August 7, 2019

CYBERSECURITY RISK ASSESSMENT FOR SAFETY-CRITICAL SYSTEMS

AUTHORS:

DR. LY VESSELS,
DR. DANIEL JOHNSON &
DR. KEN HEFFNER

Honeywell

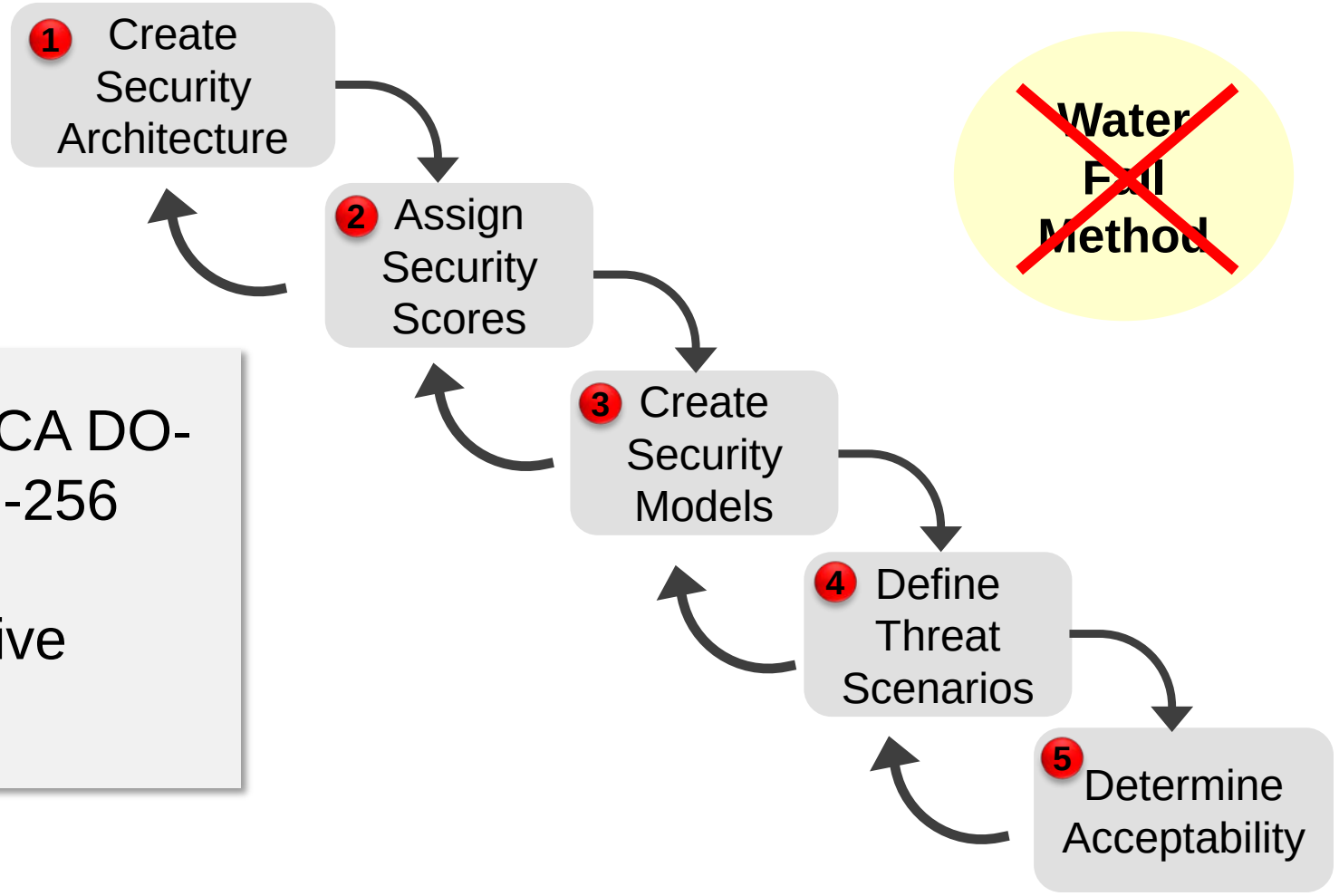
MOTIVATIONS

- **Lack of available tools to model security risks**
  - Currently available tools focuses on threat modeling
  - Requires extensive security knowledge to use
  - Time consuming to model an enterprise
  - Focuses more on enterprise instead of critical infrastructure systems

- **Currently available security risk assessment**
  - Depends on experts with deep knowledge in security and mathematics to calculate the probabilities and risks
  - Manual computation that is time consuming and error-prone

A repeatable framework is needed to rapidly and easily assess the security risk of the existing space systems.

HONEYWELL SECURITY RISK ASSESSMENT FRAMEWORK

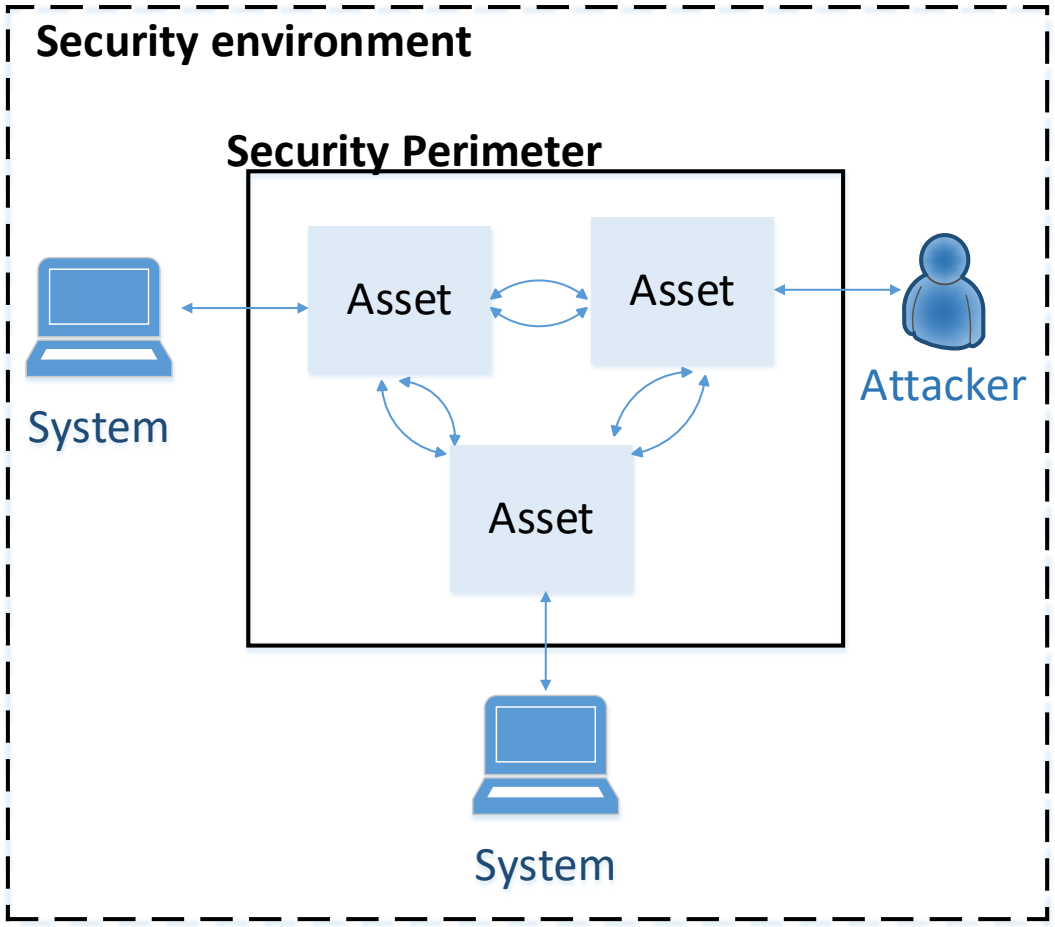


- Based on RTCA DO-326A and DO-256
- Consists of Five major Steps

An iterative with feedback process to rapidly assess risks of a system.

1 CREATE SECURITY ARCHITECTURE

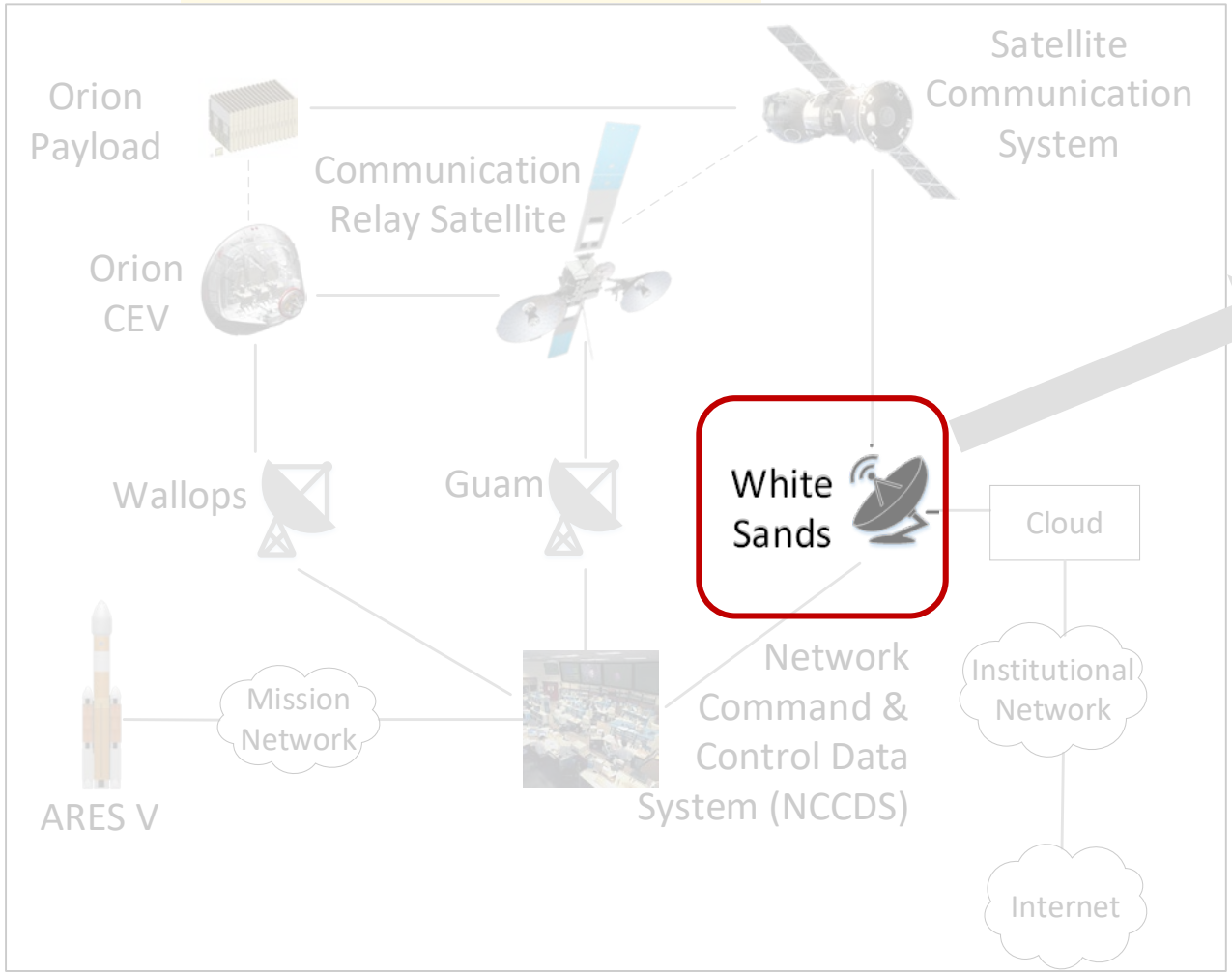
1. Determine the Security Perimeter
2. Determine the security-relevant assets of the system
   - *Primary Assets* are functions or data that must cannot compromised
   - *Secondary Assets* are assets that support the primary assets
   - Security Functions / Security Data are secondary assets
3. Determine external systems
4. Determine connections



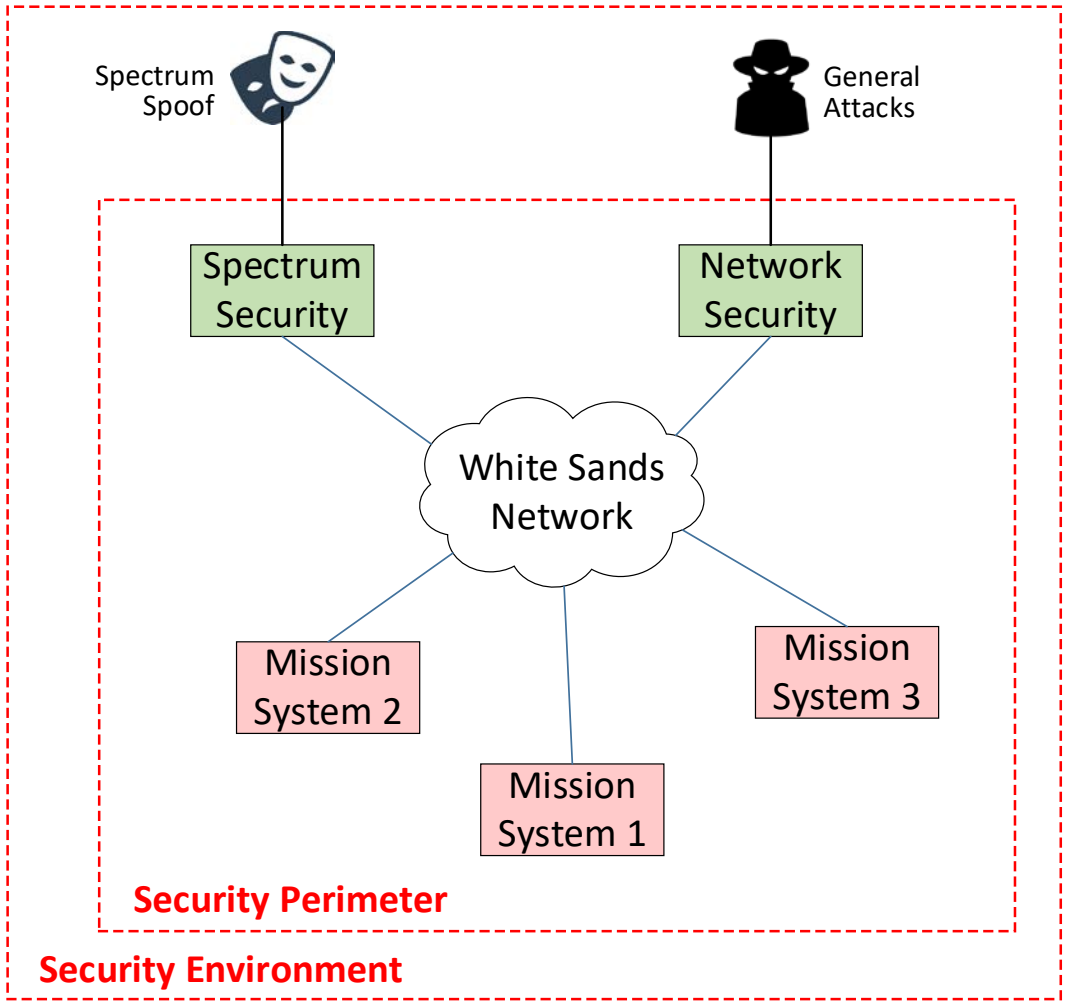
Security Architecture is the based to all the steps of the framework.

1 AN EXAMPLE OF CREATE SECURITY ARCHITECTURE

SpaceX Example

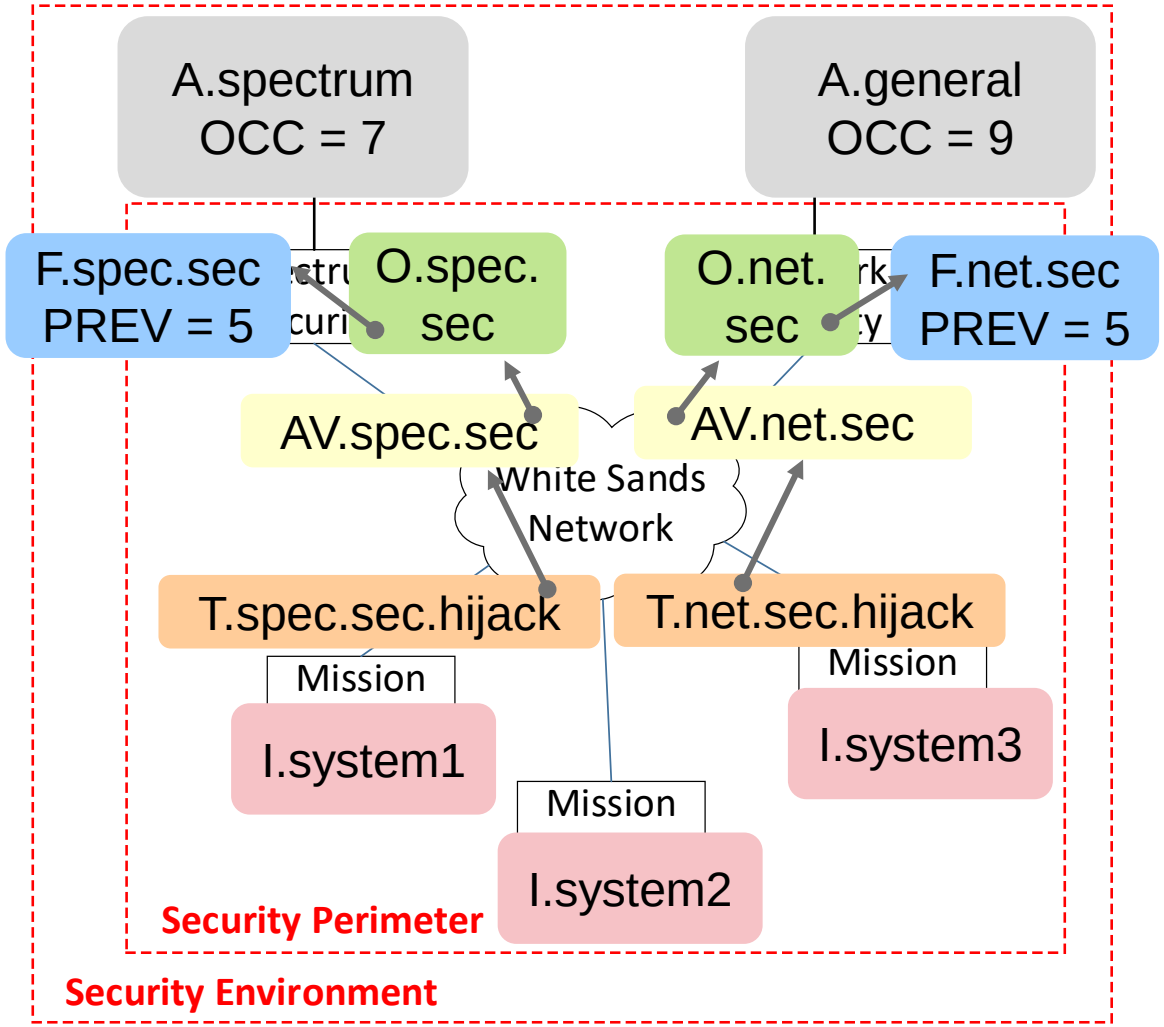


White Sands Security Architecture



2 ASSIGN SECURITY SCORES

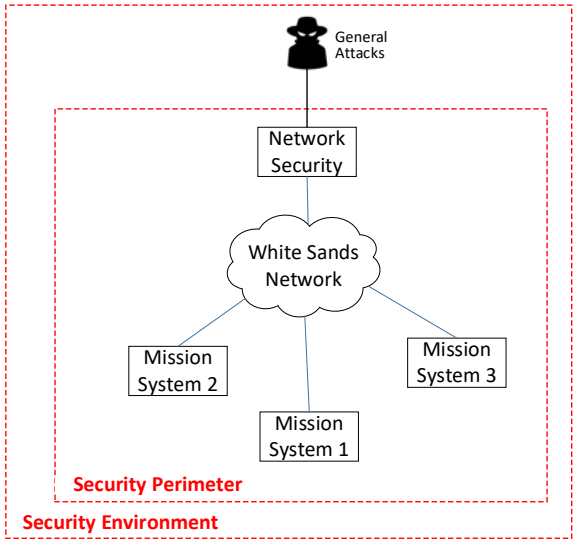
1. **Identify Attackers, and assign**
   - Name (F.*)
   - OCCURRENCE values (OCC)
2. **Identify Vulnerabilities, and assign**
   - Name (F.*)
   - PREVENTION values (PREV)
3. **Identify Security Measure, and assign**
   - Name (O.*)
   - Vulnerabilities
4. **Identify Attack Vector,**
   - Assign a Name(AV.*)
   - If one exist, assign the Secure Measure and the Attacker, Access Vectors, or Threat Conditions
5. **Identify Threat Conditions,**
   - Assign a Name(TS.*)
   - If one exist, assign the Secure Measures and Attacker, Access Vectors, or Threat Conditions
6. **Identify the Asset and assign a Name (I.*)**



Security Scores are the inputs to the Honeywell Security Modeling Engine.

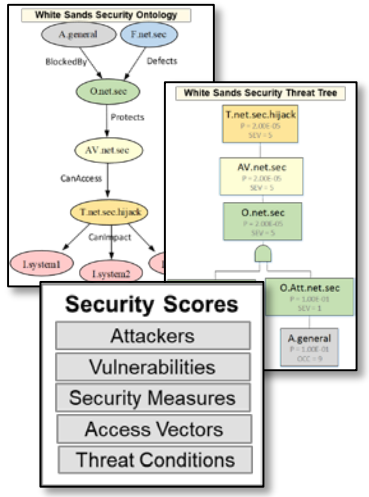
3 CREATE SECURITY MODELS & CUTSETS

White Sands Security Architecture

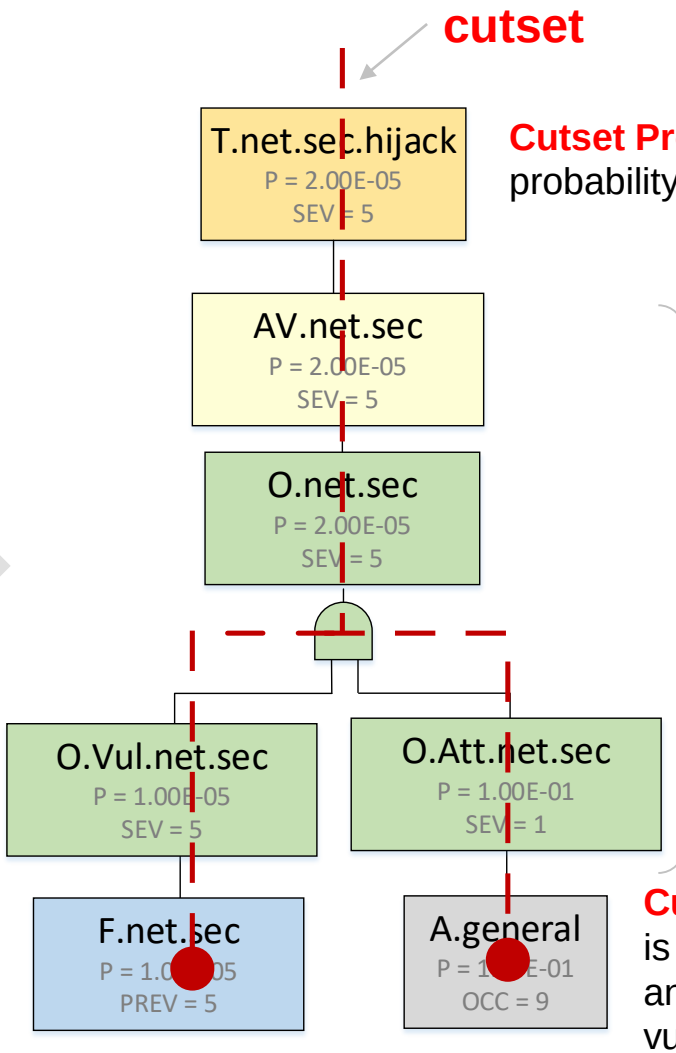


Honeywell Security Ontology and Threat – based Modeling Engine

inputs into



generates



Cutset Probability is probability of the top node

Cutset Internal Nodes are secondary target of attack

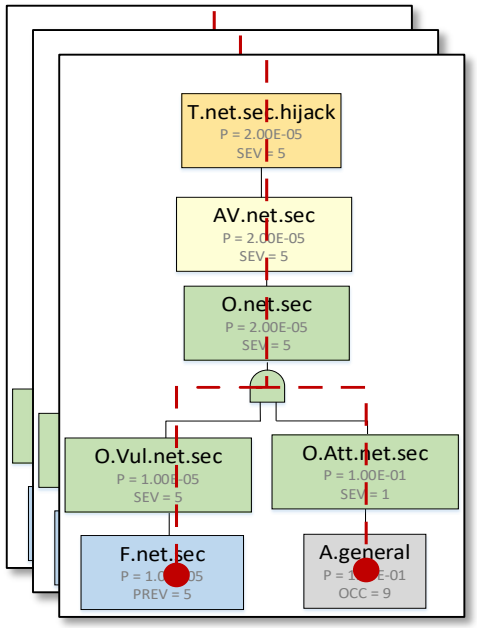
Cutset Attackers are the lowest level leaf node and shows who can attack.

Cutset Vulnerability is the lowest leaf node and shows how it is vulnerable

Cutsets are collections of vulnerabilities and attackers sufficient to cause the threat conditions, and they are used to generate threat scenarios.

4 DEFINE THREAT SCENARIOS

Use the cutsets to create Threat Scenarios by group cutsets within a threat scenario.



White Sands Cutsets

inputs into

generates

Honeywell Security Risk Calculation Engine

Threat Scenarios

Threat Scenarios	SEV	Mitigated Probabilities	Risk Level
TS.general.attack.ground.to.satellite	5	3.04E-06	-0.5

Honeywell Security Risk Calculation Engine consolidates and computes the given cutsets into a single security risk number for a given threat scenario.

5 DETERMINE ACCEPTABILITY

Determine Acceptability using the Security Acceptability Matrix

Threat Scenarios

Threat Scenarios	SEV	Mitigated Probabilities	Risk Level
TS.general.attack. ground.to.satellite	5	3.04E-06	-0.5

lookup

Acceptability Matrix

			Risk Level	Criticality of Asset to Flight Safety				
				No Safety Effect E	Minor D	Major C	Hazardous B	Catastrophic A
Net Effect of Protection and Trust within Threat Scenario	No Protection/Trust	E		0	1	2	3	4
	Moderate	D		-1	0	1	2	3
	High	C		-2	-1	0	1	2
	Very High	B		-3	-2	-1	0	1
	Extremely High	A		-4	-3	-2	-1	0

Risk Level	Label	Certification	Continuing Secure
RL <= 0	Low	Acceptable with existing operational mitigation	Acceptable
RL = 1	Medium	Acceptable with additional operational mitigation	Acceptable with appropriate mitigations and timely correction
RL >= 2	High	Unacceptable until design changed	Urgent need for correction

Acceptable Risk
for spectrum spoofing from the ground to satellite

Security Risk Assessment Framework provides a security risk score and the complete traceability for how it was computed.

NEXT STEPS

- **End-to-end automation to provide**
  - Rapid security risk assessment
  - Ease of the process
  - Lessen the dependency on an expert knowledge

- **Standardize on the scores assigned to the vulnerabilities and attackers.**

A method for assessing the cybersecurity risk of space systems.

IN SUMMARY

- **More and more space systems will be targeted for monetary, nation-state, and establish creditability**

- **Many of the existing safety-critical systems**
  - Was designed without any security safeguards
  - Has hidden vulnerabilities that are exploitable
  - Unknown understanding of its security risks

- **Honeywell has developed a Security Risk Assessment Framework (based on RTCA standards) to asset critical-infrastructure such as space systems**

Dr. Ly Vessels
Cybersecurity Architect
Ly.Vessels@honeywell.com

Dr. Daniel Johnson
Engineer Fellow
Daniel.p.Johnson@honeywell.com

Dr. Kenneth Heffner
Senior Engineer Fellow
Kenneth.h.Heffner@honeywell.com