AADL Modeling and Analysis tool for Cyber Resiliency - GE VERDICT / DARPA CASE

AADL/ACVIP User Days 2021

Michael Durling – GE Research – durling@ge.com

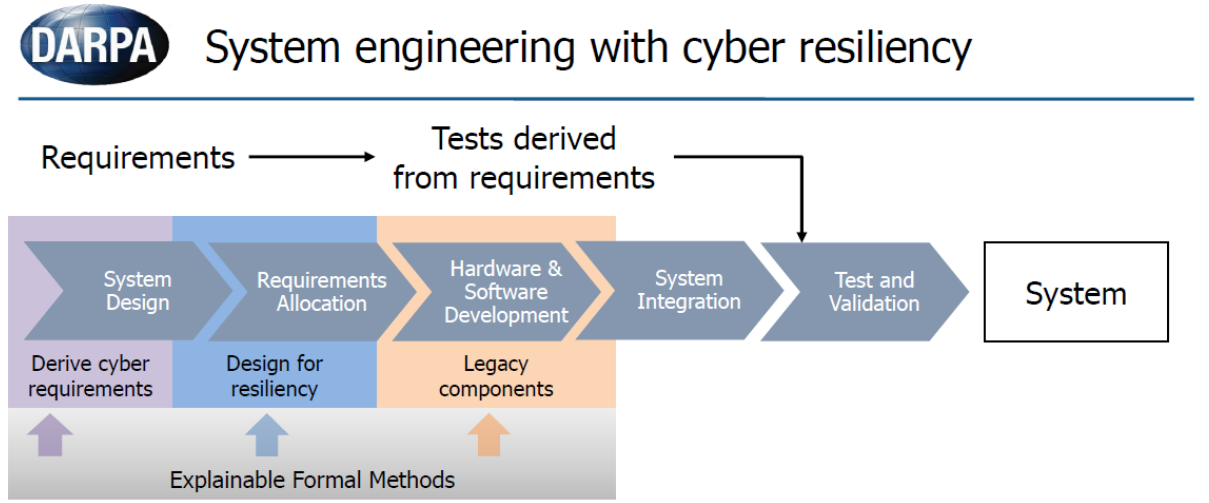
GRC: Michael Durling, Kit Siu, Abha Moitra, Paul Meng, John Interrante, Heber Herencia-zapana
GEAS: Daniel Prince
University of Iowa: Cesare Tinelli, Omar Chowdhury, Daniel Larraz, Moosa Yahyazadeh, Fareed Arif

February 15, 2021

Agenda

- ❑ DARPA CASE Program
- ❑ What is the VERDICT Tool?
- ❑ Working example
- ❑ Tool availability
- ❑ Publications
- ❑ Questions

Cyber Assured Systems Engineering (CASE)



Explicit system properties

- Reliability
- Availability
- Maintainability
- Performance
- Safety
- many more...
- Cyber resiliency

1. Shall...
2. Shall...
3. Shall...

1. Shall not...
2. Shall not ...
3. Shall not ...

- Design-in cyber resiliency as an explicit property of the system
- Enable informed design decisions when resiliency conflicts with other system properties
- Provide formal methods tools to validate systems resiliency properties
- Eliminate need for costly redesign

Goal for the CASE Program:

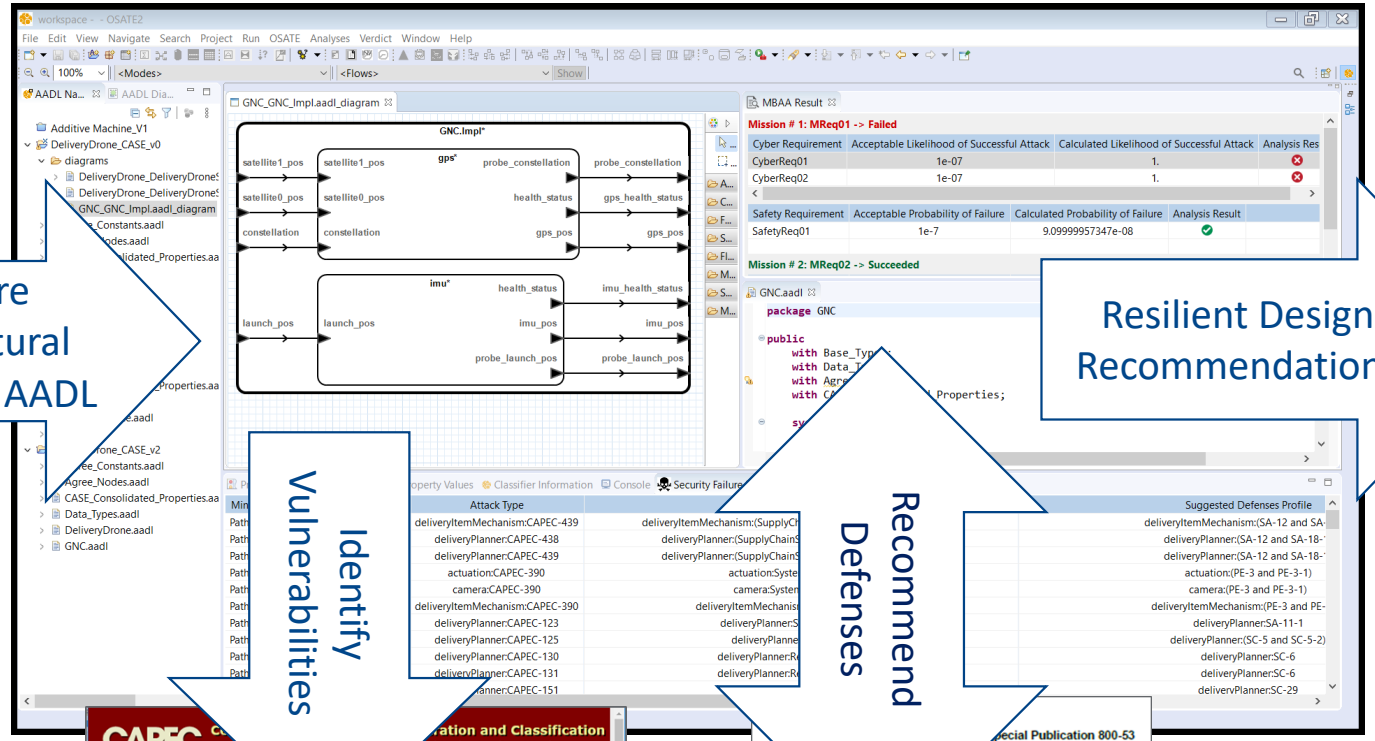
Develop *advanced design and analysis tools* that establish *cyber resiliency as an explicit property* for complex cyber physical systems.

Model-based identification of Security Threats & Mitigations to enable Cyber Resiliency

Security Requirements & Policies

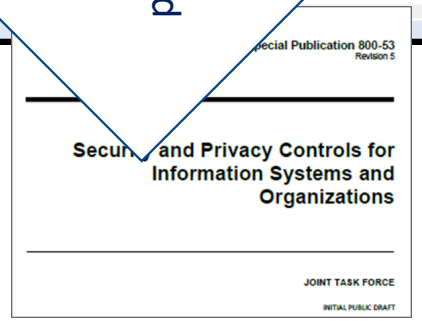
Capture architectural models in AADL

VERDICT Cyber Resilience Design Tool



Identify Vulnerabilities

Recommend Defenses



Resilient Design Recommendations

Security Requirements & Policies

What can we do now that we could not do before CASE?

State of industry before CASE

× Labor-intensive, Slow

× Separate from Systems Modeling and Safety Analysis

× Often Not Threat-based

× Does not consider mission

× Strictly process assurance based

Today with VERDICT

✓ Automated (Real-time feedback to designers on potential attacks, control suggestions, behavioral weaknesses)

✓ Integrated (Safety and Security analyses in the same tool)

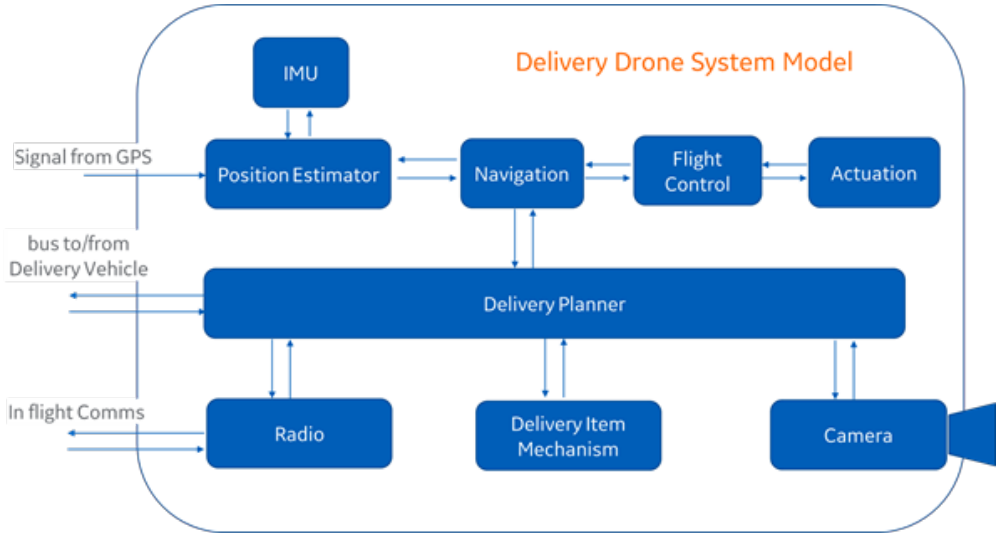
✓ Built-in (Utilizes wealth of data available in models instead of collecting data from various sources)

✓ Mission-Centric (Controls suggested against specific threats that have a direct effect on the mission)

✓ Blended (Benefits from traditional and formal verification)

Demo: Delivery Drone

- Scenario: a truck with packages to be delivered using one or more delivery drones.
- Truck arrives at a location close to multiple delivery sites. Delivery drones are initialized with their current position, delivery locations, and loaded with the package.
- Drone uses:
  - Inputs from GPS and IMU to navigate
  - Camera to capture an image of receiving site and to confirm site is free of obstacles
  - Radio to get confirmation from truck operator if delivering a high-value package
- Delivery Planner activates the Delivery Item Mechanism to drop off the package.

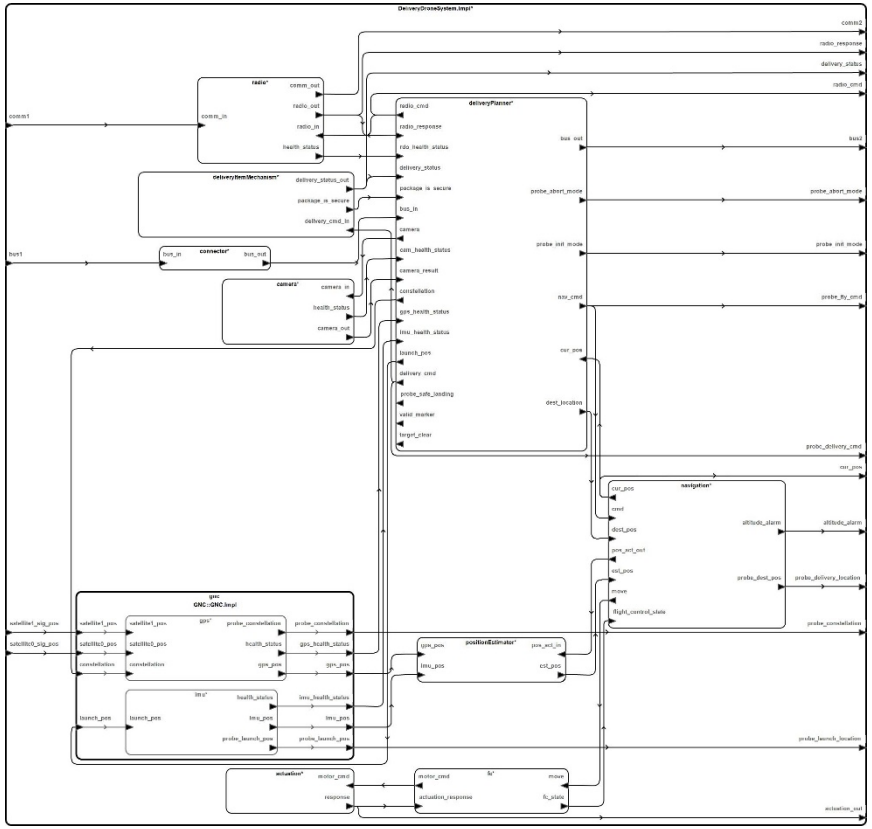


Develop the Architectural Model in AADL

Define architectural components

```
system GNC
    features
        -- inputs
        constellation: in data port Data_Types::Constellation;
        satellite0_pos: in data port Data_Types::Position.impl;
        satellite1_pos: in data port Data_Types::Position.impl;
        launch_pos: in data port Data_Types::Position.impl;

        -- outputs
        gps_pos: out data port Data_Types::Position.impl;
        gps_health_status: out data port Base_Types::Boolean;
        probe_constellation: out data port Data_Types::Constellation
        {CASE_Consolidated_Properties::probe => true; };
        imu_pos: out data port Data_Types::Position.impl;
        imu_health_status: out data port Base_Types::Boolean;
        probe_launch_pos: out data port Data_Types::Position.impl
        {CASE_Consolidated_Properties::probe => true; };


end GNC;
```

Generate diagram



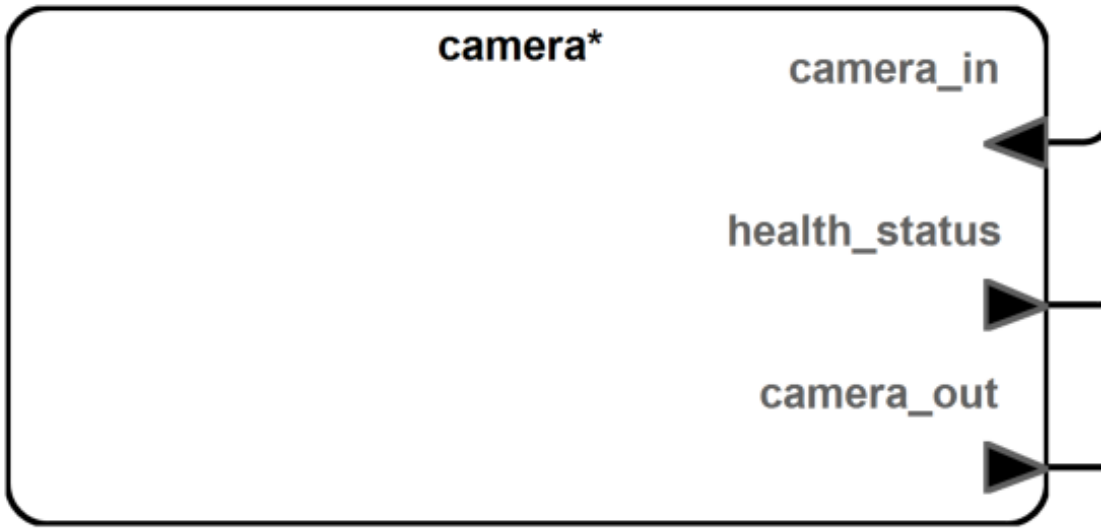
Capture Mission, Cyber and Safety Requirements with VERDICT annex

```
annex verdict{**
    CyberReq {
    id = "CyberReq01"
    description = "The drone shall be resilient to loss of ability to deliver a package to
                   the appropriate consumer location"
    condition = actuation_out:I or actuation_out:A or delivery_status:I or delivery_status:A
    cia = I
    severity = Hazardous
        };
    SafetyReq {
    id = "SafetyReq02"
    description = "Delivery Item Mechanism is reliable, where an undetected erroneous command shall be less than 1e-7 pfh"
    condition = delivery_status:I
    targetProbability = 1e-07
        };
    MissionReq {
        id ="MReq01"
        description = "Deliver a package to the intended location."
        reqs = "CyberReq01","CyberReq02","SafetyReq01"
    };
**};
```

Acceptable Likelihood of Successful Attack	Consequence	Required Security Design Assurance Level
1 e -9	Catastrophic	A
1 e -7	Hazardous	B
1 e -5	Major	C
1 e -3	Minor	D
1	None	E

Set Cyber and Safety Relations

```
system Camera
    features
        camera_in: in data port Base_Types::Boolean;
        camera_out: out data port Base_Types::Integer;
        health_status: out data port Base_Types::Boolean;

    annex verdict {**
        CyberRel "camera_out_I" = camera_in:I => camera_out:I;
        CyberRel "camera_out_A" = camera_in:A => camera_out:A;
        Event {
            id = "loa_event"
            probability = 1.0e-8
            comment = "loss of availability of the Camera"
            description = "LOA"
        }
        Event {
            id = "ued_event"
            probability = 1.0e-9
            comment = "undetected erroneous data of the Camera"
            description = "UED"
        }
        SafetyRel "camera_out_UED" = happens("ued_event") or camera_in:I => camera_out:I;
        SafetyRel "camera_out_LOA" = happens("loa_event") or camera_in:A => camera_out:A;
    **};
end Camera;
```



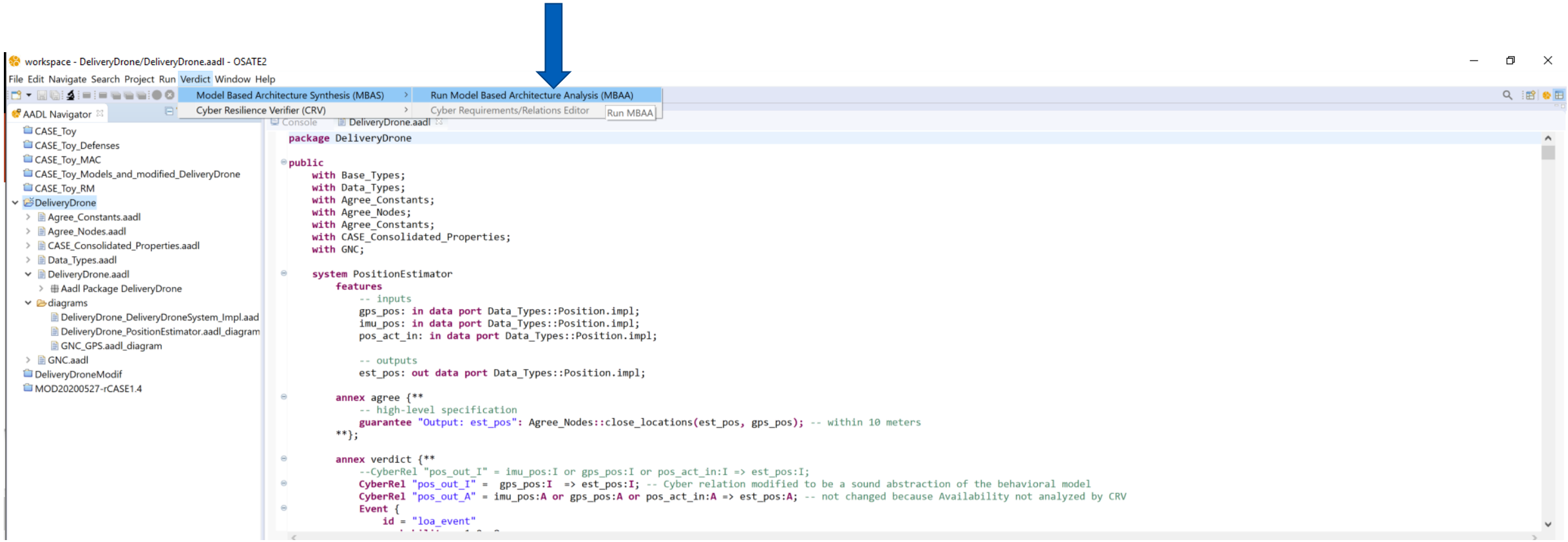
Set Mandatory Properties

```
radio: system Radio
{
    -- VERDICT Component Properties

    CASE_Consolidated_Properties::canReceiveConfigUpdate => true;
    CASE_Consolidated_Properties::canReceiveSWUpdate => true;
    CASE_Consolidated_Properties::componentType => Hybrid;
    CASE_Consolidated_Properties::hasSensitiveInfo => true;
    CASE_Consolidated_Properties::insideTrustedBoundary => true;
    CASE_Consolidated_Properties::pedigree => COTS;
```

Console | CASE_Consolidated_Properties.aadl

```
------------------------------------------------------------------------
--- Mandatory User Defined Component Properties
---          NOTE: The mandatory user defined component properties must be assigned for each applicable component as a minimum for VERDICT to execute.
------------------------------------------------------------------------

--- MBAA:
---    canReceiveConfigUpdate is a property used to determine whether the system is susceptible to attacks attempting to tamper with the configuration
---    of a system. Apply this property if the configuration of software or hardware within the system can be updated outside of the original
---    manufacturer's facility.

canReceiveConfigUpdate: aadlboolean => True applies to (abstract, bus, device, system, process, processor, thread);

--- MBAA:
---    canRecieveSWUpdate is a property used to determine whether the system is susceptible to attacks attempting to install malicious software
---    updates. Apply this property if the software within the system can be updated outside of the original manufacturer's facility.

canReceiveSWUpdate: aadlboolean => True applies to (abstract, bus, device, system, process, processor, thread);

--- MBAA:
---    componentType is a property used to determine whether the system is subject to attacks targeting software, hardware, humans, or hybrid
---    (software and hardware). For example, systems that represent software only will not be subject to CAPEC-440 Hardware Integrity Attack.
--- CRV:
---    A componentType designates whether a component is a Software, Hardware, Human, Software-Hardware Hybrid, Software-Human Hybrid,
---    Hardware-Human Hybrid, or Hybrid.
---    This helps CRV to decide what sort of attack can the component be susceptible to. For instance, a Hybrid component can be susceptible
---    to both hardware trojan and software Virus/Worm/Malware attacks whereas a Human component can only be susceptible to insider/outsider threat.

componentType: enumeration (Software, Hardware, Human, SwHwHybrid, SwHumanHybrid, HwHumanHybrid, Hybrid) => Hybrid applies to (abstract, bus, device, system, process, processor, thread);
```

Run VERDICT MBAA



Review VERDICT tool user feedback

Problems | Properties | AADL Property Values | Classifier Information | Console | MBAA Result

Mission # 1: MReq01 -> Failed

Cyber Requirement	Severity of Successful Attack	Implemented Security Design Assurance Level	Analysis Result
CyberReq01	Hazardous	E	✗
CyberReq02	Hazardous	E	✗

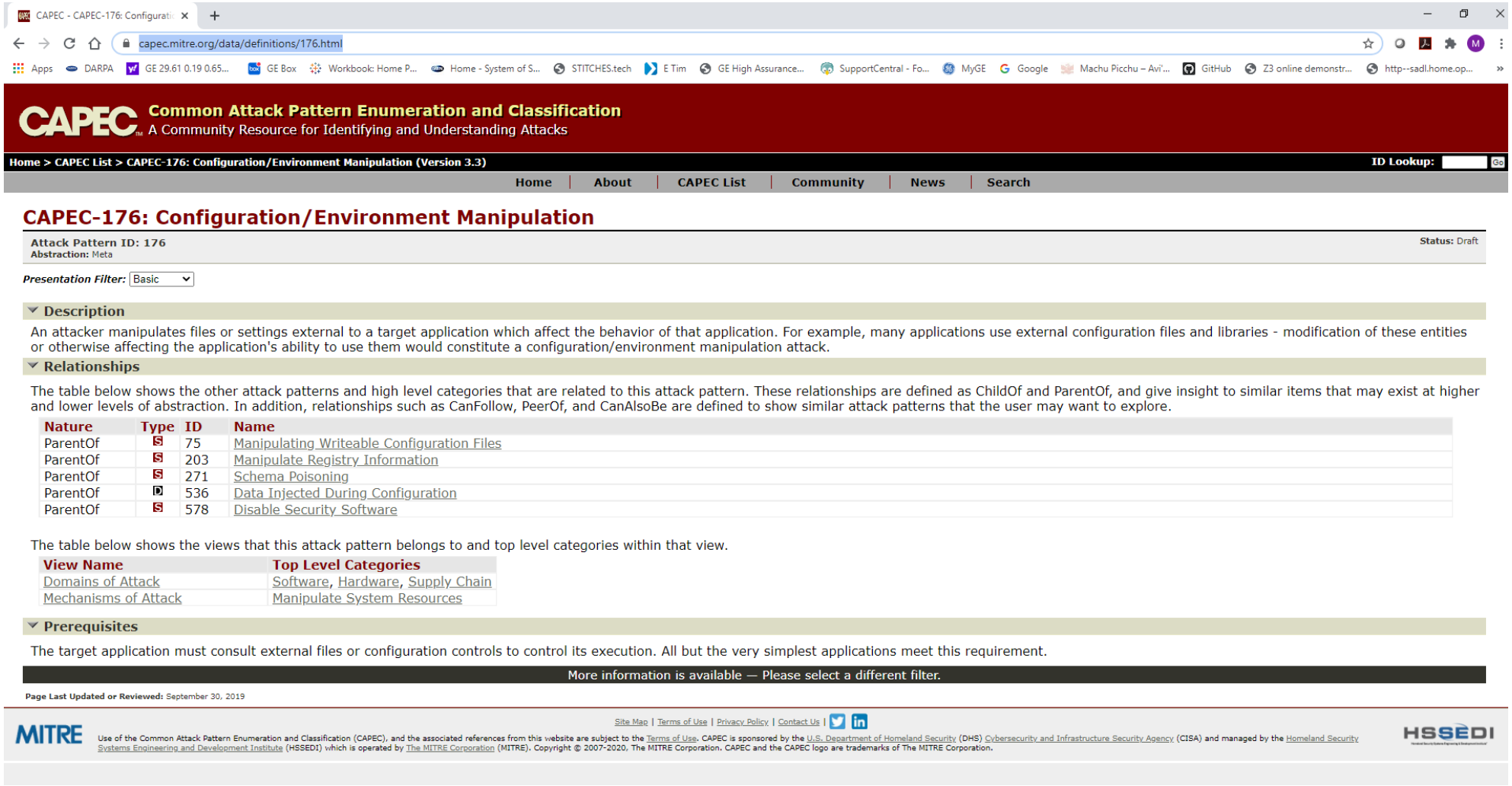
Safety Requirement	Acceptable Probability of Failure	Calculated Probability of Failure	Analysis Result
SafetyReq01	1e-7	9.09999957347e-08	✓

Security Failure Paths

Minimal Failure Path	Path Likelihood	Attack Type	Suggested Defenses	Suggested Defenses Profile
Path # 1	1.	deliveryItemMechanism:CAPEC-439	deliveryItemMechanism:(SupplyChainSecurity and TamperProtection)	deliveryItemMechanism:(SA-12 and SA-18-1)
Path # 2	1.	deliveryPlanner:CAPEC-438	deliveryPlanner:(SupplyChainSecurity and TamperProtection)	deliveryPlanner:(SA-12 and SA-18-1)
Path # 3	1.	deliveryPlanner:CAPEC-439	deliveryPlanner:(SupplyChainSecurity and TamperProtection)	deliveryPlanner:(SA-12 and SA-18-1)
Path # 4	1e-07	actuation:CAPEC-390	actuation:SystemAccessControl	actuation:(PE-3 and PE-3-1)
Path # 5	1e-07	camera:CAPEC-390	camera:SystemAccessControl	camera:(PE-3 and PE-3-1)
Path # 6	1e-07	deliveryItemMechanism:CAPEC-390	deliveryItemMechanism:SystemAccessControl	deliveryItemMechanism:(PE-3 and PE-3-1)
Path # 7	1e-07	deliveryPlanner:CAPEC-123	deliveryPlanner:StaticCodeAnalysis	deliveryPlanner:SA-11-1
Path # 8	1e-07	deliveryPlanner:CAPEC-125	deliveryPlanner:DosProtection	deliveryPlanner:(SC-5 and SC-5-2)

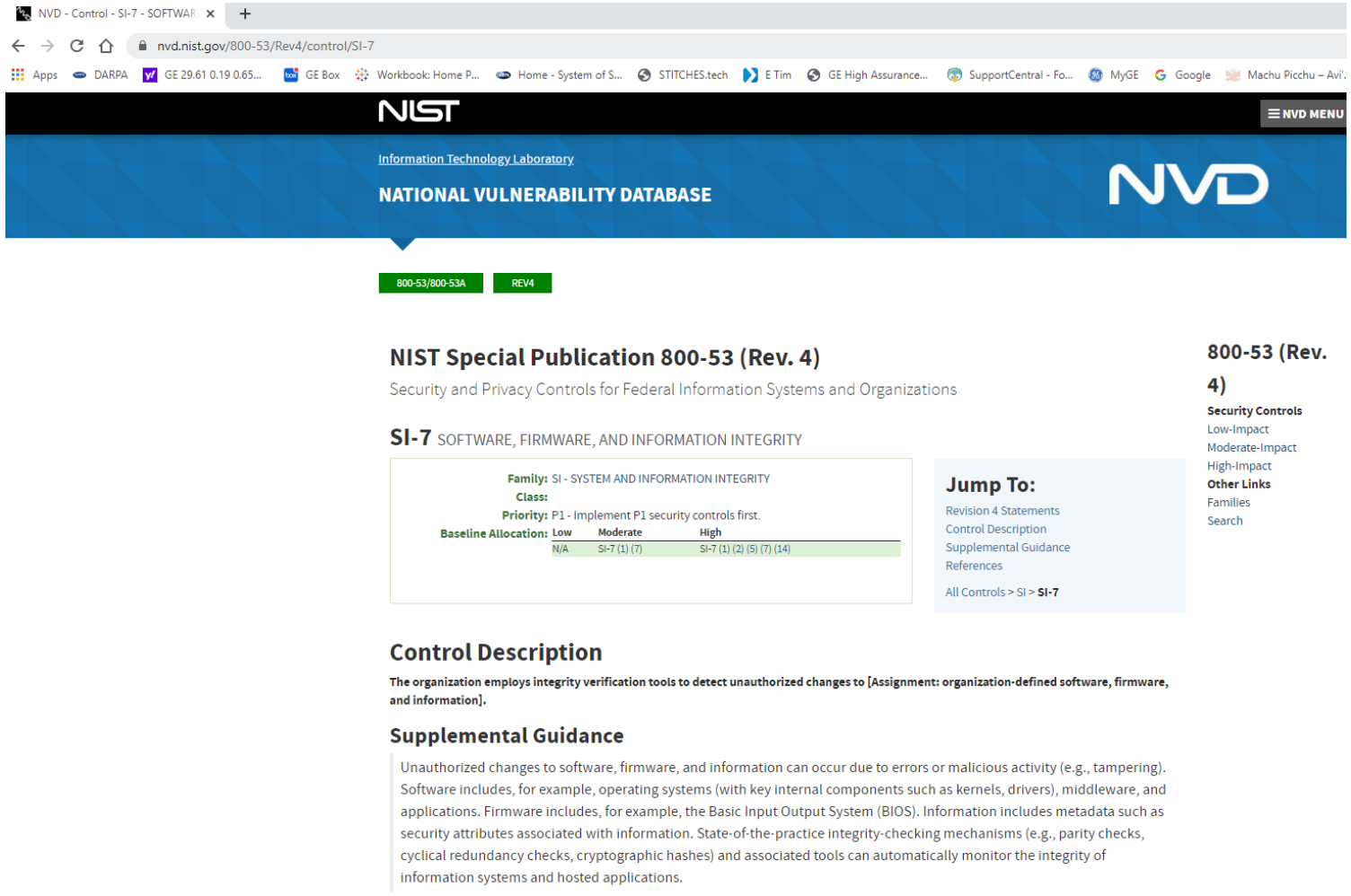
Clear feedback on each mission, cyber and safety requirement – localized to components

CAPEC library



https://capec.mitre.org/data/definitions/176.html

NIST 800-53 Defense Controls



https://nvd.nist.gov/800-53/Rev4/control/SI-7

Our recommended defenses serve as implementation requirements to the Additive Machine team

Update AADL Model

```
radio: system Radio
{
    -- VERDICT Component Properties

    CASE_Consolidated_Properties::canReceiveConfigUpdate => true;
    CASE_Consolidated_Properties::canReceiveSWUpdate => true;
    CASE_Consolidated_Properties::componentType => Hybrid;
    CASE_Consolidated_Properties::hasSensitiveInfo => true;
    CASE_Consolidated_Properties::insideTrustedBoundary => true;
    CASE_Consolidated_Properties::pedigree => COTS;

    -- VERDICT Cyber Defense and DAL Mitigations

    CASE_Consolidated_Properties::dosProtection => 7;
    CASE_Consolidated_Properties::failSafe =>7;
    CASE_Consolidated_Properties::inputValidation => 7;
    CASE_Consolidated_Properties::logging => 7;
    CASE_Consolidated_Properties::memoryProtection => 7;
    CASE_Consolidated_Properties::physicalAccessControl => 7;
    CASE_Consolidated_Properties::remoteAttestation => 7;
    CASE_Consolidated_Properties::resourceAvailability => 7;
    CASE_Consolidated_Properties::secureBoot => 7;
    CASE_Consolidated_Properties::staticCodeAnalysis => 7;
    CASE_Consolidated_Properties::strongCryptoAlgorithms => 7;
    CASE_Consolidated_Properties::supplyChainSecurity => 0;
    CASE_Consolidated_Properties::systemAccessControl => 7;

};
```

Based on feedback from VERDICT

- Set Cyber Defense properties
- Change component properties
- Move Trust Boundary

Update and rerun tool until satisfied with the results

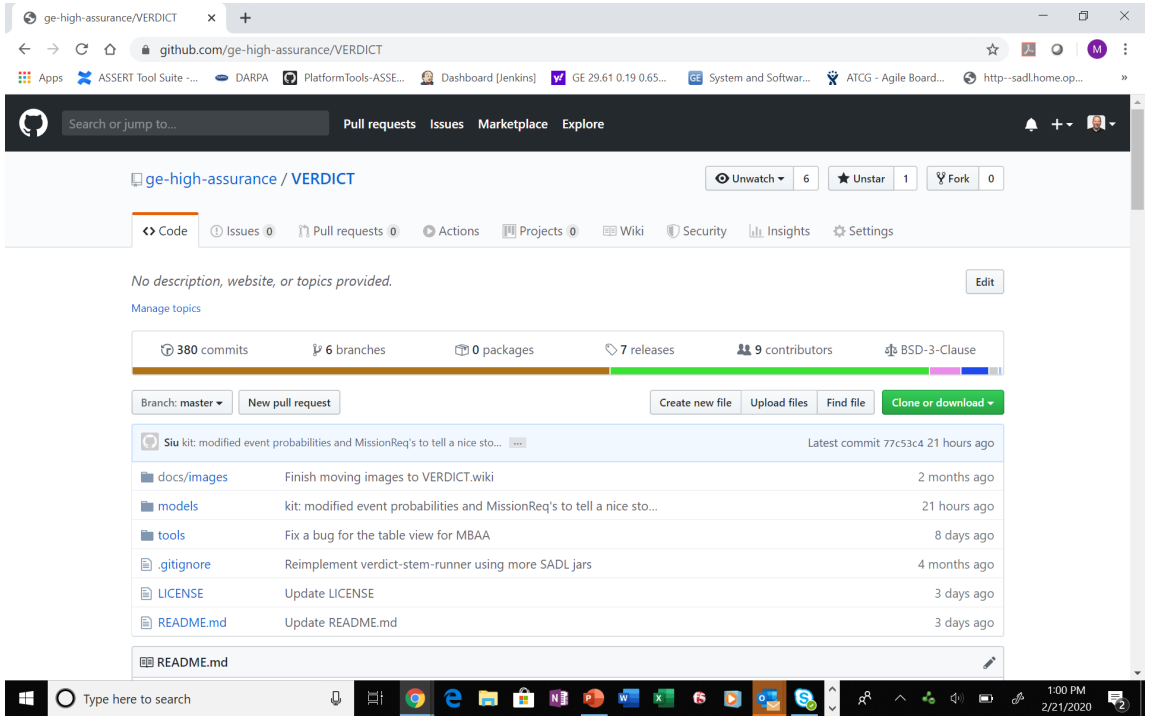
Problems | Properties | AADL Property Values | Classifier Information | Console | MBAA Result

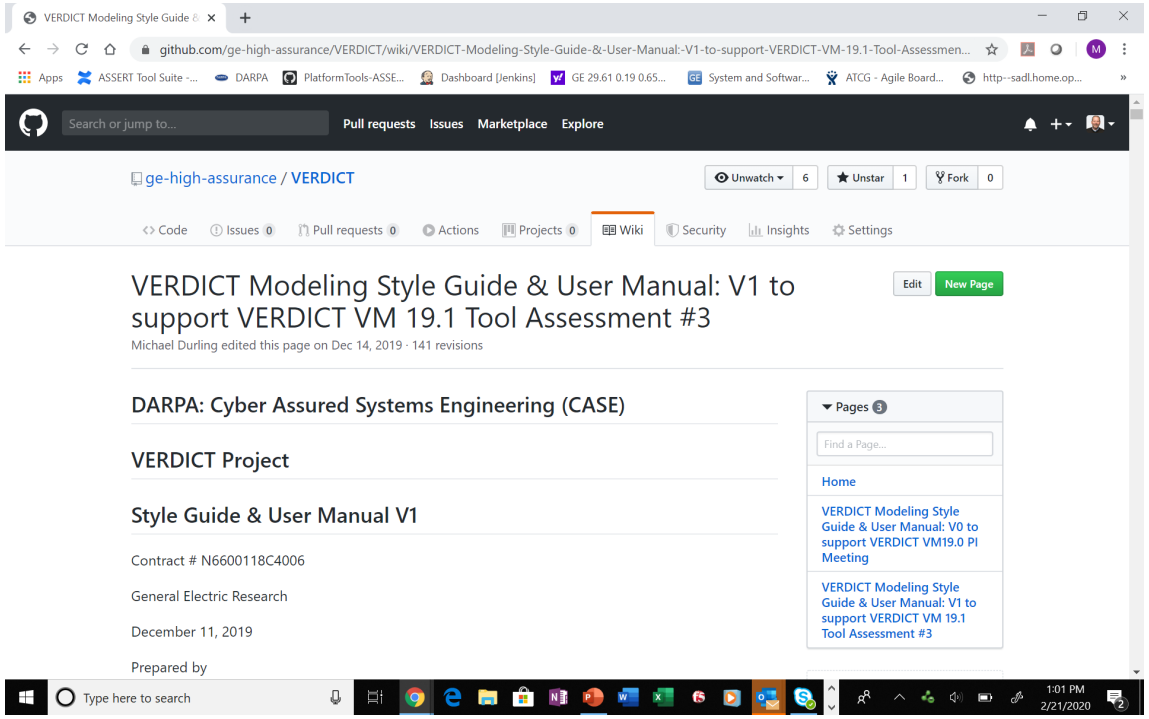
Mission # 1: MReq01 -> Succeeded

Cyber Requirement	Severity of Successful Attack	Implemented Security Design Assurance Level	Analysis Result
CyberReq01	Hazardous	B	✓
CyberReq02	Hazardous	B	✓

Safety Requirement	Acceptable Probability of Failure	Calculated Probability of Failure	Analysis Result
SafetyReq01	1e-7	9.09999957347e-08	✓

VERDICT Open Source on GitHub





https://github.com/ge-high-assurance/VERDICT

VERDICT Publications

- "Architectural and Behavior Analysis for Cyber Security", *Digital Avionics Systems Conference (DASC)*, September 2019.
- "A Model Based Framework for Analyzing the Security of System Architectures", *Reliability and Maintainability Symposium (RAMS)*, January 2020.
- "DARPA Project Producing Tool to Help Anticipate Military and Industrial Systems' Cyber Threats", *NextGov.com*, April 2020.
- "Threat Identification and Defense Control Selection", accepted by *SAE International Journal of Transportation Cybersecurity and Privacy*, June 2020.
- "Towards Developing Formalized Assurance Case", accepted by *Digital Avionics Systems Conference (DASC)*, October 2020.
- "Expat: Expectation-based Policy Analysis and Enforcement for Appified Smart-Home Platforms", accepted at ACM SACMAT 2019.
- "PatrIoT: Policy-assisted Resilient Programmable IoT system", accepted at Runtime Verification (RV), 2020.