noblis®

For the best of reasons

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

Patrick Meharg

Chief Architect, Model Based System Engineering, Noblis Inc.

Overview

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

WHAT IS ZERO TRUST

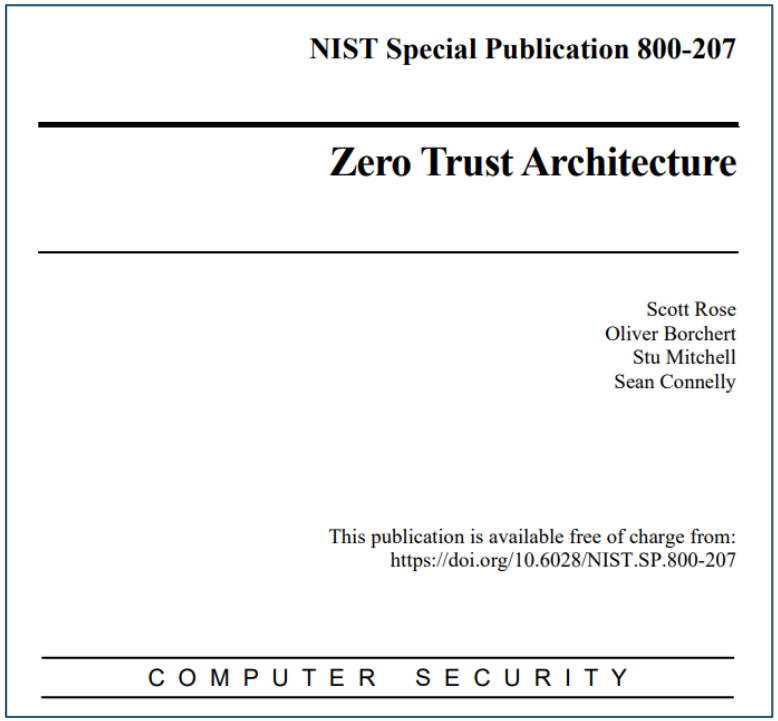
Strategy and Architecture

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

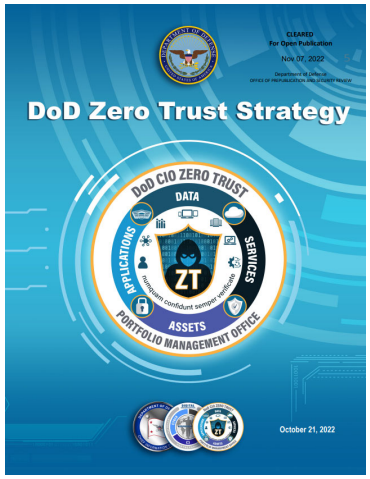
noblis

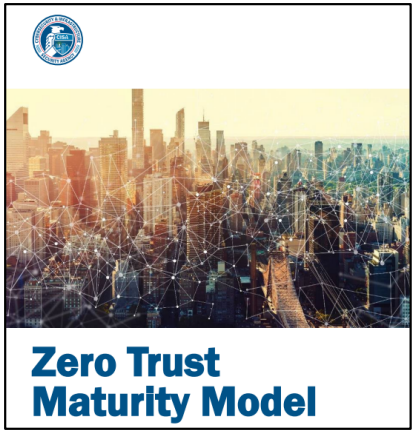
WHAT IS THE AVAILABLE ZERO TRUST ARCHITECTURES?

CISA and DoD Strategies

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.





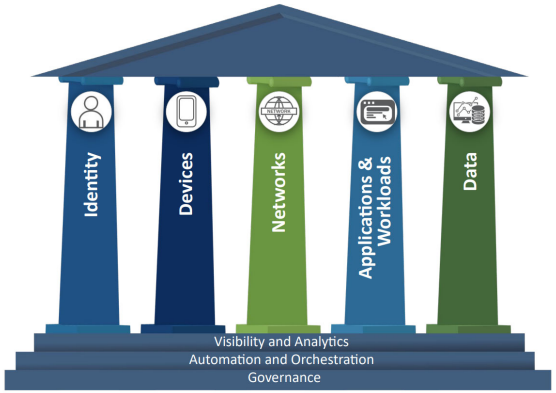
- The challenge government agencies face today is how to transition to a Zero Trust Architecture without impeding operations or compromising security.

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.

noblis

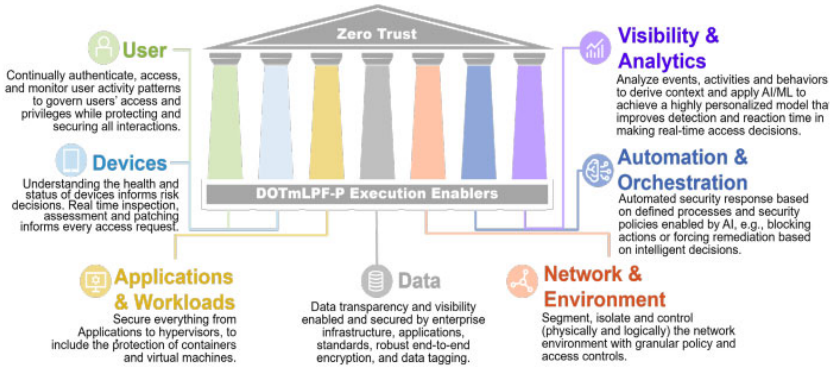
Comparing CISA and DoD Strategies

CISA Approach



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

DoD Approach



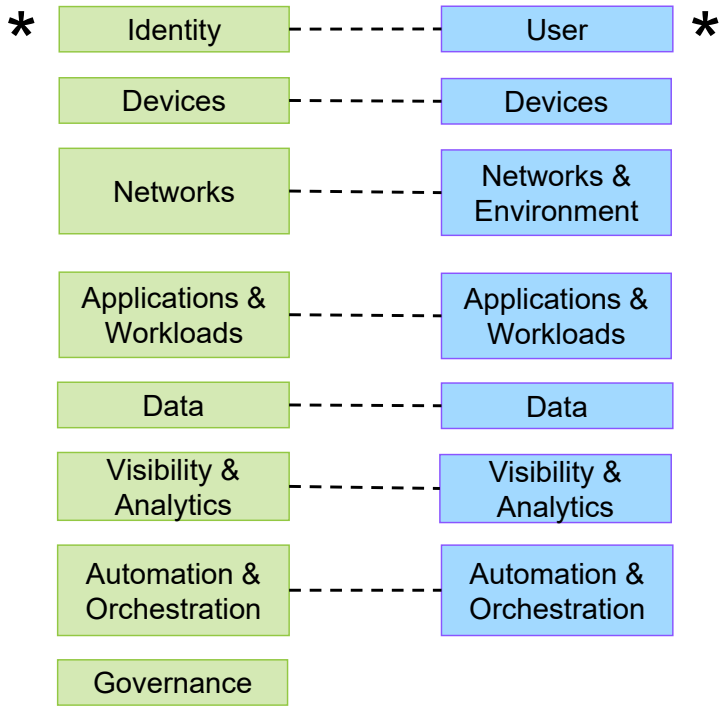
- 7 Pillars
- 152 Lower-Level Functions
- 3 Levels of Implementation

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

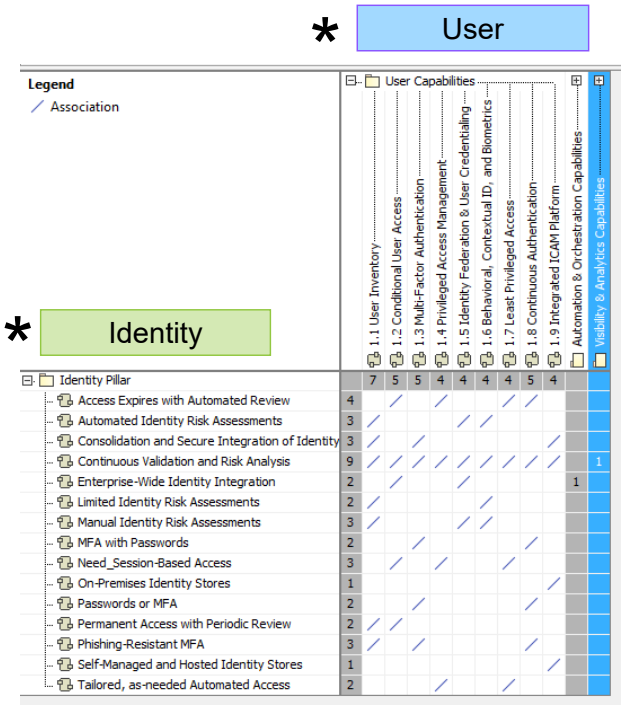
noblis

Mapping Pillars in the Model

CISA Pillar to DoD Pillar Mapping



CISA Lower-Level Activity to DoD Lower-Level Activity



Compare and Contrast Strategies – To identify alignment and perform gap analysis

noblis

Mapping Lower-Level Functions in the Model

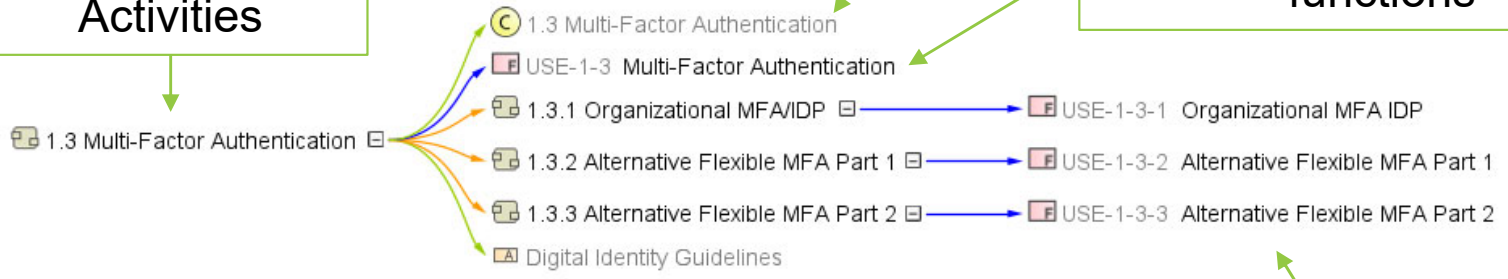
CISA Pillar to DoD Pillar Mapping

Identity ---------- User

Enterprise Level Model of Capabilities

Draft set of higher-level functions

Lower-Level Activities



Complete traceability from strategy pillars to security and privacy controls

NIST 800-63-3 Digital Identity Guidelines Reference

Security and Privacy Controls (800-53 Rev 5) Lower-Level Functions

noblis

HOW TO APPROACH MODELING ZERO TRUST

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

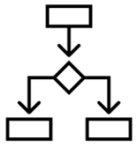
noblis

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

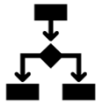
- Establish modeling approach.
- Identify traceability approaches.
- Develop modeling approach for requirements, behaviors, interfaces, structure, references and analysis.



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.

noblis

Model Traceability and Transformation Overview

Goal 1

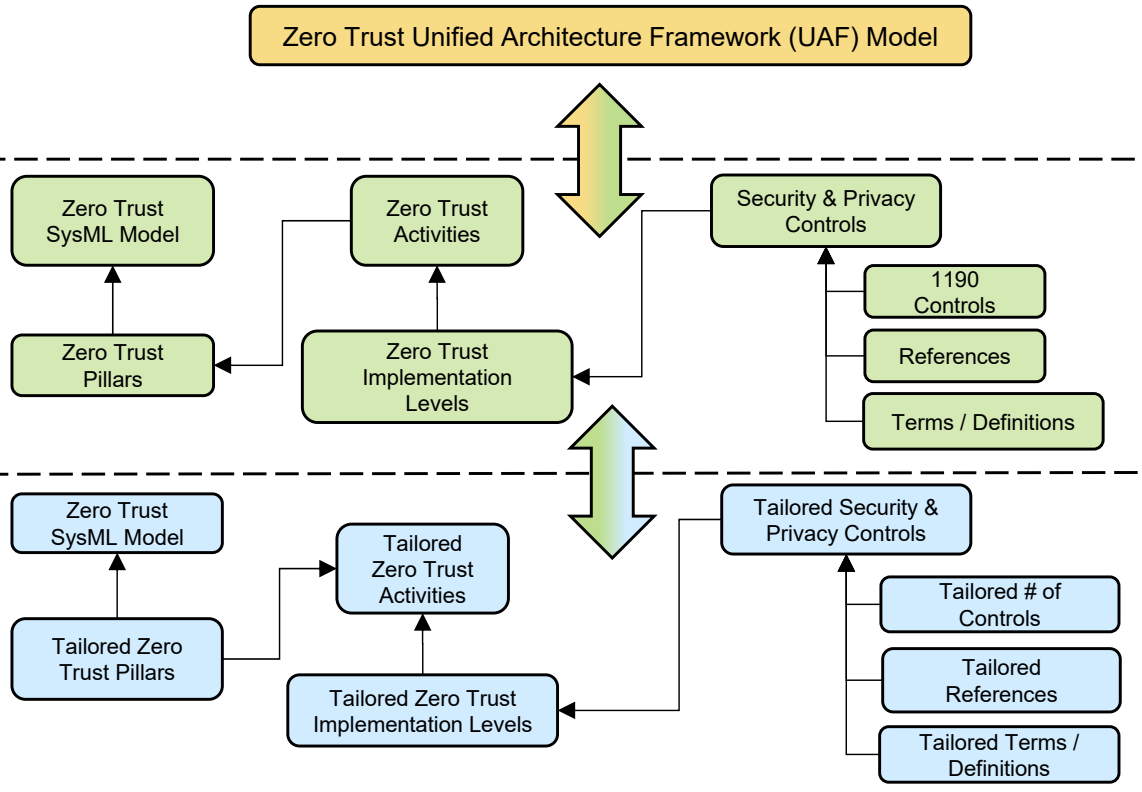
Enterprise Level UAF Model – Tailored to specific needs of Zero Trust (ex. Enterprise Level Capabilities and Execution Timelines)

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

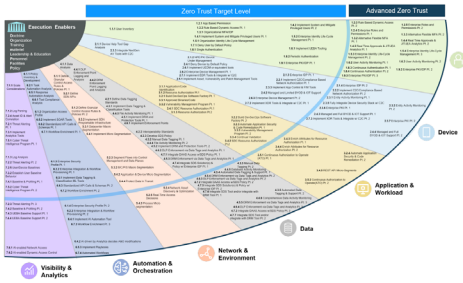
- **Models containing tailored set of Requirements, Behavior, Interfaces, Structures, References and Analysis Artifacts**

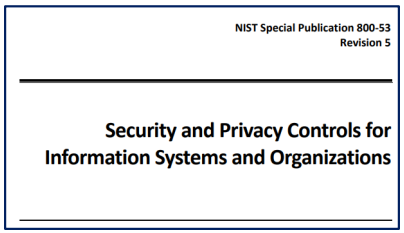


Document Based to Model Based

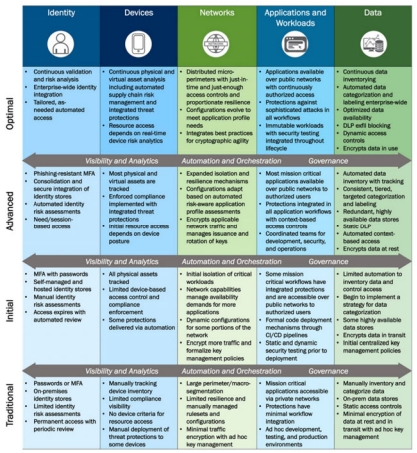
Goal 2

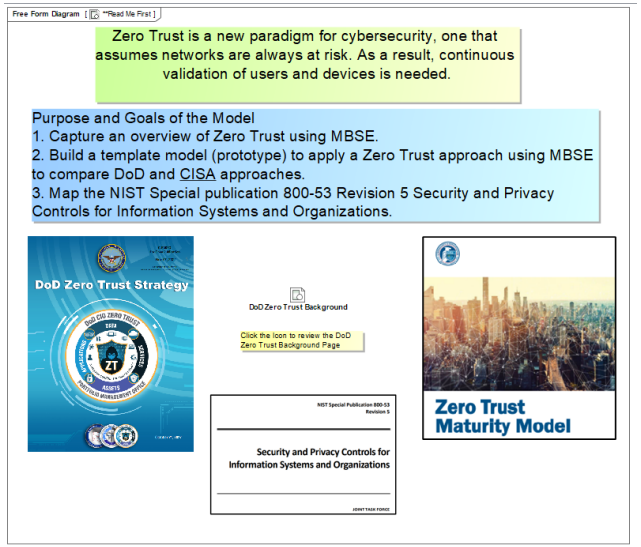
DoD Zero Trust Strategy

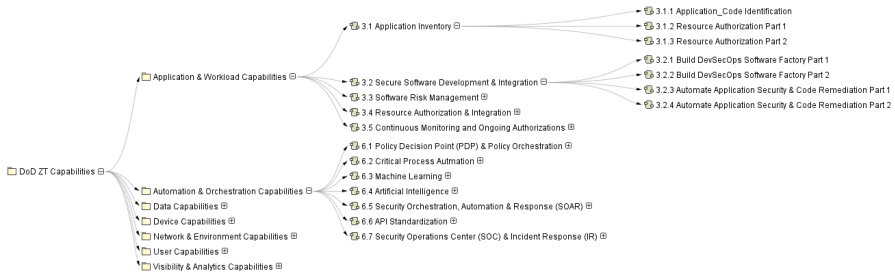




CISA Zero Trust Maturity Model





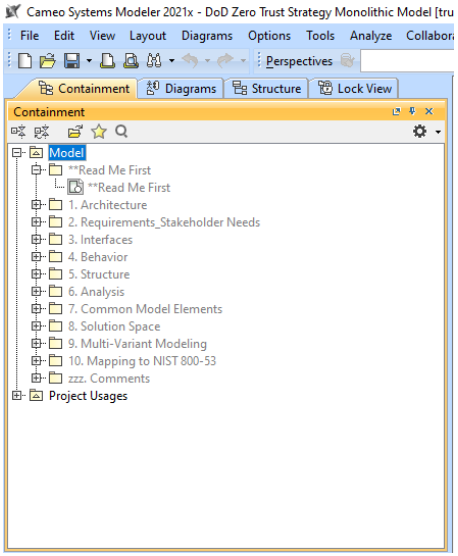


The MBSE approach transforms the DoD and CISA Zero Trust Strategies, documents, spreadsheets, and other forms of 'flat files' into a set of coherent and consistent models (both UAF and SysML) specifically designed for reuse.

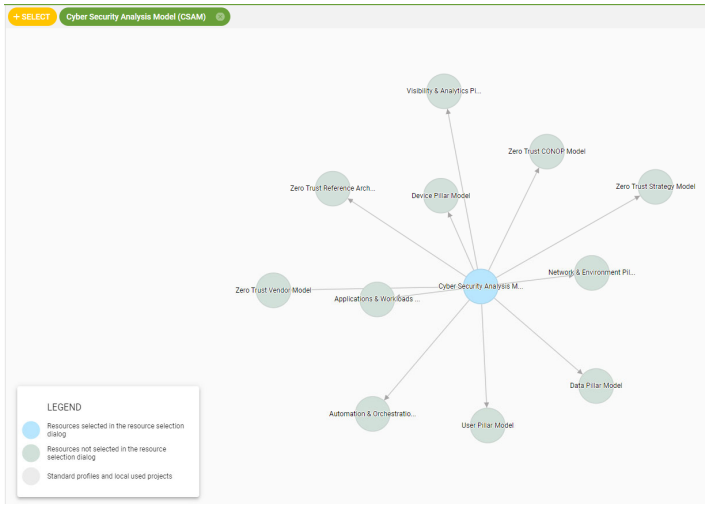
noblis

Architecture Modeling Approaches

Goal 3



Trade Study



Monolithic Model Architecture built in Cameo Teamwork Cloud.

OR

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

noblis

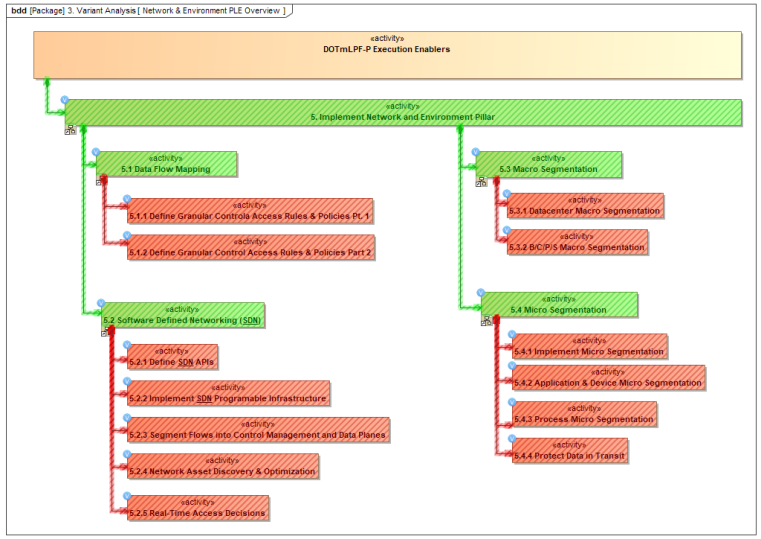
Product Line Engineering (PLE)

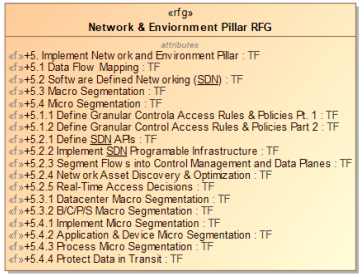
Goal 4

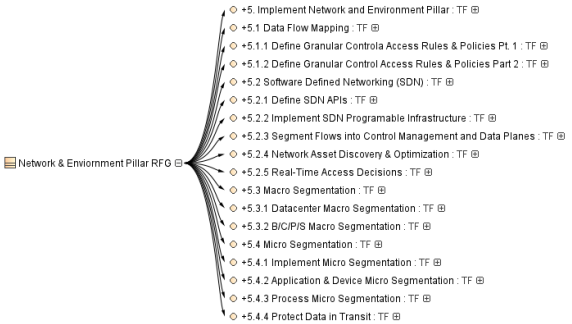
Product Line Engineering (PLE) is a product development method creating a common design that encompasses the entire variability spectrum of the products (150% model).

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.







noblis

Early Verification and Validation Using Digital Twins

Goal 5

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.”

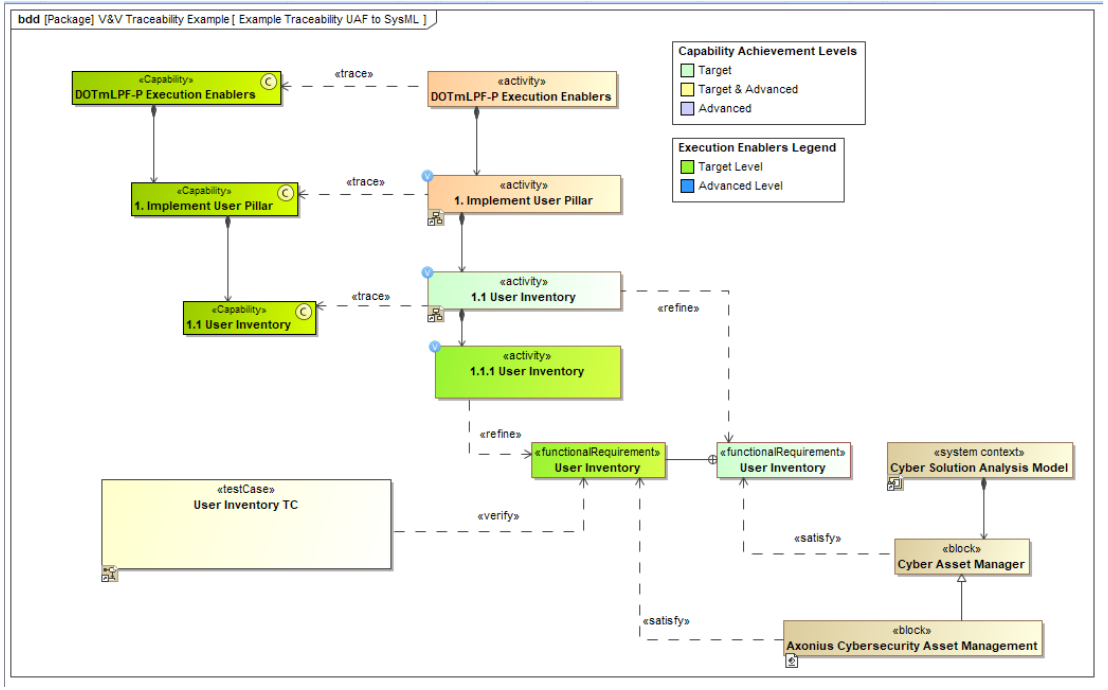
- **The model provides full capability and requirements traceability down to Level (3) or lower.**

Defense Acquisition University (DAU)

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.”

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

Defense Acquisition University (DAU)



References and Documentation

NIST and CISA Standards

- NIST Special Publication 800-207 Zero Trust Architecture
- NIST Special Publication 1800-35A Implementing a Zero Trust Architecture Volume A – Executive Summary
- NIST Special Publication 1800-35B Implementing a Zero Trust Architecture Volume B – Approach, Architecture, and Security Characteristics
- NIST Special Publication 1800-35C Implementing a Zero Trust Architecture Volume C – How-to Guides
- NIST Special Publication 1800-35D Implementing a Zero Trust Architecture Volume D – Functional Demonstrations
- NIST Special Publication 1800-35E Implementing a Zero Trust Architecture Volume E – Risk and Compliance Management
- NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations (w/spreadsheet)
- Department of Defense (DoD) Zero Trust Reference Architecture Version 2.0 July 2022
- Department of Defense (DoD) Zero Trust Strategy Nov 7, 2022
- Department of the Air Force (DAF) Enterprise Zero Trust Roadmap
- Executive Office of the President – Moving the U.S. Government Toward Zero Trust Cybersecurity Principles Jan 26, 2022
- CISA Zero Trust Maturity Model
- CISA Applying Zero Trust Principles to Enterprise Mobility

NATO Standards

- STANAG 4774 – Confidential Metadata Label Syntax
- ADatP-4774.1 Confidentiality Metadata Label Syntax (CMLS) Implementation Guide
- ADatP-4774.2 Guidance on the Digital Labelling of NATO Information
- ADatP-4774.5 Confidentiality Metadata Label Syntax Information Exchange Package Documentation
- STANAG 4778 – Metadata Binding Mechanism
- ADatP-4778 Metadata Binding Mechanism
- ADatP-4778.2 Profiles for Binding Metadata to a Data Object

Used as reference added to the model library

Under consideration

noblis