Resilience Evaluation for Timing Systems

Dr. Bradley A. Moran, Dr. Patricia Larkoski

Homeland Security Systems Engineering & Development Institute, operated by The MITRE Corporation

Presentation on 14 Mar 2023 at Workshop on Synchronization and Timing Systems (WSTS)

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Acknowledgement for DHS Sponsored Tasks

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. MITRE Corp. operates the Homeland Security Systems Engineering and Development Institute (HSSEDI) as an FFRDC for DHS under contract 70RSAT20D00000001.

The HSSEDI FFRDC provides the government with the necessary systems engineering and development expertise to conduct complex acquisition planning and development; concept exploration, experimentation and evaluation; information technology, communications and cyber security processes, standards, methodologies and protocols; systems architecture and integration; quality and performance review, best practices and performance measures and metrics; and, independent test and evaluation activities. The HSSEDI FFRDC also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The HSSEDI FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under:

70RSAT20FR0000062, Next Gen Resilient Position, Navigation, and Timing (PNT), to develop and maintain the Nation's technical expertise, frameworks and artifacts necessary to guide users, product integrators and supply chain manufacturers on government expectations related to PNT system resilience.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

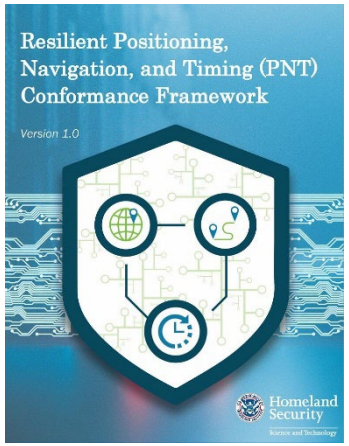
Critical Infrastructure Depends on Resilient Timing

- **CI Sectors and related systems depend widely on PNT, *especially T***
  - Use cases for both standalone Timing and full Positioning, Navigation & Timing
  - GNSS, particularly GPS, widely relied on for precise time synchronization
  - Impact of source degradation / loss often not well understood
- **Application-specific use cases drive needs**
  - Performance bounds (accuracy, availability), threats & disruptions
  - Resilience is the ability to meet performance bounds when subject to specific threat scenarios

Chemical, Communications, Emergency Services, Energy, Financial, Food & Agriculture, Information Technology Transportation Systems are some of the Critical Infrastructure Sectors vital to the United States

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Resilience Milestones and Beyond



December 2020

DHS S&T and CISA publish

Resilient PNT Conformance Framework V1.0

Outlines degrees of PNT resilience in coordination with industry and government partners

September 2021

Kickoff meeting for

IEEE P1952™ Working Group

To develop a voluntary industry Standard for Resilient Position, Navigation, and Timing (PNT) User Equipment (UE)

https://sagroups.ieee.org/p1952/

May 2022

DHS S&T and CISA publish

Resilient PNT Conformance Framework V2.0

Expands evaluation guidance in coordination with industry and government partners

https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework

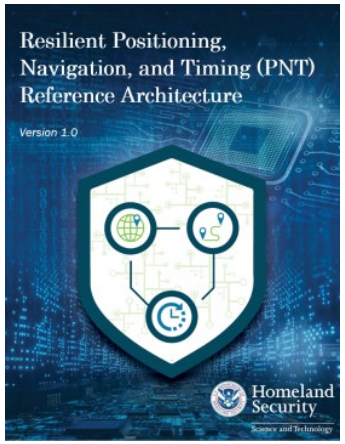
June 2022

DHS S&T publish the

Resilient PNT Reference Architecture V1.0

Supports the Resilient PNT Conformance Framework with examples

https://www.dhs.gov/science-and-technology/publication/resilient-pnt-reference-architecture



Early 2023

Kickoff meeting for

IEEE Conformity Assessment Program (ICAP)

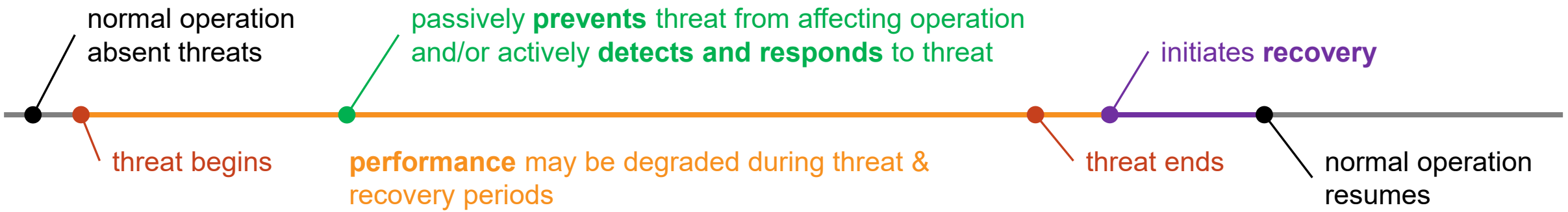
To develop assessment programs to accelerate market adoption supporting the IEEE P1952 Standard

HSSEDI
Homeland Security Systems Engineering & Development Institute™

P1952 Purpose and Scope

- **P1952 is a voluntary IEEE industry standard, intended**
  - to develop common language that describes resilience of PNT user equipment for end users, suppliers, and government agencies seeking improvements for Critical Infrastructure
  - to be implementation neutral
- **P1952 Project Authorization Request (PAR) focus on user equipment vs upstream infrastructure**
  - GNSS space and control segments, for example, out of scope
  - Details available from IEEE SA (https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/9060)
  - Success hinges on ability to evaluate PNT user equipment with respect to resilience standard

Resilient User Equipment Encountering a Threat



- **Aspects of resilient behavior for user equipment (UE) when encountering threat or disruption**
  - **Prevention:** what passive UE capabilities might prevent adverse impact on operation?
  - **Detection & Response:** After the threat begins, how do we know the UE has detected and responded appropriately? How long does it take?
  - **Performance:** how well does UE maintain performance while the threat persists?
  - **Recovery:** can the UE recover nominal performance after the threat is over?

Scenario Specific Resilience Evaluation

How well?

Measure performance

- Performance during the threat
  - Degree of degradation
  - Duration of degradation
- Performance after the threat

only option for passive prevention measures

How quickly?

Assess responsiveness

- Detection delay
- Lag between detection and response
- Lag between threat end and recovery initiation
- Recovery time

How explicitly?

Examine internal state

- Threat detection alerts
- Response indicators
- Performance quality reporting (including assurance and/or integrity)
- Recovery notification

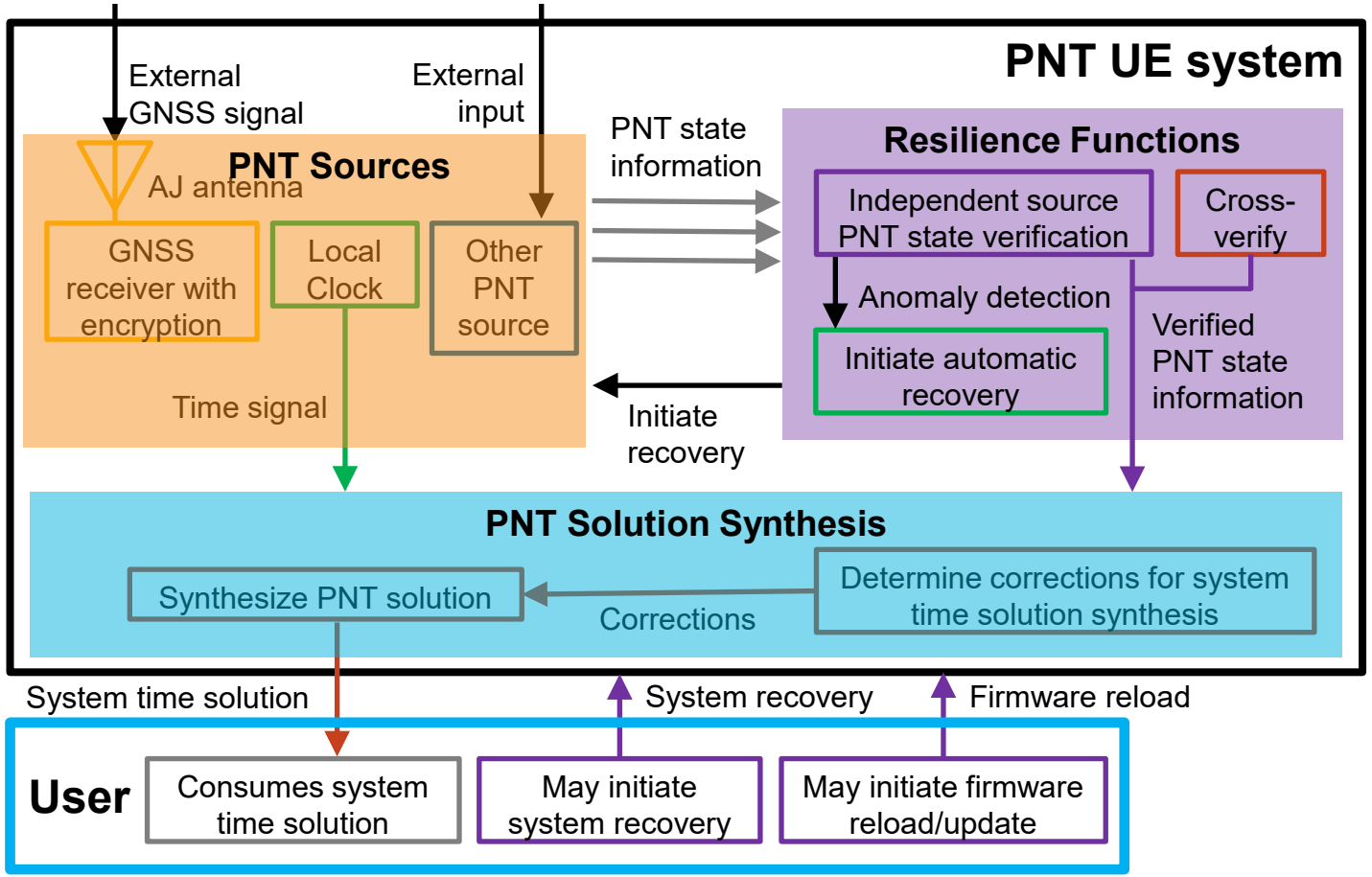
Resilient PNT Reference Architecture

- **PNT Source(s)**
  - Quantity & diversity, independence
- **Resilience Functions**
  - Threat detection
  - System response
  - Recovery
- **PNT Solution Synthesis**
  - Compensation terms
  - Blending
  - Output drivers

Many opportunities for UE to provide evidence of resilient behavior in output performance and reportable internal state change events

Logical Elements of Resilient PNT

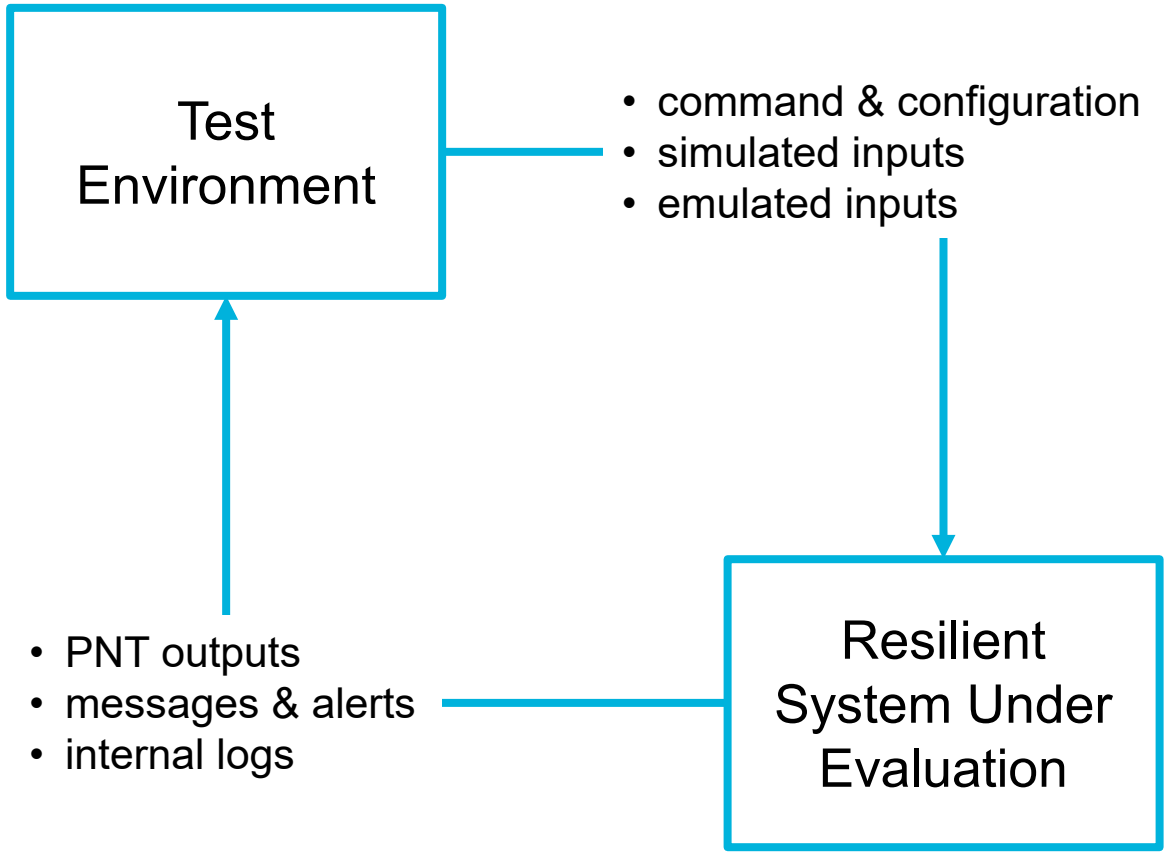
from *Resilient PNT Reference Architecture*, https://www.dhs.gov/science-and-technology/publication/resilient-pnt-reference-architecture



HSSEDI
Homeland Security Systems Engineering & Development Institute™

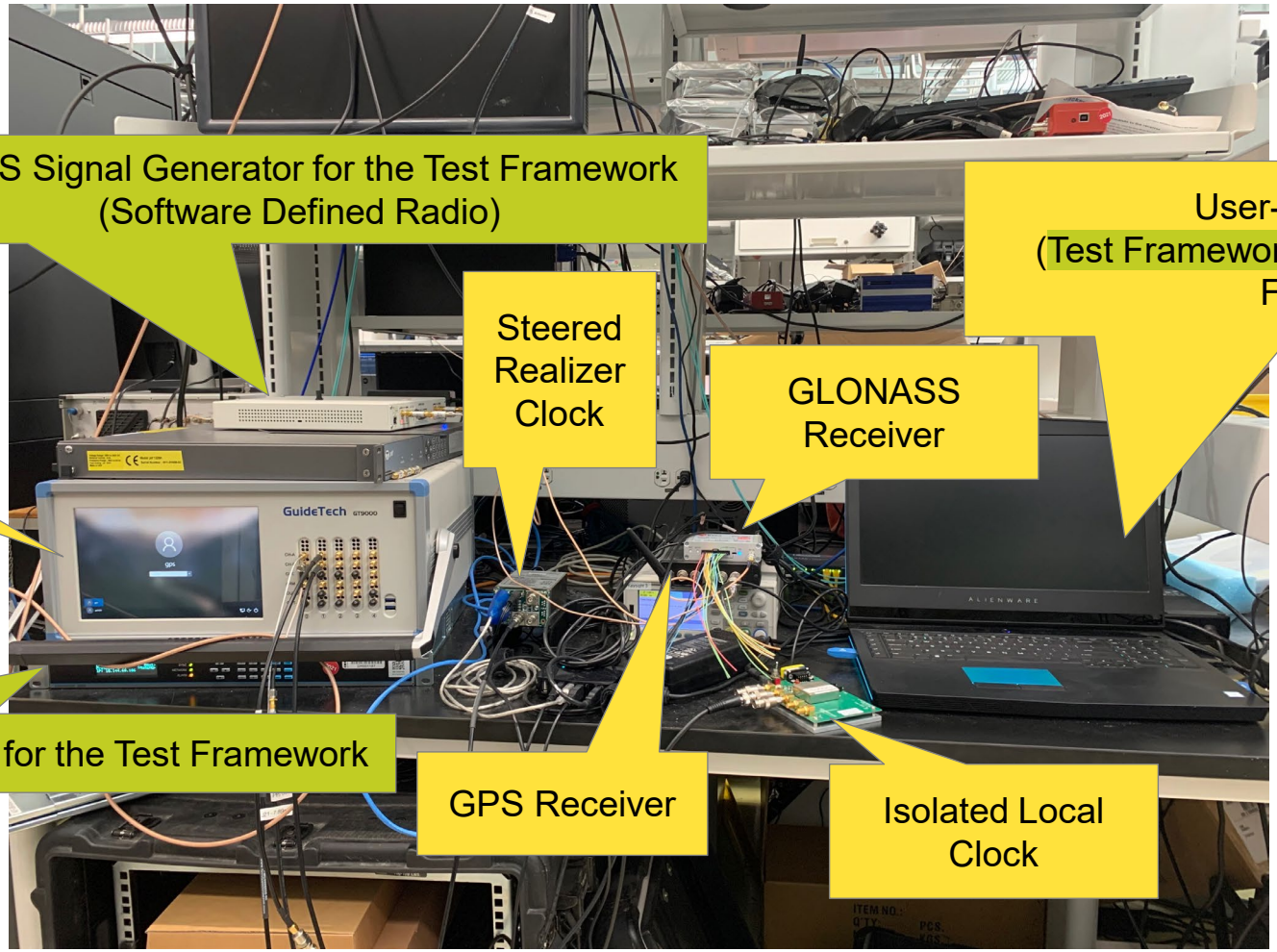
Resilient PNT Evaluation Infrastructure

- **Developing a modular toolkit to evaluate PNT resilience**
  - Provides user command, scenario generation, PNT source emulation, logging and analysis
- **Demonstrating evaluation of resilience approaches described in the Reference Architecture**
  - Initial focus on timing systems with detectable time ramp threat scenarios



HSSEDI
Homeland Security Systems Engineering & Development Institute™

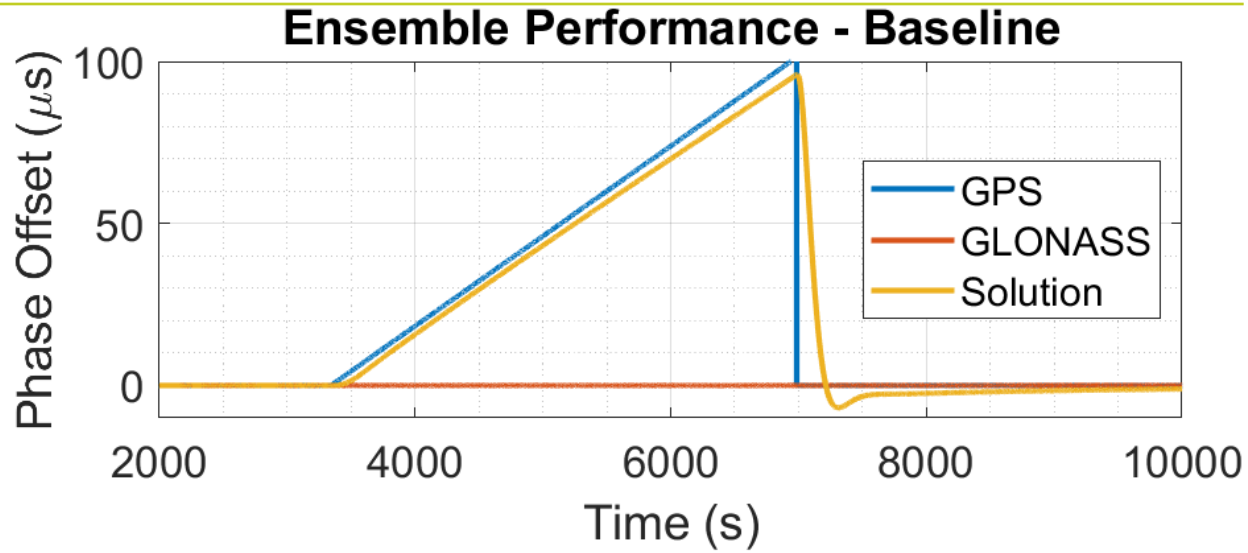
Lab Setup for Continuous Resilience Demonstration

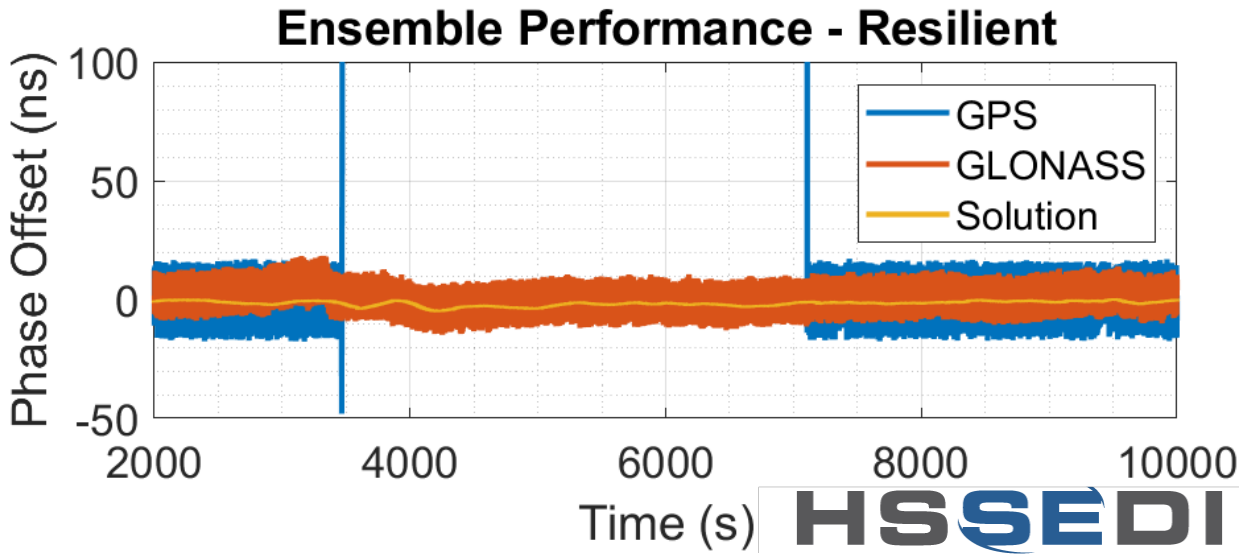


HSSEDI
Homeland Security Systems Engineering & Development Institute™

Resilience Demonstration Results

- **Input scenario**
  - 1 hr nominal, 2 hr threat, …
  - Measurement spoof on GPS constellation, time ramp ~25 ns/s
  - GLONASS undisturbed
- **Resilient vs baseline behavior**
  - Solution walks off when ensemble includes all input sources
  - Resilient system isolates GPS from solution, showing minor degradation that remains bounded
  - Recovery includes re-integration of GPS source





HSSEDI
Homeland Security Systems Engineering & Development Institute™

Resilience Metrics Verified in Demonstration

How well?

Measure performance

- **Functional & Performance Metrics**
  - Bounded degradation during the threat
  - System performance recovery after the threat
  - Automatic source recovery after the threat

How quickly?

Assess responsiveness

- **Delay Metrics**
  - Threat detection delay
  - Recovery initiation time

How explicitly?

Examine internal state

- **Reporting Metrics**
  - Threat detection reporting
  - Threat response reporting when compromised PNT source isolated from ensemble solution
  - System recovery reporting when PNT source returned to ensemble

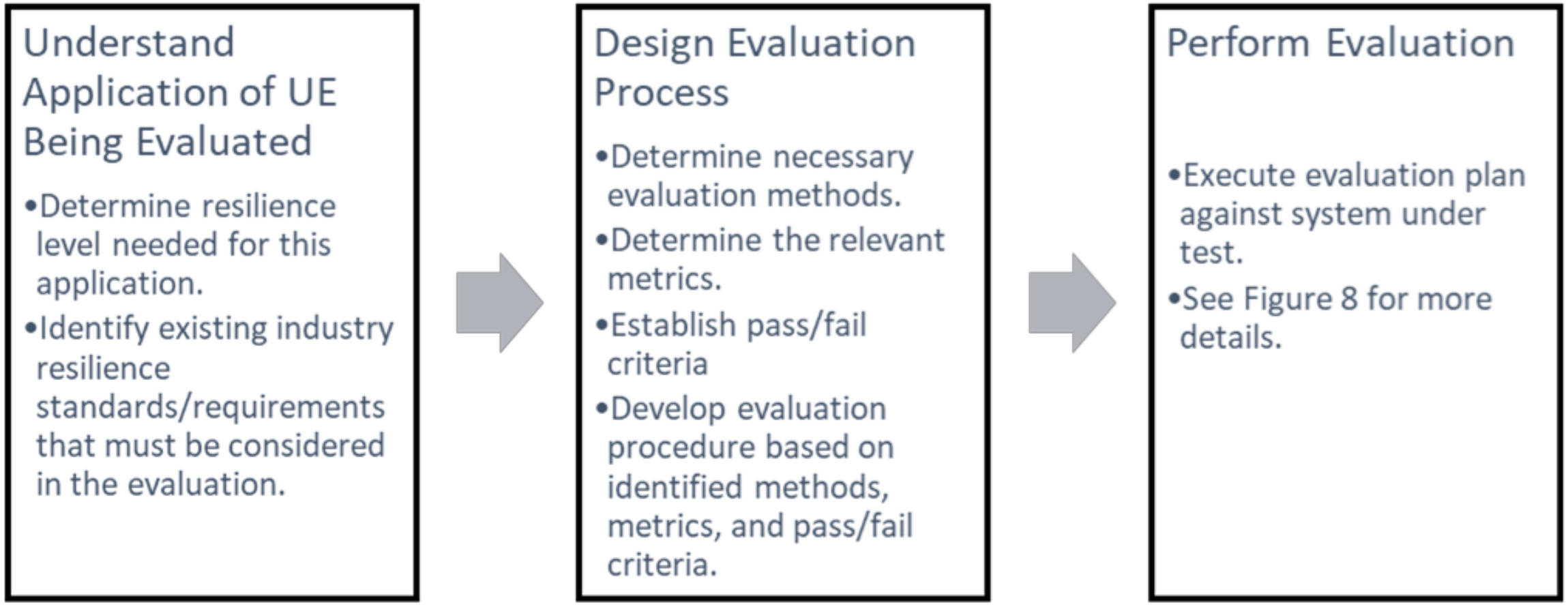
Evaluation Metrics		
RMS Error Performance	Initial	1.0 ns
	During threat	2.6 ns
	Post recovery	1.2 ns
Response times	Threat detection	3 s
	Recovery initiation	46 s

Considerations and Recommendations

- **For Resilient PNT End Users:**
  - What drives resilience requirements for your application, e.g., criticality, safety, regulatory?
  - What evidence of resilient behavior do you need …
    - … for the user equipment to share with the application layer?
    - … for the development team to satisfy regulatory requirements, if applicable?
  - How well does the supply chain currently meet your needs?
  - What dialog should you be having with developers?
- **For Resilient PNT Developers:**
  - What performance and threat use cases does your resilient solution address?
  - What operational information, including internal state, can provide evidence to end users of resilient behavior?
  - What messages and protocols to communicate resilience?
  - Leverage existing? Develop novel? Collective development?

Backups

Conformance Framework Evaluation Concepts



Overall Evaluation Process from Conformance Framework

Level 3 Reference Implementation Diagram

PNT Sources:

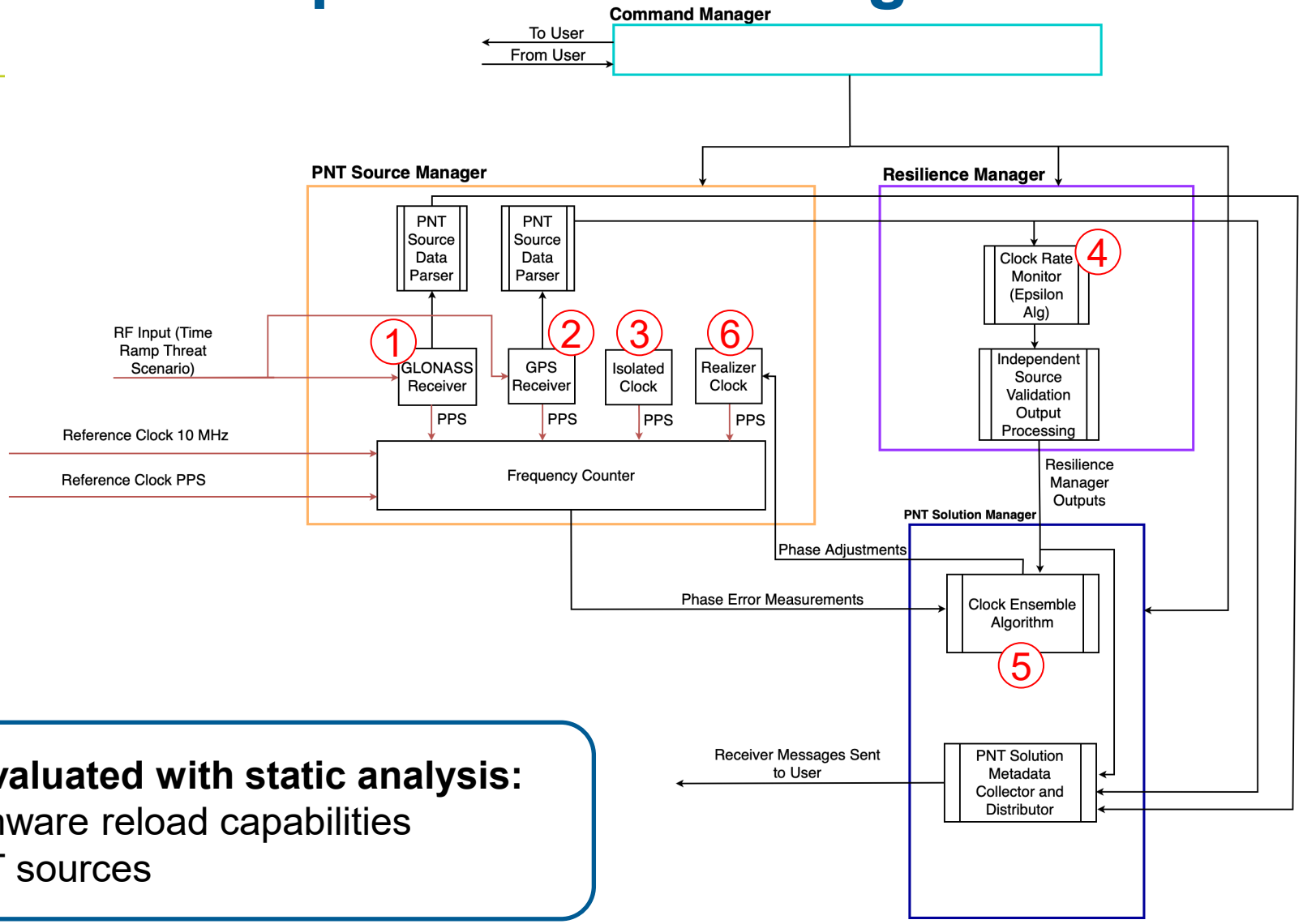
1. GLONASS receiver
2. GPS receiver
3. Isolated clock

Resilience manager:

4. Clock rate monitor

Solution Output:

5. Ensemble algorithm
6. Realizer clock



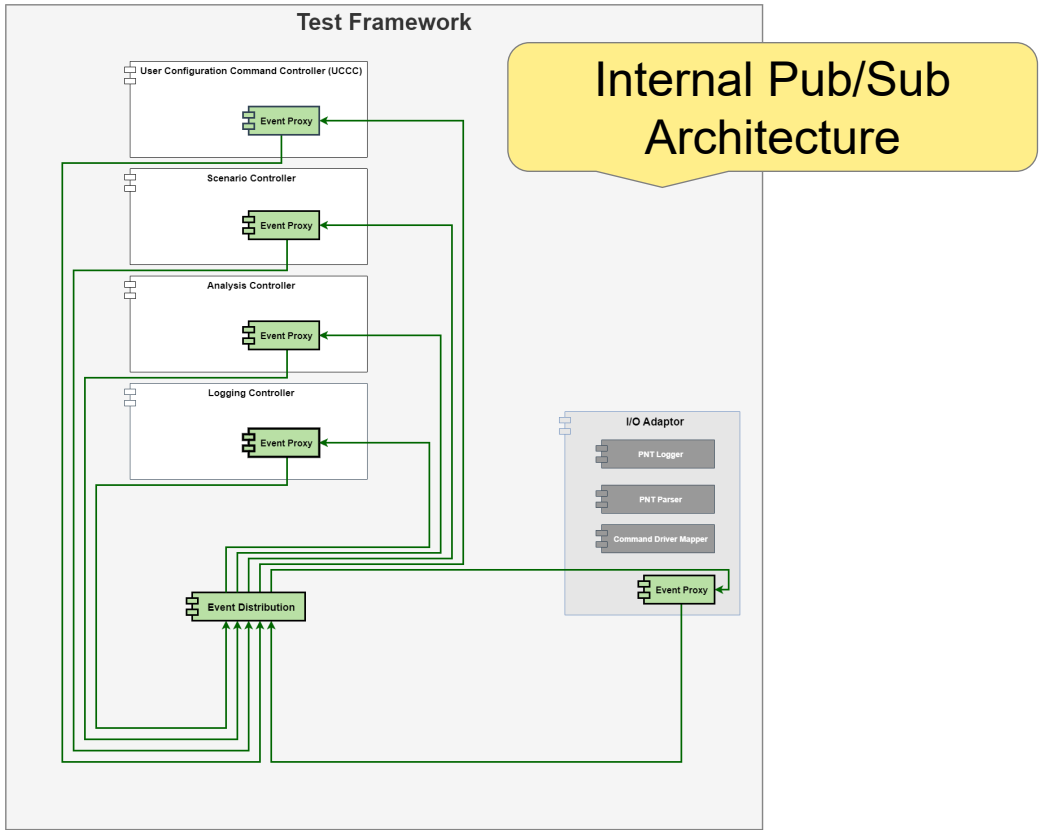
Level 3 requirements evaluated with static analysis:

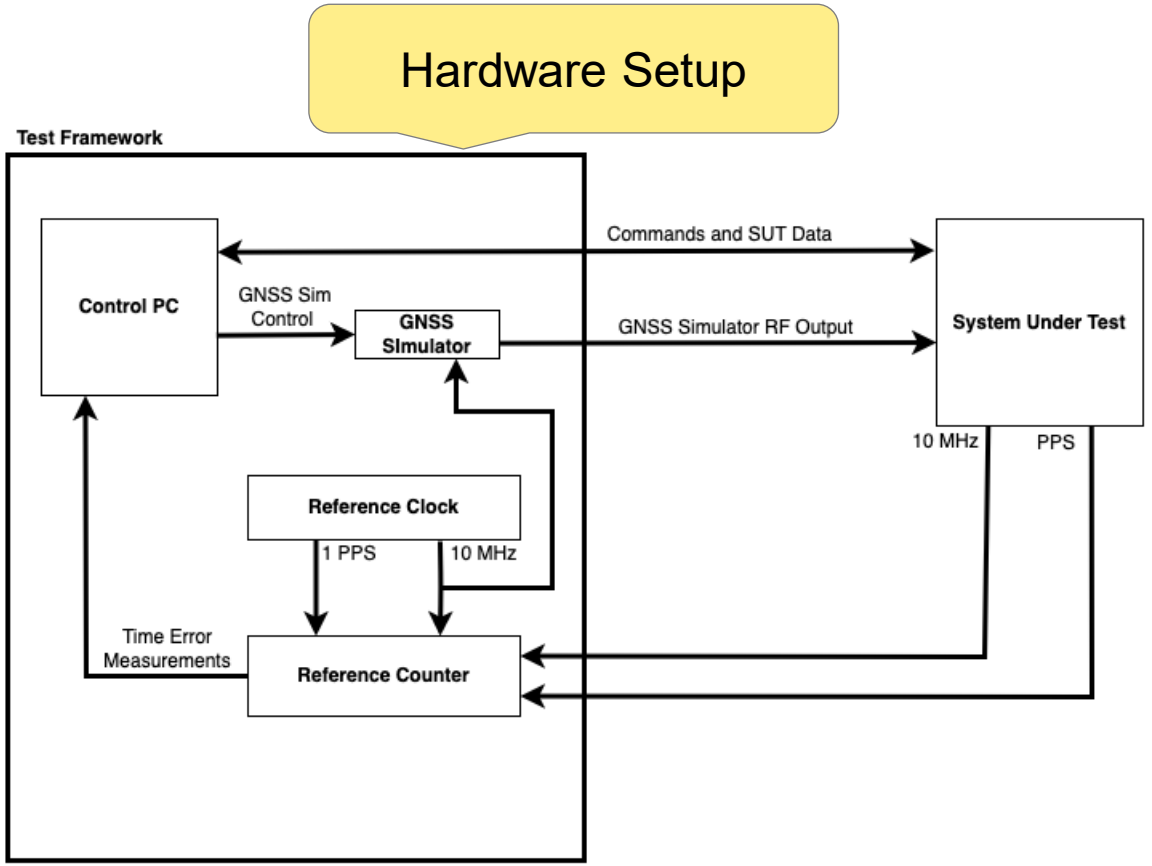
- Components have firmware reload capabilities
- Isolation between PNT sources

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Test Framework Description

- The ***Test Framework*** is a flexible test harness for resilience evaluation for 'black box' PNT Systems.

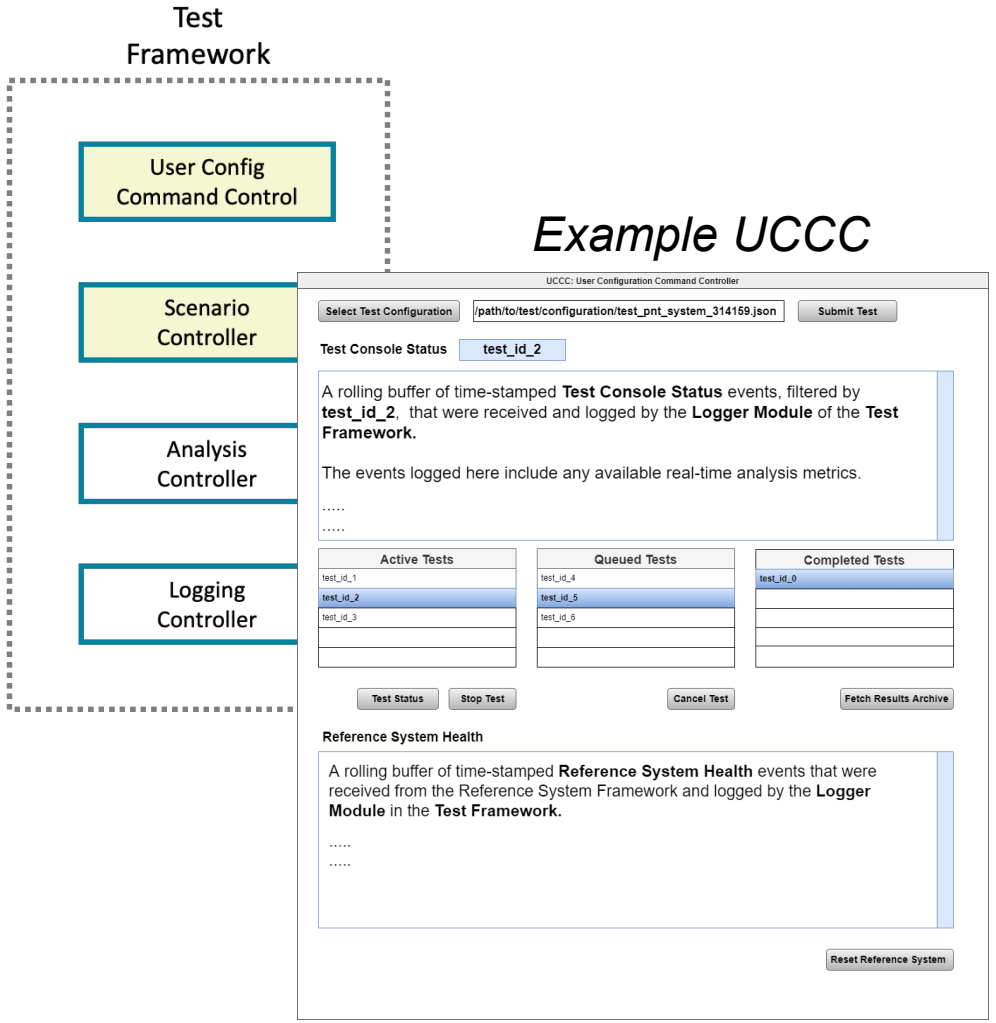




HSSEDI
Homeland Security Systems Engineering & Development Institute™

Test Framework Components

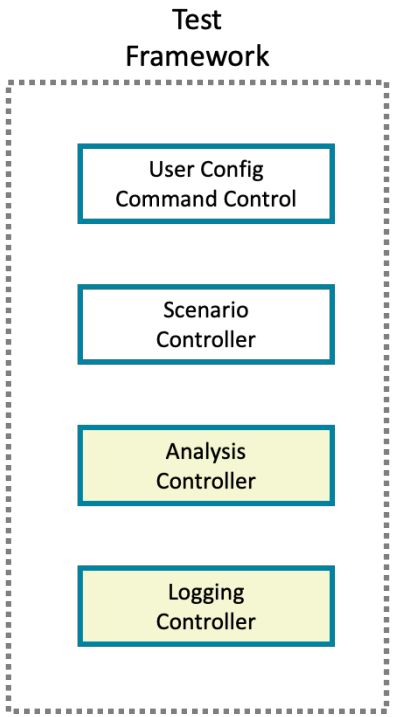
- **User Configuration Command Controller (UCCC)**
  - Allow the user to configure PNT resilience test scenario
  - Monitor and control test scenarios
  - Display logging and analysis data
  - Trigger reset and recovery of the resilient PNT system reference implementation under test
- **Scenario Controller**
  - Provide signal sources to the resilient PNT system reference implementation under test
  - Enable controls of the signal sources (e.g., configure, start, and stop) in a threat scenario



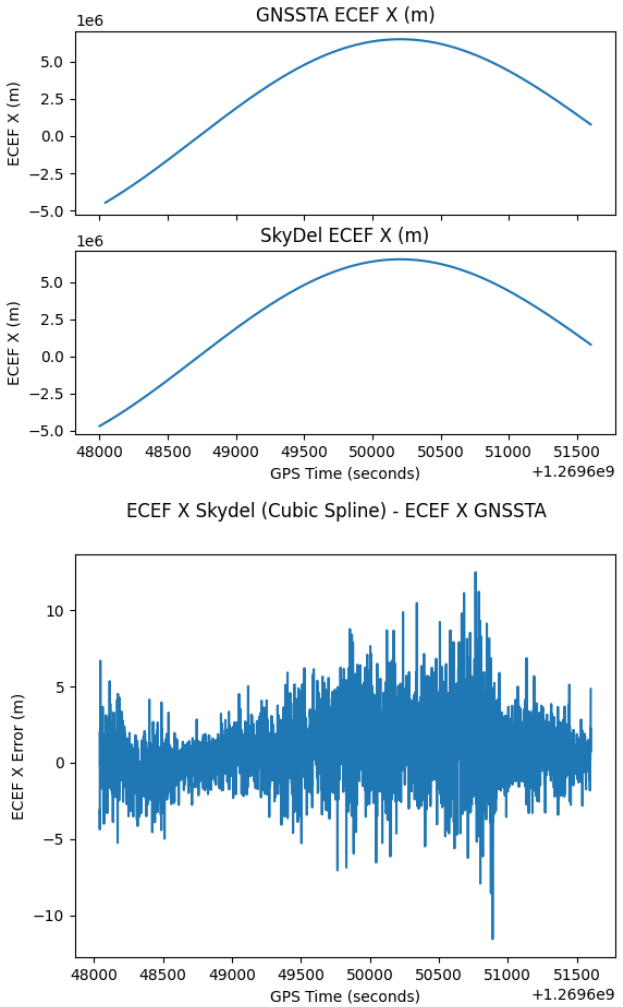
HSSEDI
Homeland Security Systems Engineering & Development Institute™

Test Framework Components

- **Analysis Controller**
  - Compute and visualize error metrics
  - Support real-time and post-test analysis
- **Logging Controller**
  - Log and parse data from both internal test framework components and PNT SUT



Example Analysis Results



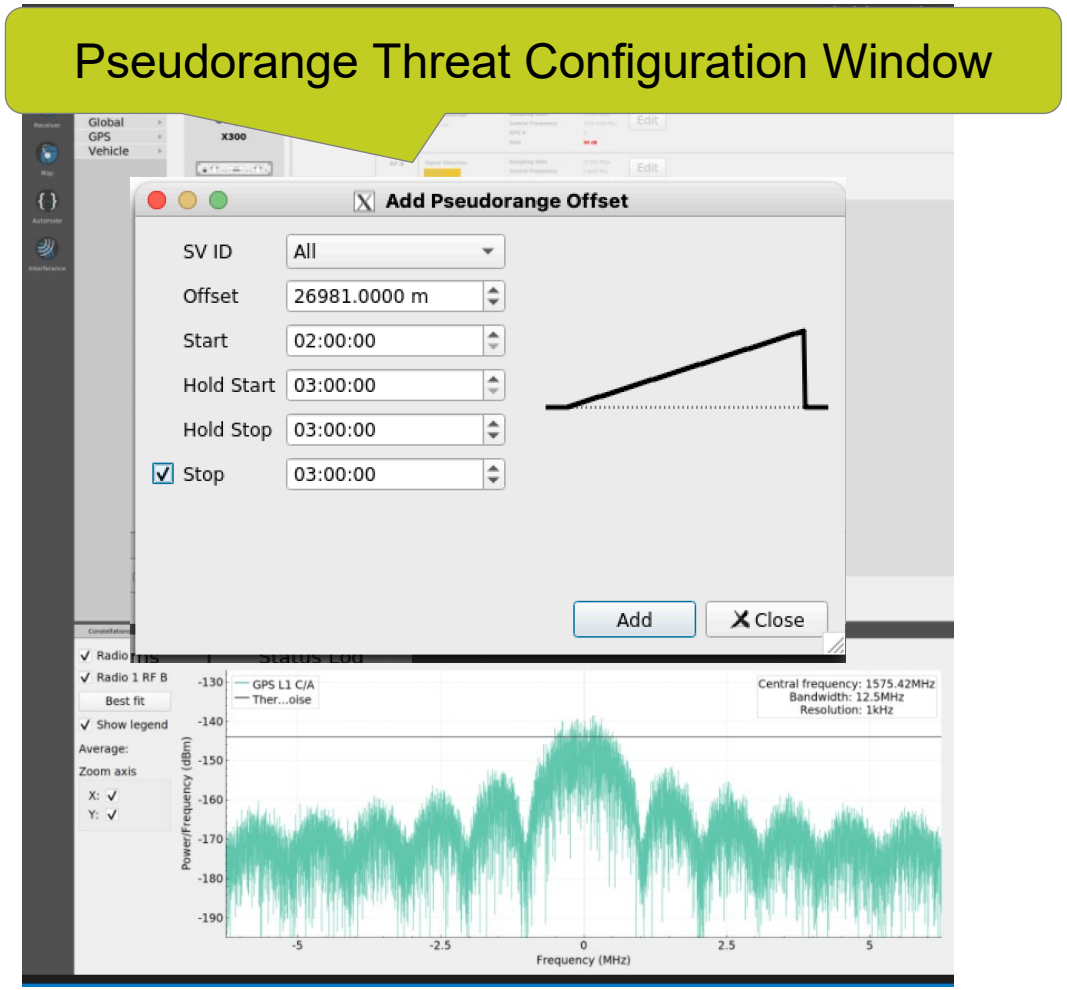
HSSEDI
Homeland Security Systems Engineering & Development Institute™

Publish/Subscribe Architecture

- **All interfaces between the modules of the Test Framework will use a Publish Subscribe (pub/sub) design pattern (TCP/IP)**
- **The message payload of each pub/sub message (derived from a base Event class) will be in JSON format**
  - supports numerous numeric and non-numeric data types
  - supports schema validation
  - serialization/deserialization libraries are native to Python
  - support rapid and flexible payload schema updates
  - supports rapid and flexible addition of new message types
  - human-readable payloads when deserialized
  - intrinsically well-suited to data logging in Python
- **The rationale for selecting TCP/IP and the data transport protocol is to have a connection-based mechanism that guarantees delivery of the message**

Scenario Description

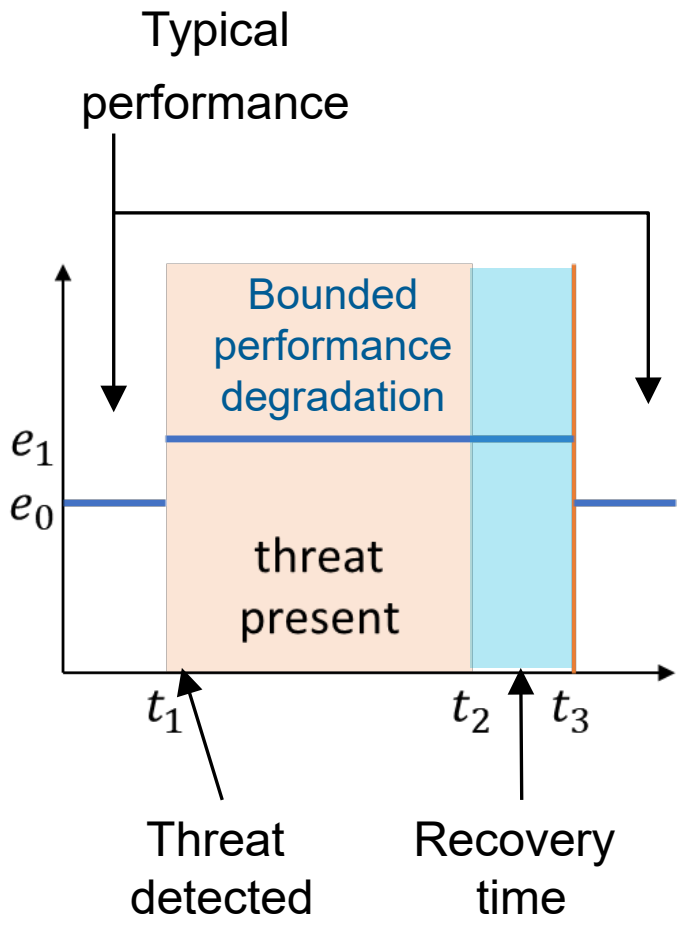
- **Time Ramp Threat Scenario**
  - Skydel generates GPS and GLONASS RF
  - Starts with 2 hours of nominal operation
  - Then a 25 ns/s time ramp on GPS for 1 hour
  - Then snaps back to nominal operation and runs for another 2 hours



HSSEDI
Homeland Security Systems Engineering & Development Institute™

Conformance Framework Level 3 PNT Resilience Requirements

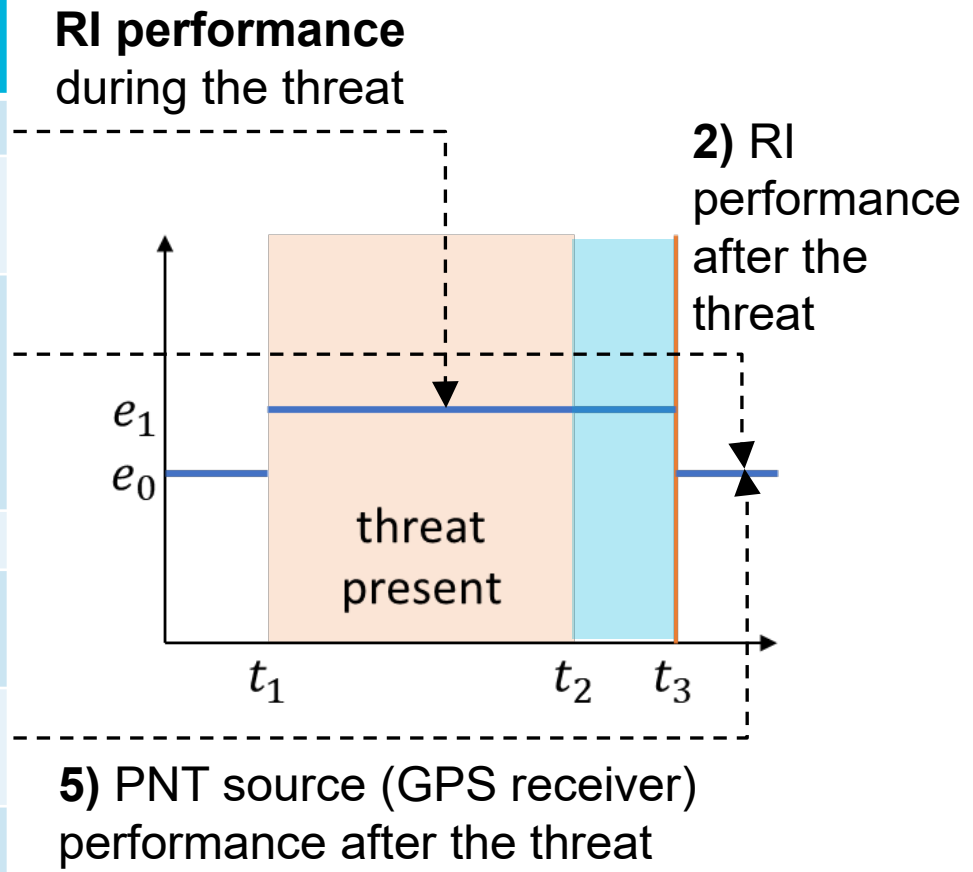
Requirement Number	Requirement Text
Performance	Provides a solution (with bounded degradation) during threat.
1	Must verify that stored data from external inputs adheres to values and formats of established standards.
2	Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat.
3	Must include the ability to securely reload or update firmware.
4	Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions.
5	Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output.
6	Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source.
7	Must cross-verify between PNT solutions from all PNT sources.



HSSEDI
Homeland Security Systems Engineering & Development Institute™

Requirements Evaluated with Performance Metrics

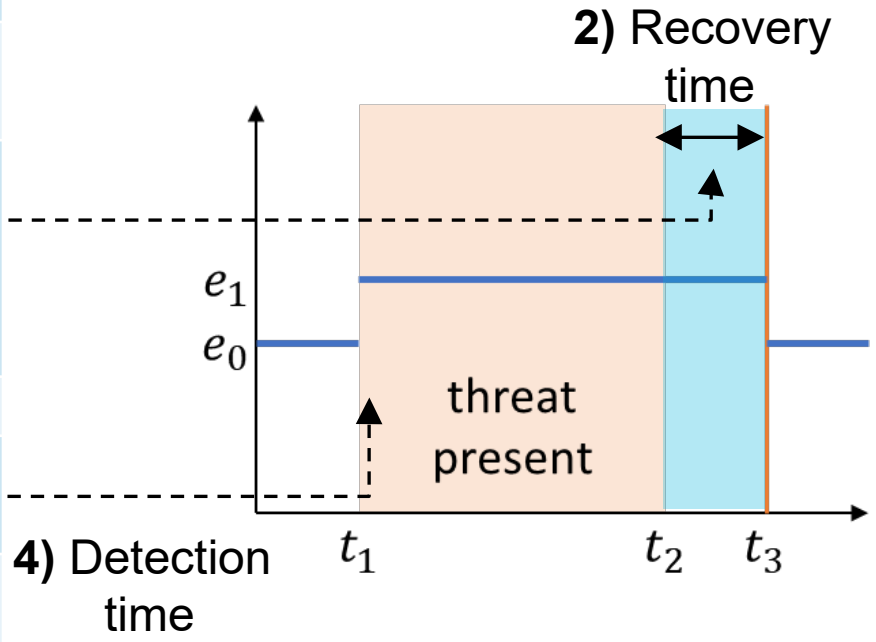
Requirement Number	Requirement Text
Performance	Provides a solution (with bounded degradation) during threat.
1	Must verify that stored data from external inputs adheres to values and formats of established standards.
2	Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat.
3	Must include the ability to securely reload or update firmware.
4	Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions.
5	Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output.
6	Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source.
7	Must cross-verify between PNT solutions from all PNT sources.



HSSEDI
Homeland Security Systems Engineering & Development Institute™

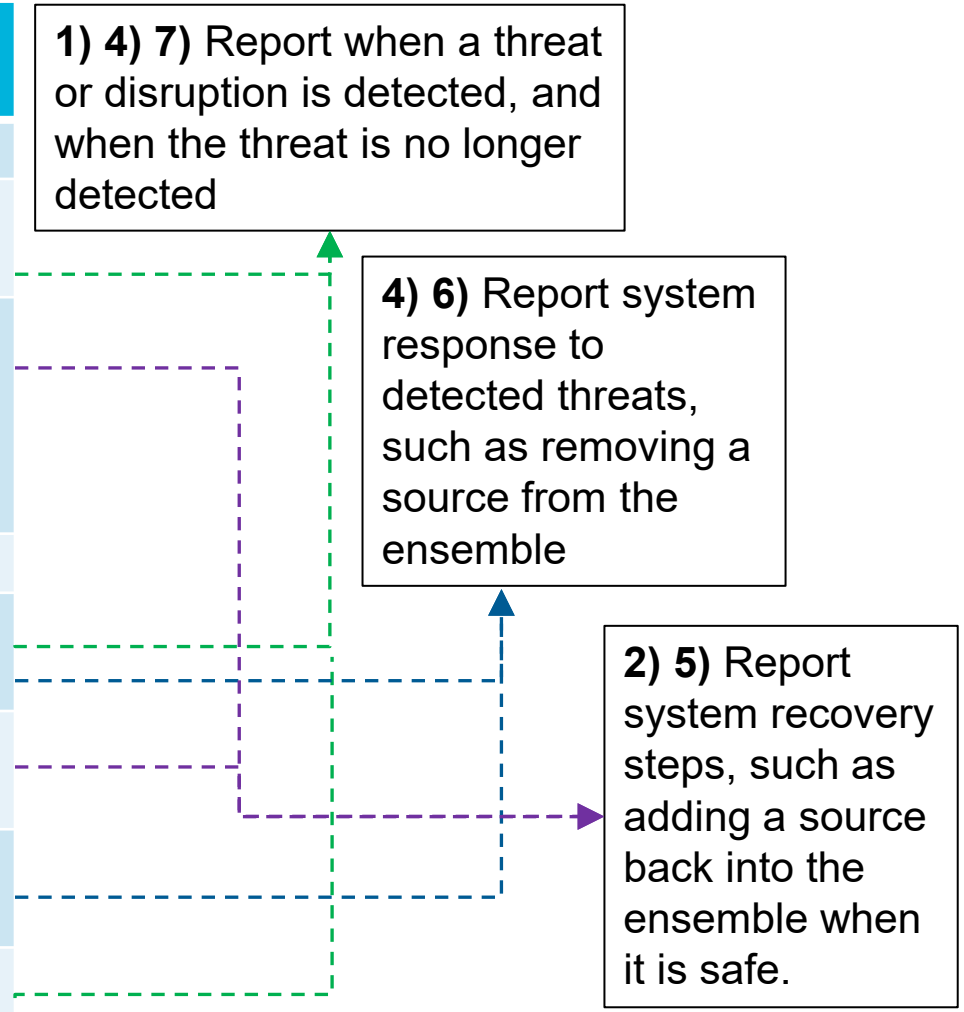
Requirements Evaluated with Measures of Delay

Requirement Number	Requirement Text
Performance	Provides a solution (with bounded degradation) during threat.
1	Must verify that stored data from external inputs adheres to values and formats of established standards.
2	Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat.
3	Must include the ability to securely reload or update firmware.
4	Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions.
5	Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output.
6	Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source.
7	Must cross-verify between PNT solutions from all PNT sources.



Requirements Evaluated with Reporting

Requirement Number	Requirement Text
Performance	Provides a solution (with bounded degradation) during threat.
1*	Must verify that stored data from external inputs adheres to values and formats of established standards.
2	Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat.
3	Must include the ability to securely reload or update firmware.
4	Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions.
5	Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output.
6	Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source.
7*	Must cross-verify between PNT solutions from all PNT sources.



*Level 3 threat scenario does not test this kind of threat detection

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Requirements Evaluated with Static Analysis

Requirement Number	Requirement Text
Performance	Provides a solution (with bounded degradation) during threat.
1	Must verify that stored data from external inputs adheres to values and formats of established standards.
2	Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat.
3	Must include the ability to securely reload or update firmware.
4	Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions.
5	Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output.
6	Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source.
7*	Must cross-verify between PNT solutions from all PNT sources.

In general, does the system design support all the requirements?

3) Does each component have a firmware reload capability?

6) Does the implementation architecture maintain isolation between PNT sources?

7) Does the implementation architecture compare PNT sources?

*Level 3 threat scenario does not test this kind of threat detection

HSSEDI
Homeland Security Systems Engineering & Development Institute™