34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

Risa Gorospe & Shannon Dubicki
The Johns Hopkins University Applied Physics Laboratory

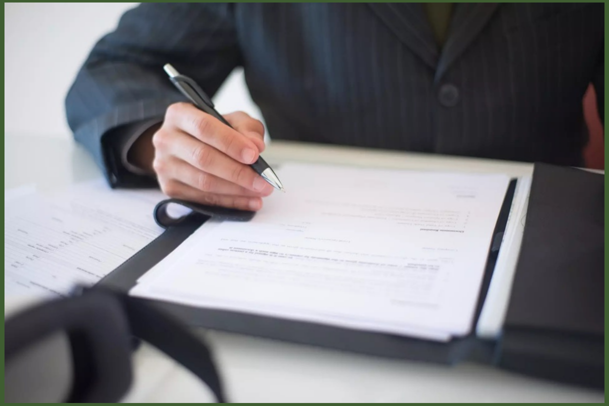
A Technical Approach to the Digital Signature of MBSE Models

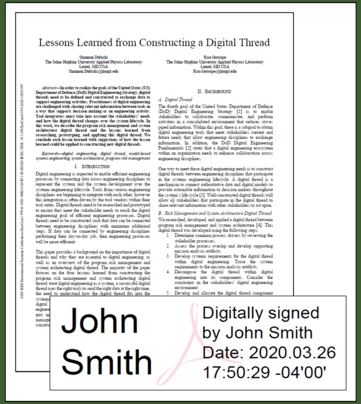
Session Objectives

- In this session, we will discuss:
  - An overview on digital signatures
  - How digitally signing model-based systems engineering (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
  - Due to the nature of MBSE models, 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

Digital Signature Overview

- Digital signature is a common cryptographic technique that enables a users to sign digital content (signer) and to verify the integrity of the signed content (verifier/reviewer)
  - With the purpose of capturing the signing party's "intention to sign" (McCullagh et al., 1998)
- Digital signature processes such as public key infrastructure (PKI) have been well-defined and implemented for regular digital documentation (Kaur & Kaur, 2012)





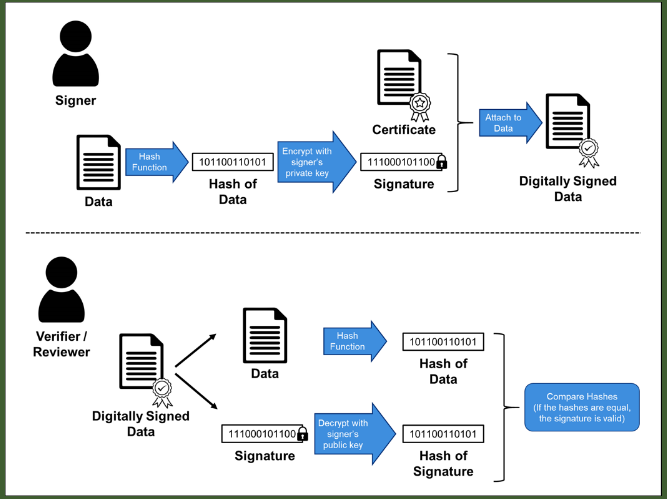
Lessons Learned from Constructing a Digital Thread

Shannon Dubicki
The Johns Hopkins University Applied Physics Laboratory
Laurel, MD USA
Shannon.Dubicki@jhuapl.edu

Risa Gorospe
The Johns Hopkins University Applied Physics Laboratory
Laurel, MD USA
Risa.Gorospe@jhuapl.edu

John Smith

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

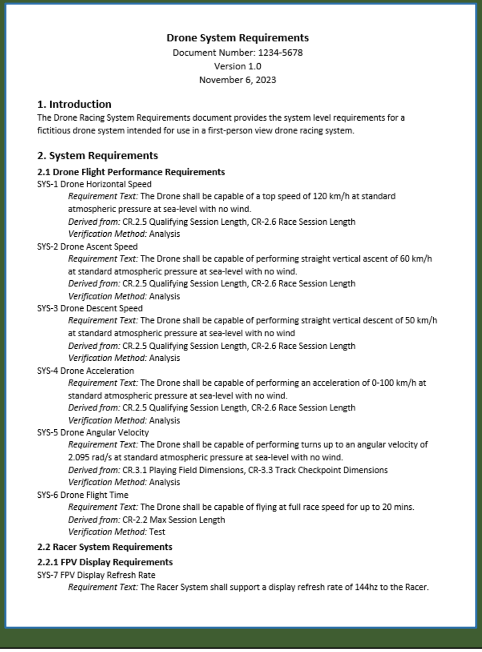


McCullagh, A., Little, P., & Caelli, W. (1998). Electronic Signatures: Understand the past to develop the future. *UNSWLJ.*

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

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)
- Model-based systems engineering (MBSE) model data needs to be presented to the user, which creates challenges for 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) with all its data, 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

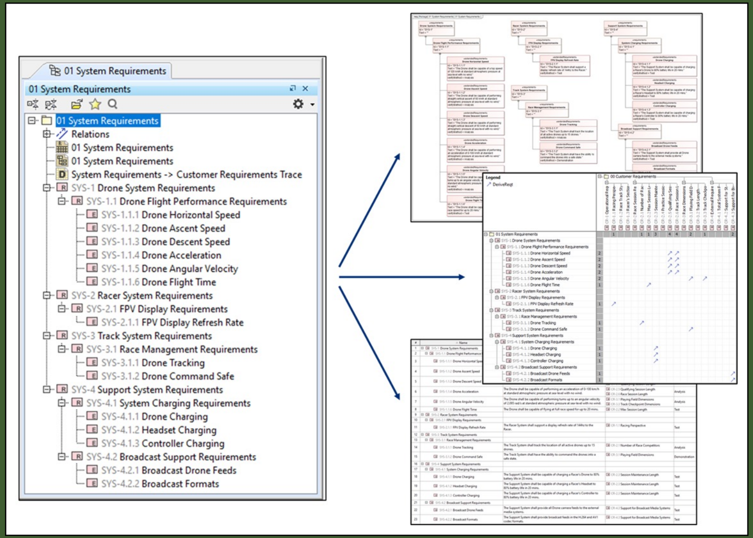
SYS-5 Drone Angular Velocity
Requirement Text: The Drone shall be capable of performing turns up to an angular velocity of 2.095 rad/s at standard atmospheric pressure at sea-level with no wind.
Derived from: CR.3.1 Playing Field Dimensions, CR-3.3 Track Checkpoint Dimensions
Verification Method: Analysis

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

Blackburn, Peak, Baker, Ballard, Rhodes, Bone, Dzielski, Giffin, Kruse, Smith, & Austin. (2019). Transforming Systems Engineering through Model-Centric Engineering (A013 Final Technical Report SERC-2019-TR-005).

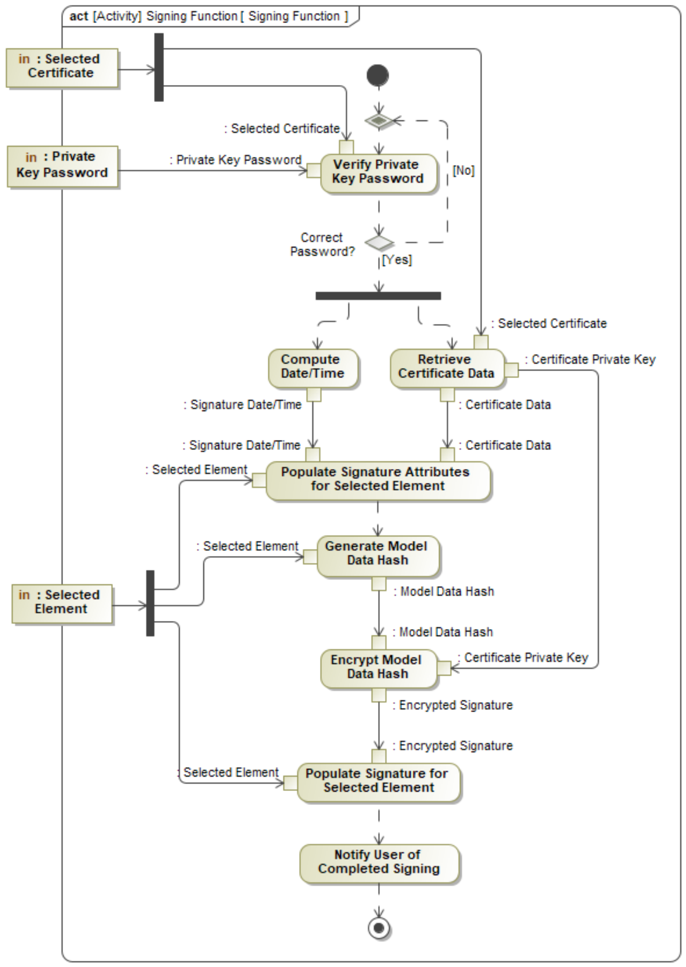
Logan, P., Harvey, D., & Spencer, D. (2012). Documents are an Essential Part of Model Based Systems Engineering. *INCOSE International Symposium*,

Research Objectives

- Our research explored developing a prototype to apply digital signature approaches to MBSE models with the following objectives:
  - The prototype will enable the user to sign specific sections of the model content using a certificate that represents the user
  - The prototype will embed the signature information directly into the model data when the user signs the model content
  - The prototype will enable the user to verify the signed model content using the signature information contained within the signed model content
  - The prototype will present signature actions in an unambiguous way to the user
  - The prototype will use existing signature techniques where possible

Technical Approach

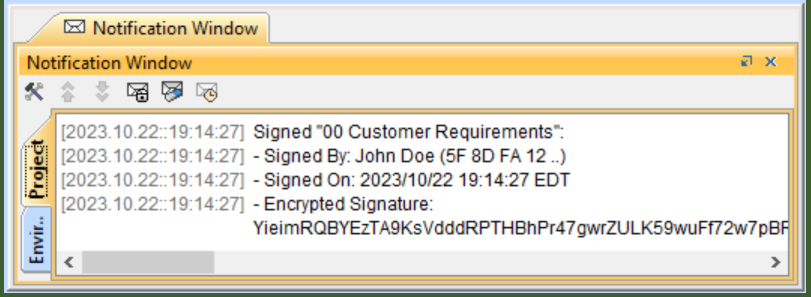
- Our research took the desired objectives and executed the following technical approach:
  1. Design and document any additional design specifications
     - e.g. functional flow of the digital signature process, generating signature hash from model data, etc.
  2. Develop a prototype to the design specifications
  3. Capture findings, observations, and additional considerations



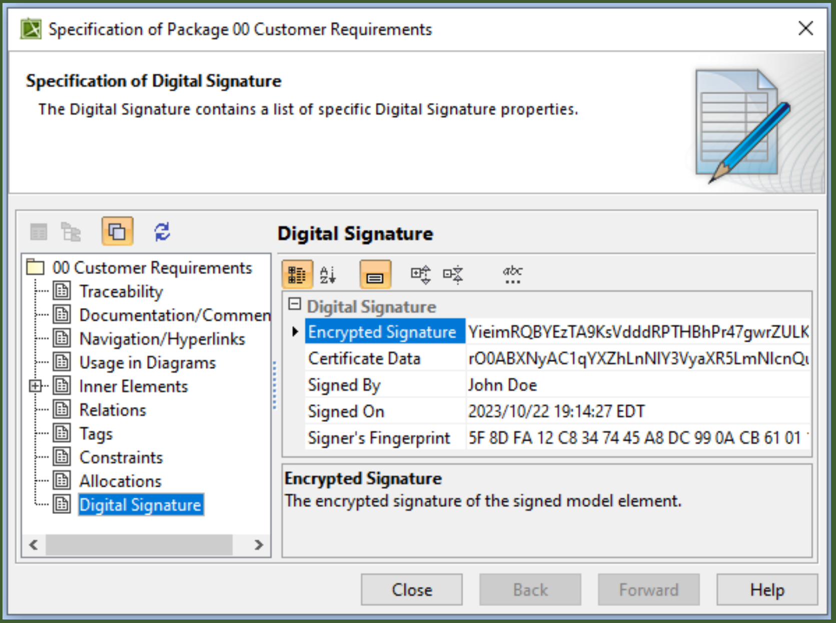
Research Prototype

Features and Characteristics

- Our research produced a prototype to explore the research objectives
- The research prototype has the following features and characteristics:
  1. The prototype is implemented as custom profile and plugin to Dassault Systems Cameo Systems Modeler 2022x designed to work with the SysML 1.7 language
  2. The prototype follows the traditional PKI digital signature processes, but with model data converted into a text string format that can be supported by standard hashing and encryption algorithms
  3. The prototype uses the Secure Hash Algorithm 256-bit (SHA-256) for hash calculations and Rivest–Shamir–Adleman (RSA) with 2,048-bit keys for signing and verification
     - The prototype can work with different hash algorithms and asymmetric encryption methods



```
[2023.10.22::19:14:27]  Signed "00 Customer Requirements":
[2023.10.22::19:14:27]  - Signed By: John Doe (5F 8D FA 12 ..)
[2023.10.22::19:14:27]  - Signed On: 2023/10/22 19:14:27 EDT
[2023.10.22::19:14:27]  - Encrypted Signature:
                        YieimRQBYEzTA9KsVdddRPTHBhPr47gwrZULK59wuFf72w7pBF
```



Specification of Digital Signature

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

Digital Signature

Digital Signature	
Encrypted Signature	YieimRQBYEzTA9KsVdddRPTHBhPr47gwrZULK
Certificate Data	rO0ABXNyAC1qYXZhLnNlY3VyaXR5LmNlcnQ
Signed By	John Doe
Signed On	2023/10/22 19:14:27 EDT
Signer's Fingerprint	5F 8D FA 12 C8 34 74 45 A8 DC 99 0A CB 61 01

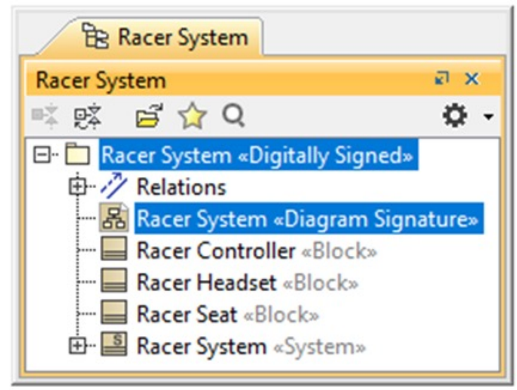
Encrypted Signature

The encrypted signature of the signed model element.

Research Prototype

Features and Characteristics (Continued)

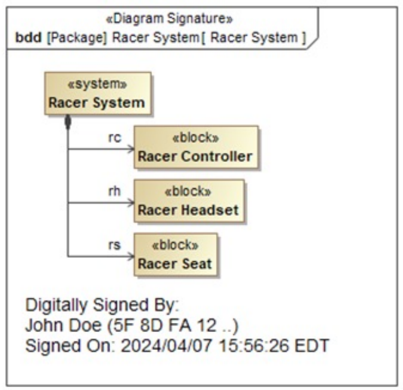
- The research prototype has the following features and characteristics:
  4. The user can select any element in the containment tree and sign its contents
  5. When the user selects to verify the signed element, the prototype assesses for changes to the signed element and all of its contained elements against the signed element's signature
  6. The prototype pushes signature information to the all diagrams contained within the signed element the moment when the element is signed
  7. The prototype can use digital certificates from the Windows OS certificate store including hardware certificates enabling smart card signing and verification



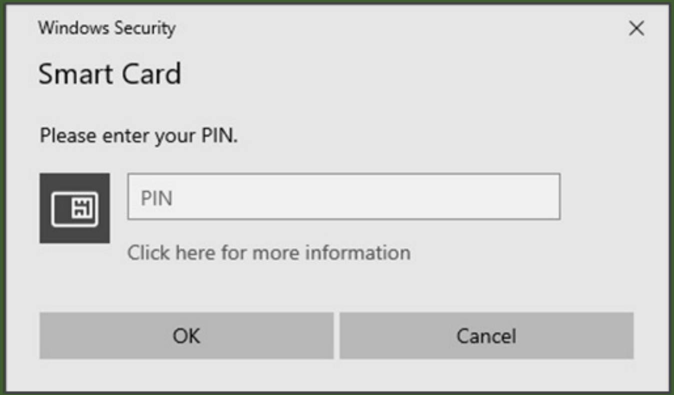
Racer System

Racer System

- Racer System «Digitally Signed»
  - Relations
  - Racer System «Diagram Signature»
  - Racer Controller «Block»
  - Racer Headset «Block»
  - Racer Seat «Block»
  - Racer System «System»



Digitally Signed By:
John Doe (5F 8D FA 12 ..)
Signed On: 2024/04/07 15:56:26 EDT



Windows Security

Smart Card

Please enter your PIN.

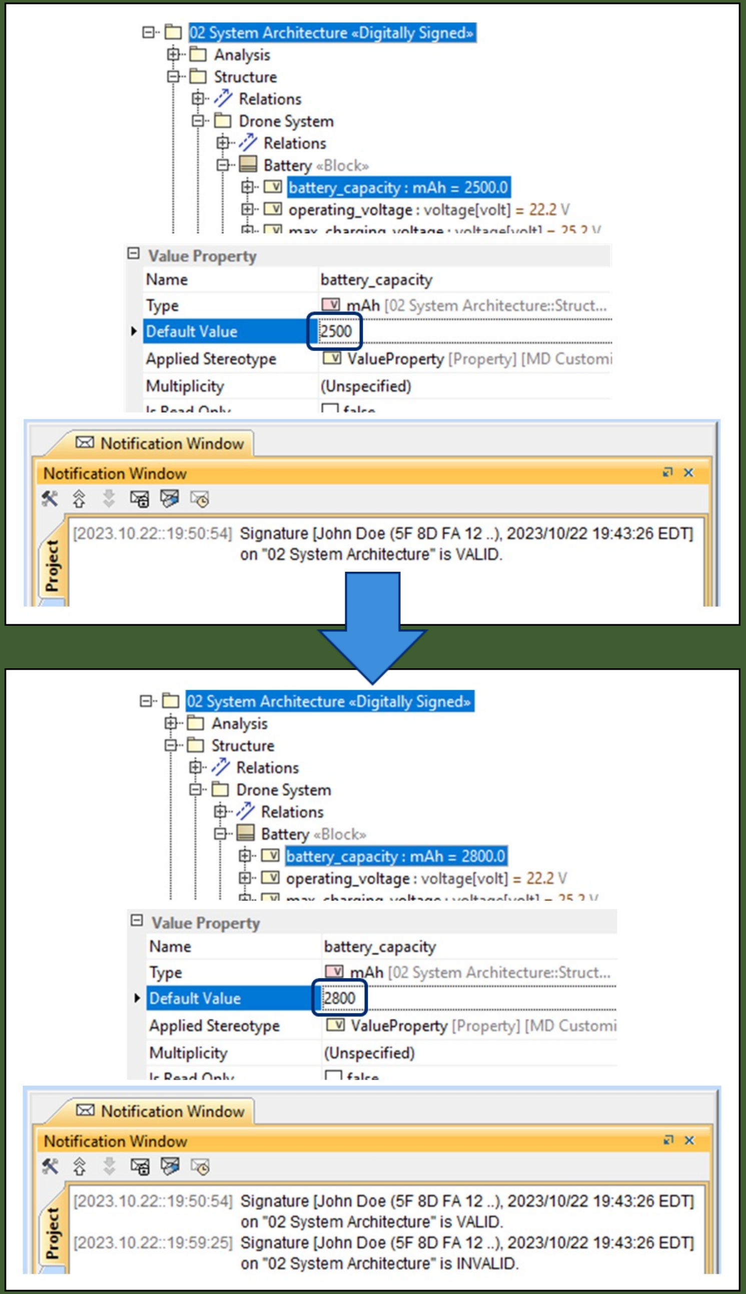
PIN

Click here for more information

Research Observations

Signature Verification of Deeply Nested Model Data

- The prototype can detect model element changes deeply nested within the containment tree:
  - The model data hash includes the attributes of the signed element and all its contained elements
  - Changes to the model data will reflect in the model data string and in the hash calculations
  - The prototype worked for all test models tried
    - Additional exploration may be needed for large models for computational performance and verification accuracy



02 System Architecture «Digitally Signed»
Analysis
Structure
Relations
Drone System
Relations
Battery «Block»
battery_capacity : mAh = 2500.0
operating_voltage : voltage[volt] = 22.2 V

Value Property

Name	battery_capacity
Type	mAh [02 System Architecture::Struct...
Default Value	2500
Applied Stereotype	ValueProperty [Property] [MD Customi
Multiplicity	(Unspecified)

Notification Window

```
[2023.10.22::19:50:54] Signature [John Doe (5F 8D FA 12 ..), 2023/10/22 19:43:26 EDT]
                       on "02 System Architecture" is VALID.
```

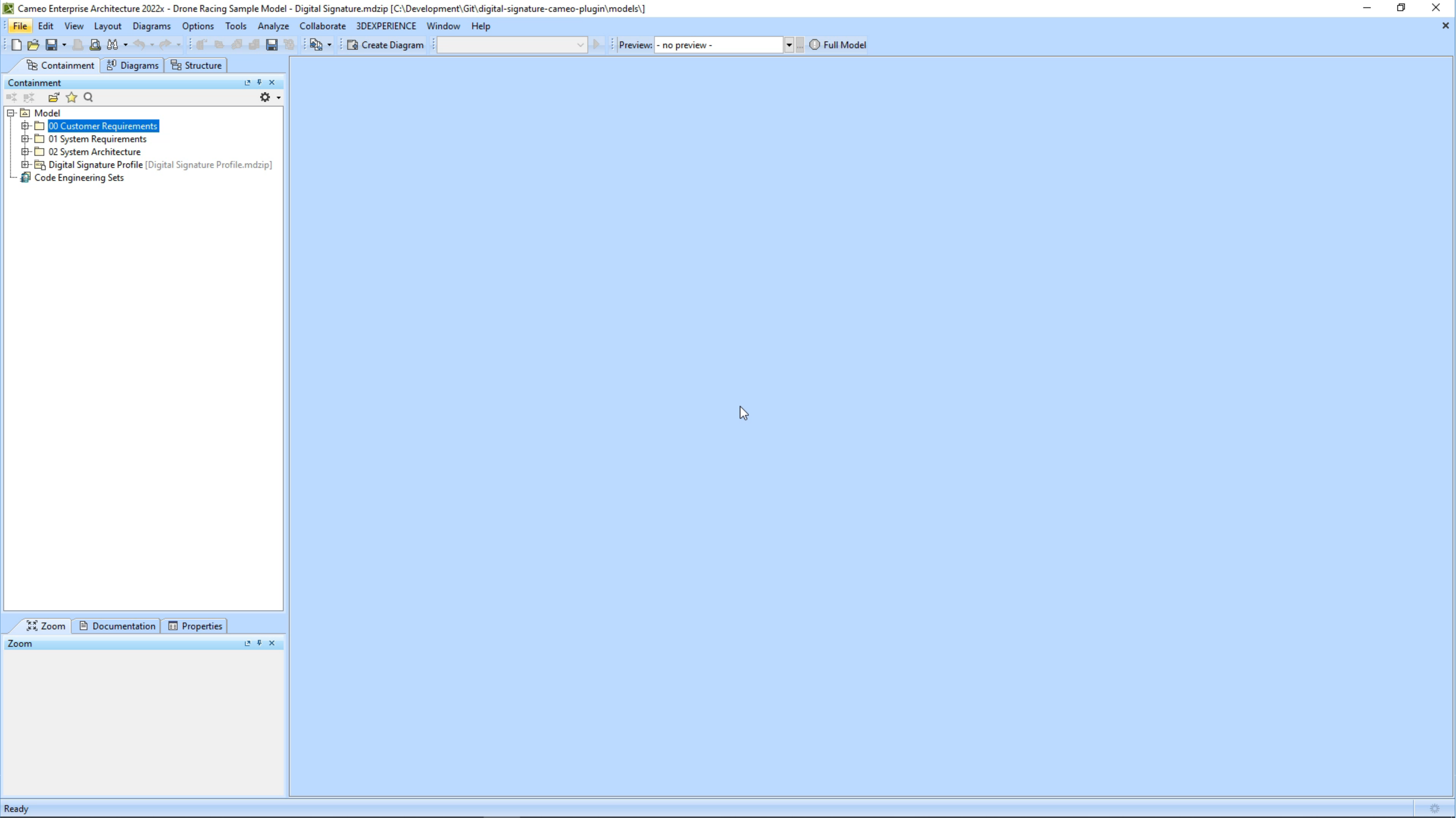
02 System Architecture «Digitally Signed»
Analysis
Structure
Relations
Drone System
Relations
Battery «Block»
battery_capacity : mAh = 2800.0
operating_voltage : voltage[volt] = 22.2 V

Value Property

Name	battery_capacity
Type	mAh [02 System Architecture::Struct...
Default Value	2800
Applied Stereotype	ValueProperty [Property] [MD Customi
Multiplicity	(Unspecified)

Notification Window

```
[2023.10.22::19:50:54] Signature [John Doe (5F 8D FA 12 ..), 2023/10/22 19:43:26 EDT]
                       on "02 System Architecture" is VALID.
[2023.10.22::19:59:25] Signature [John Doe (5F 8D FA 12 ..), 2023/10/22 19:43:26 EDT]
                       on "02 System Architecture" is INVALID.
```

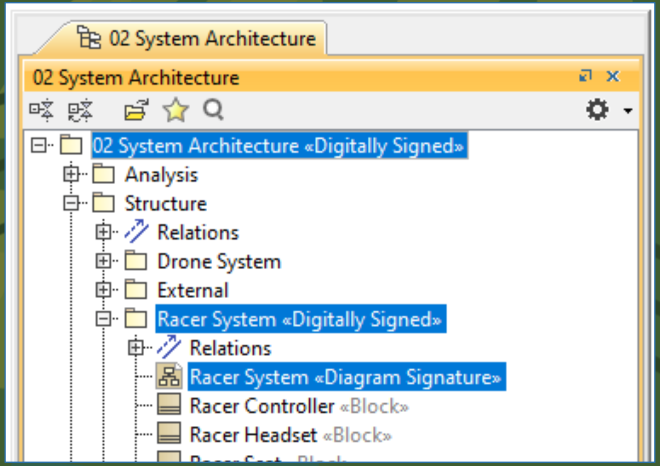


Cameo Enterprise Architecture 2022x - Drone Racing Sample Model - Digital Signature.mdzip [C:\Development\Git\digital-signature-cameo-plugin\models\]

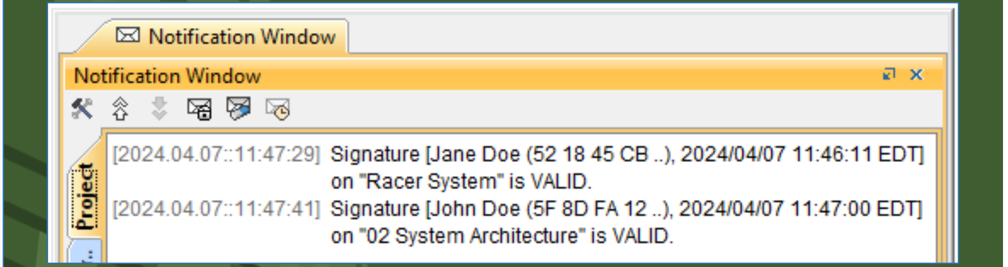
Research Observations

Additional Capability – Tiered Countersignature

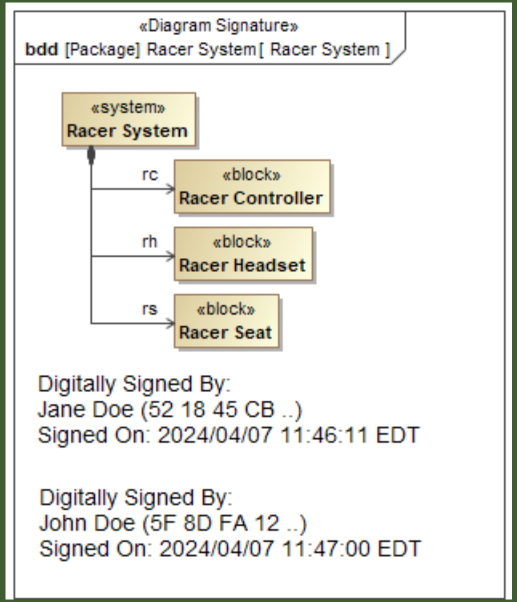
- The prototype can nest signatures within each other for tiered countersignature
  - e.g., an engineer signs a subsystem package and the engineering manger signs the higher system package



02 System Architecture «Digitally Signed»
Analysis
Structure
Relations
Drone System
External
Racer System «Digitally Signed»
Relations
Racer System «Diagram Signature»
Racer Controller «Block»
Racer Headset «Block»
Racer Seat «Block»

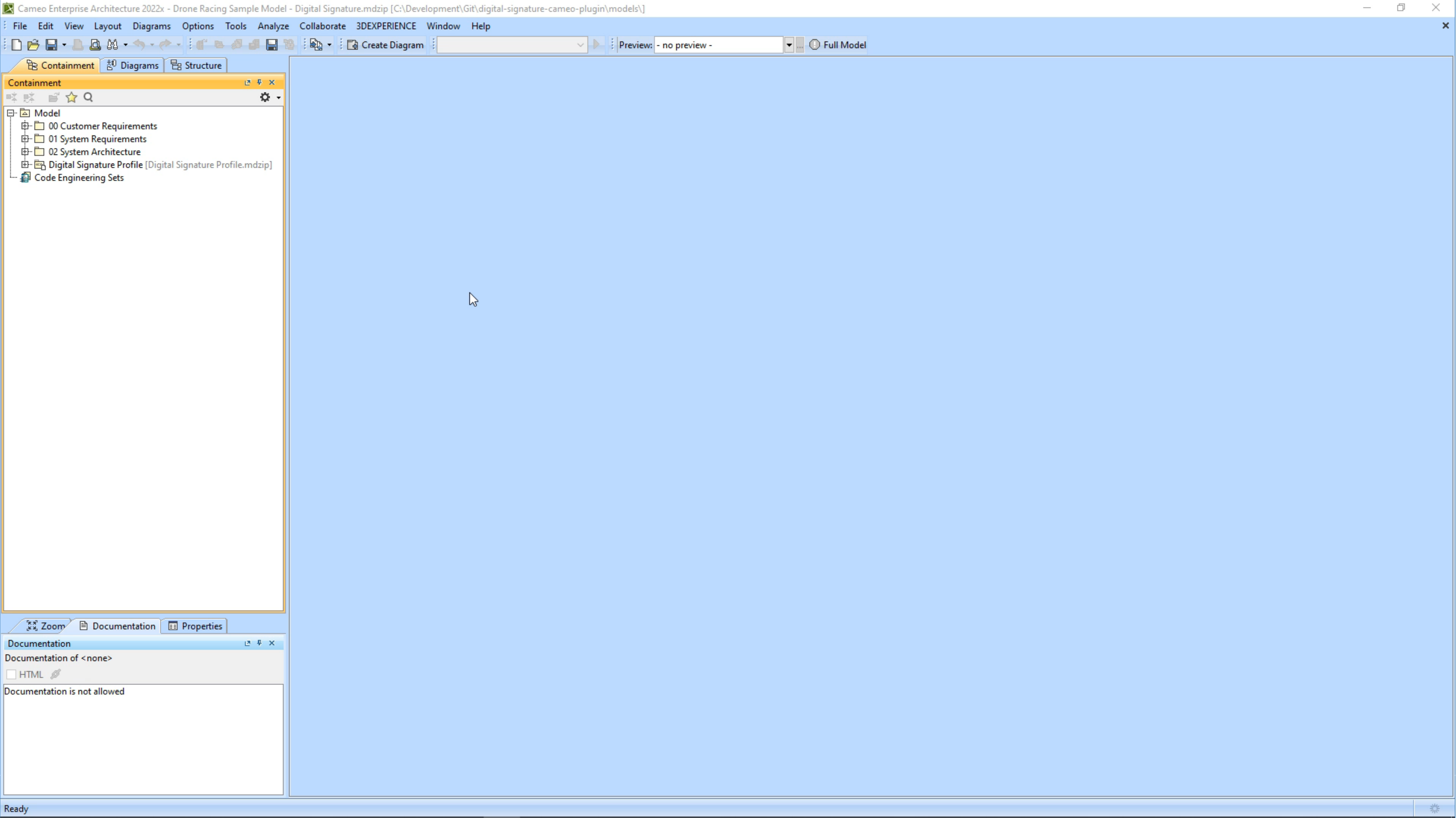


```
[2024.04.07::11:47:29] Signature [Jane Doe (52 18 45 CB ..), 2024/04/07 11:46:11 EDT]
                       on "Racer System" is VALID.
[2024.04.07::11:47:41] Signature [John Doe (5F 8D FA 12 ..), 2024/04/07 11:47:00 EDT]
                       on "02 System Architecture" is VALID.
```



Digitally Signed By:
Jane Doe (52 18 45 CB ..)
Signed On: 2024/04/07 11:46:11 EDT

Digitally Signed By:
John Doe (5F 8D FA 12 ..)
Signed On: 2024/04/07 11:47:00 EDT



Cameo Enterprise Architecture 2022x - Drone Racing Sample Model - Digital Signature.mdzip [C:\Development\Git\digital-signature-cameo-plugin\models\]

- Model
  - 00 Customer Requirements
  - 01 System Requirements
  - 02 System Architecture
  - Digital Signature Profile [Digital Signature Profile.mdzip]
- Code Engineering Sets

Documentation of <none>

Documentation is not allowed

Ready

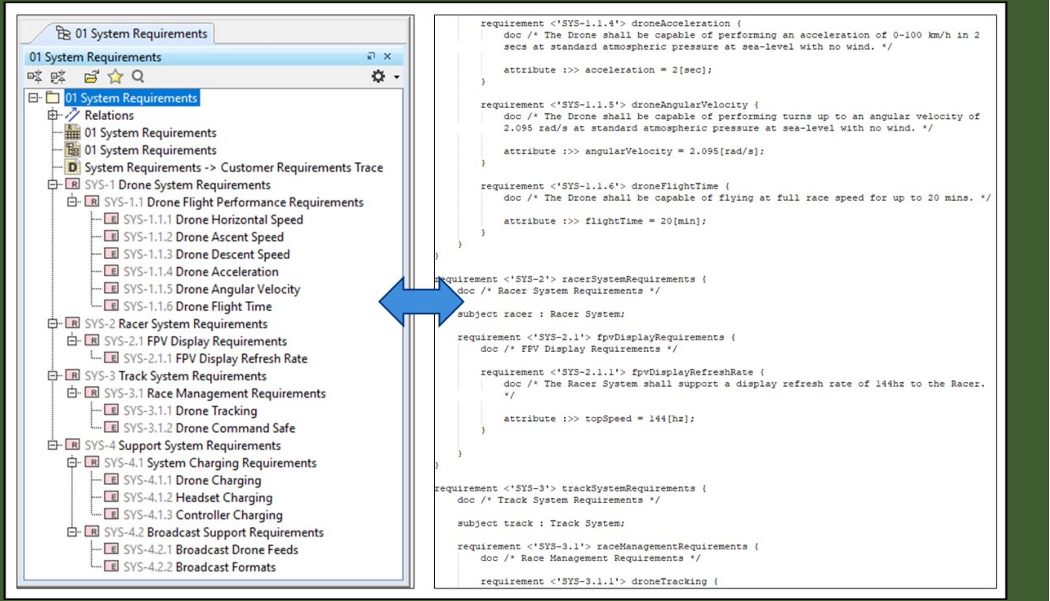
Research Observations

Technical Challenges

- A number of technical challenges were discovered developing the prototype as a custom Cameo plugin:
  - There are specific situations where Cameo will alter model data contents unprompted by the user causing the inadvertent failure of the signature verification process
    - This causes potential model integrity concerns in those situations
  - Some attributes have to be ignored from the hash calculations to prevent unnecessary signature verification failures when the signed element is moved (e.g., 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 digital signature techniques can be applied to MBSE models:
  - The industry can implement existing approaches today and gain a baseline level of digital signing capability
  - There are potentially new ways to conduct digital signature due to the unique nature of MBSE models (e.g., tiered countersignature)
- Our research provides a basis for future work:
  - Expansion of the digital signature to external model review tools (e.g., Cameo Collaborator, OpenMBEE, etc.)
  - Addition of other alternative signing mechanisms
  - Exploration of potential new workflows due to future changes to the modeling standards (e.g., SysML 2’s textual and modeling API standards)



```
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@jhuapl.edu
Shannon.Dubicki@jhuapl.edu

34th Annual **INCOSE**
international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS