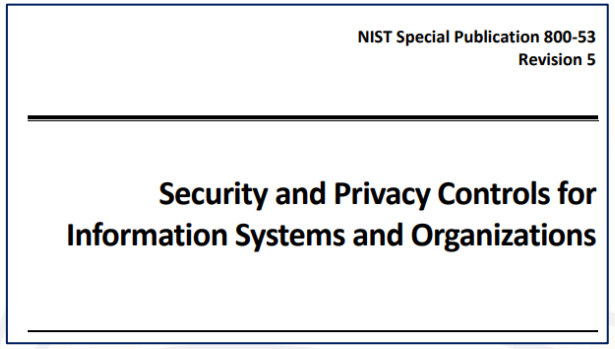


Goal 2

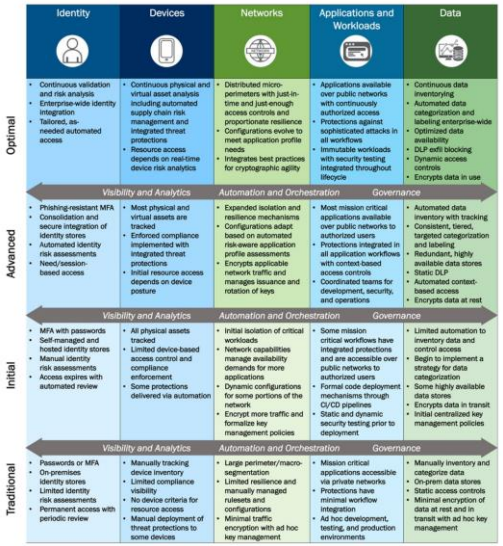
Document Based to Model Based

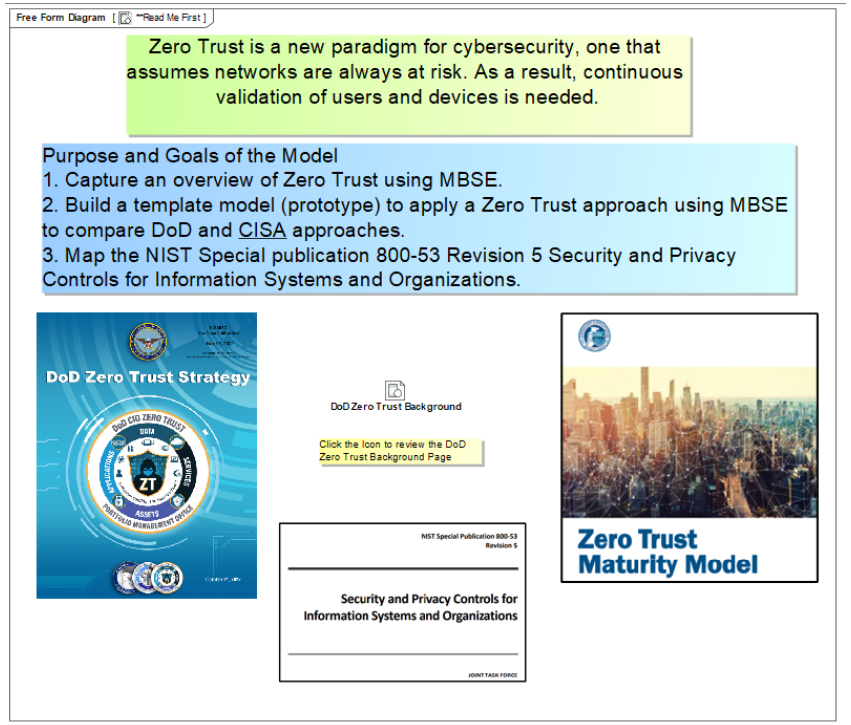
DoD Zero Trust Strategy

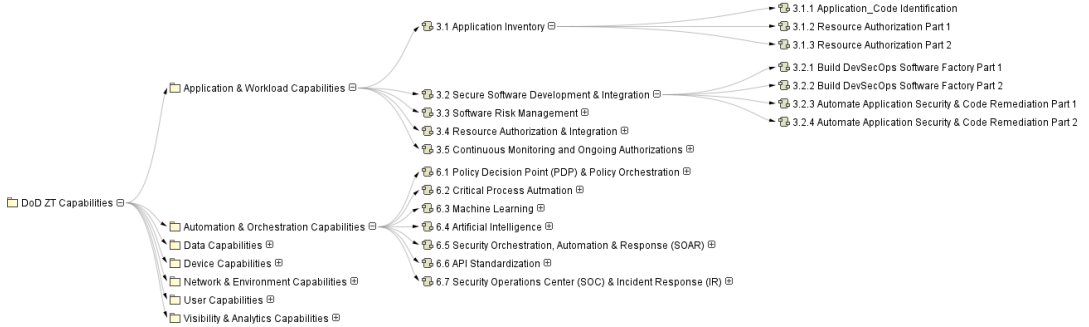




CISA Zero Trust Maturity Model



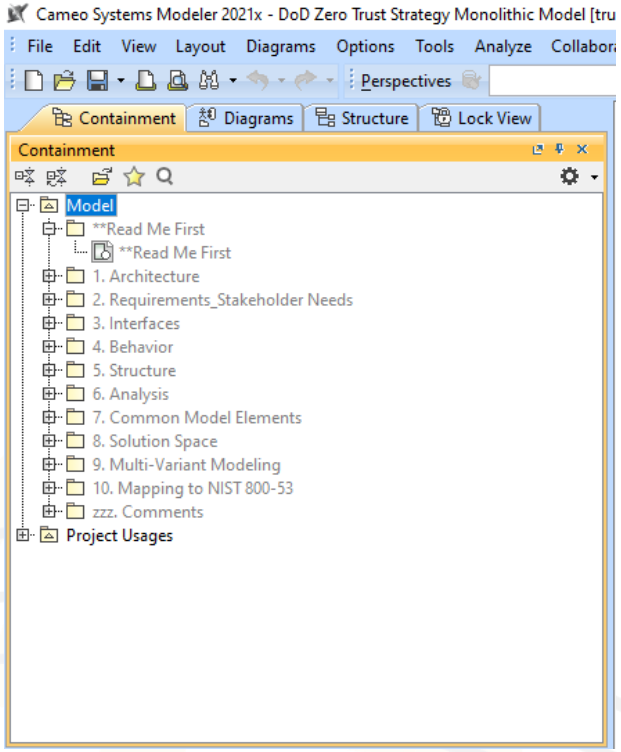




The MBSE approach transforms the DoD and CISA Zero Trust Strategies, documents, spreadsheets, and other forms of 'flat files' into a set of coherent and consistent models (both UAF and SysML) specifically designed for reuse.

Goal 3

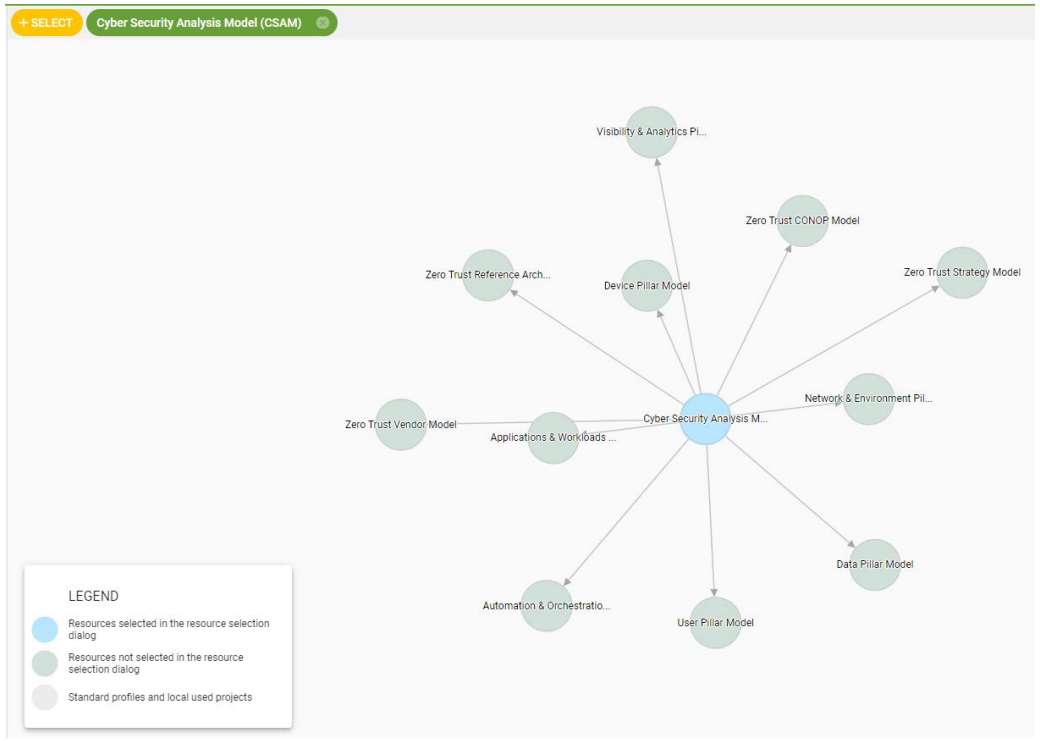
Architecture Modeling Approaches



Monolithic Model Architecture built in Cameo Teamwork Cloud.

Trade Study

OR



Federated Model Architecture built in Cameo Teamwork Cloud displaying model usage.

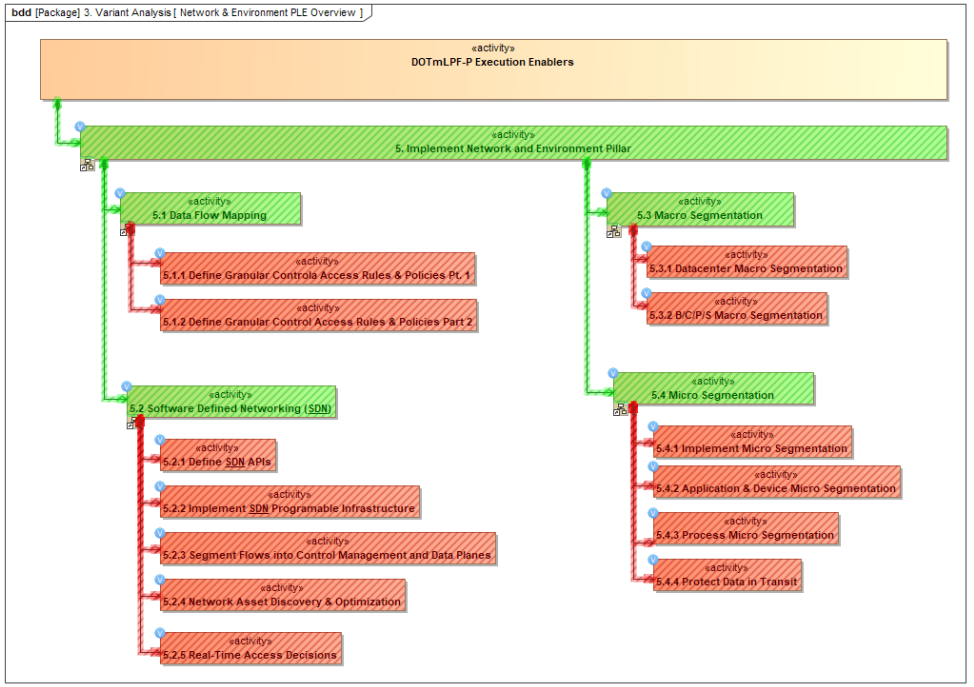
Goal 4

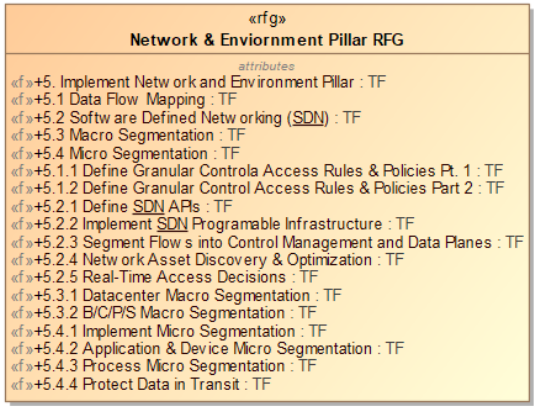
Product Line Engineering (PLE)

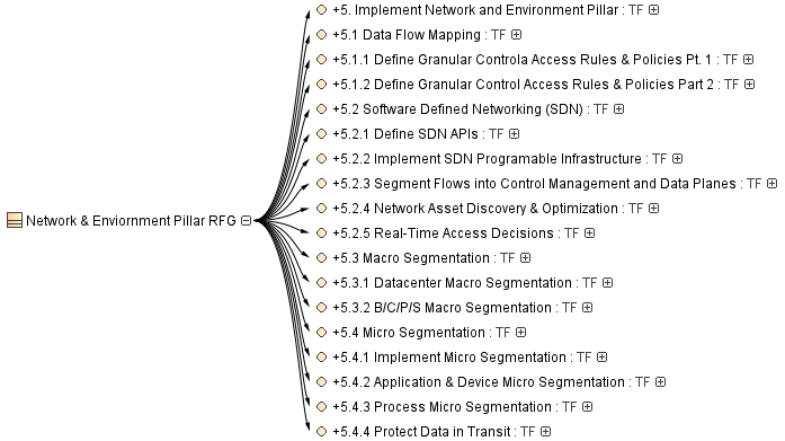
Product Line Engineering (PLE) is a product development method creating a common design that encompasses the entire variability spectrum of the products (150% model).

Using a MBSE approach, the available feature choices are described, and a connection is established between the feature choices and particular points in the design that need to vary depending on feature choice.

A design for a particular product can be produced based on the feature selections (green = selected, red = not selected) for tailored program/project implementation.







Goal 5

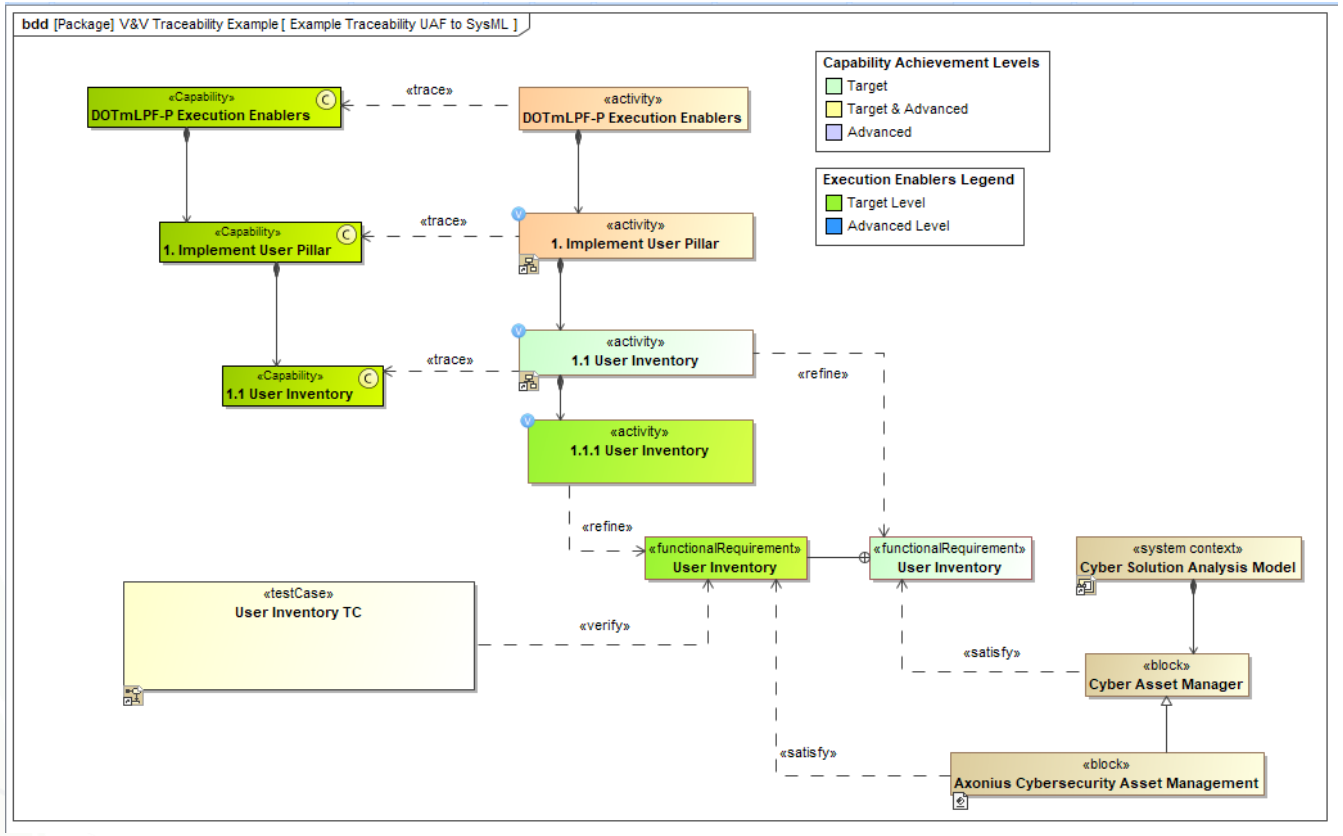
Early Verification and Validation Using Digital Twins

Verification = “Confirms that a system element meets design-to or build-to specifications. Throughout the system's life cycle, design solutions at all levels of the physical architecture are verified through a cost-effective combination of analysis, examination, demonstration, and testing.” Defense Acquisition University (DAU)

- The model provides full capability and requirements traceability down to Level (3) or lower.

Validation = “The process of evaluating a system or software component during, or at the end of, the development process to determine whether it satisfies specified requirements.” Defense Acquisition University (DAU)

- The model provides specific Test Cases containing verified products of the realized system linked to the system definition requirements.



33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

www.incose.org/symp2023