



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

*AADL/ACVIP User Days 2021*

Michael Durling – GE Research – [durling@ge.com](mailto: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



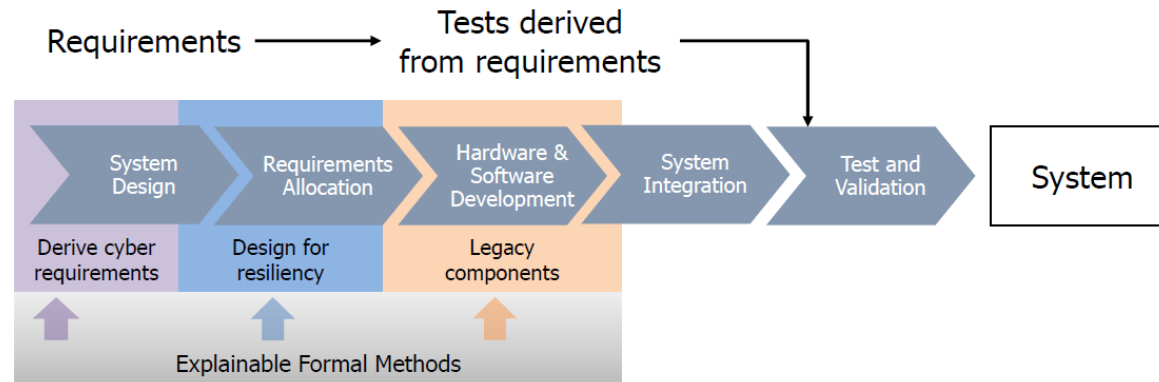
- DARPA CASE Program
- What is the VERDICT Tool?
- Working example
- Tool availability
- Publications
- Questions



# Cyber Assured Systems Engineering (CASE)



## **DARPA** System engineering with cyber resiliency

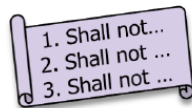


### Explicit system properties

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



- **Cyber resiliency**



- 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:**

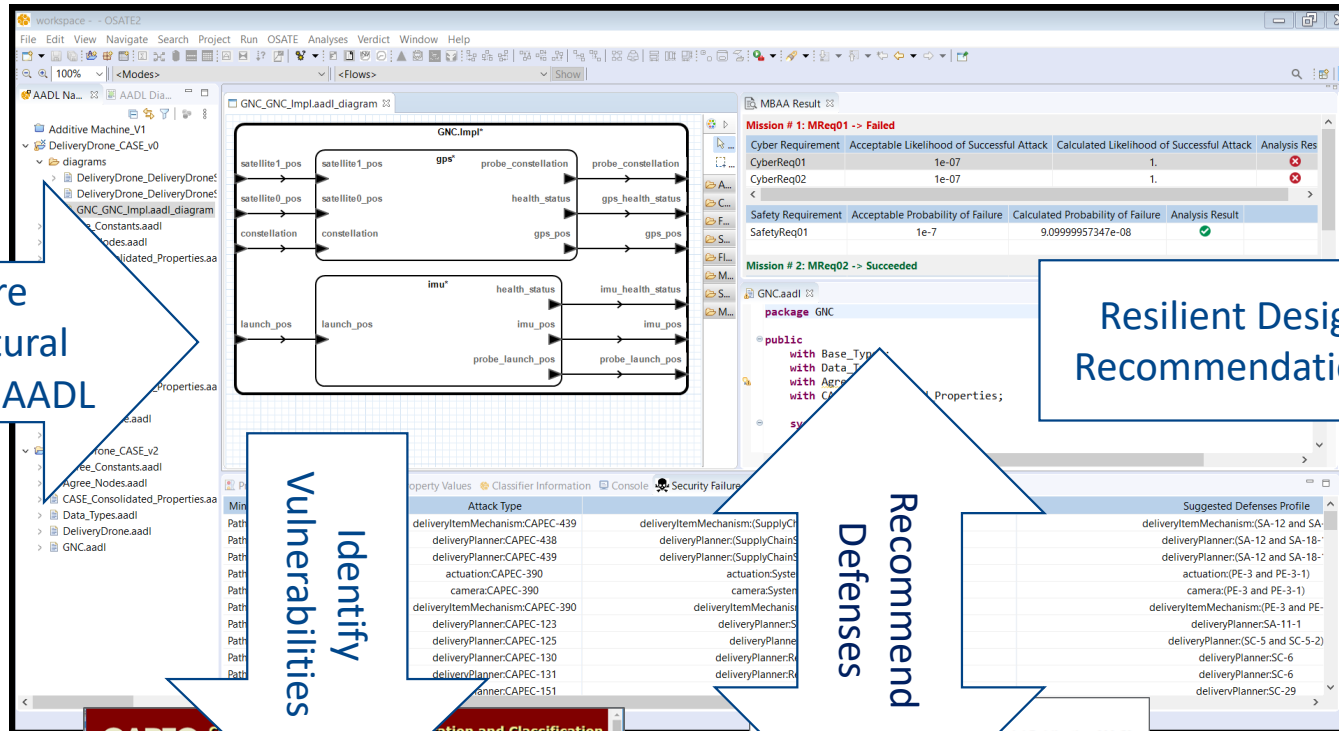
Develop *advanced design and analysis tools* that establish *cyber resiliency as an explicit property* for complex cyber physical systems.



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



## VERDICT Cyber Resilience Design Tool



Capture architectural models in AADL

Resilient Design Recommendations

Identify Vulnerabilities

Recommend Defenses

Security and Privacy Controls for Information Systems and Organizations



Security Requirements & Policies



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

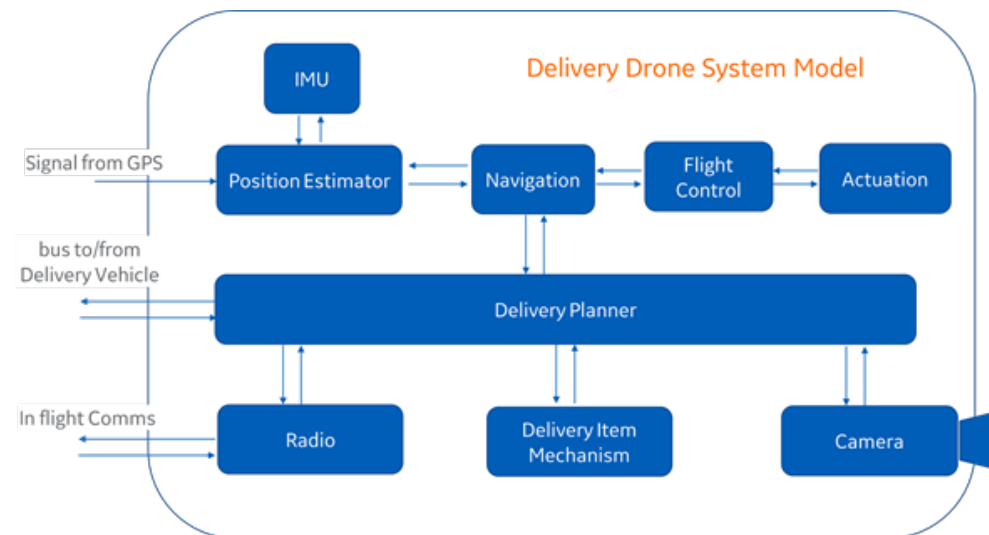
- ✓ Automated (Real-time feedback to designers on potential attacks, control suggestions, behavioral weaknesses)
- ✓ Integrated (Safety and Security analyses in the same tool)
- ✓ Built-in (Utilizes wealth of data available in models instead of collecting data from various sources)
- ✓ Mission-Centric (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



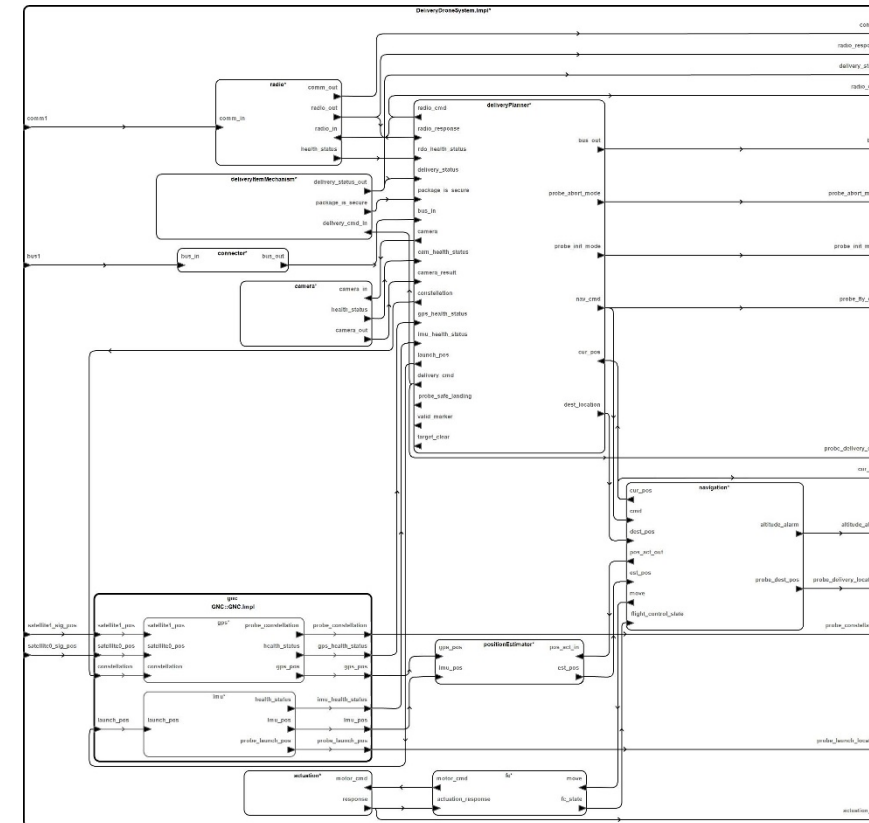
Define architectural components

Generate diagram

```

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;
  
```



# 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



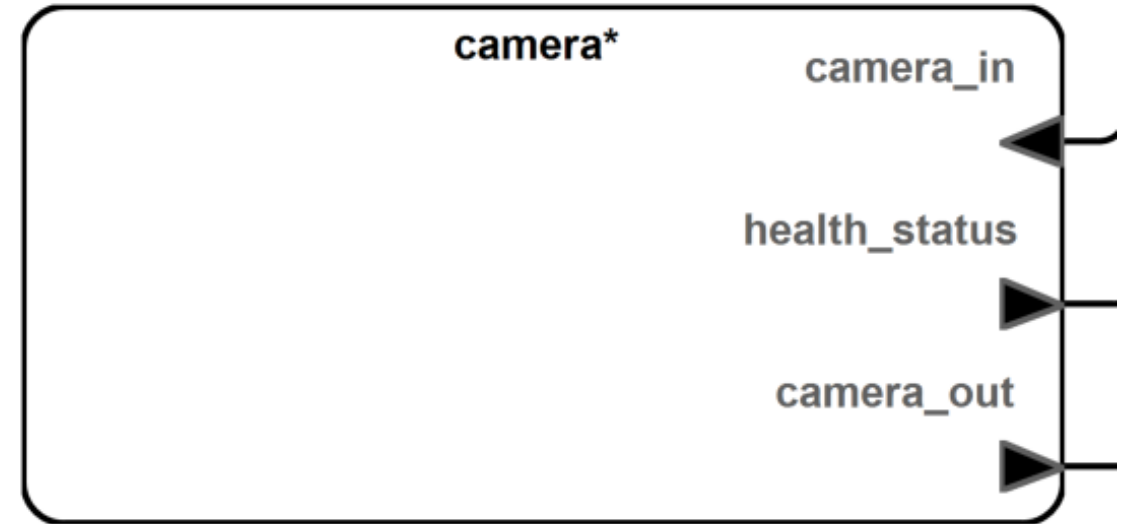


# Set Cyber and Safety Relations



```
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



```
workspace - DeliveryDrone/DeliveryDrone.aadl - OSATE2
File Edit Navigate Search Project Run Verdict Window Help
Model Based Architecture Synthesis (MBAS) > Run Model Based Architecture Analysis (MBAA)
Cyber Resilience Verifier (CRV) > Cyber Requirements/Relations Editor Run MBAA

package DeliveryDrone
public
  with Base_Types;
  with Data_Types;
  with Agree_Constants;
  with Agree_Nodes;
  with Agree_Constants;
  with CASE_Consolidated_Properties;
  with GNC;

  system PositionEstimator
    features
      -- inputs
      gps_pos: in data port Data_Types::Position.impl;
      imu_pos: in data port Data_Types::Position.impl;
      pos_act_in: in data port Data_Types::Position.impl;

      -- outputs
      est_pos: out data port Data_Types::Position.impl;

    annex agree {**
      -- high-level specification
      guarantee "Output: est_pos": Agree_Nodes::close_locations(est_pos, gps_pos); -- within 10 meters
    **};

    annex verdict {**
      --CyberRel "pos_out_I" = imu_pos:I or gps_pos:I or pos_act_in:I => est_pos:I;
      CyberRel "pos_out_I" = gps_pos:I => est_pos:I; -- Cyber relation modified to be a sound abstraction of the behavioral model
      CyberRel "pos_out_A" = imu_pos:A or gps_pos:A or pos_act_in:A => est_pos:A; -- not changed because Availability not analyzed by CRV
      Event {
        id = "loa_event"
      }
    **};
end package
```



# 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 - CAPEC-176: Configurati...

capec.mitre.org/data/definitions/176.htm

**CAPEC** Common Attack Pattern Enumeration and Classification  
A Community Resource for Identifying and Understanding Attacks

Home > CAPEC List > CAPEC-176: Configuration/Environment Manipulation (Version 3.3) ID Lookup: [ ]

Home | About | CAPEC List | Community | News | Search

## CAPEC-176: Configuration/Environment Manipulation

Attack Pattern ID: 176 Status: Draft  
Abstraction: Meta

Presentation Filter: Basic

### Description

An attacker manipulates files or settings external to a target application which affect the behavior of that application. For example, many applications use external configuration files and libraries - modification of these entities or otherwise affecting the application's ability to use them would constitute a configuration/environment manipulation attack.

### Relationships

The table below shows the other attack patterns and high level categories that are related to this attack pattern. These relationships are defined as ChildOf and ParentOf, and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as CanFollow, PeerOf, and CanAlsoBe are defined to show similar attack patterns that the user may want to explore.

Nature	Type	ID	Name
ParentOf	S	75	<a href="#">Manipulating Writeable Configuration Files</a>
ParentOf	S	203	<a href="#">Manipulate Registry Information</a>
ParentOf	S	271	<a href="#">Schema Poisoning</a>
ParentOf	D	536	<a href="#">Data Injected During Configuration</a>
ParentOf	S	578	<a href="#">Disable Security Software</a>

The table below shows the views that this attack pattern belongs to and top level categories within that view.

View Name	Top Level Categories
<a href="#">Domains of Attack</a>	<a href="#">Software</a> , <a href="#">Hardware</a> , <a href="#">Supply Chain</a>
<a href="#">Mechanisms of Attack</a>	<a href="#">Manipulate System Resources</a>

### Prerequisites

The target application must consult external files or configuration controls to control its execution. All but the very simplest applications meet this requirement.

More information is available — Please select a different filter.

Page Last Updated or Reviewed: September 30, 2019

MITRE Use of the Common Attack Pattern Enumeration and Classification (CAPEC), and the associated references from this website are subject to the [Terms of Use](#). CAPEC is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and managed by the Homeland Security Systems Engineering and Development Institute (HSSEDI) which is operated by The MITRE Corporation (MITRE). Copyright © 2007-2020, The MITRE Corporation. CAPEC and the CAPEC logo are trademarks of The MITRE Corporation.

Site Map | Terms of Use | Privacy Policy | Contact Us | [Twitter](#) | [LinkedIn](#)

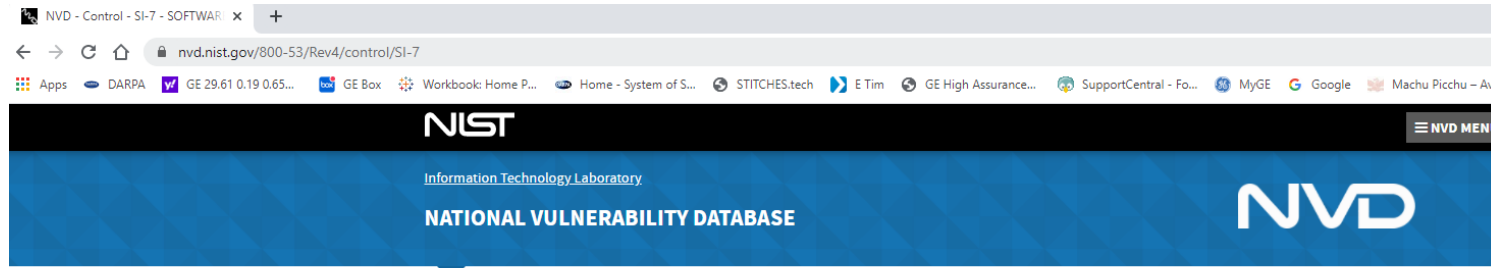
HSSEDI

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





# NIST 800-53 Defense Controls



800-53/800-53A REV4

## NIST Special Publication 800-53 (Rev. 4)

Security and Privacy Controls for Federal Information Systems and Organizations

### SI-7 SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

<b>Family:</b> SI - SYSTEM AND INFORMATION INTEGRITY		
<b>Class:</b>		
<b>Priority:</b> P1 - Implement P1 security controls first.		
<b>Baseline Allocation:</b> Low	Moderate	High
N/A	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)

#### Jump To:

- Revision 4 Statements
- Control Description
- Supplemental Guidance
- References
- All Controls > SI > SI-7

### 800-53 (Rev. 4)

- Security Controls
- Low-Impact
- Moderate-Impact
- High-Impact
- Other Links
- Families
- Search

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

### Control Description

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

### Supplemental Guidance

Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications.

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

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



ge-high-assurance / VERDICT

Unwatch 6 | Unstar 1 | Fork 0

Code | Issues 0 | Pull requests 0 | Actions | Projects 0 | Wiki | Security | Insights | Settings

No description, website, or topics provided.

Manage topics

380 commits | 6 branches | 0 packages | 7 releases | 9 contributors | BSD-3-Clause

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

Commit	Message	Time
Siu kit: modified event probabilities and MissionReq's to tell a nice sto...	Latest commit 77c53c4	21 hours ago
docs/images	Finish moving images to VERDICT.wiki	2 months ago
models	kit: modified event probabilities and MissionReq's to tell a nice sto...	21 hours ago
tools	Fix a bug for the table view for MBAA	8 days ago
.gitignore	Reimplement verdict-stem-runner using more SADL jars	4 months ago
LICENSE	Update LICENSE	3 days ago
README.md	Update README.md	3 days ago

VERDICT Modeling Style Guide & User Manual: V1 to support VERDICT VM 19.1 Tool Assessment #3

Michael Durling edited this page on Dec 14, 2019 · 141 revisions

DARPA: Cyber Assured Systems Engineering (CASE)

VERDICT Project

Style Guide & User Manual V1

Contract # N6600118C4006

General Electric Research

December 11, 2019

Prepared by

Pages 3

- Home
- VERDICT Modeling Style Guide & User Manual: V0 to support VERDICT VM19.0 PI Meeting
- VERDICT Modeling Style Guide & User Manual: V1 to support VERDICT VM 19.1 Tool Assessment #3

<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.
- “PatIoT: Policy-assisted Resilient Programmable IoT system”, accepted at Runtime Verification (RV), 2020.



