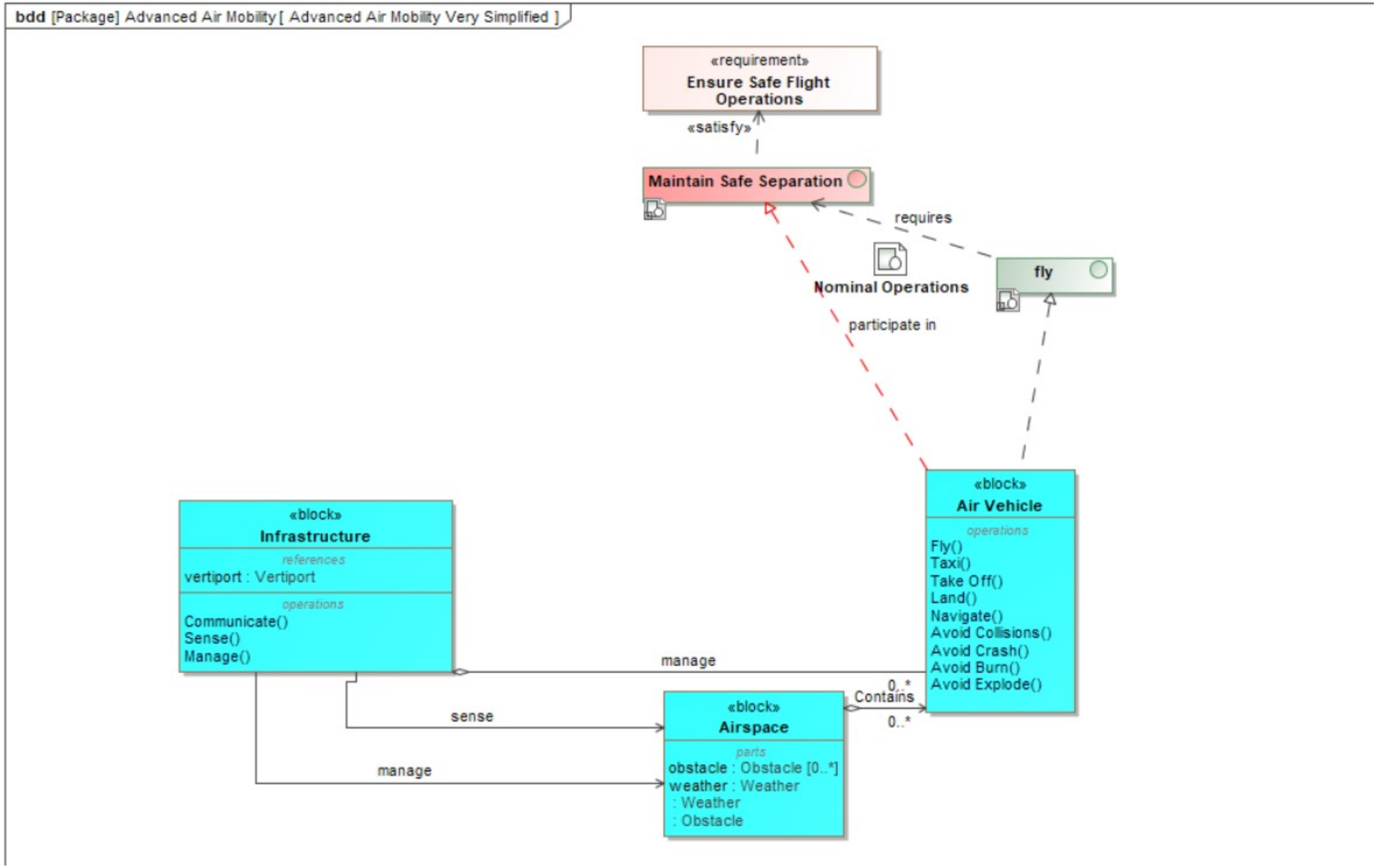
NASA CYBERSECURITY
AERONAUTICS RESEARCH MISSION

# Secure Architecture with Model Based Security Systems Engineering

Brian T. Nolan, Ph.D.

# Let’s start simply—Fly Safely



bdd [Package] Advanced Air Mobility [ Advanced Air Mobility Very Simplified ]

«requirement»
Ensure Safe Flight Operations

«satisfy»

Maintain Safe Separation

requires

Nominal Operations

fly

participate in

«block»
Infrastructure
references
vertiport : Vertiport
operations
Communicate()
Sense()
Manage()

«block»
Air Vehicle
operations
Fly()
Taxi()
Take Off()
Land()
Navigate()
Avoid Collisions()
Avoid Crash()
Avoid Burn()
Avoid Explode()

manage

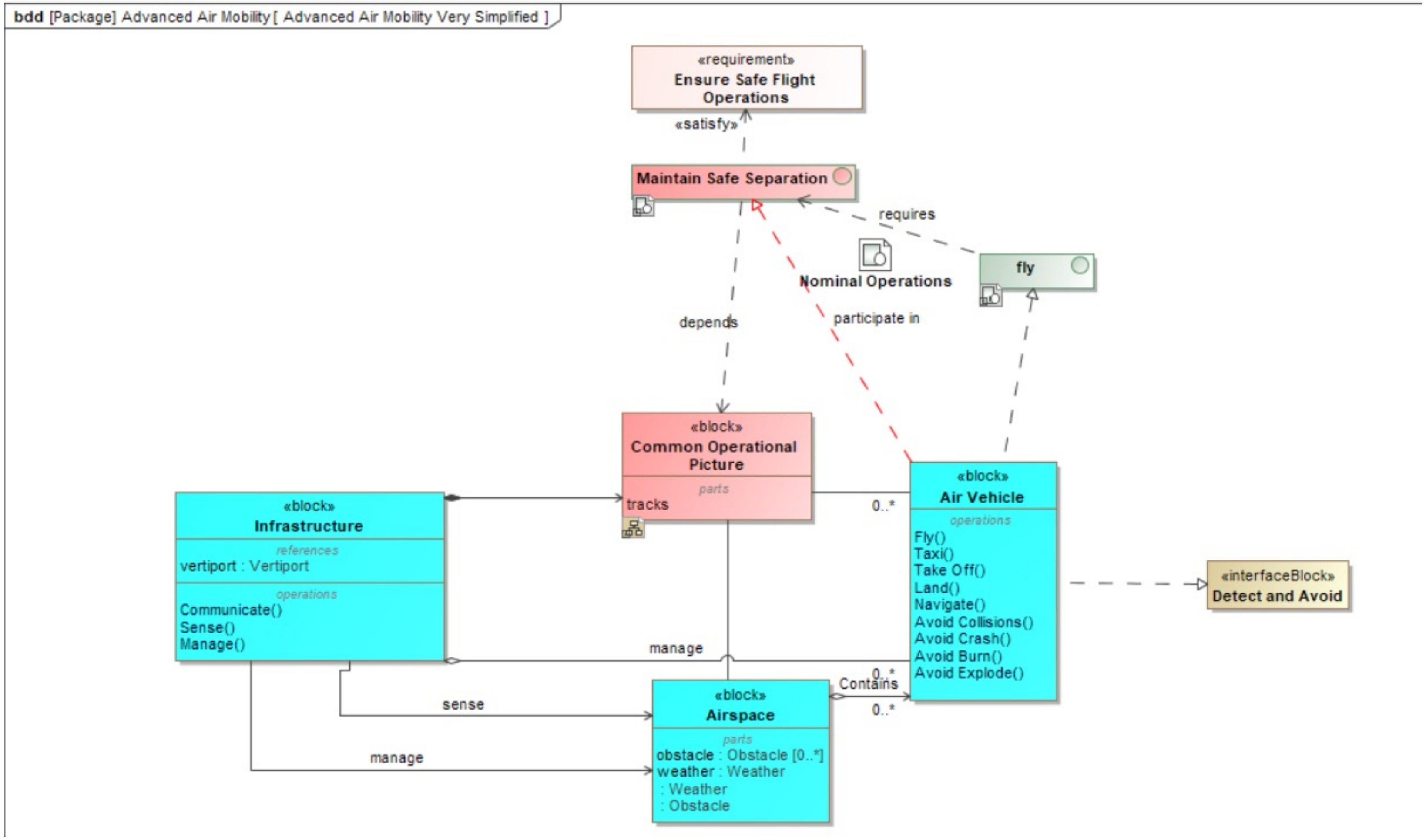
0..*
Contains
0..*

sense

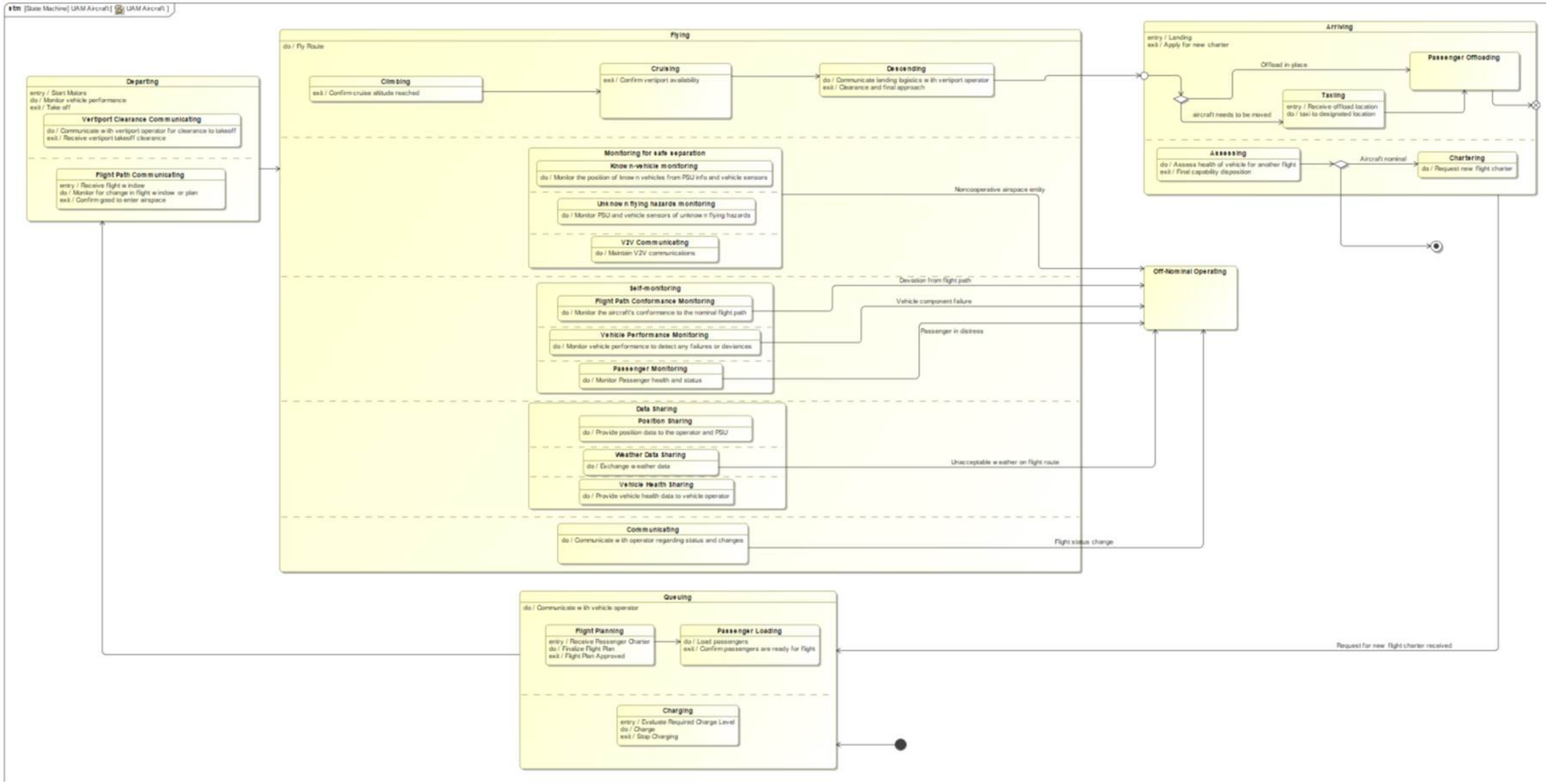
manage

«block»
Airspace
parts
obstacle : Obstacle [0..*]
weather : Weather
: Weather
: Obstacle

# One Goal, One Constraint: Fly safely



# States/Process of Flying



stm [State Machine] UAM Aircraft [ UAM Aircraft ]

**Departing**
entry / Start Motors
do / Monitor vehicle performance
exit / Take off

**Vertiport Clearance Communicating**
do / Communicate with vertiport operator for clearance to takeoff
exit / Receive vertiport takeoff clearance

**Flight Path Communicating**
entry / Receive flight window
do / Monitor for change in flight window or plan
exit / Confirm good to enter airspace

**Flying**
do / Fly Route

**Climbing**
exit / Confirm cruise altitude reached

**Cruising**
exit / Confirm vertiport availability

**Descending**
do / Communicate landing logistics with vertiport operator
exit / Clearance and final approach

**Monitoring for safe separation**

**Known-vehicle monitoring**
do / Monitor the position of known vehicles from PSU info and vehicle sensors

**Unknown flying hazards monitoring**
do / Monitor PSU and vehicle sensors of unknown flying hazards

**V2V Communicating**
do / Maintain V2V communications

**Self-monitoring**

**Flight Path Conformance Monitoring**
do / Monitor the aircraft's conformance to the nominal flight path

**Vehicle Performance Monitoring**
do / Monitor vehicle performance to detect any failures or deviances

**Passenger Monitoring**
do / Monitor Passenger health and status

**Data Sharing**

**Position Sharing**
do / Provide position data to the operator and PSU

**Weather Data Sharing**
do / Exchange weather data

**Vehicle Health Sharing**
do / Provide vehicle health data to vehicle operator

**Communicating**
do / Communicate with operator regarding status and changes

**Arriving**
entry / Landing
exit / Apply for new charter

Offload in-place

aircraft needs to be moved

**Passenger Offloading**

**Taxiing**
entry / Receive offload location
do / taxi to designated location

**Assessing**
do / Assess health of vehicle for another flight
exit / Final capability disposition

Aircraft nominal

**Chartering**
do / Request new flight charter

**Off-Nominal Operating**

Noncooperative airspace entity

Deviation from flight path

Vehicle component failure

Passenger in distress

Unacceptable weather on flight route

Flight status change

**Queuing**
do / Communicate with vehicle operator

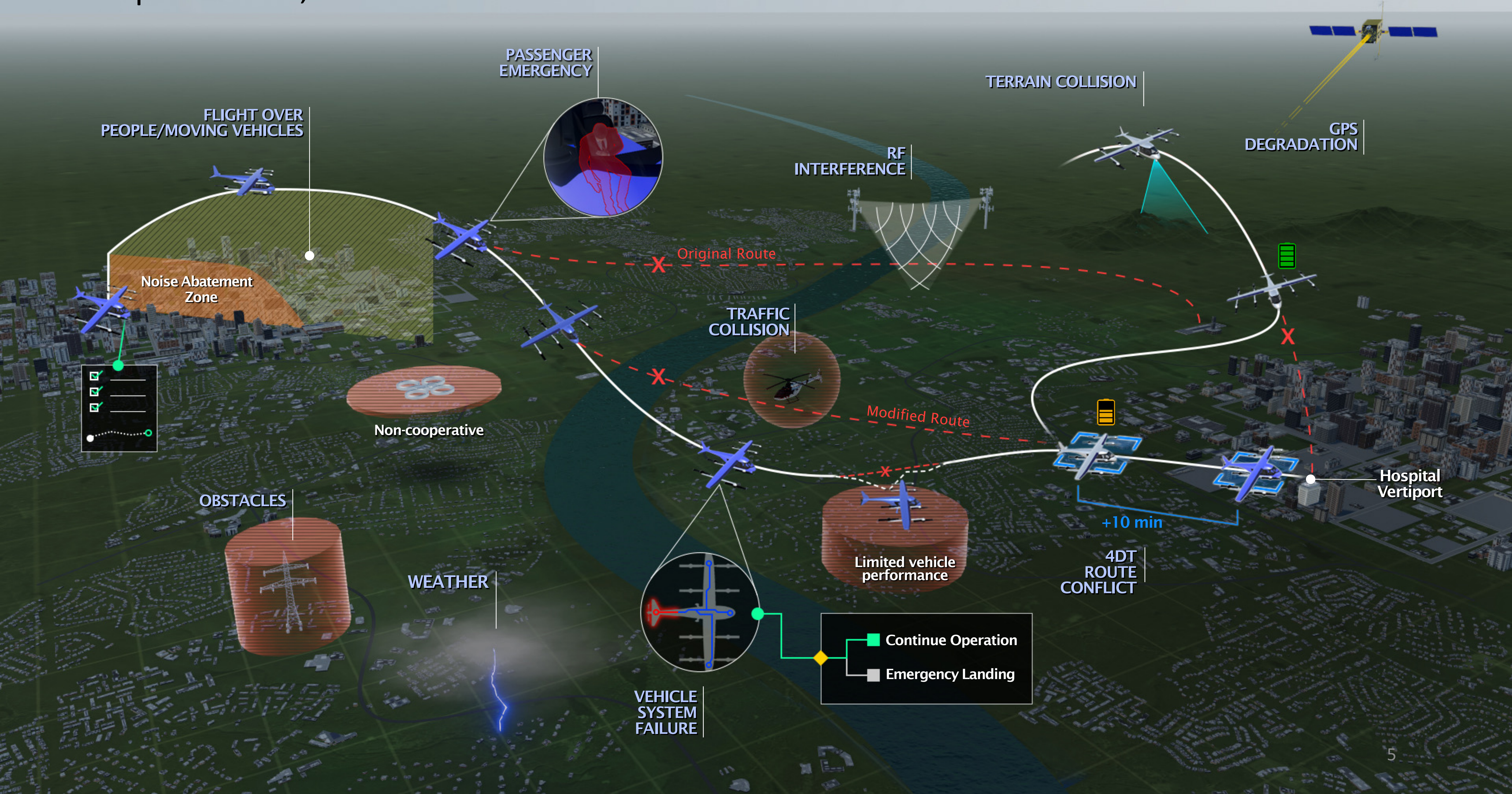
**Flight Planning**
entry / Receive Passenger Charter
do / Finalize Flight Plan
exit / Flight Plan Approved

**Passenger Loading**
do / Load passengers
exit / Confirm passengers are ready for flight

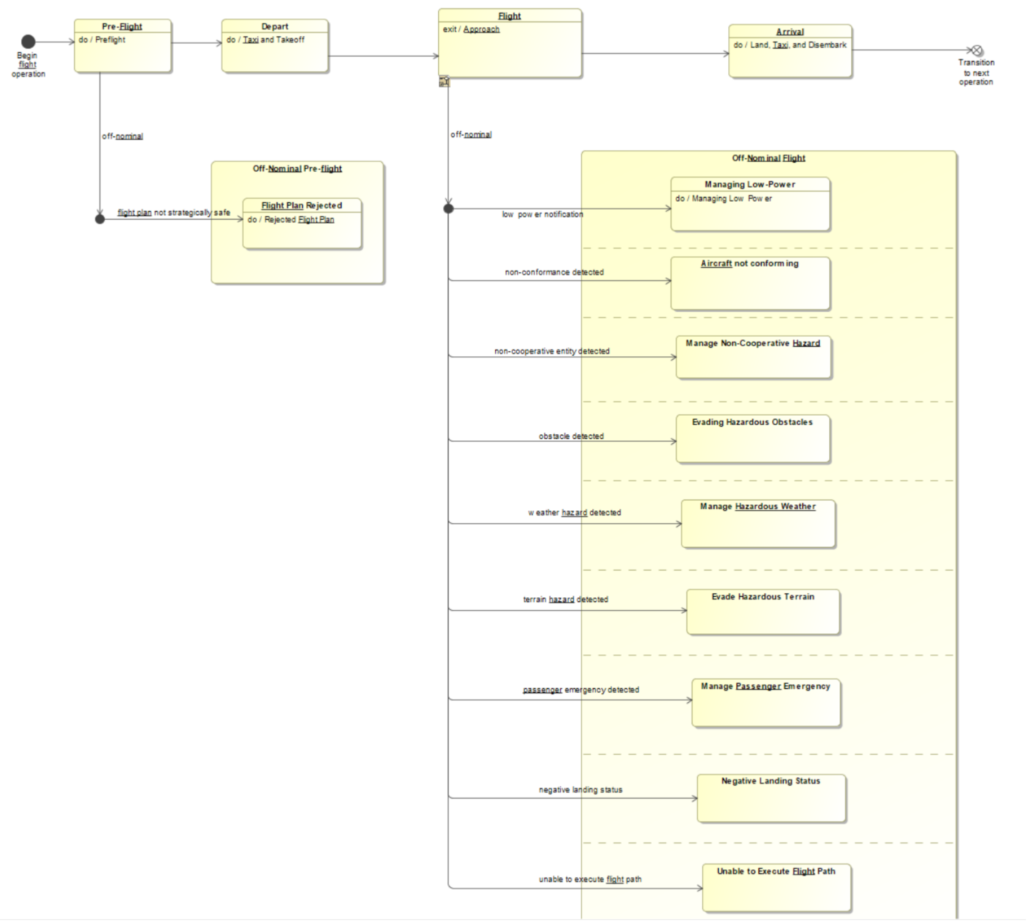
**Charging**
entry / Evaluate Required Charge Level
do / Charge
exit / Stop Charging

Request for new flight charter received

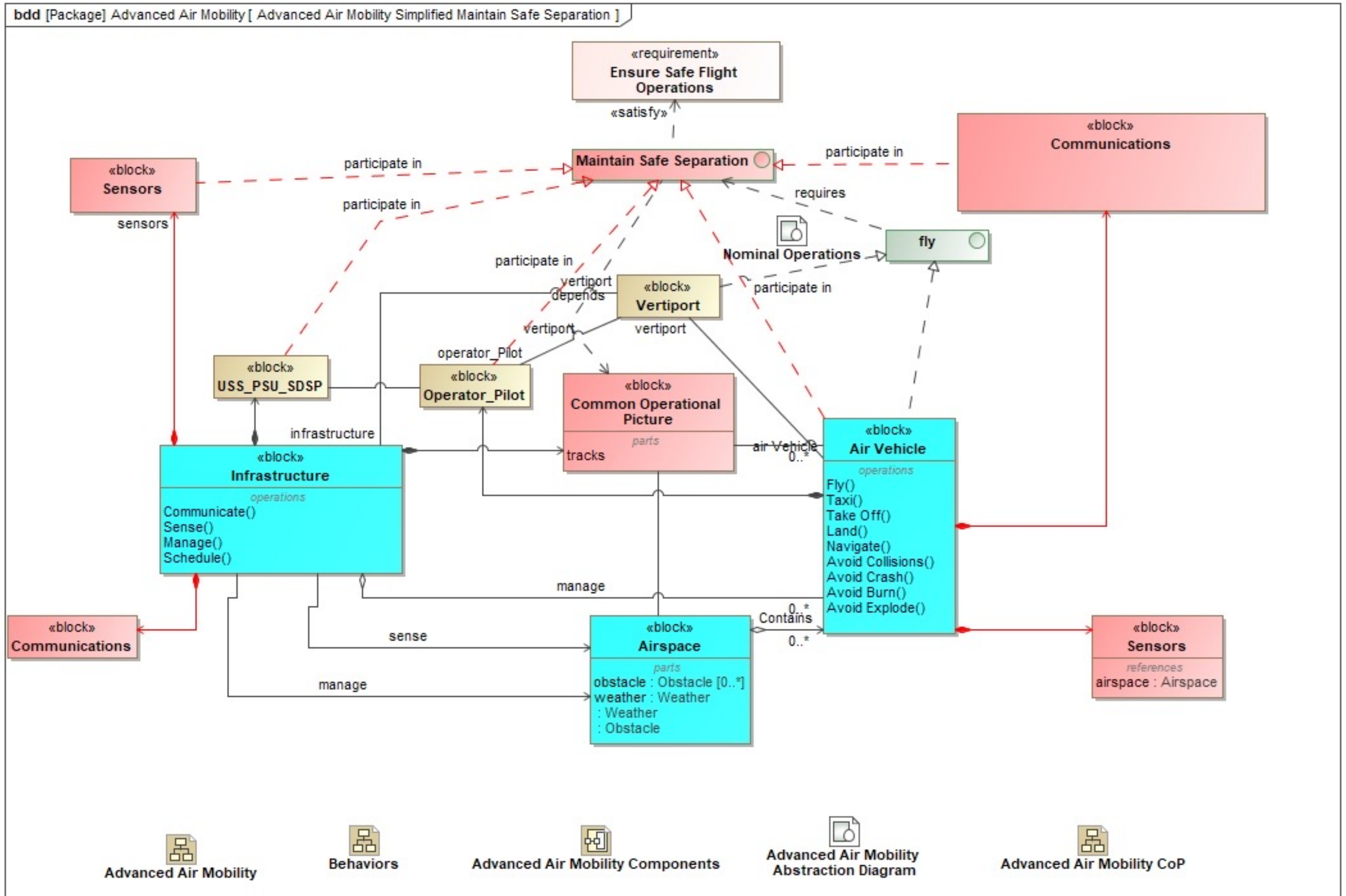
# Complexities, Risks and Constraints



# Off-Nominal States



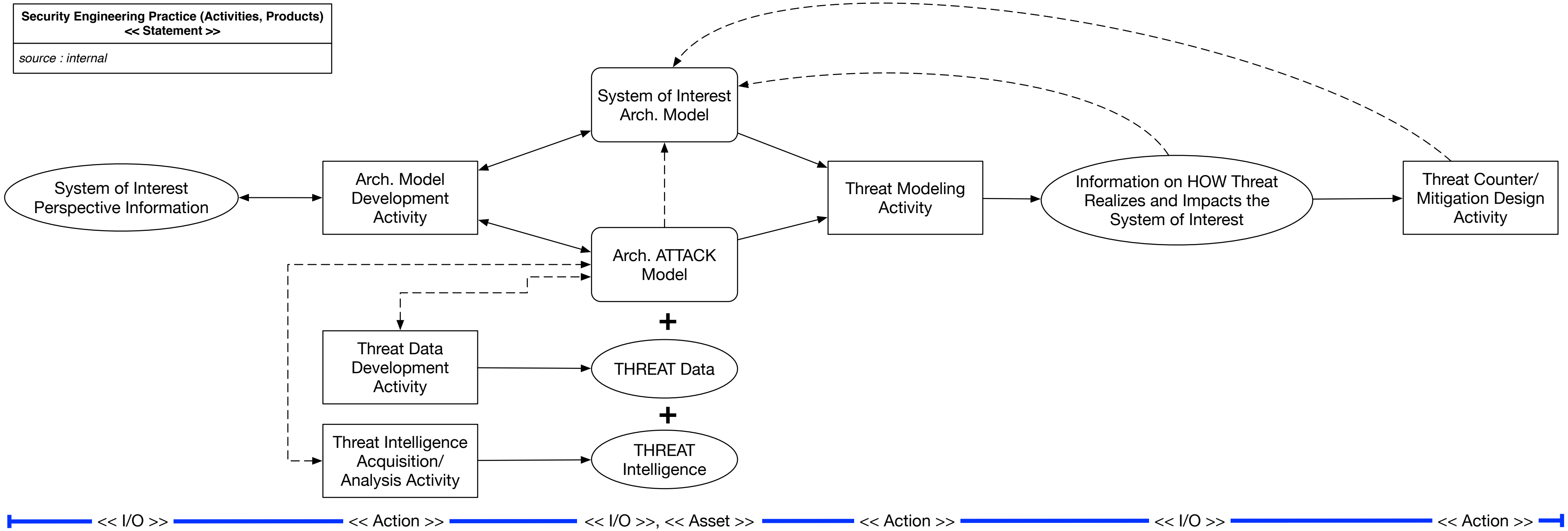
# (Very) Preliminary Analysis: Disruption of Sensors or Communications disrupts Safe Operation



# Our Cybersecurity Engineering Approach

- Cybersecurity Management Plan
- Cybersecurity Model (Cybersecurity MBSE)
- NIST 800-160 v.1-2 ( an extension of ISO/IEC/IEEE 15288)
- STPA-Sec

# System Security Engineering Practice



**Security Engineering Practice (Activities, Products)**
**<< Statement >>**

*source : internal*

System of Interest Perspective Information

Arch. Model Development Activity

System of Interest Arch. Model

Arch. ATTACK Model

+

Threat Data Development Activity

THREAT Data

+

Threat Intelligence Acquisition/ Analysis Activity

THREAT Intelligence

Threat Modeling Activity

Information on HOW Threat Realizes and Impacts the System of Interest

Threat Counter/ Mitigation Design Activity

<< I/O >> — << Action >> — << I/O >>, << Asset >> — << Action >> — << I/O >> — << Action >>

1. Information from the System of Interest (SoI) is used as input

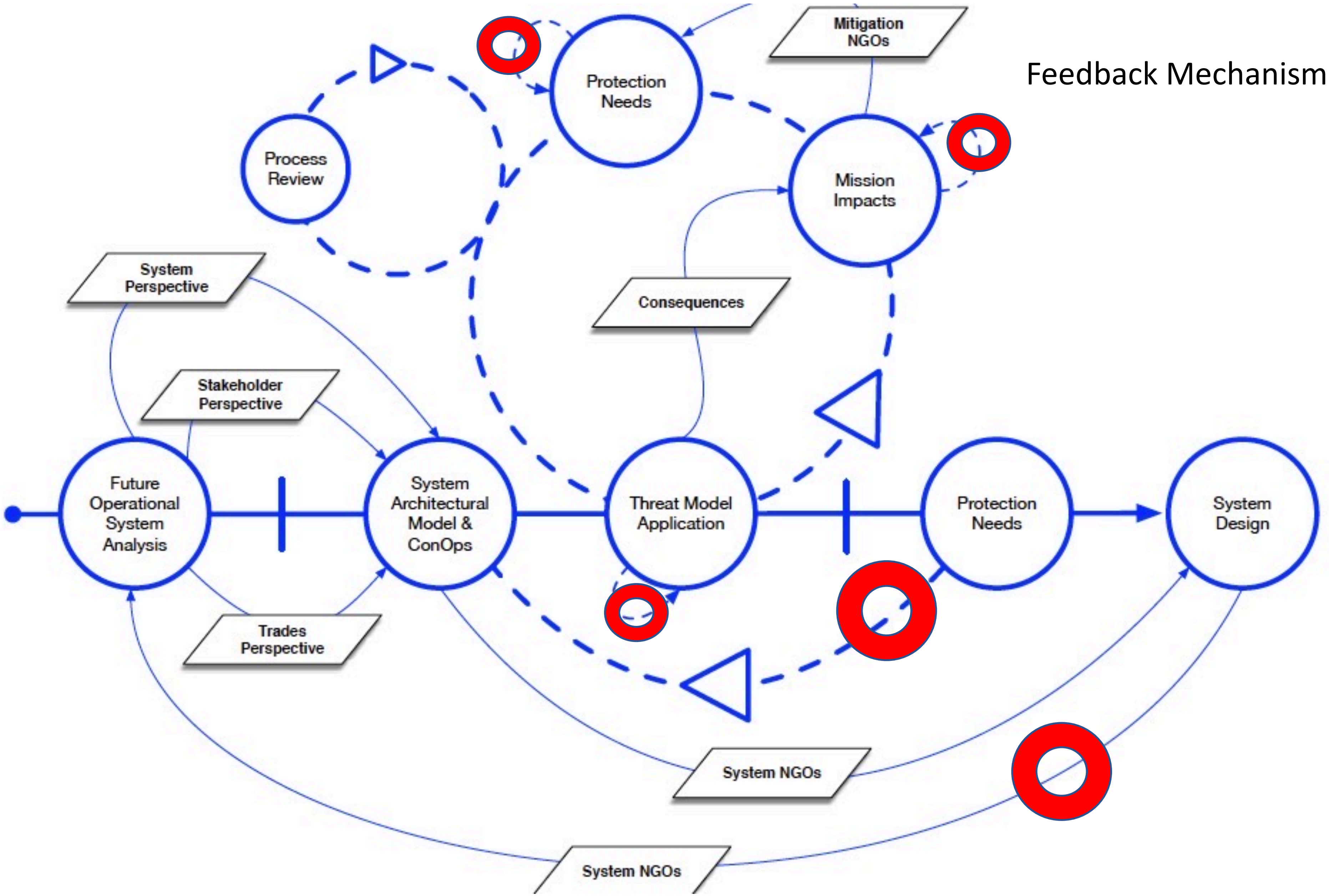
2. Into a Model Development Activity to develop a SoI Architectural Model along with a suitable Attack Model and Threat Data which are then used as inputs

3. Into a Threat Modeling Activity aka an Analysis of the interactions between the SoI Model and the Attack Model (+Threat Data)

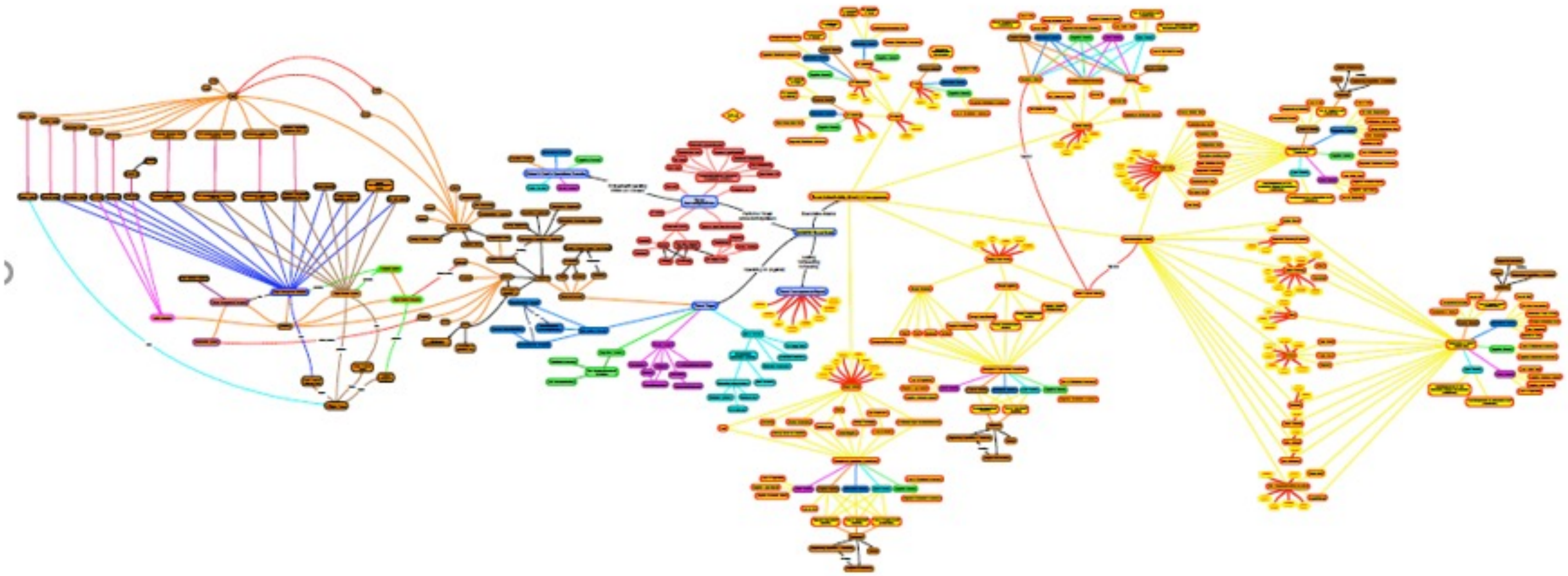
4. To analyze and discover how the SoI will react and respond to any given attack

5. This information is then used to update the SoI design so as to increase its robustness and resilience to said attacks

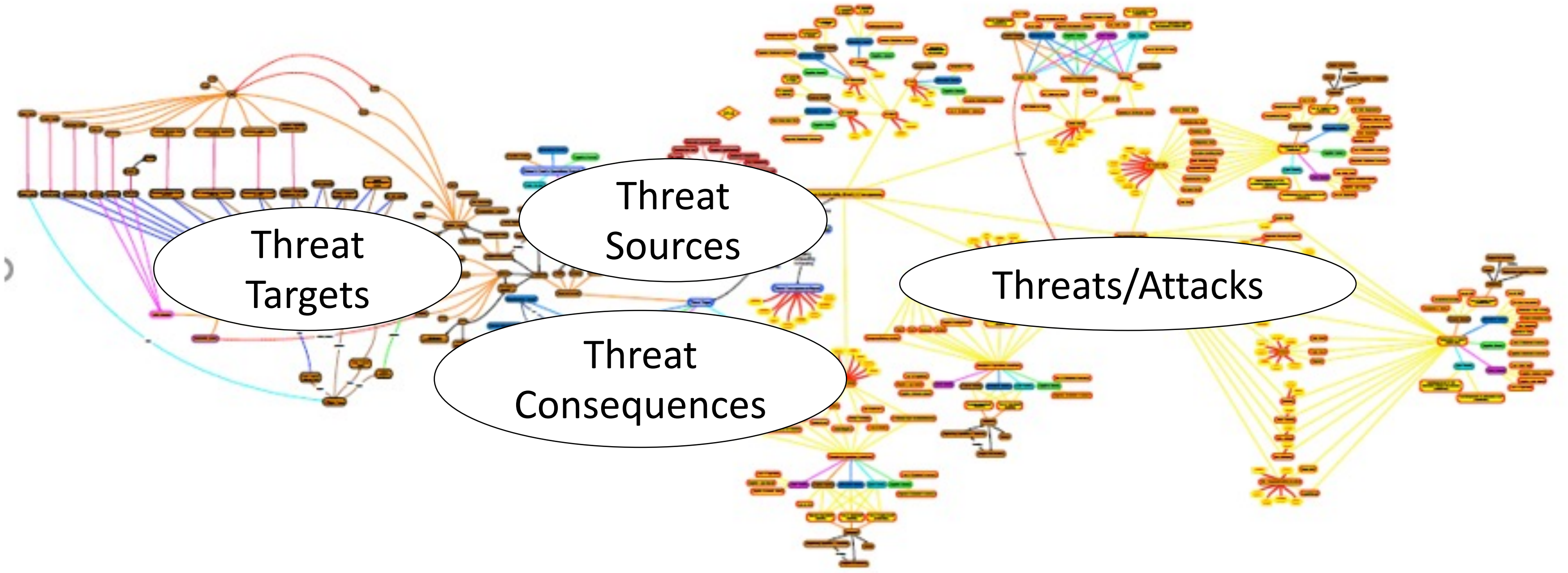
# Feedback Mechanisms



# NAS Threat Model: Attackers, Threats, Assets, Impacts

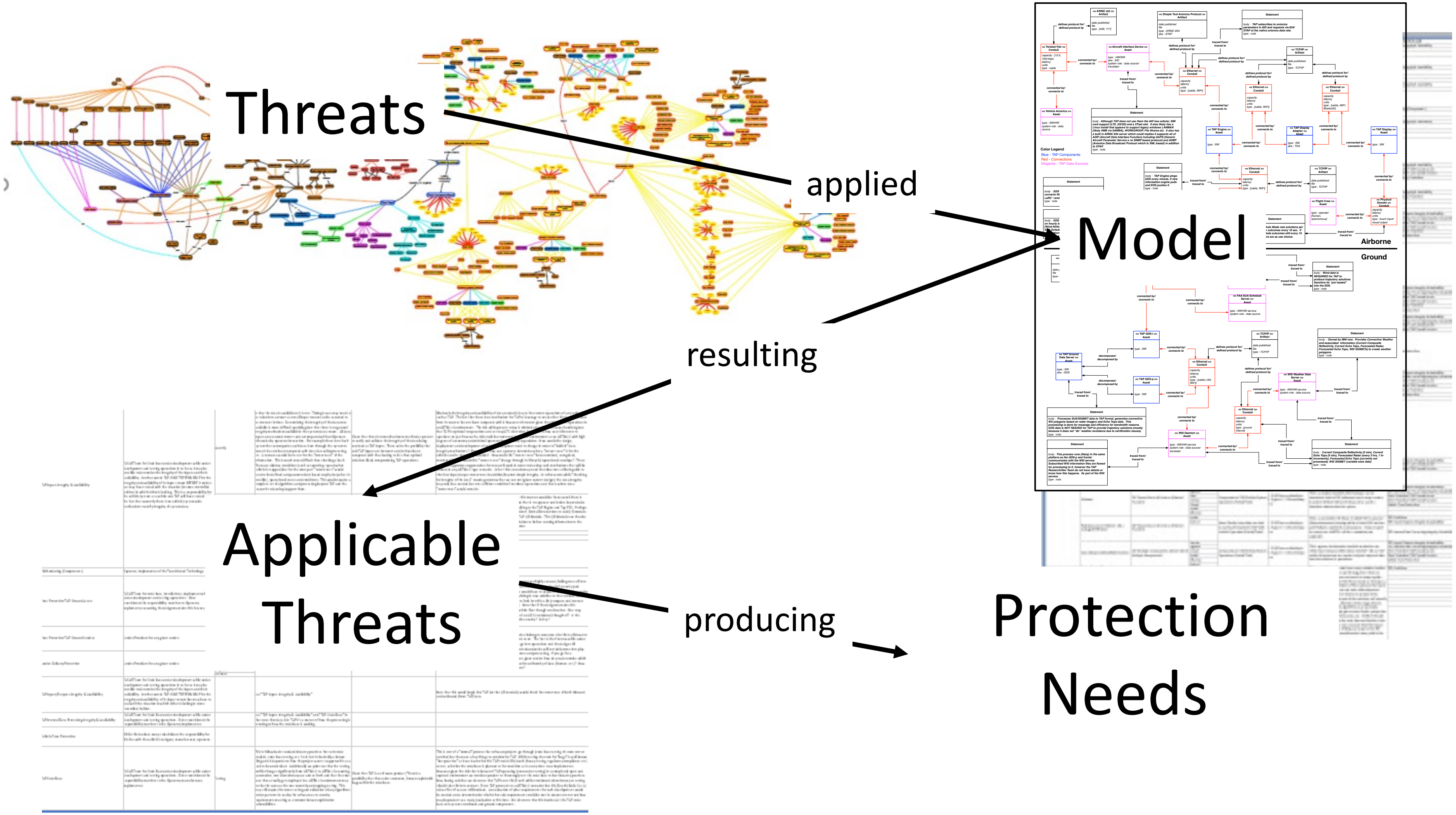


# A Threat Model For The NAS



Threat == {Threat Source} executing an {Attack} on a {Threat Target} resulting in a {Threat Consequence} (i.e. mission impact)

# Threat Model Application Analysis



Threats applied

Model

resulting

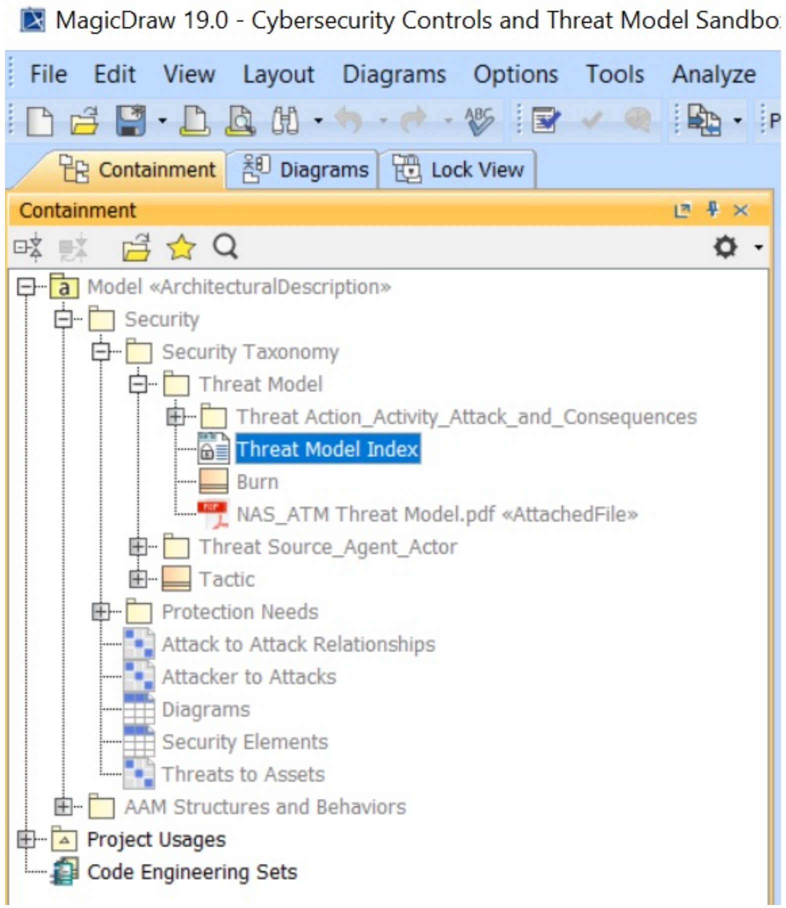
Applicable Threats

producing

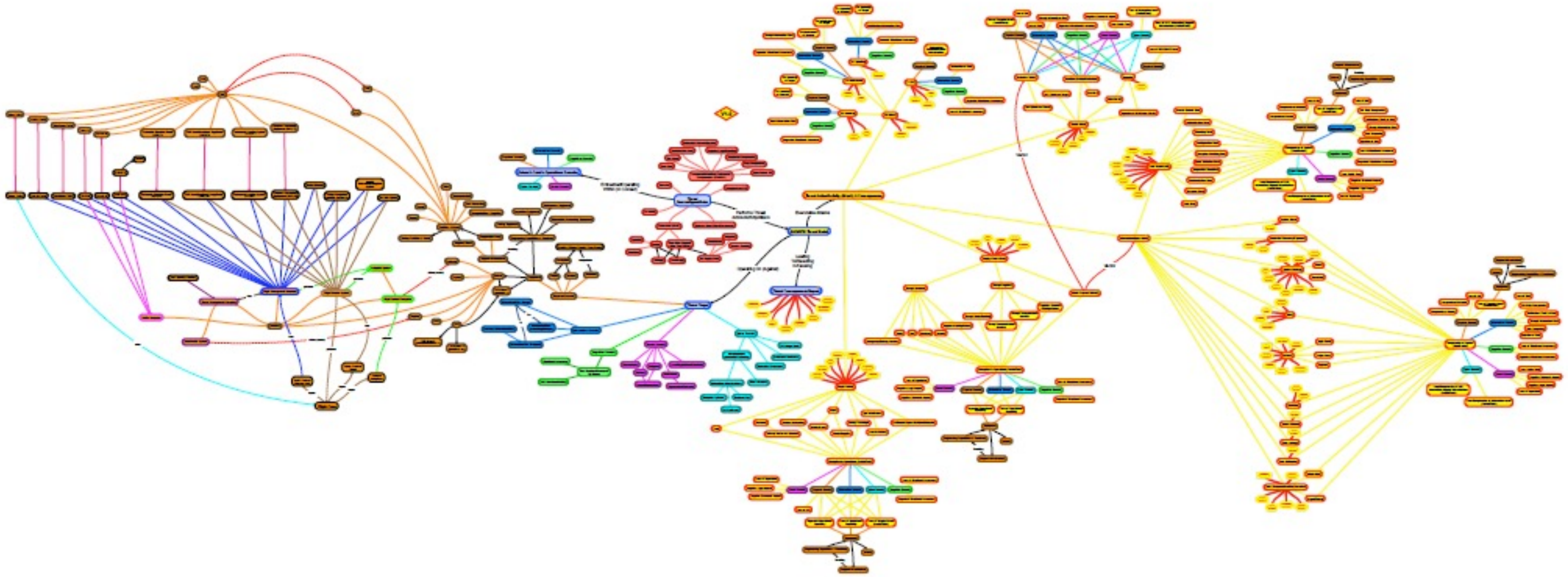
Protection Needs

# Cybersecurity model overview

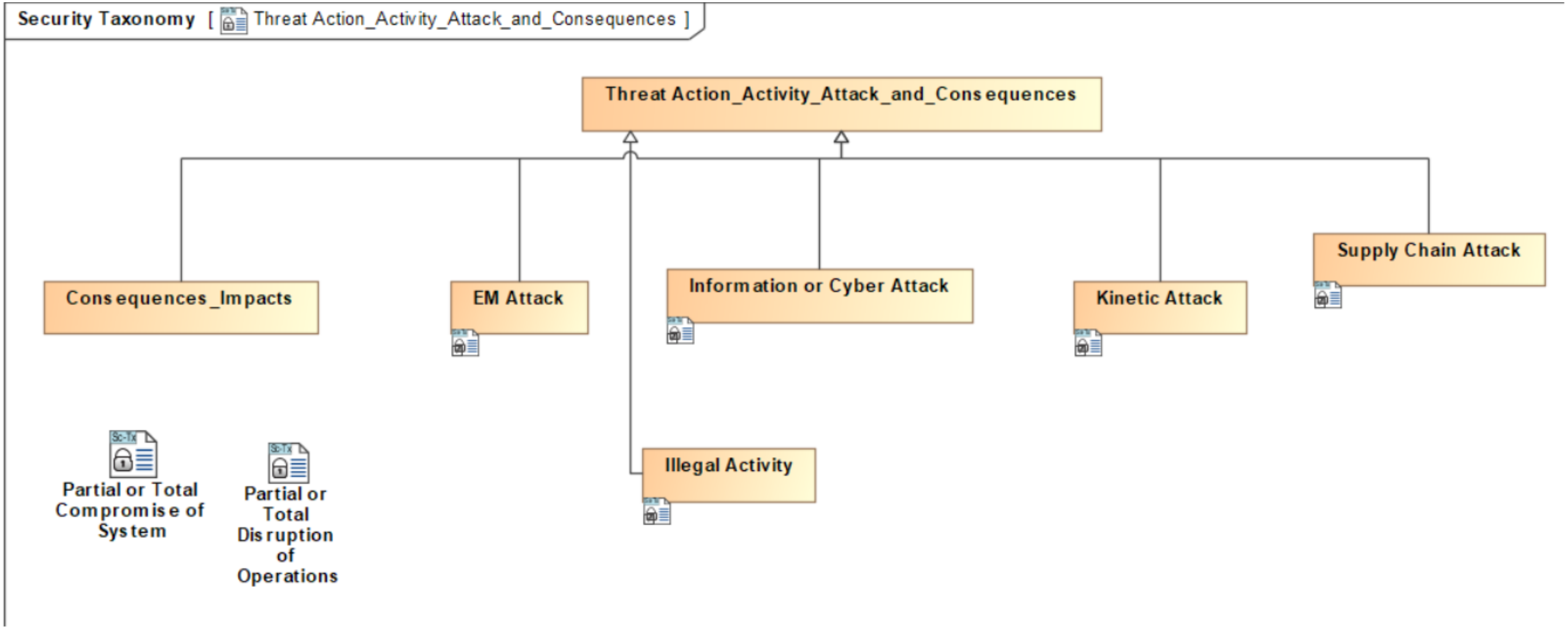
# Browser Outline


MagicDraw 19.0 - Cybersecurity Controls and Threat Model Sandbo
File
Edit
View
Layout
Diagrams
Options
Tools
Analyze
Containment
Diagrams
Lock View
Containment
Model «ArchitecturalDescription»
Security
Security Taxonomy
Threat Model
Threat Action_Activity_Attack_and_Consequences
Threat Model Index
Burn
NAS_ATM Threat Model.pdf «AttachedFile»
Threat Source_Agent_Actor
Tactic
Protection Needs
Attack to Attack Relationships
Attacker to Attacks
Diagrams
Security Elements
Threats to Assets
AAM Structures and Behaviors
Project Usages
Code Engineering Sets

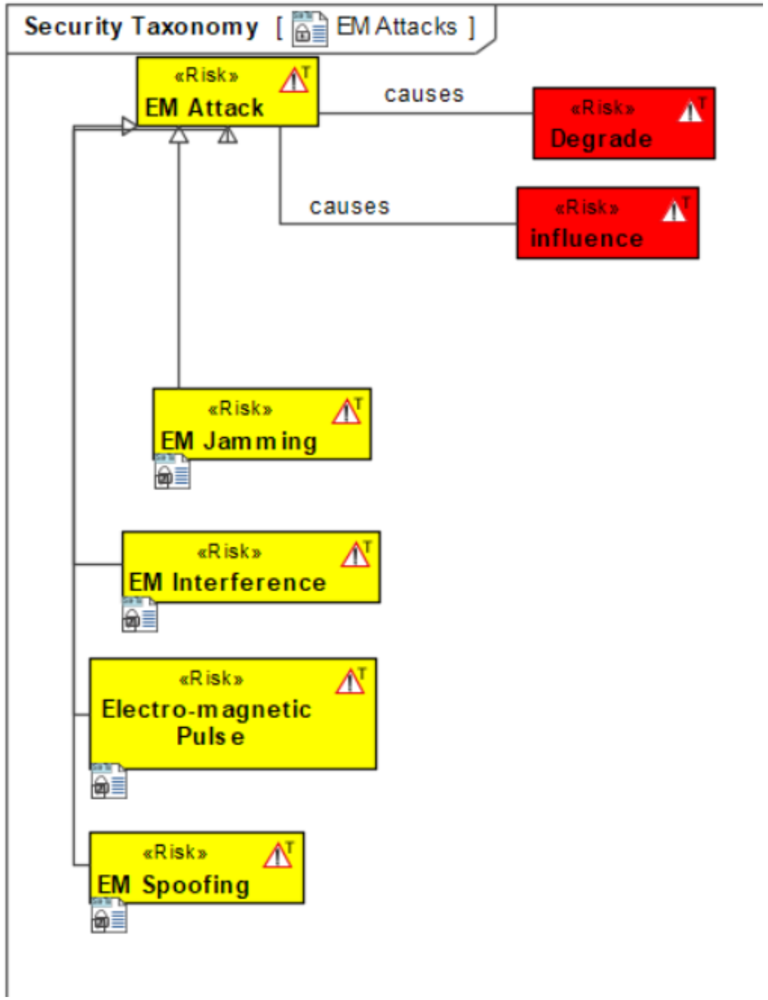
# NAS Threat Model



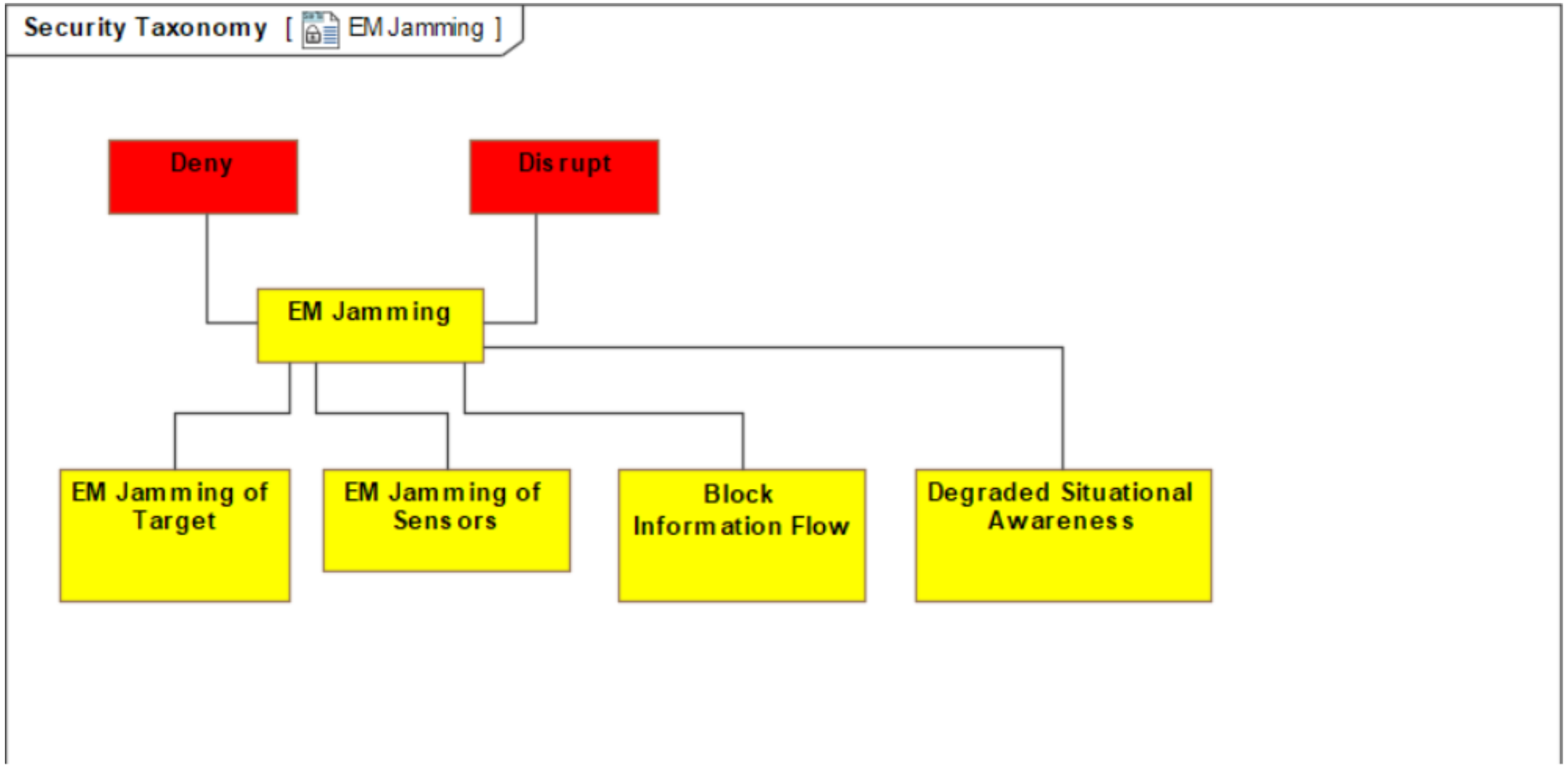
# Threat Tree


Security Taxonomy [ Threat Action_Activity_Attack_and_Consequences ]
Threat Action_Activity_Attack_and_Consequences
Consequences_Impacts
EM Attack
Information or Cyber Attack
Kinetic Attack
Supply Chain Attack
Illegal Activity
Partial or Total Compromise of System
Partial or Total Disruption of Operations

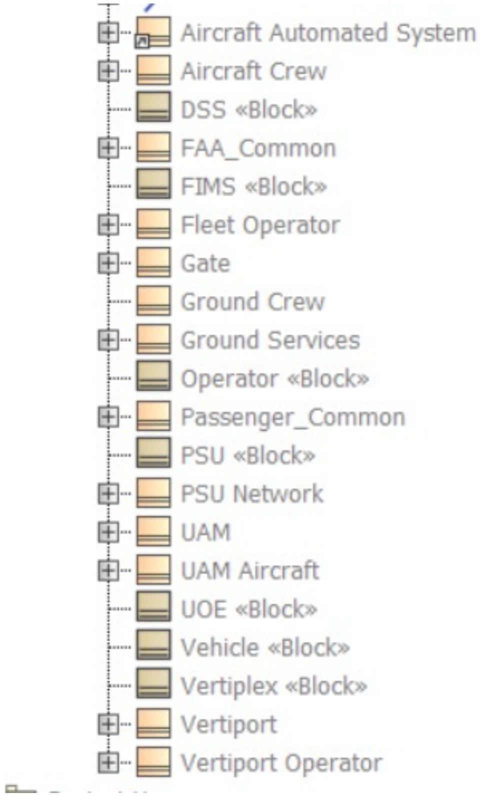
# EM Attack


Security Taxonomy [ EM Attacks ]
«Risk»
EM Attack
causes
«Risk»
Degrade
causes
«Risk»
influence
«Risk»
EM Jamming
«Risk»
EM Interference
«Risk»
Electro-magnetic Pulse
«Risk»
EM Spoofing

# EM Jamming

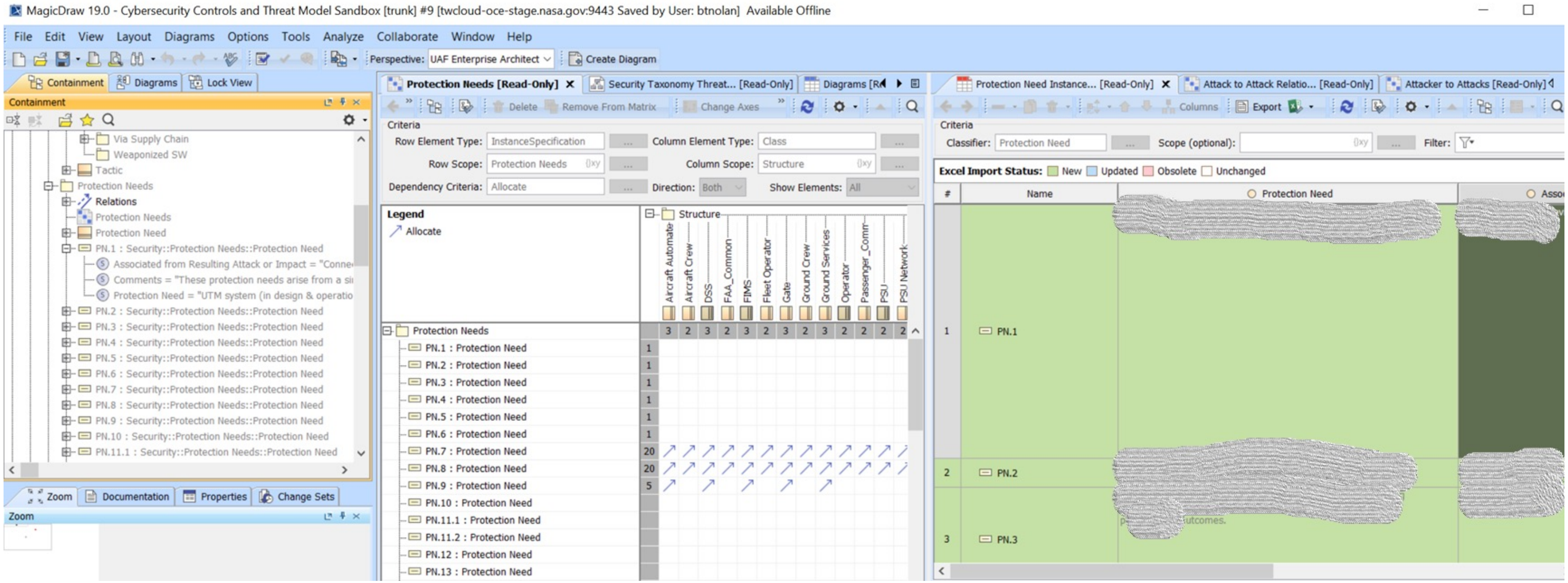

Security Taxonomy [ EM Jamming ]
Deny
Disrupt
EM Jamming
EM Jamming of Target
EM Jamming of Sensors
Block Information Flow
Degraded Situational Awareness

# For now, simple asset list for AAM



Aircraft Automated System
Aircraft Crew
DSS «Block»
FAA_Common
FIMS «Block»
Fleet Operator
Gate
Ground Crew
Ground Services
Operator «Block»
Passenger_Common
PSU «Block»
PSU Network
UAM
UAM Aircraft
UOE «Block»
Vehicle «Block»
Vertiplex «Block»
Vertiport
Vertiport Operator

# Protection Needs: Browser, Matrix, Table


MagicDraw 19.0 - Cybersecurity Controls and Threat Model Sandbox [trunk] #9 [twcloud-oce-stage.nasa.gov:9443 Saved by User: btnolan]  Available Offline
File
Edit
View
Layout
Diagrams
Options
Tools
Analyze
Collaborate
Window
Help
Create Diagram
Containment
Diagrams
Lock View
Protection Needs [Read-Only]
Security Taxonomy Threat... [Read-Only]
Diagrams [R
Protection Need Instance... [Read-Only]
Attack to Attack Relatio... [Read-Only]
Attacker to Attacks [Read-Only]
Delete
Remove From Matrix
Change Axes
Columns
Export
Zoom
Documentation
Properties
Change Sets

Perspective: UAF Enterprise Architect

Containment

- Via Supply Chain
- Weaponized SW
- Tactic
- Protection Needs
  - Relations
  - Protection Needs
  - Protection Need
  - PN.1 : Security::Protection Needs::Protection Need
    - Associated from Resulting Attack or Impact = "Conne
    - Comments = "These protection needs arise from a si
    - Protection Need = "UTM system (in design & operatio
  - PN.2 : Security::Protection Needs::Protection Need
  - PN.3 : Security::Protection Needs::Protection Need
  - PN.4 : Security::Protection Needs::Protection Need
  - PN.5 : Security::Protection Needs::Protection Need
  - PN.6 : Security::Protection Needs::Protection Need
  - PN.7 : Security::Protection Needs::Protection Need
  - PN.8 : Security::Protection Needs::Protection Need
  - PN.9 : Security::Protection Needs::Protection Need
  - PN.10 : Security::Protection Needs::Protection Need
  - PN.11.1 : Security::Protection Needs::Protection Need

Criteria

Row Element Type: InstanceSpecification
Column Element Type: Class
Row Scope: Protection Needs
Column Scope: Structure
Dependency Criteria: Allocate
Direction: Both
Show Elements: All

Legend
↗ Allocate

| Structure | | Aircraft Automate | Aircraft Crew | DSS | FAA_Common | FIMS | Fleet Operator | Gate | Ground Crew | Ground Services | Operator | Passenger_Comm | PSU | PSU Network |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Protection Needs | | 3 | 2 | 3 | 2 | 3 | 2 | 3 | 2 | 3 | 2 | 2 | 2 | 2 |
| PN.1 : Protection Need | 1 | | | | | | | | | | | | | |
| PN.2 : Protection Need | 1 | | | | | | | | | | | | | |
| PN.3 : Protection Need | 1 | | | | | | | | | | | | | |
| PN.4 : Protection Need | 1 | | | | | | | | | | | | | |
| PN.5 : Protection Need | 1 | | | | | | | | | | | | | |
| PN.6 : Protection Need | 1 | | | | | | | | | | | | | |
| PN.7 : Protection Need | 20 | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ |
| PN.8 : Protection Need | 20 | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ |
| PN.9 : Protection Need | 5 | ↗ | | ↗ | | ↗ | | ↗ | | ↗ | | | | |
| PN.10 : Protection Need | | | | | | | | | | | | | | |
| PN.11.1 : Protection Need | | | | | | | | | | | | | | |
| PN.11.2 : Protection Need | | | | | | | | | | | | | | |
| PN.12 : Protection Need | | | | | | | | | | | | | | |
| PN.13 : Protection Need | | | | | | | | | | | | | | |

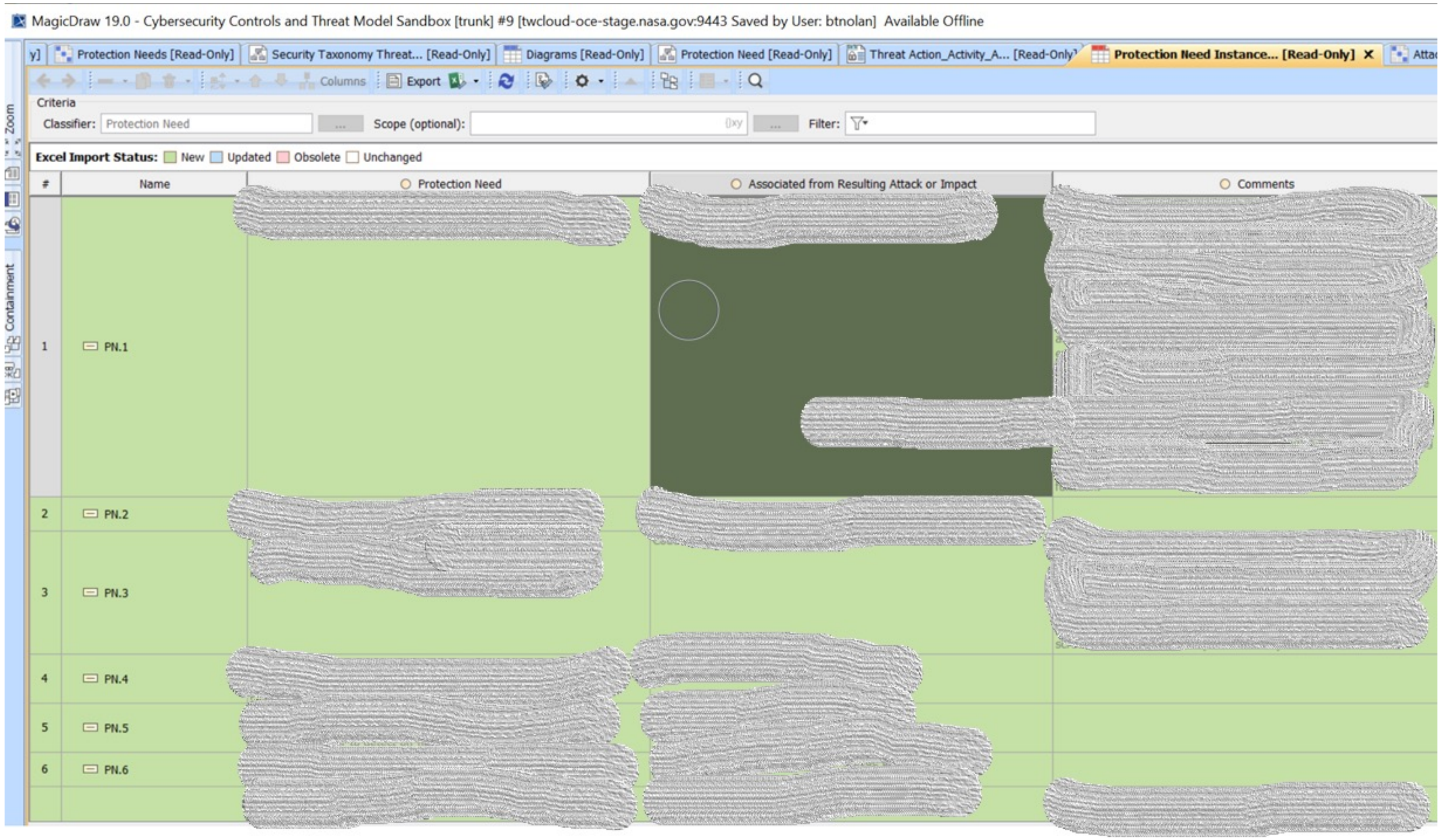
Criteria

Classifier: Protection Need
Scope (optional):
Filter:

Excel Import Status: 🟩 New 🟦 Updated 🟥 Obsolete □ Unchanged

| # | Name | ○ Protection Need | ○ Asso |
|---|---|---|---|
| 1 | PN.1 | [redacted] | [redacted] |
| 2 | PN.2 | [redacted] | [redacted] |
| 3 | PN.3 | [redacted] | [redacted] |

# Protection Needs Table (imported from Excel)



MagicDraw 19.0 - Cybersecurity Controls and Threat Model Sandbox [trunk] #9 [twcloud-oce-stage.nasa.gov:9443 Saved by User: btnolan] Available Offline

y] | Protection Needs [Read-Only] | Security Taxonomy Threat... [Read-Only] | Diagrams [Read-Only] | Protection Need [Read-Only] | Threat Action_Activity_A... [Read-Only] | Protection Need Instance... [Read-Only] ✕ | Attac
Columns
Export
Zoom
Containment

Criteria

Classifier: Protection Need

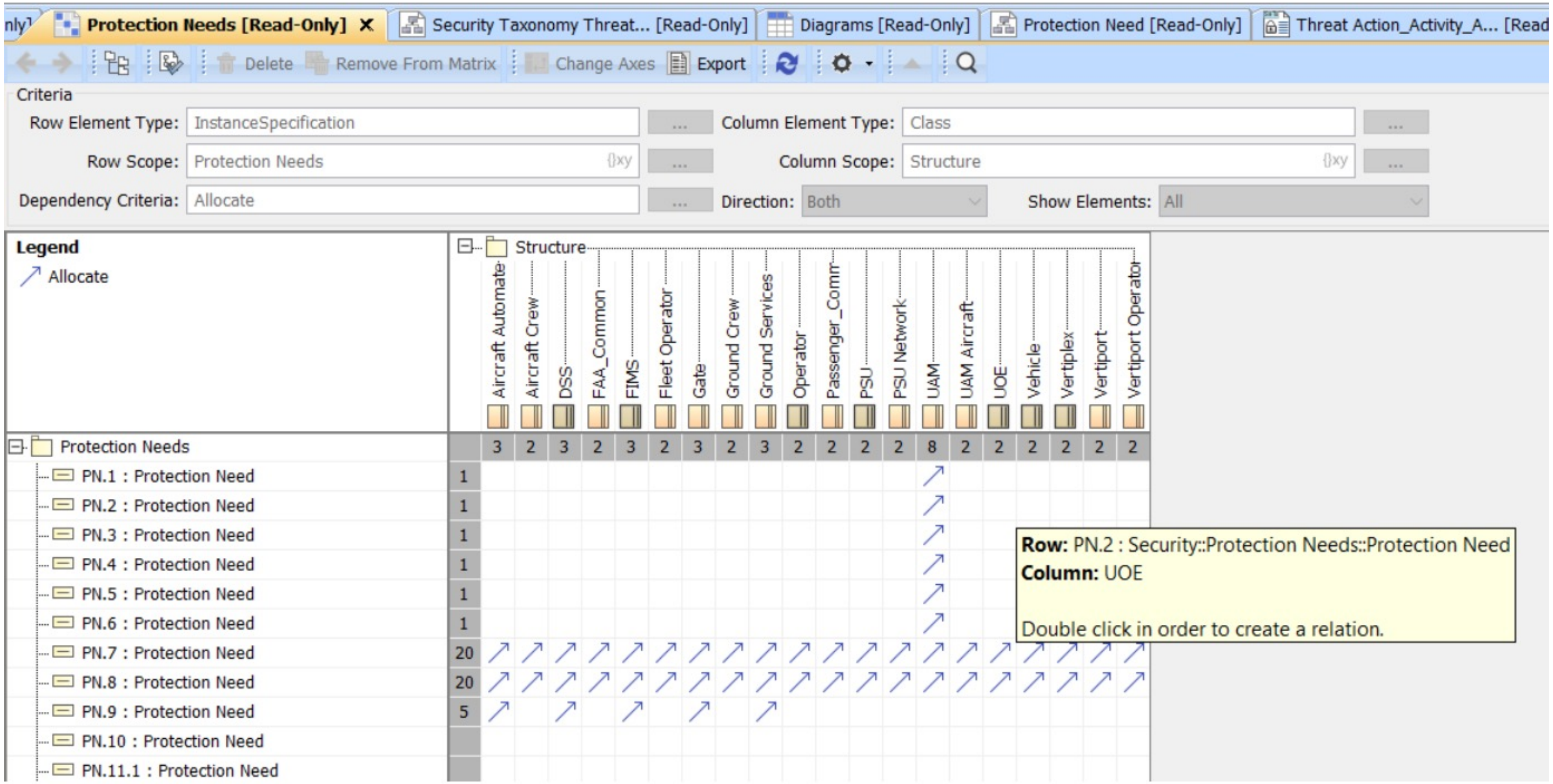
Scope (optional):

Filter:

**Excel Import Status:** 🟩 New 🟦 Updated 🟥 Obsolete □ Unchanged

| # | Name | ○ Protection Need | ○ Associated from Resulting Attack or Impact | ○ Comments |
|---|---|---|---|---|
| 1 | PN.1 | [redacted] | [redacted] | [redacted] |
| 2 | PN.2 | [redacted] | [redacted] | [redacted] |
| 3 | PN.3 | | | |
| 4 | PN.4 | [redacted] | [redacted] | |
| 5 | PN.5 | [redacted] | [redacted] | |
| 6 | PN.6 | [redacted] | [redacted] | [redacted] |

# Matrix: Protection Needs applied to Assets (rough draft/proof of concept)



nly]
Protection Needs [Read-Only] ✕
Security Taxonomy Threat... [Read-Only]
Diagrams [Read-Only]
Protection Need [Read-Only]
Threat Action_Activity_A... [Read
Delete
Remove From Matrix
Change Axes
Export

Criteria

Row Element Type: InstanceSpecification

Column Element Type: Class

Row Scope: Protection Needs

Column Scope: Structure

Dependency Criteria: Allocate

Direction: Both

Show Elements: All

Legend

↗ Allocate

| Structure | | Aircraft Automate | Aircraft Crew | DSS | FAA_Common | FIMS | Fleet Operator | Gate | Ground Crew | Ground Services | Operator | Passenger_Comm | PSU | PSU Network | UAM | UAM Aircraft | UOE | Vehicle | Vertiplex | Vertiport | Vertiport Operator |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Protection Needs | | 3 | 2 | 3 | 2 | 3 | 2 | 3 | 2 | 3 | 2 | 2 | 2 | 2 | 8 | 2 | 2 | 2 | 2 | 2 | 2 |
| PN.1 : Protection Need | 1 | | | | | | | | | | | | | | ↗ | | | | | | |
| PN.2 : Protection Need | 1 | | | | | | | | | | | | | | ↗ | | | | | | |
| PN.3 : Protection Need | 1 | | | | | | | | | | | | | | ↗ | | | | | | |
| PN.4 : Protection Need | 1 | | | | | | | | | | | | | | ↗ | | | | | | |
| PN.5 : Protection Need | 1 | | | | | | | | | | | | | | ↗ | | | | | | |
| PN.6 : Protection Need | 1 | | | | | | | | | | | | | | ↗ | | | | | | |
| PN.7 : Protection Need | 20 | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ |
| PN.8 : Protection Need | 20 | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ | ↗ |
| PN.9 : Protection Need | 5 | ↗ | | ↗ | | ↗ | | ↗ | | ↗ | | | | | | | | | | | |
| PN.10 : Protection Need | | | | | | | | | | | | | | | | | | | | | |
| PN.11.1 : Protection Need | | | | | | | | | | | | | | | | | | | | | |

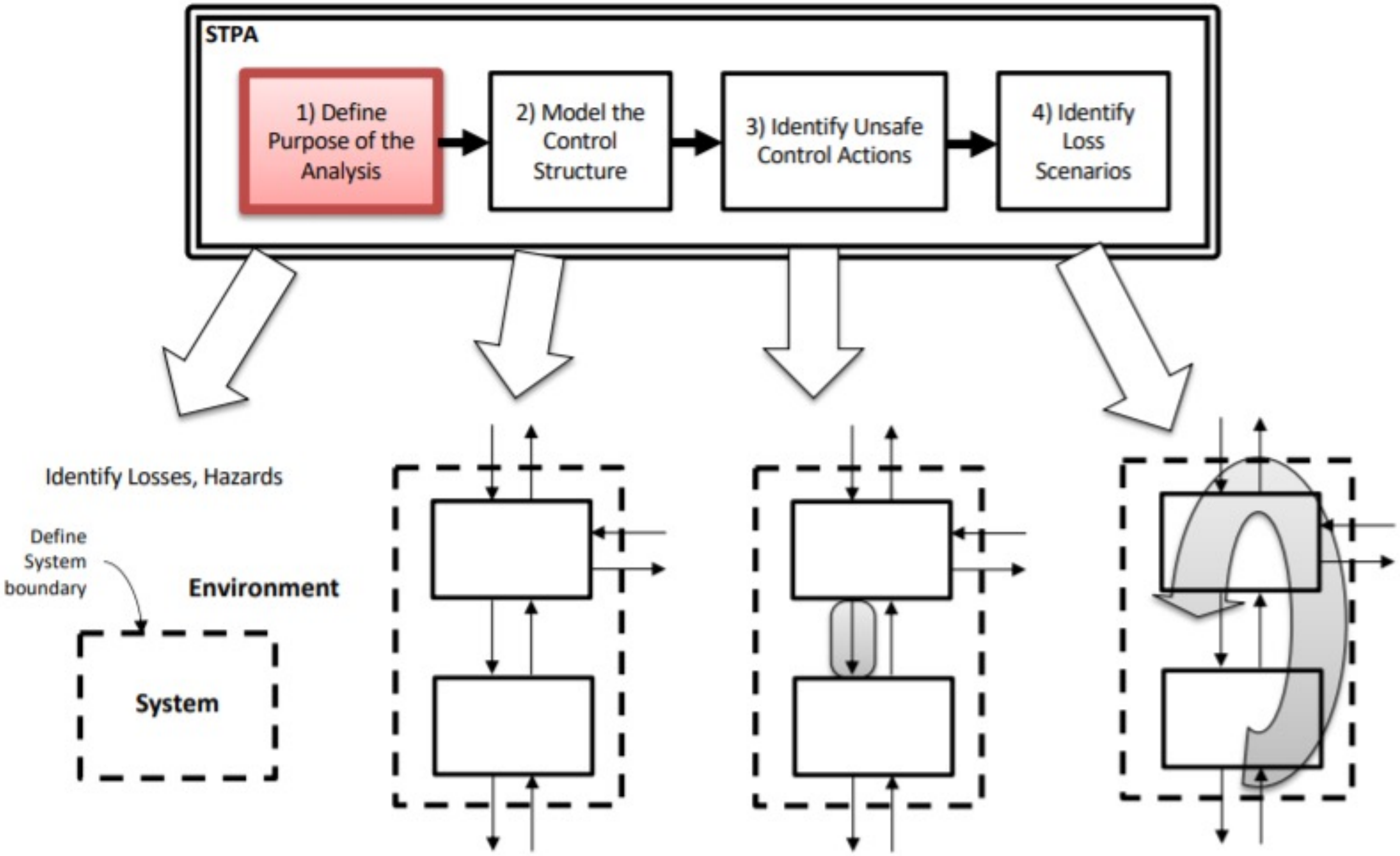
**Row:** PN.2 : Security::Protection Needs::Protection Need
**Column:** UOE

Double click in order to create a relation.

# Additional Material

- STPA-Sec
- NIST 800-53 Controls
- Mitre Att&ck

# STPA-Sec: System Theoretic Process Analysis for Security

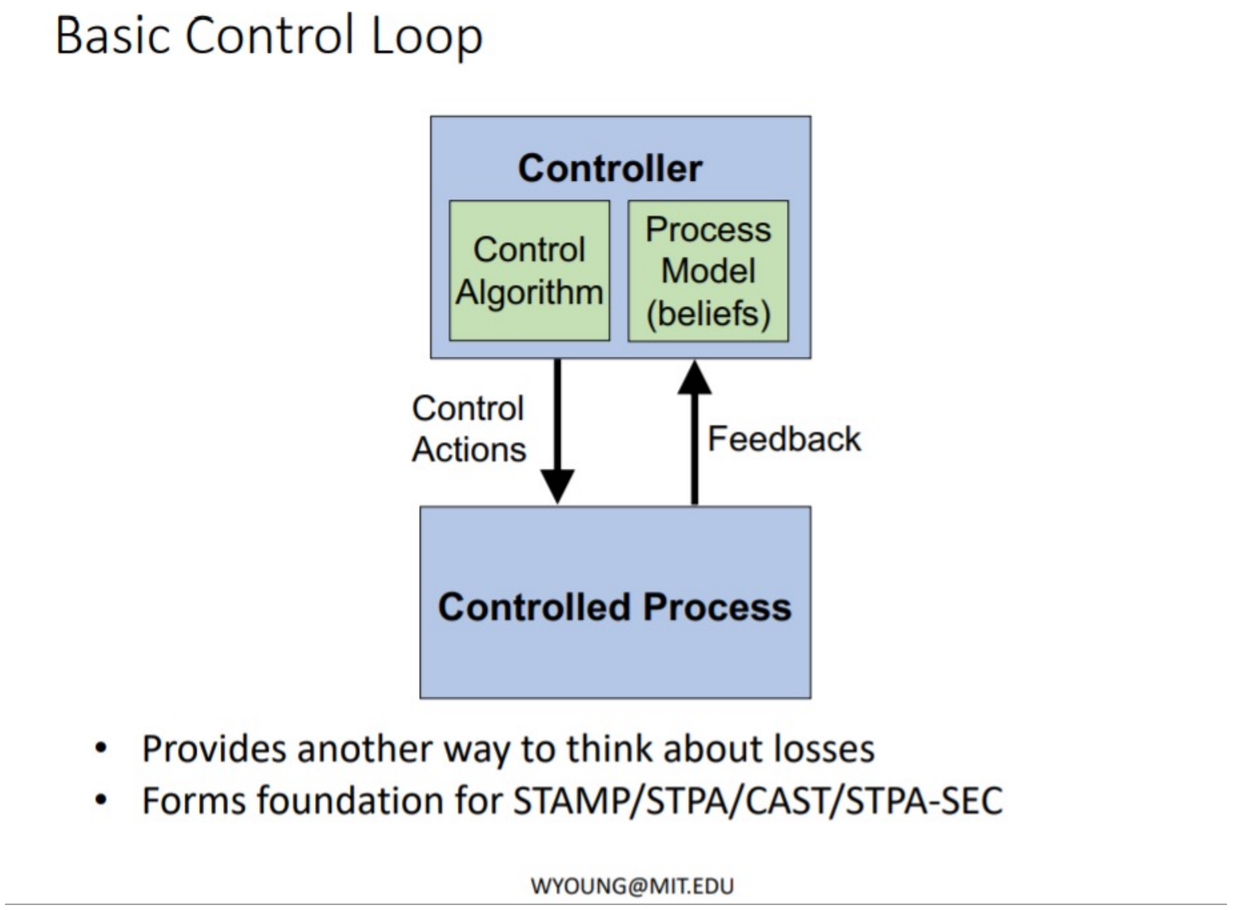

STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

(Leveson and Thomas, 2018)

# Start at a high level, and work your way down

- Also how we model

# Look for, and model, control processes (recursively)

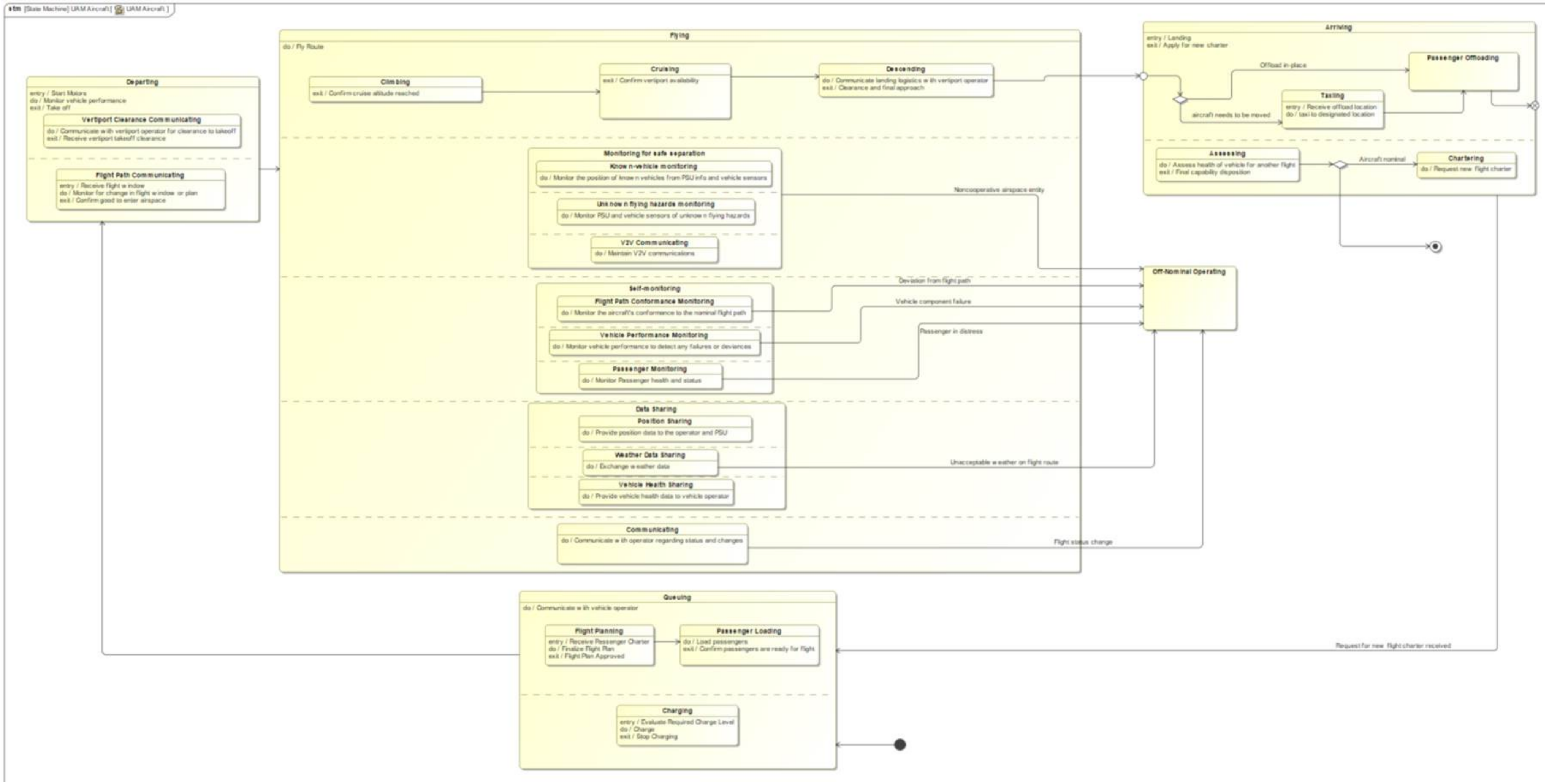


Basic Control Loop

- Provides another way to think about losses
- Forms foundation for STAMP/STPA/CAST/STPA-SEC

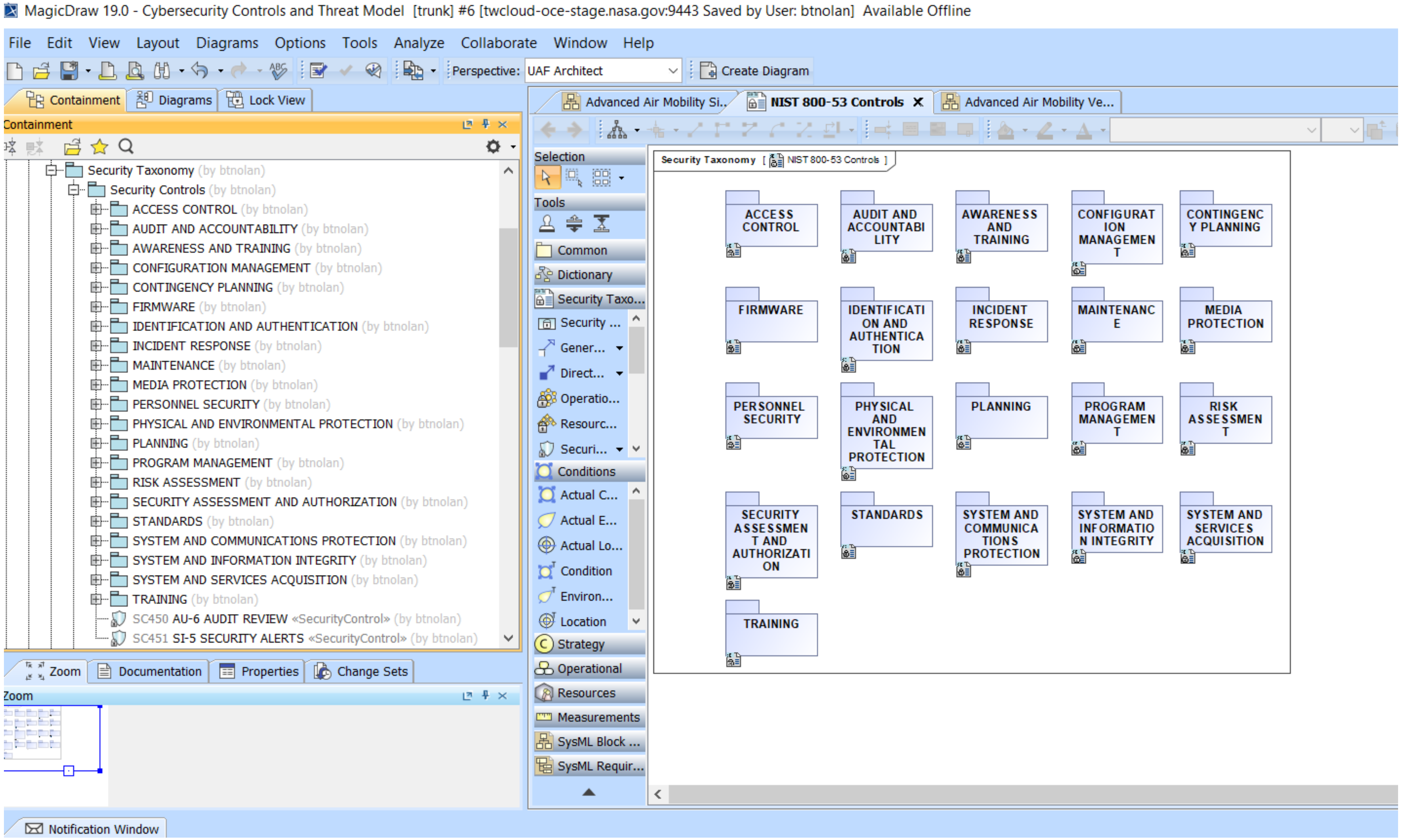
WYOUNG@MIT.EDU

# States/Process of Flying



stm [State Machine] UAM Aircraft [ UAM Aircraft ]
Departing
entry / Start Motors
do / Monitor vehicle performance
exit / Take off
Vertiport Clearance Communicating
do / Communicate with vertiport operator for clearance to takeoff
exit / Receive vertiport takeoff clearance
Flight Path Communicating
entry / Receive flight window
do / Monitor for change in flight window or plan
exit / Confirm good to enter airspace
Flying
do / Fly Route
Climbing
exit / Confirm cruise altitude reached
Cruising
exit / Confirm vertiport availability
Descending
do / Communicate landing logistics with vertiport operator
exit / Clearance and final approach
Monitoring for safe separation
Known-vehicle monitoring
do / Monitor the position of known vehicles from PSU info and vehicle sensors
Unknown flying hazards monitoring
do / Monitor PSU and vehicle sensors of unknown flying hazards
V2V Communicating
do / Maintain V2V communications
Self-monitoring
Flight Path Conformance Monitoring
do / Monitor the aircraft's conformance to the nominal flight path
Vehicle Performance Monitoring
do / Monitor vehicle performance to detect any failures or deviances
Passenger Monitoring
do / Monitor Passenger health and status
Data Sharing
Position Sharing
do / Provide position data to the operator and PSU
Weather Data Sharing
do / Exchange weather data
Vehicle Health Sharing
do / Provide vehicle health data to vehicle operator
Communicating
do / Communicate with operator regarding status and changes
Noncooperative airspace entity
Deviation from flight path
Vehicle component failure
Passenger in distress
Unacceptable weather on flight route
Flight status change
Arriving
entry / Landing
exit / Apply for new charter
Offload in-place
Passenger Offloading
Taxiing
entry / Receive offload location
do / taxi to designated location
aircraft needs to be moved
Assessing
do / Assess health of vehicle for another flight
exit / Final capability disposition
Aircraft nominal
Chartering
do / Request new flight charter
Off-Nominal Operating
Queuing
do / Communicate with vehicle operator
Flight Planning
entry / Receive Passenger Charter
do / Finalize Flight Plan
exit / Flight Plan Approved
Passenger Loading
do / Load passengers
exit / Confirm passengers are ready for flight
Charging
entry / Evaluate Required Charge Level
do / Charge
exit / Stop Charging
Request for new flight charter received

# NIST 800-53 Controls



MagicDraw 19.0 - Cybersecurity Controls and Threat Model [trunk] #6 [twcloud-oce-stage.nasa.gov:9443 Saved by User: btnolan] Available Offline

Perspective: UAF Architect

Containment

- Security Taxonomy (by btnolan)
  - Security Controls (by btnolan)
    - ACCESS CONTROL (by btnolan)
    - AUDIT AND ACCOUNTABILITY (by btnolan)
    - AWARENESS AND TRAINING (by btnolan)
    - CONFIGURATION MANAGEMENT (by btnolan)
    - CONTINGENCY PLANNING (by btnolan)
    - FIRMWARE (by btnolan)
    - IDENTIFICATION AND AUTHENTICATION (by btnolan)
    - INCIDENT RESPONSE (by btnolan)
    - MAINTENANCE (by btnolan)
    - MEDIA PROTECTION (by btnolan)
    - PERSONNEL SECURITY (by btnolan)
    - PHYSICAL AND ENVIRONMENTAL PROTECTION (by btnolan)
    - PLANNING (by btnolan)
    - PROGRAM MANAGEMENT (by btnolan)
    - RISK ASSESSMENT (by btnolan)
    - SECURITY ASSESSMENT AND AUTHORIZATION (by btnolan)
    - STANDARDS (by btnolan)
    - SYSTEM AND COMMUNICATIONS PROTECTION (by btnolan)
    - SYSTEM AND INFORMATION INTEGRITY (by btnolan)
    - SYSTEM AND SERVICES ACQUISITION (by btnolan)
    - TRAINING (by btnolan)
    - SC450 AU-6 AUDIT REVIEW «SecurityControl» (by btnolan)
    - SC451 SI-5 SECURITY ALERTS «SecurityControl» (by btnolan)

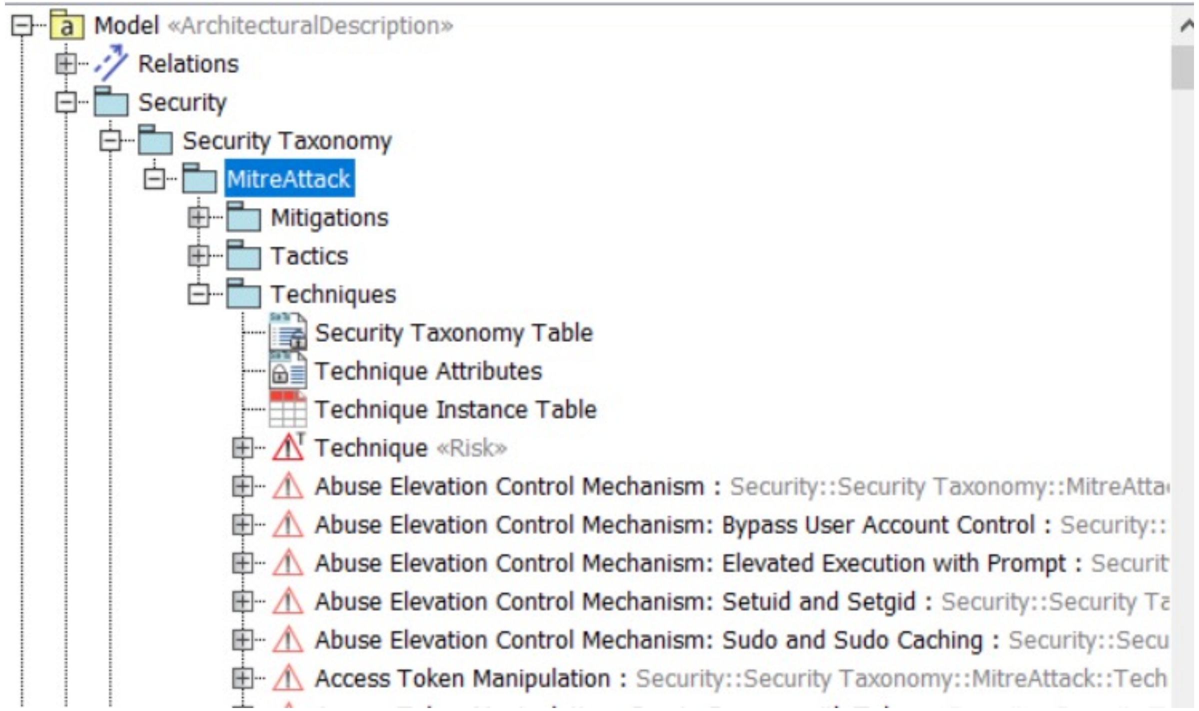
Security Taxonomy [ NIST 800-53 Controls ]

| | | | | |
|---|---|---|---|---|
| ACCESS CONTROL | AUDIT AND ACCOUNTABILITY | AWARENESS AND TRAINING | CONFIGURATION MANAGEMENT | CONTINGENCY PLANNING |
| FIRMWARE | IDENTIFICATION AND AUTHENTICATION | INCIDENT RESPONSE | MAINTENANCE | MEDIA PROTECTION |
| PERSONNEL SECURITY | PHYSICAL AND ENVIRONMENTAL PROTECTION | PLANNING | PROGRAM MANAGEMENT | RISK ASSESSMENT |
| SECURITY ASSESSMENT AND AUTHORIZATION | STANDARDS | SYSTEM AND COMMUNICATIONS PROTECTION | SYSTEM AND INFORMATION INTEGRITY | SYSTEM AND SERVICES ACQUISITION |
| TRAINING | | | | |

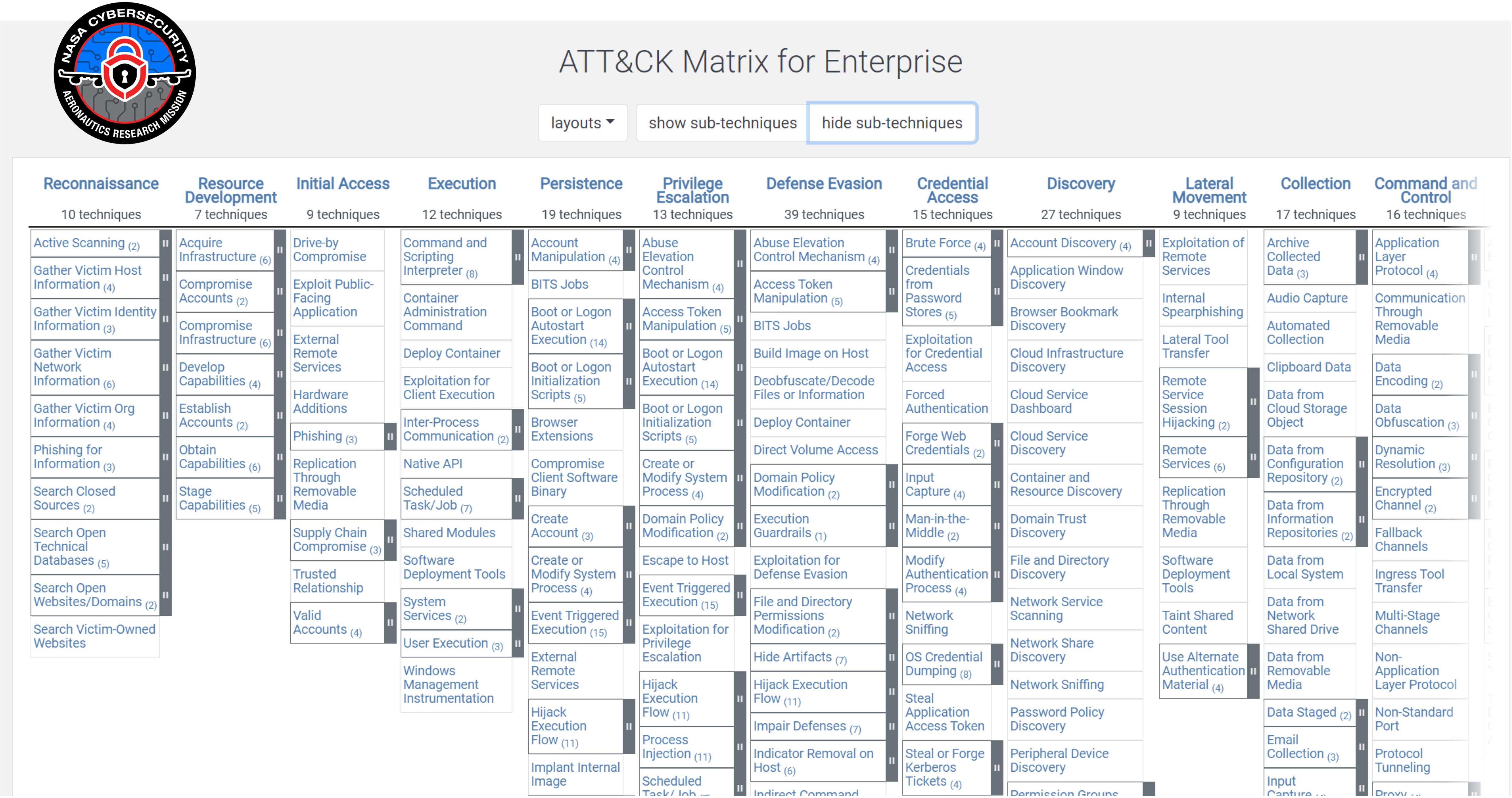
# NIST 800-53 Controls

- Sub Controls need to be parsed and added

# Mitre Att&ck Model (in progress)



- Model «ArchitecturalDescription»
  - Relations
  - Security
    - Security Taxonomy
      - MitreAttack
        - Mitigations
        - Tactics
        - Techniques
          - Security Taxonomy Table
          - Technique Attributes
          - Technique Instance Table
          - Technique «Risk»
          - Abuse Elevation Control Mechanism : Security::Security Taxonomy::MitreAtta
          - Abuse Elevation Control Mechanism: Bypass User Account Control : Security::
          - Abuse Elevation Control Mechanism: Elevated Execution with Prompt : Securit
          - Abuse Elevation Control Mechanism: Setuid and Setgid : Security::Security Ta
          - Abuse Elevation Control Mechanism: Sudo and Sudo Caching : Security::Secu
          - Access Token Manipulation : Security::Security Taxonomy::MitreAttack::Tech

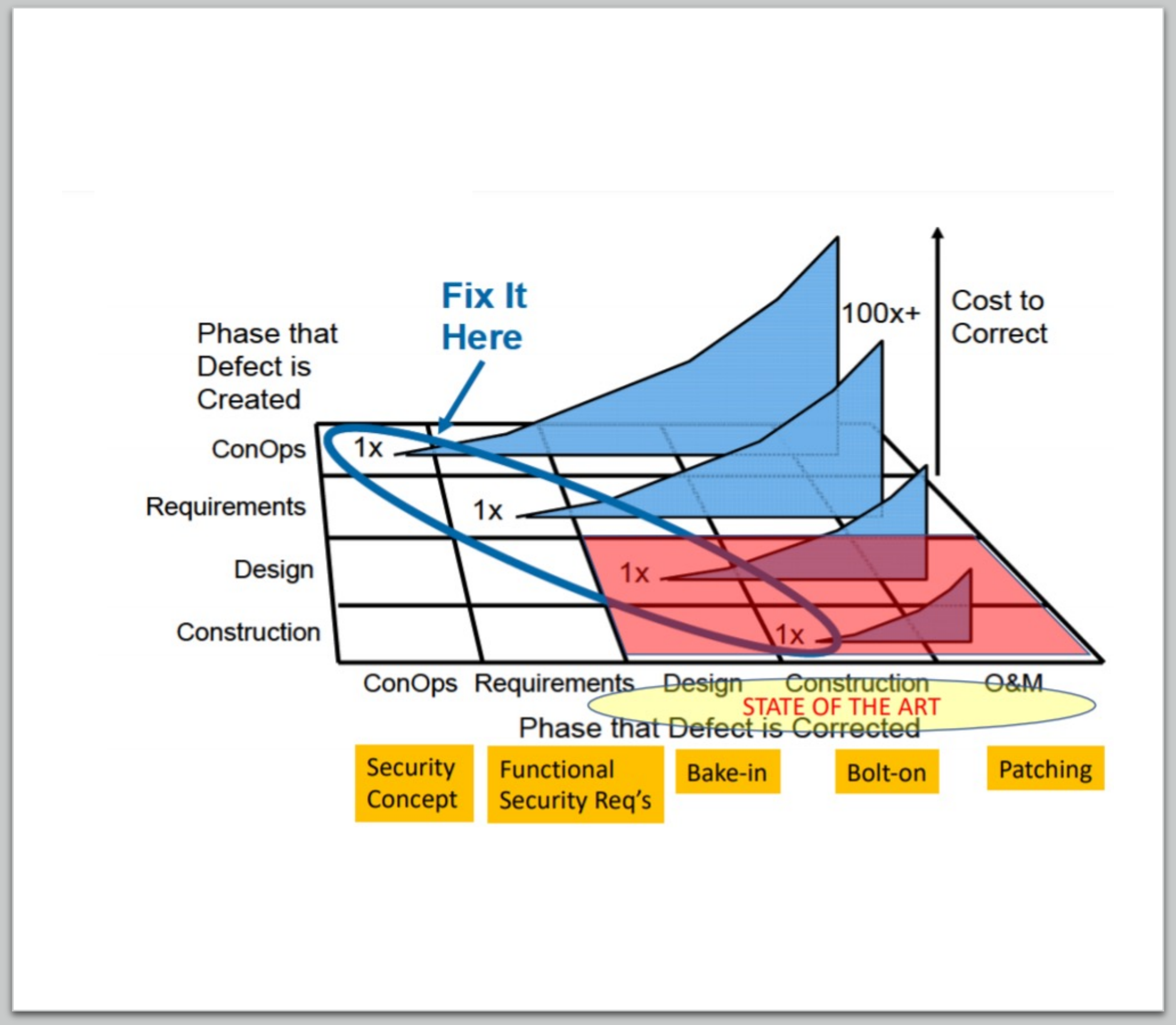


# ATT&CK Matrix for Enterprise

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 techniques | 7 techniques | 9 techniques | 12 techniques | 19 techniques | 13 techniques | 39 techniques | 15 techniques | 27 techniques | 9 techniques | 17 techniques | 16 techniques |
| Active Scanning (2) | Acquire Infrastructure (6) | Drive-by Compromise | Command and Scripting Interpreter (8) | Account Manipulation (4) | Abuse Elevation Control Mechanism (4) | Abuse Elevation Control Mechanism (4) | Brute Force (4) | Account Discovery (4) | Exploitation of Remote Services | Archive Collected Data (3) | Application Layer Protocol (4) |
| Gather Victim Host Information (4) | Compromise Accounts (2) | Exploit Public-Facing Application | Container Administration Command | BITS Jobs | Access Token Manipulation (5) | Access Token Manipulation (5) | Credentials from Password Stores (5) | Application Window Discovery | Internal Spearphishing | Audio Capture | Communication Through Removable Media |
| Gather Victim Identity Information (3) | Compromise Infrastructure (6) | External Remote Services | Deploy Container | Boot or Logon Autostart Execution (14) | Boot or Logon Autostart Execution (14) | BITS Jobs | Exploitation for Credential Access | Browser Bookmark Discovery | Lateral Tool Transfer | Automated Collection | Data Encoding (2) |
| Gather Victim Network Information (6) | Develop Capabilities (4) | Hardware Additions | Exploitation for Client Execution | Boot or Logon Initialization Scripts (5) | Boot or Logon Initialization Scripts (5) | Build Image on Host | Forced Authentication | Cloud Infrastructure Discovery | Remote Service Session Hijacking (2) | Clipboard Data | Data Obfuscation (3) |
| Gather Victim Org Information (4) | Establish Accounts (2) | Phishing (3) | Inter-Process Communication (2) | Browser Extensions | Create or Modify System Process (4) | Deobfuscate/Decode Files or Information | Forge Web Credentials (2) | Cloud Service Dashboard | Remote Services (6) | Data from Cloud Storage Object | Dynamic Resolution (3) |
| Phishing for Information (3) | Obtain Capabilities (6) | Replication Through Removable Media | Native API | Compromise Client Software Binary | Domain Policy Modification (2) | Deploy Container | Input Capture (4) | Cloud Service Discovery | Replication Through Removable Media | Data from Configuration Repository (2) | Encrypted Channel (2) |
| Search Closed Sources (2) | Stage Capabilities (5) | Supply Chain Compromise (3) | Scheduled Task/Job (7) | Create Account (3) | Escape to Host | Direct Volume Access | Man-in-the-Middle (2) | Container and Resource Discovery | Software Deployment Tools | Data from Information Repositories (2) | Fallback Channels |
| Search Open Technical Databases (5) | | Trusted Relationship | Shared Modules | Create or Modify System Process (4) | Event Triggered Execution (15) | Domain Policy Modification (2) | Modify Authentication Process (4) | Domain Trust Discovery | Taint Shared Content | Data from Local System | Ingress Tool Transfer |
| Search Open Websites/Domains (2) | | Valid Accounts (4) | Software Deployment Tools | Event Triggered Execution (15) | Exploitation for Privilege Escalation | Execution Guardrails (1) | Network Sniffing | File and Directory Discovery | Use Alternate Authentication Material (4) | Data from Network Shared Drive | Multi-Stage Channels |
| Search Victim-Owned Websites | | | System Services (2) | External Remote Services | Hijack Execution Flow (11) | Exploitation for Defense Evasion | OS Credential Dumping (8) | Network Service Scanning | | Data from Removable Media | Non-Application Layer Protocol |
| | | | User Execution (3) | Hijack Execution Flow (11) | Process Injection (11) | File and Directory Permissions Modification (2) | Steal Application Access Token | Network Share Discovery | | Data Staged (2) | Non-Standard Port |
| | | | Windows Management Instrumentation | Implant Internal Image | Scheduled Task/Job | Hide Artifacts (7) | Steal or Forge Kerberos Tickets (4) | Network Sniffing | | Email Collection (3) | Protocol Tunneling |
| | | | | | | Hijack Execution Flow (11) | | Password Policy Discovery | | Input Capture | Proxy |
| | | | | | | Impair Defenses (7) | | Peripheral Device Discovery | | | |
| | | | | | | Indicator Removal on Host (6) | | Permission Groups | | | |
| | | | | | | Indirect Command | | | | | |

# Conclusion

- We are using and will use MBSE to facilitate our Cybersecurity Systems Engineering
- We need to work the project and its subprojects to ensure that we end up with a secure, resilient architecture.
- We can’t do this in isolation, after the fact, or as a compliance bolt-on.


Fix It Here
Phase that Defect is Created
100x+
Cost to Correct
ConOps
Requirements
Design
Construction
1x
1x
1x
1x
ConOps
Requirements
Design
Construction
O&M
STATE OF THE ART
Phase that Defect is Corrected
Security Concept
Functional Security Req’s
Bake-in
Bolt-on
Patching