JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road
Laurel, MD 20723-6099

Understanding the Digital Signature of Model-Based Systems Engineering (MBSE) Models

Research Overview

Risa Gorospe (risa.gorospe@jhuapl.edu)
Shannon Dubicki (shannon.dubicki@jhuapl.edu)

Session Objectives

- In this session, we will discuss:
  - An overview on digital signatures
  - How digitally signing MBSE models is more challenging than regular digital documentation
  - A research prototype that applies digital signature approaches to MBSE models as an example of the art-of-the-possible

- We hope that you take away the following:
  - The industry can implement these approaches today and gain a baseline level of digital signing capability
  - There are unique ways to apply digital signatures to a model that differ from digital signatures for static documentation
  - There is potential to influence standards and tool implementation to provide a more robust MBSE digital signing capability

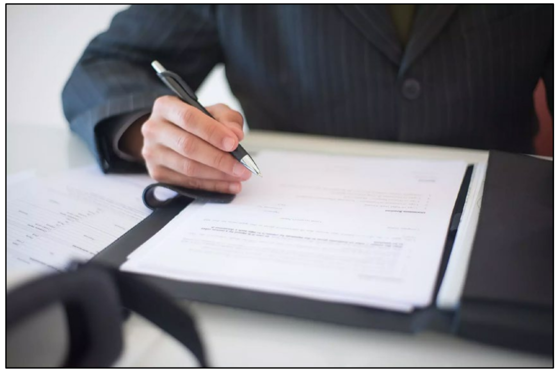
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

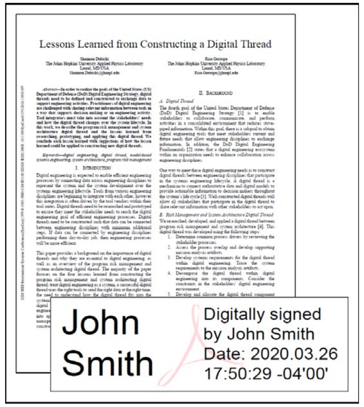
McCullagh, A., Little, P., & Caelli, W. (1998). Electronic Signatures: Understand the past to develop the future. *UNSWLJ*.

Kaur, R., & Kaur, A. (2012). Digital Signature. 2012 International Conference on Computing Sciences.

Digital Signature Overview

- Digital signature is a common cryptographic technique that enables users to sign and verify digital content
- Digital signature is broken into two main processes:
  - Signing – The signer signs digital data using a cryptographic component unique to the signer
  - Verification – A verifier verifies that signature matches the digital data that the signer signed
- Digital signature enables the capture of the signing party's "intention to sign" (McCullagh et al., 1998) and enforces that the signing action cannot be repudiated
- Digital signature processes such as public key infrastructure (PKI) have been well-defined and implemented for regular digital documentation (Kaur & Kaur, 2012)

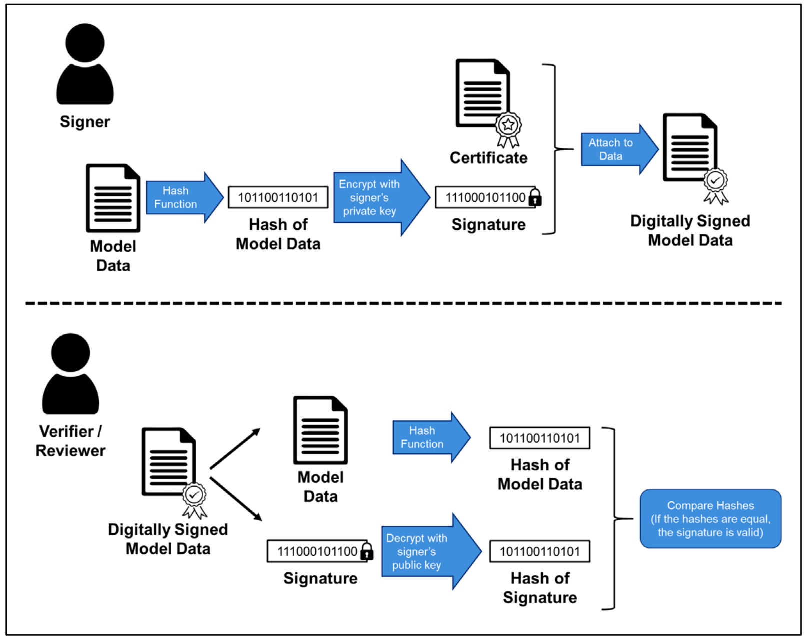




Lessons Learned from Constructing a Digital Thread

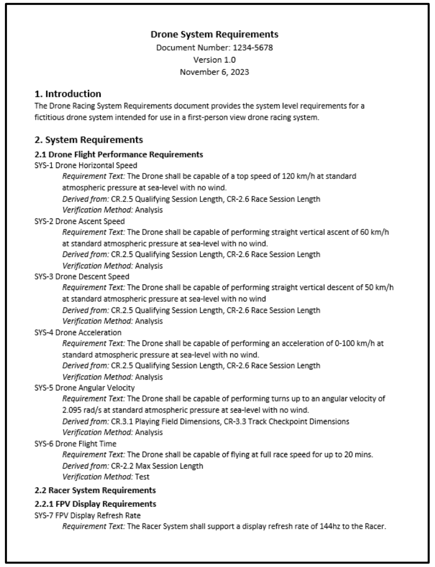
John Smith

Digitally signed by John Smith
Date: 2020.03.26 17:50:29 -04'00'



Research Problem

- Regular digital documentation is “What You See Is What You Get” (WYSIWYG) enabling the signer to fully comprehend the information that they are signing (Logan et al., 2012)
- MBSE model data is formatted and presented to the user through model views
- This creates challenges for MBSE digital signature:
    - MBSE model views display selected model data at a given time
        - Techniques that only apply signatures to a model-view level (Blackburn et al., 2019) have its signatures disconnected from the model data
            - This can be difficult to verify the integrity of the signed information
    - MBSE models can be translated into human-readable formats (e.g., XML), but can be difficult for the signer to comprehend the information (Logan et al., 2012)
- How could digital signature approaches be applied to MBSE models?



Drone System Requirements

Document Number: 1234-5678

Version 1.0

November 6, 2023

1. Introduction

The Drone Racing System Requirements document provides the system level requirements for a fictitious drone system intended for use in a first-person view drone racing system.

2. System Requirements

2.1 Drone Flight Performance Requirements

SYS-1 Drone Horizontal Speed

Requirement Text: The Drone shall be capable of a top speed of 120 km/h at standard atmospheric pressure at sea-level with no wind.

Derived from: CR.2.5 Qualifying Session Length, CR-2.6 Race Session Length

Verification Method: Analysis

SYS-2 Drone Ascent Speed

Requirement Text: The Drone shall be capable of performing straight vertical ascent of 60 km/h at standard atmospheric pressure at sea-level with no wind.

Derived from: CR.2.5 Qualifying Session Length, CR-2.6 Race Session Length

Verification Method: Analysis

SYS-3 Drone Descent Speed

Requirement Text: The Drone shall be capable of performing straight vertical descent of 50 km/h at standard atmospheric pressure at sea-level with no wind

Derived from: CR.2.5 Qualifying Session Length, CR-2.6 Race Session Length

Verification Method: Analysis

SYS-4 Drone Acceleration

Requirement Text: The Drone shall be capable of performing an acceleration of 0-100 km/h at standard atmospheric pressure at sea-level with no wind.

Derived from: CR.2.5 Qualifying Session Length, CR-2.6 Race Session Length

Verification Method: Analysis

SYS-5 Drone Angular Velocity

Requirement Text: The Drone shall be capable of performing turns up to an angular velocity of 2.095 rad/s at standard atmospheric pressure at sea-level with no wind.

Derived from: CR.3.1 Playing Field Dimensions, CR-3.3 Track Checkpoint Dimensions

Verification Method: Analysis

SYS-6 Drone Flight Time

Requirement Text: The Drone shall be capable of flying at full race speed for up to 20 mins.

Derived from: CR-2.2 Max Session Length

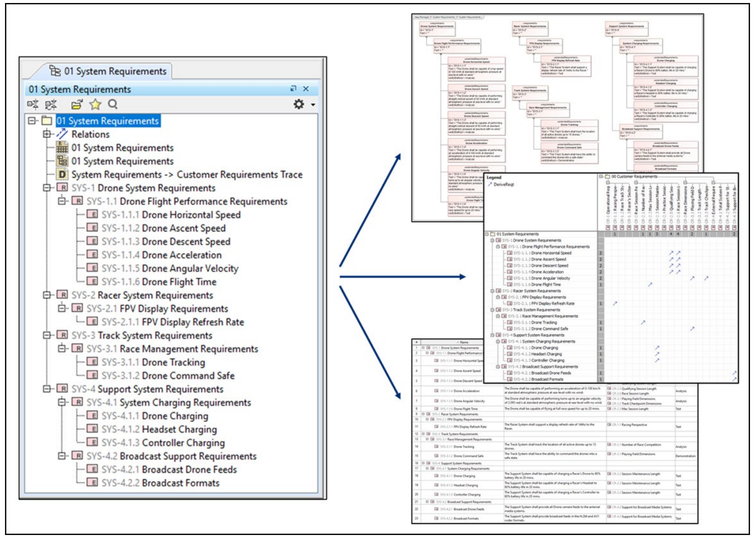
Verification Method: Test

2.2 Racer System Requirements

2.2.1 FPV Display Requirements

SYS-7 FPV Display Refresh Rate

Requirement Text: The Racer System shall support a display refresh rate of 144hz to the Racer.



01 System Requirements

01 System Requirements

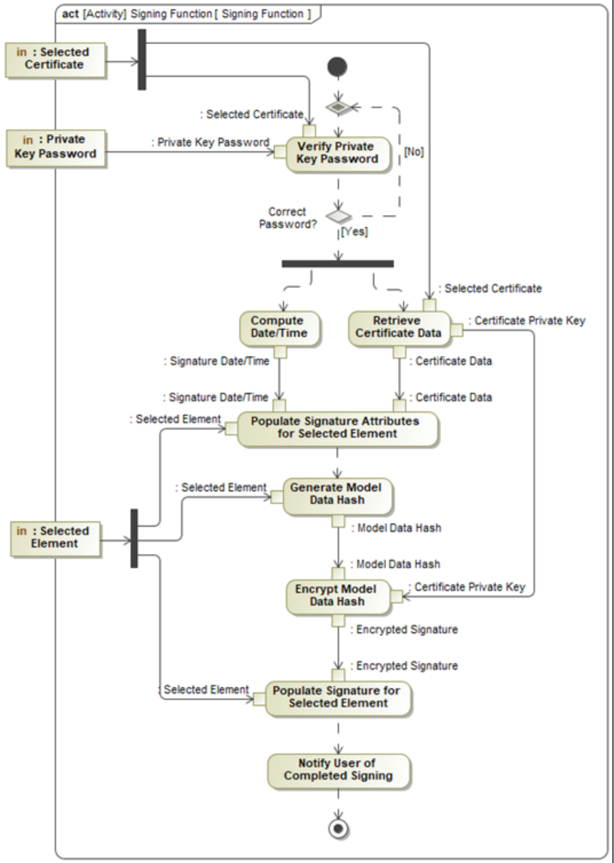
- 01 System Requirements
    - Relations
    - 01 System Requirements
    - 01 System Requirements
    - System Requirements -> Customer Requirements Trace
    - SYS-1 Drone System Requirements
        - SYS-1.1 Drone Flight Performance Requirements
            - SYS-1.1.1 Drone Horizontal Speed
            - SYS-1.1.2 Drone Ascent Speed
            - SYS-1.1.3 Drone Descent Speed
            - SYS-1.1.4 Drone Acceleration
            - SYS-1.1.5 Drone Angular Velocity
            - SYS-1.1.6 Drone Flight Time
    - SYS-2 Racer System Requirements
        - SYS-2.1 FPV Display Requirements
            - SYS-2.1.1 FPV Display Refresh Rate
    - SYS-3 Track System Requirements
        - SYS-3.1 Race Management Requirements
            - SYS-3.1.1 Drone Tracking
            - SYS-3.1.2 Drone Command Safe
    - SYS-4 Support System Requirements
        - SYS-4.1 System Charging Requirements
            - SYS-4.1.1 Drone Charging
            - SYS-4.1.2 Headset Charging
            - SYS-4.1.3 Controller Charging
        - SYS-4.2 Broadcast Support Requirements
            - SYS-4.2.1 Broadcast Drone Feeds
            - SYS-4.2.2 Broadcast Formats

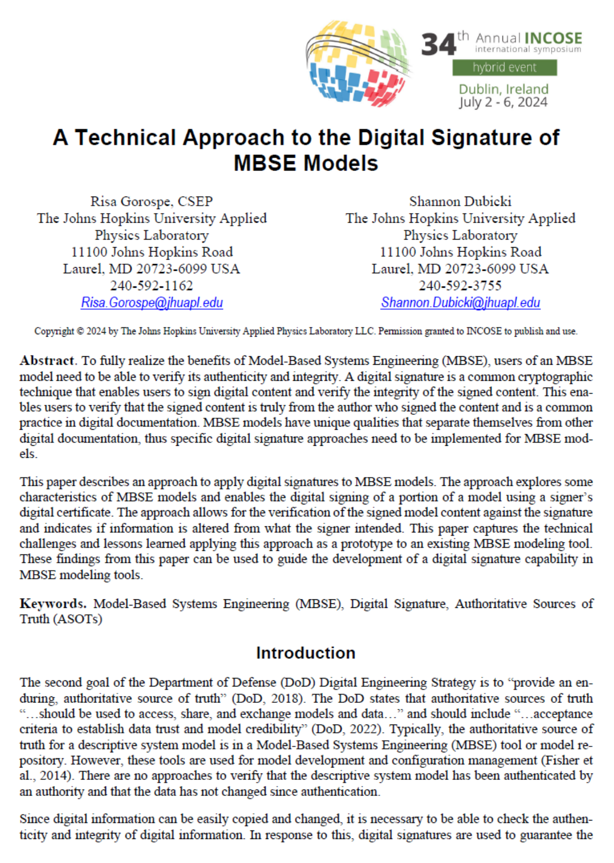
Logan, P., Harvey, D., & Spencer, D. (2012). Documents are an Essential Part of Model Based Systems Engineering. *INCOSE International Symposium.*

Blackburn et al., (2019). Transforming Systems Engineering through Model-Centric Engineering (A013 Final Technical Report SERC-2019-TR-005).

Research Approach & Paper

- Our research explores developing a prototype to explore these challenges
  - We defined objectives for the prototype that targets these challenges
  - We designed and documented design specifications to meet the prototype's objectives
    - e.g., functional flow of the digital signature process
  - We developed a software prototype to the design specifications
  - We captured any findings, observations, and additional considerations
- For the technical details, please review the 2024 INCOSE International Symposium paper:
  - "A Technical Approach to the Digital Signature of MBSE Models"





34th Annual INCOSE international symposium
hybrid event
Dublin, Ireland
July 2 - 6, 2024

A Technical Approach to the Digital Signature of MBSE Models

Risa Gorospe, CSEP
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723-6099 USA
240-592-1162
Risa.Gorospe@jhuapl.edu

Shannon Dubicki
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723-6099 USA
240-592-3755
Shannon.Dubicki@jhuapl.edu

Abstract. To fully realize the benefits of Model-Based Systems Engineering (MBSE), users of an MBSE model need to be able to verify its authenticity and integrity. A digital signature is a common cryptographic technique that enables users to sign digital content and verify the integrity of the signed content. This enables users to verify that the signed content is truly from the author who signed the content and is a common practice in digital documentation. MBSE models have unique qualities that separate themselves from other digital documentation, thus specific digital signature approaches need to be implemented for MBSE models.

This paper describes an approach to apply digital signatures to MBSE models. The approach explores some characteristics of MBSE models and enables the digital signing of a portion of a model using a signer's digital certificate. The approach allows for the verification of the signed model content against the signature and indicates if information is altered from what the signer intended. This paper captures the technical challenges and lessons learned applying this approach as a prototype to an existing MBSE modeling tool. These findings from this paper can be used to guide the development of a digital signature capability in MBSE modeling tools.

Keywords. Model-Based Systems Engineering (MBSE), Digital Signature, Authoritative Sources of Truth (ASOTs)

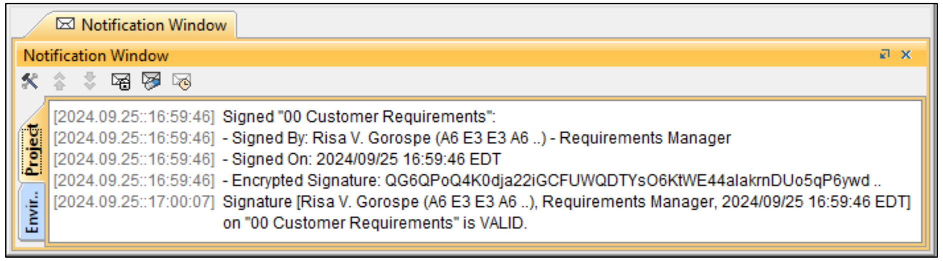
Introduction

The second goal of the Department of Defense (DoD) Digital Engineering Strategy is to "provide an enduring, authoritative source of truth" (DoD, 2018). The DoD states that authoritative sources of truth "…should be used to access, share, and exchange models and data…" and should include "…acceptance criteria to establish data trust and model credibility" (DoD, 2022). Typically, the authoritative source of truth for a descriptive system model is in a Model-Based Systems Engineering (MBSE) tool or model repository. However, these tools are used for model development and configuration management (Fisher et al., 2014). There are no approaches to verify that the descriptive system model has been authenticated by an authority and that the data has not changed since authentication.

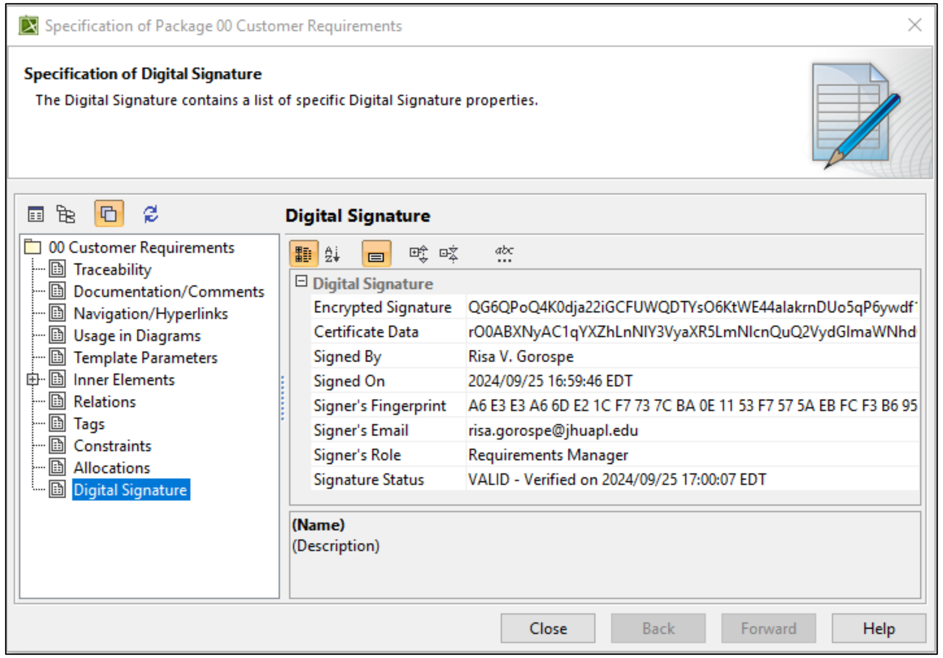
Since digital information can be easily copied and changed, it is necessary to be able to check the authenticity and integrity of digital information. In response to this, digital signatures are used to guarantee the

Research Prototype

- The prototype is implemented as a custom profile and plugin to Dassault Systems Cameo Systems Modeler 2022x with the SysML 1.7 language
- A user of the prototype can perform the following:
  - A signer can select any element in the containment tree to sign it and its contents
    - The prototype computes the signature information from the signer's certificate and the model data
    - The prototype embeds signature information into the selected element as a stereotype that can be reviewed
    - The prototype pushes signature information to all diagrams contained within the signed element
  - A verifier can select a signed element in the containment tree and verify the validity of the signature
    - The prototype assess the integrity of the model data against the signature information in the signed element
    - The prototype notifies the user if the model data or signature has been altered since signing



```
[2024.09.25::16:59:46]  Signed "00 Customer Requirements":
[2024.09.25::16:59:46]  - Signed By: Risa V. Gorospe (A6 E3 E3 A6 ..) - Requirements Manager
[2024.09.25::16:59:46]  - Signed On: 2024/09/25 16:59:46 EDT
[2024.09.25::16:59:46]  - Encrypted Signature: QG6QPoQ4K0dja22iGCFUWQDTYsO6KtWE44alakrnDUo5qP6ywd ..
[2024.09.25::17:00:07]  Signature [Risa V. Gorospe (A6 E3 E3 A6 ..), Requirements Manager, 2024/09/25 16:59:46 EDT]
                        on "00 Customer Requirements" is VALID.
```



Specification of Digital Signature

The Digital Signature contains a list of specific Digital Signature properties.

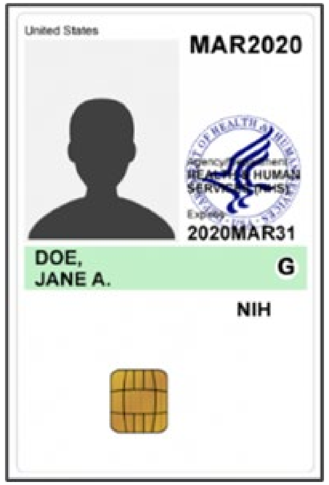
Digital Signature

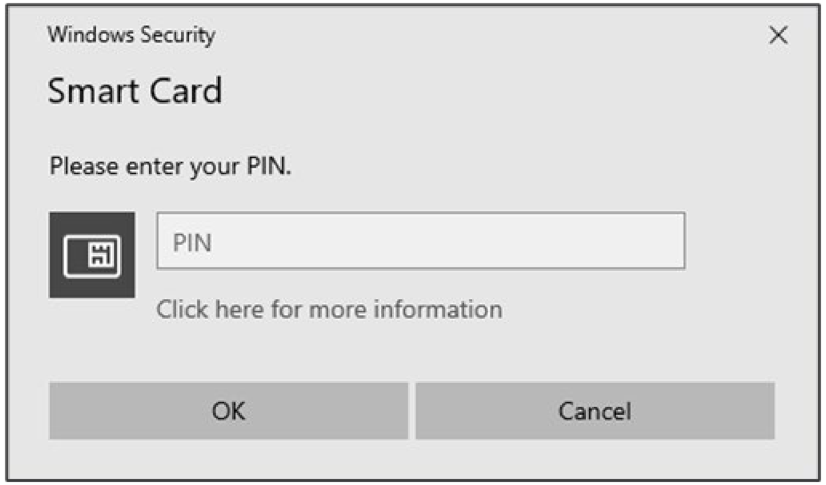
Digital Signature	
Encrypted Signature	QG6QPoQ4K0dja22iGCFUWQDTYsO6KtWE44alakrnDUo5qP6ywdf
Certificate Data	rO0ABXNyAC1qYXZhLnNlY3VyaXR5LmNlcnQuQ2VydGlmaWNhd
Signed By	Risa V. Gorospe
Signed On	2024/09/25 16:59:46 EDT
Signer's Fingerprint	A6 E3 E3 A6 6D E2 1C F7 73 7C BA 0E 11 53 F7 57 5A EB FC F3 B6 95
Signer's Email	risa.gorospe@jhuapl.edu
Signer's Role	Requirements Manager
Signature Status	VALID - Verified on 2024/09/25 17:00:07 EDT

(Name)
(Description)

Research Prototype (Continued)

- The prototype follows the traditional PKI digital signature processes
  - Model data is converted into a text string format that can be supported by standard hashing and encryption algorithms
- The prototype can use digital certificates from the Windows operating system certificate store
  - This includes hardware certificates which enables smart card signing and verification




Windows Security

Smart Card

Please enter your PIN.

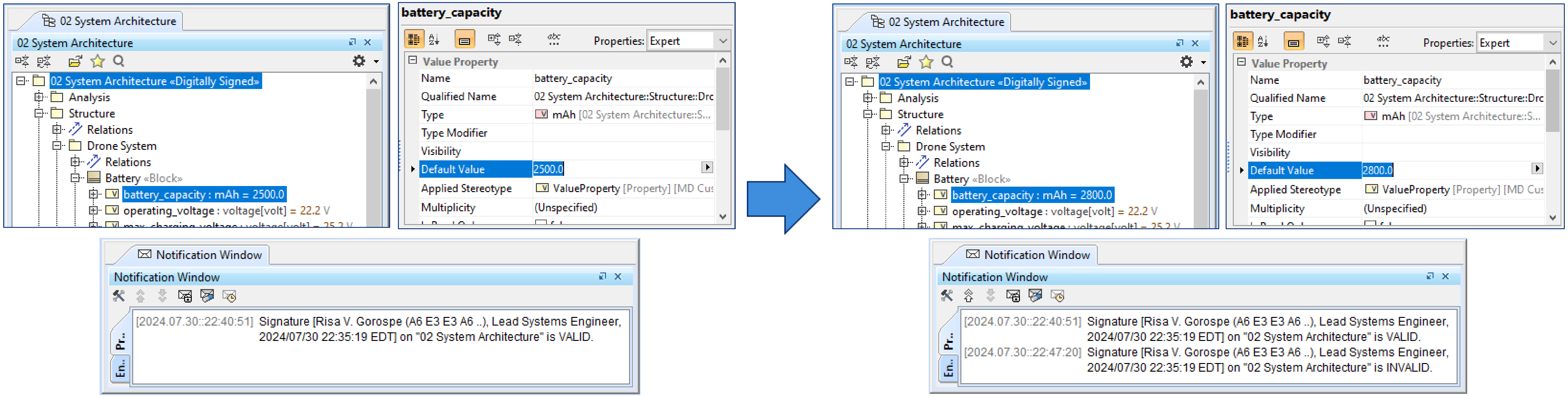
PIN

Click here for more information

Research Observations

Signature Verification of Deeply Nested Model Data

- The prototype's signature verification can detect model element changes deeply nested within the containment tree:
  - The model data integrity check includes the attributes of the signed element and all its contained elements
- The prototype's signature verification worked for all test models tried
  - Additional exploration may be needed for large models for computational performance and verification accuracy



Value Property	
Name	battery_capacity
Qualified Name	02 System Architecture::Structure::Drc
Type	mAh [02 System Architecture::S...
Type Modifier	
Visibility	
Default Value	2500.0
Applied Stereotype	ValueProperty [Property] [MD Cus
Multiplicity	(Unspecified)

```
[2024.07.30::22:40:51] Signature [Risa V. Gorospe (A6 E3 E3 A6 ..), Lead Systems Engineer,
                       2024/07/30 22:35:19 EDT] on "02 System Architecture" is VALID.
```

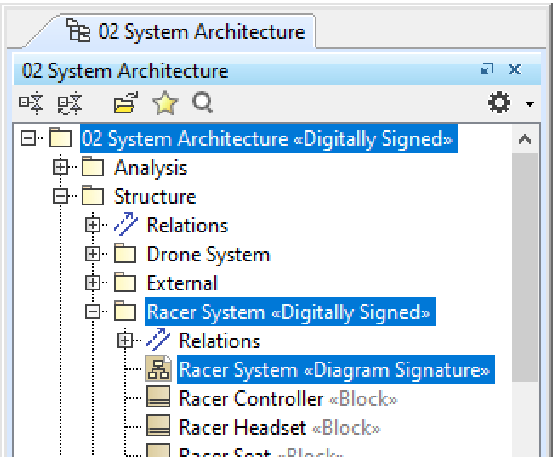
Value Property	
Name	battery_capacity
Qualified Name	02 System Architecture::Structure::Drc
Type	mAh [02 System Architecture::S...
Type Modifier	
Visibility	
Default Value	2800.0
Applied Stereotype	ValueProperty [Property] [MD Cus
Multiplicity	(Unspecified)

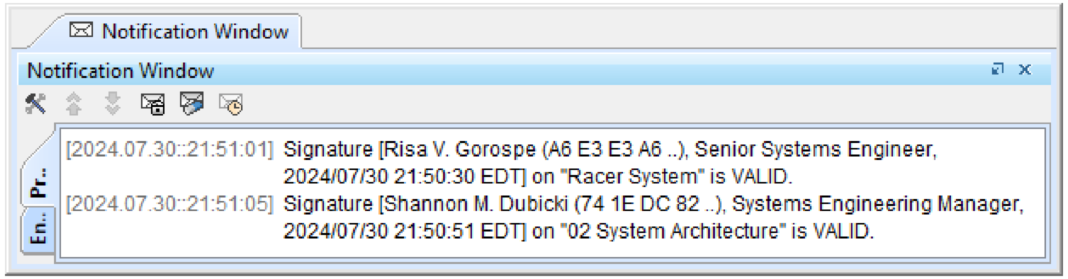
```
[2024.07.30::22:40:51] Signature [Risa V. Gorospe (A6 E3 E3 A6 ..), Lead Systems Engineer,
                       2024/07/30 22:35:19 EDT] on "02 System Architecture" is VALID.
[2024.07.30::22:47:20] Signature [Risa V. Gorospe (A6 E3 E3 A6 ..), Lead Systems Engineer,
                       2024/07/30 22:35:19 EDT] on "02 System Architecture" is INVALID.
```

Research Observations

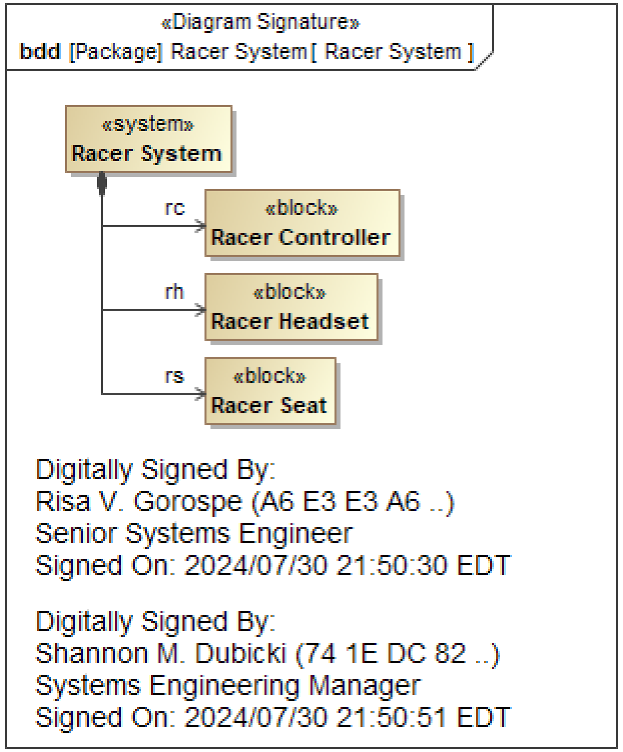
Tiered Countersignature

- The prototype enables signed elements to be nested within each other for tiered countersignature
  - e.g., an engineer signs a subsystem package and the engineering manager signs the higher system package





```
[2024.07.30::21:51:01] Signature [Risa V. Gorospe (A6 E3 E3 A6 ..), Senior Systems Engineer,
                       2024/07/30 21:50:30 EDT] on "Racer System" is VALID.
[2024.07.30::21:51:05] Signature [Shannon M. Dubicki (74 1E DC 82 ..), Systems Engineering Manager,
                       2024/07/30 21:50:51 EDT] on "02 System Architecture" is VALID.
```



Digitally Signed By:
Risa V. Gorospe (A6 E3 E3 A6 ..)
Senior Systems Engineer
Signed On: 2024/07/30 21:50:30 EDT

Digitally Signed By:
Shannon M. Dubicki (74 1E DC 82 ..)
Systems Engineering Manager
Signed On: 2024/07/30 21:50:51 EDT

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Research Observations

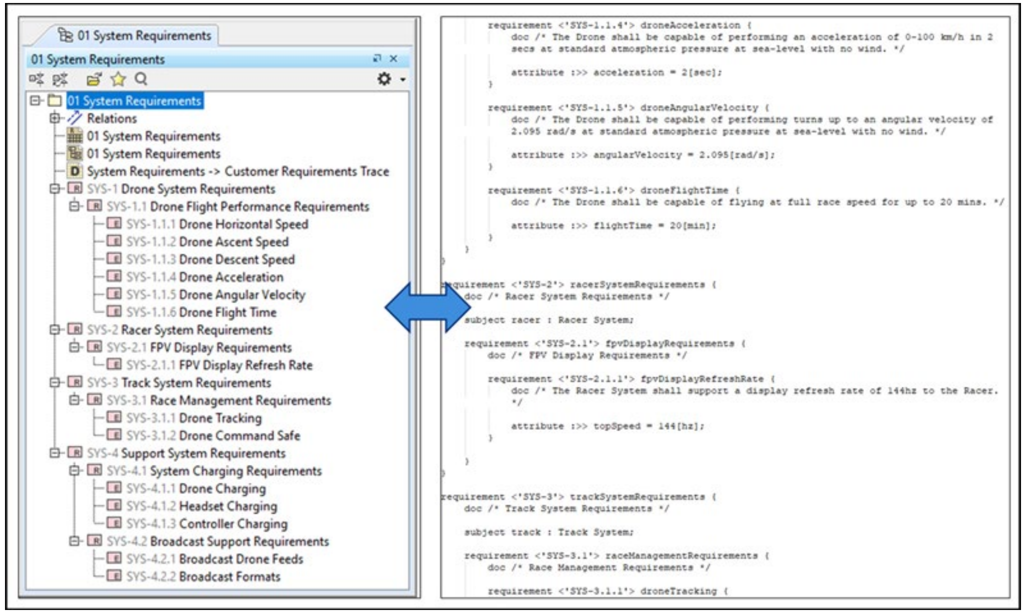
Technical Challenges

- A number of technical challenges were discovered developing the prototype:
  - There are specific situations where Cameo will alter model data contents upon the reopening of a model project
    - This happens to specific attributes and is completely unprompted by the user
    - This causes prototype to falsely fail signature verification
  - Some attributes have to be ignored from the model data integrity check to enable moving of the signed element (e.g., fully qualified name)
    - Other attributes are verified to capture containment changes within the signed element
- The researchers plan to engage MBSE software vendors on the findings

Conclusions and Future Work

- Our research demonstrates that traditional digital signature techniques can be applied to MBSE models:
  - The industry can implement these approaches today and gain a baseline level of digital signing capability
  - There is potentially new capability due to the unique nature of MBSE models (e.g., tiered countersignature)

- Our research provides a basis for future work:
  - Expanding digital signature to external model review tools (e.g., Cameo Collaborator, OpenMBEE, etc.)
  - Integrating MBSE digital signature with other engineering tools (i.e., digital thread)
  - Exploring potential new workflows due to future changes to the modeling standards
    - Such as SysML 2’s text-based model definition and system modeling API



- 01 System Requirements
  - Relations
  - 01 System Requirements
  - 01 System Requirements
  - System Requirements -> Customer Requirements Trace
  - SYS-1 Drone System Requirements
    - SYS-1.1 Drone Flight Performance Requirements
      - SYS-1.1.1 Drone Horizontal Speed
      - SYS-1.1.2 Drone Ascent Speed
      - SYS-1.1.3 Drone Descent Speed
      - SYS-1.1.4 Drone Acceleration
      - SYS-1.1.5 Drone Angular Velocity
      - SYS-1.1.6 Drone Flight Time
  - SYS-2 Racer System Requirements
    - SYS-2.1 FPV Display Requirements
      - SYS-2.1.1 FPV Display Refresh Rate
  - SYS-3 Track System Requirements
    - SYS-3.1 Race Management Requirements
      - SYS-3.1.1 Drone Tracking
      - SYS-3.1.2 Drone Command Safe
  - SYS-4 Support System Requirements
    - SYS-4.1 System Charging Requirements
      - SYS-4.1.1 Drone Charging
      - SYS-4.1.2 Headset Charging
      - SYS-4.1.3 Controller Charging
    - SYS-4.2 Broadcast Support Requirements
      - SYS-4.2.1 Broadcast Drone Feeds
      - SYS-4.2.2 Broadcast Formats

```
        requirement <'SYS-1.1.4'> droneAcceleration {
            doc /* The Drone shall be capable of performing an acceleration of 0-100 km/h in 2
            secs at standard atmospheric pressure at sea-level with no wind. */

            attribute :>> acceleration = 2[sec];
        }

        requirement <'SYS-1.1.5'> droneAngularVelocity {
            doc /* The Drone shall be capable of performing turns up to an angular velocity of
            2.095 rad/s at standard atmospheric pressure at sea-level with no wind. */

            attribute :>> angularVelocity = 2.095[rad/s];
        }

        requirement <'SYS-1.1.6'> droneFlightTime {
            doc /* The Drone shall be capable of flying at full race speed for up to 20 mins. */

            attribute :>> flightTime = 20[min];
        }
    }
}

requirement <'SYS-2'> racerSystemRequirements {
    doc /* Racer System Requirements */

    subject racer : Racer System;

    requirement <'SYS-2.1'> fpvDisplayRequirements {
        doc /* FPV Display Requirements */

        requirement <'SYS-2.1.1'> fpvDisplayRefreshRate {
            doc /* The Racer System shall support a display refresh rate of 144hz to the Racer.
            */

            attribute :>> topSpeed = 144[hz];
        }

    }
}

requirement <'SYS-3'> trackSystemRequirements {
    doc /* Track System Requirements */

    subject track : Track System;

    requirement <'SYS-3.1'> raceManagementRequirements {
        doc /* Race Management Requirements */

        requirement <'SYS-3.1.1'> droneTracking {
```

Questions?

Risa Gorospe (risa.gorospe@jhuapl.edu)
Shannon Dubicki (shannon.dubicki@jhuapl.edu)

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY